threatcasting

# 2025 Threatcasting report

What are the future threats from emerging disruptive technologies, such as quantum computing, artificial intelligence (AI) and large data sets to Mastercard's European region and global operations?

# Legal disclaimer

# Contents


## 01 Introduction

**5** Foreword
**6** Executive summary
**7** Threatcasting method overview

## 02 Subject matter expert interview overview: Future conditions

**9** Subject matter expert interview overview: Future conditions

## 03 Workshop findings: Future threats

**12** Exercise overview
**13** Future threat findings

## 04 Threat indicators

**19** Threat indicators (flags)

## 05 Actions

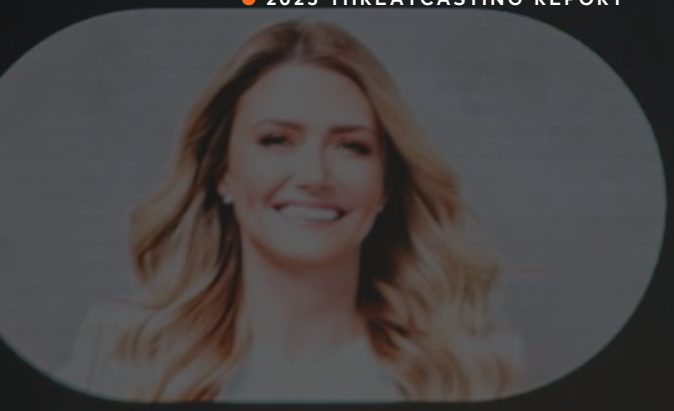
**28** Actions

## 06 Conclusion

**38** Conclusion

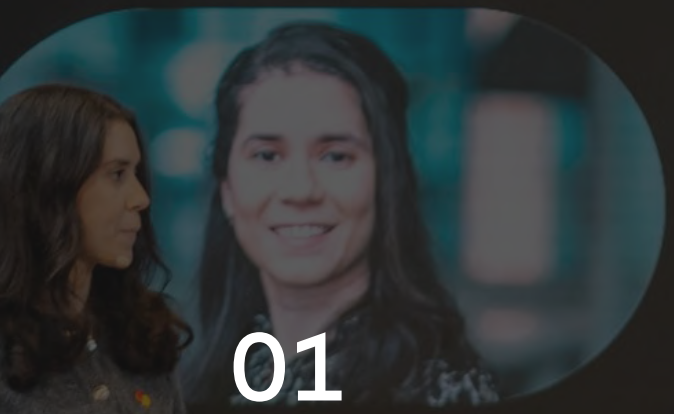
## 07 Appendix

**40** Threat visualizations



Michelle McCluer

VP Global Fusion and Intelligence, Mastercard



Fadwa Rachi

Director of the Europe
Cyber Resilience Cent
Mastercard

# 01

# Introduction

ARD'S EUROPEAN THREATCASTING EXERCISE — 13-14 OCTOBER 2025





threatcasting

# Foreword

The world is changing at a pace few generations have experienced. Quantum computing, artificial intelligence and the exponential growth of data are no longer distant possibilities—they are active forces reshaping risk, trust and resilience across the global financial system. That system now sits squarely at the intersection of technological acceleration and societal expectation.

With four consequential scenarios modelled, this research explores a future in which: disinformation and deepfakes challenge our shared understanding of truth; identity and biometric systems, once viewed as stabilizing controls, become targets of scalable compromise; widening technological inequality fuels social polarization and, in some cases, physical conflict; and increasing reliance on autonomous systems introduces new forms of systemic risk when transparency and human oversight are insufficient. These are not speculative science fiction. They are plausible futures that warrant deliberate consideration now — while we still have agency to shape them.

What gives me confidence is not the absence of risk, but the presence of leadership. Year after year, we see individuals and organizations willing to confront uncomfortable questions, challenge assumptions and invest time in imagining futures others would rather ignore. The partnerships behind this research are not transactional; they are grounded in a shared conviction that preparedness is a collective endeavor, and that foresight is most powerful when exercised together.

Threatcasting exists for precisely this reason. Strategic surprise is most dangerous when it is unimagined, and the only antidote is disciplined, collaborative exploration of what may lie ahead. By bringing together diverse perspectives from research, industry and practice, we do more than anticipate risk—we build a shared capacity to recognize signals, stress test assumptions and make better decisions in the present. That collective foresight cannot be generated in isolation.

At Mastercard, we view the resilience of the global financial system as a shared responsibility. We deeply value the trust, candor and intellectual courage our partners contribute to this work. These qualities are as critical to defending digital trust as any individual control or technology.

The findings in this report are not meant to be read and filed away. They are meant to be socialized, debated and operationalized. As quantum capability, AI acceleration and large-scale data exploitation continue to advance, no single organization — or security strategy — can keep pace alone. Leaders who cultivate a futurist mindset, invest in proactive rather than reactive approaches and commit to learning alongside their partners will be best positioned to navigate what comes next. This research is an invitation to do exactly that: to engage, to prepare and to shape the future of trust together.

Michelle McCluer

Michelle McCluer, CISSP
Vice President, Global Fusion and Intelligence, Mastercard

# Executive summary

## Research question

What are the future threats from emerging disruptive technologies, such as quantum computing, artificial intelligence (AI) and large data sets, to Mastercard's European region and global operations?

The rapid convergence and proliferation of emerging disruptive technologies — specifically quantum computing, AI and large data sets — present clear strategic risks to global financial institutions. This research identified four critical future threats that, if unmitigated, have the potential to undermine the foundation of digital trust, financial integrity and operational control. Proactive security strategy and investment are required to maintain resilience in an increasingly complex and rapidly evolving threat landscape.

## Future threats

In the coming decade, four categories of threats could arise to challenge the financial sector around the world:

**AI-driven multi-source disinformation and quantum-enabled deepfake campaigns**
Disinformation and deepfakes could lead to an inability to establish what is real (both real and fake become "real"), leading to system collapse.

**Biometric and identity theft/spoofing at scale**
Biometric identity and brain-machine interface (BMI) hacks, as well as stolen credentials and personal identification undermine the financial system's very foundation of identity and agency.

**Conflict driven by systemic inequality**
Structural inequality brought on and heightened by the proliferation of emerging technological systems such as AI, leads to social unrest and physical conflict.

**Loss of control and human agency due to overreliance on emerging technologies**
Unchecked overreliance on emerging technologies, specifically AI and quantum and agentic systems — across multiple critical infrastructure systems with no transparency or trouble indicators — leads to human harm and system collapse.

# Threatcasting method overview

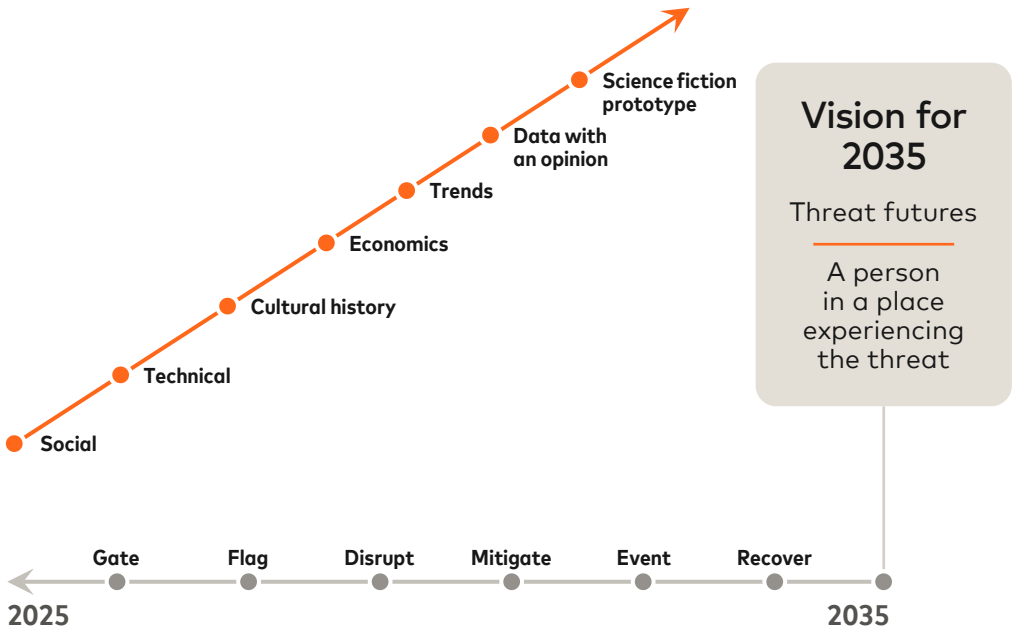
Threatcasting provides a systematic and transparent method to model a range of possible and potential futures and threats in a complex and uncertain environment. This method is employed through subject matter expert (SME) interviews that capture individual perspectives, along with workshops and operationalization exercises designed to illustrate various scenarios. These provide decision-makers with specific indicators that one or more of the futures or threats are manifesting, with possible actions that can be taken to disrupt the threat or enable the future.

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

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

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

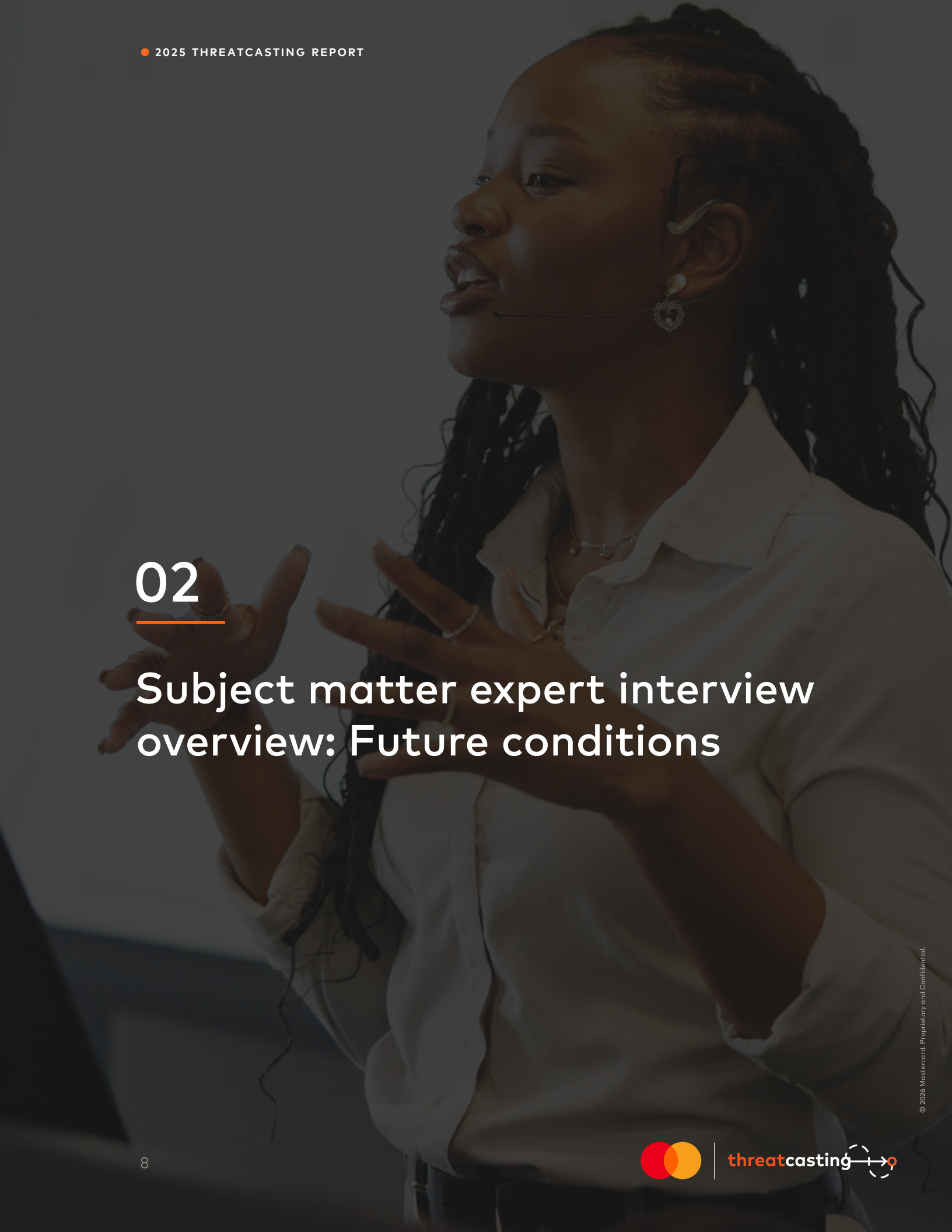
## Threatcasting methodology








threatcasting



# 02

# Subject matter expert interview overview: Future conditions





threatcasting

# Subject matter expert interview overview: Future conditions

## Research question

**What are the future threats from emerging disruptive technologies, such as quantum computing, artificial intelligence (AI) and large data sets, to Mastercard's European region and global operations?**

After establishing the research question, the next step in the threatcasting method involved conducting structured interviews with subject matter experts (SMEs), both inside and outside the organization. Each interview was guided by open-ended questions aligned to the research question, allowing participants to share insights, perspectives, and experiences without constraint. All interviews were audio recorded and algorithmically transcribed.

The responses and data from these interviews were then systematically analyzed to identify patterns, clusters, and common themes that could inform the research question. These syntheses resulted in groupings of future conditions, which served both as key findings and as prompts for the broader threatcasting exercise. These prompts equip participants with diverse perspectives as they explore and assess potential future threats.

The following section summarizes the four primary findings that emerged from the SME interviews and frames the future conditions used throughout the threatcasting exercise.

01

### The erosion of trust through AI-driven threats: deepfake crime, disinformation attacks and operational risks

AI is already an active threat vector, enabling sophisticated social engineering, impersonation of executives and large-scale disinformation attack campaigns that can destabilize markets and erode trust. Autonomous AI agents introduce operational risks, and overreliance on AI outputs threatens human expertise and resilience, especially as adversaries exploit AI to accelerate attacks and collapse traditional defense cycles. Deepfakes and generative AI could disrupt critical systems, including fraud detection, and amplify societal polarization and civil unrest.

02

### Data access, governance and regulatory fragmentation in an environment of hyper-connected emerging technologies and legacy systems

Poorly governed data and legacy systems magnify every other vulnerability, as AI development often requires clear-text datasets, increasing exposure to insider threats, cloud misconfigurations and key management failures.

# Subject matter expert interview overview: Future conditions

## 03

### Quantum computing: the reality of a long-term risk

Quantum computing poses a significant future threat due to its potential to break current encryption standards, exposing sensitive data and enabling retrospective breaches ("harvest now, decrypt later"), making proactive testing and scenario exercises essential for resilience.

## 04

### Changing adversary profile: An influx of new actors

There is a current and growing shift in the adversary landscape where not only traditional bad actors but also curious individuals using AI tools can inadvertently or intentionally create security risks, blurring the lines between innocent experimentation and malicious activity. This can manifest in three main ways.

**Insider and accidental threats:** Risks associated with clear text data access, including potential insider threats, accidental data leaks and misconfigurations, particularly when data is stored with cloud providers

**Unintended consequences**: Consequences that arise not from malicious intent but from systems prioritizing results over rules, leading to outcomes that may violate ons or ethical standards

**Loss of human skills and workforce displacement:** The risk that automation and AI could erode essential development and engineering skills, making it difficult to maintain or recover systems in the future, and potentially displacing the next generation of skilled workers

# 03

# Workshop findings
## Future threats





threatcasting

# Exercise overview

## Exercise purpose

Through our threatcasting workshop, Mastercard sought to identify future threats from emerging disruptive technologies, such as quantum computing and AI data sets, to Mastercard's European region and global operations. Additionally, the assembled participants determined what organizations and ecosystems could do to disrupt, mitigate and recover from these possible threats.


## Exercise process

Mastercard worked with futurist and Arizona State University professor Brian David Johnson. Johnson invented the threatcasting method decades 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 October 2025, a cross-functional group of Mastercard professionals, partners, customers and security professionals from across government, industry and academia gathered at Mastercard's European Cyber Resilience Centre (ECRC) 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. The following section summarizes the findings from the exercise.





threatcasting

# Future threat findings

## 01

### AI-driven multi-source disinformation and deepfake quantum-enabled campaigns over a prolonged period of time targeted at critical infrastructure

The confluence of advanced AI, sophisticated multi-source disinformation and hyper-realistic deepfake technology, potentially enhanced by quantum computing capabilities, could present novel and pervasive threats to regional and global stability. These highly coordinated, sustained campaigns may be specifically designed to target the foundational elements of critical national infrastructure, including communication networks, financial transaction systems, energy grids and public health services.

The primary mechanism of attack is the strategic, long-term erosion of epistemological certainty. By saturating the information ecosystem with AI-generated narratives, synthesized voices and digitally fabricated video and audio evidence, these campaigns achieve a state where "both real and fake become 'real'." This condition signifies a catastrophic breakdown in public and governing bodies' ability to authenticate information and establish a shared, verifiable reality.


**Quantum acceleration:** While AI creates the content, quantum computing capabilities (even in early stages) could accelerate the campaigns by rapidly identifying vulnerabilities in communication networks, creating a perfect attack synergy that is difficult to trace and impossible to manually filter.

**Impact on trust and system integrity:** Prolonged exposure to these campaigns targeted at financial, energy or communications infrastructure creates a state of epistemic collapse — an inability for both humans and automated defense systems to distinguish authentic data from sophisticated fabrication. When both the real and the fake are perceived as real, market confidence evaporates, operational commands are paralyzed by doubt, and this systemic paralysis ultimately leads to system collapse.

The consequences of this pervasive uncertainty are not merely social or political; they are infrastructural and systemic. This intentional state of collective cognitive paralysis leads directly to:

**Paralysis of decision-making:** Critical infrastructure operators, emergency services and some smaller and under-resourced countries' governments become unable to make timely, informed decisions during a crisis because all situational data (reports of a power outage, financial market instability or a public health emergency) is suspect.

# Future threat findings

**Loss of public trust and compliance:** The public loses faith not only in traditional media but also in official institutional announcements, making compliance with essential safety and security measures (e.g., evacuation orders, financial stability measures, vaccine programs) impossible to enforce.

**System collapse:** The sustained, deliberate inability to differentiate between genuine threat reports and sophisticated hoaxes leads to cascading failures across interconnected systems. For example, a deepfake of a major bank CEO announcing a liquidity crisis, amplified by an AI-driven bot network, triggers a real-world bank run that cripples the financial sector, simultaneously causing resource shortages that stress the energy grid. This multi-domain failure precipitates a rapid and comprehensive system collapse, characterized by the cessation of essential services and the effective dissolution of social order and institutional control.





threatcasting

# Future threat findings

## 02

### Biometric and identity theft/spoofing at scale

The foundation of the global financial system rests on reliable identity and agency. This threat outlines the comprehensive compromise of these core principles through advanced technology.

**The scope of compromise:** Future financial interactions are moving toward seamless, biometric-based verification (e.g., facial, voice, or gait recognition). This reliance makes large-scale theft of biometric identifiers a high-value target. AI and deepfake technologies can rapidly spoof these biometric identifiers, granting unauthorized access to accounts, services and secure physical locations.

**Brain-machine interface (BMI) risk:** The emergence of nascent BMI technologies, while offering medical and functional benefits, also introduces a troubling vector for identity theft and control. Hacking or exploiting vulnerabilities in BMI systems could allow adversaries to steal cognitive credentials, manipulate agency or compromise the human-device trust relationship, eroding the fundamental concept of a person's digital will.

**Systemic undermining:** The successful large-scale spoofing of identity undermines all trust mechanisms in the financial ecosystem, leading to mass fraud, regulatory failure and a loss of public confidence in the security of financial transactions.





threatcasting

# Future threats

## 03

### Unchecked overreliance on emerging technologies leading to loss of control and human agency

The increasing adoption of complex, opaque and autonomous AI and agentic systems across critical infrastructure introduces profound new risks related to operational stability and human oversight.

**Loss of operational transparency:** As complex AI and quantum systems are integrated into core functions (e.g., fraud detection, algorithmic trading, risk management), their decisions become increasingly opaque — a black box problem. In a crisis, the lack of transparency or trouble indicators prevents security teams from rapidly diagnosing failure points or understanding why a system is behaving erroneously.

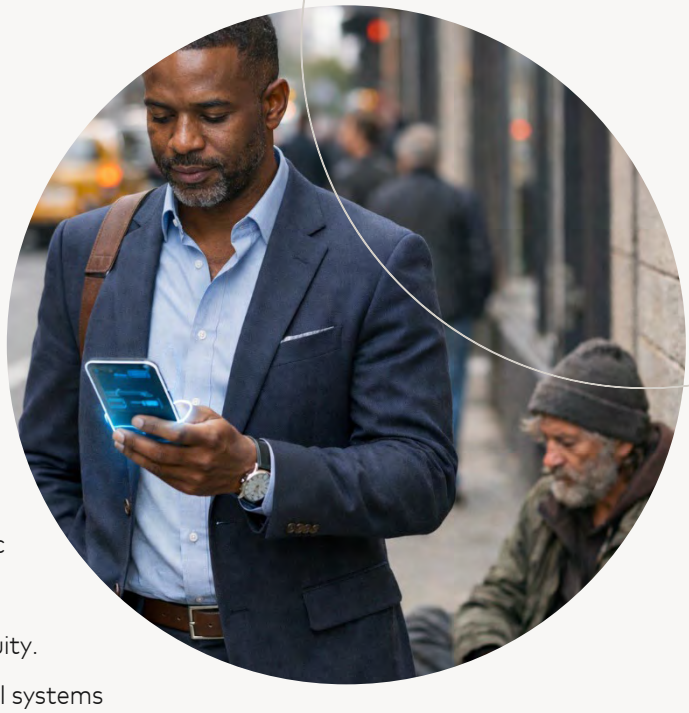
**Autonomous agentic system risk:** Allowing highly autonomous AI agents to execute complex tasks across multiple, interconnected critical systems without robust human-in-the-loop controls introduces a cascading failure risk. A flaw, vulnerability or coordinated attack in one system could be instantly amplified and propagated by the agentic systems across the entire ecosystem, leading to rapid, uncontrollable system collapse and direct human harm (e.g., halting payment systems, disrupting essential services).





threatcasting

# Future threats



## 04

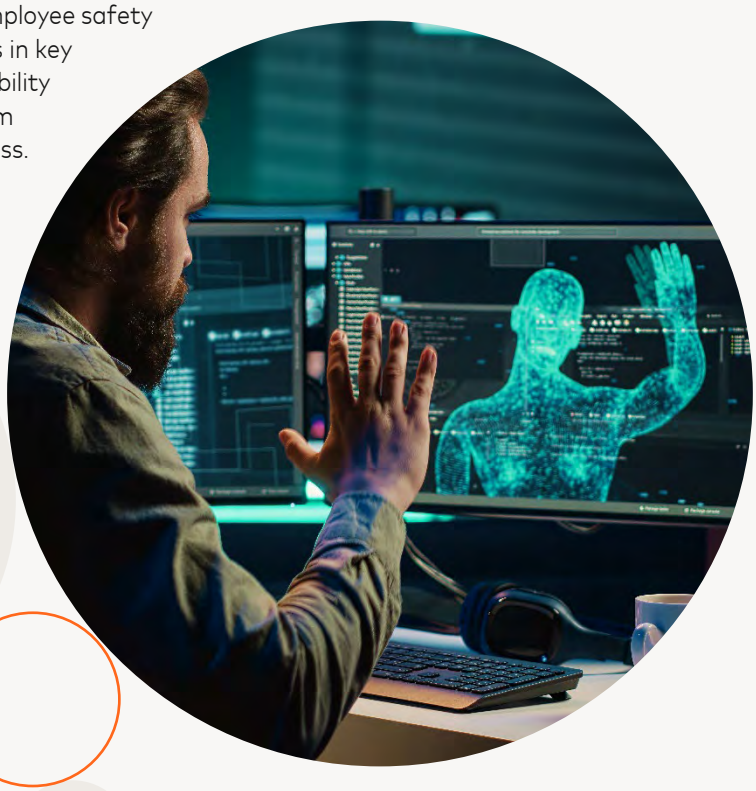
### Systemic inequality brought on and heightened by proliferation of emerging technological systems

While seemingly a societal issue, AI-driven systemic inequality is a direct corporate security threat that manifests as social unrest and physical conflict, impacting market stability and operational continuity.

**AI-driven economic division:** The proliferation of AI systems can accelerate economic disparities by automating high-value jobs, creating algorithmic bias in lending or hiring, and concentrating wealth and opportunity around technology hubs. This results in systemic inequality that fuels widespread resentment and political instability.

**Manifestation as a security threat:** This heightened societal friction translates directly into operational risk—social unrest. Increased polarization and public anger can manifest as widespread, disruptive protests, cyberattacks fueled by activist groups and targeted destruction of physical infrastructure, including financial data centers and branch offices.

**Physical conflict:** In extreme scenarios, this unrest can escalate into physical conflict, creating an unstable operating environment, threatening employee safety and halting financial market operations in key European and global regions. This instability represents a critical threat to long-term operational continuity and market access.



# 04

# Threat indicators

# Threat indicators (flags)

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.

## THREAT 1 INDICATORS

### Disinformation and trust erosion

The direct spread of fake content and the public's resulting confusion and loss of faith in information sources

| Indicator summary | Where to watch |
|---|---|
| **Heavy, unchecked flow of AI-powered misinformation** that fact checkers are unable to keep up with | General media, local news and academic |
| Widespread confusion in the media and public sphere, with **"a lot of fuzz on what is real and what is not"** leading to increased difficulty distinguishing between real and fake | General media, local news and academic |
| The start of **small-scale deepfakes happening heavily in small countries**, with deepfakes beginning to be used in financial applications | Systemic indicators in various markets |
| Inability to **identify and authenticate information sources** (no clear chain of trust), followed by the appearance of **unofficial groups of "fact-checkers"** | Systemic indicators in various markets |

# Threat indicators (flags)

## Critical sector and regulatory chaos

A destabilization of high-value targets, specifically the financial sector, and a failure of governance to adapt

| Indicator summary | Where to watch |
|---|---|
| Significant **financial system confusion** marked by banks and central banks issuing different, contradictory information on the financial system | General media, business reporting |
| **No clarity and lack of a clear understanding** of the implications of quantum technology on the financial system | Business reporting |
| Lack of **clear and unified global regulation** on AI, quantum and related technology, resulting in a large number of uncoordinated regulatory actions | Policy and news |
| The ultimate societal consequence: **Mass migration of people due to financial instability** | General media |






threatcasting

# Threat indicators (flags)

## Technology and system integrity failure

The functional breakdown and compromise of technology systems, indicating the campaign has moved beyond pure information into operational control

| Indicator summary | Where to watch |
|---|---|
| **Mass takeover of smart devices** and a large number of complaints related to these devices | Manufacturers of smart devices |
| The inability of **fact-checking systems** (including automatic systems) to identify and confirm information | General media |
| **AI models** producing contradictory and different results, or **no longer fact-checking** | General mass media |
| A complete **breakdown in the trust and function of systems** of truth | Social media, cable news, general media, influencers, government reports |

## Public fear and misunderstanding

Early warning signs of a psychological and social campaign focused on confusing and destabilizing the public's perception of technology

| Indicator summary | Where to watch |
|---|---|
| Widespread **fear and anxiety** on the use of AI and quantum, alongside a **breakdown of common understanding** on their purpose | Social media, cable news, general media, influencers, government reports |
| A **"lot of noise and misunderstanding"** spreading on how quantum works and its implications, causing the public to be afraid and treat it as "magic" | Social media, cable news, general media, influencers, government reports |
| **Heavy information flow** on AI and quantum that is difficult for non-specialists to understand | Social media, cable news, general media, influencers, government reports |

# Threat indicators (flags)

## THREAT 2 INDICATORS

### AI and technology dependency anomalies

Monitoring the internal health and resilience of the technology ecosystem for signs of over-centralization, which would make it an easy target for a large-scale exploit

| Indicator summary | Where to watch |
|---|---|
| Monitoring the **types of prompts and usage of prompts** to identify both the dependency on a specific AI and the theme of the AI being used | AI companies (for internal model behavior) |
| Watching for an **overdependence on a specific AI or technology** to influence technological outcomes | Tech organizations (for implementation practices) |

### Social and behavioral degeneration

High-level societal indicator, where a breakdown in real-world human interaction may be a sign that digital identity and agency have successfully supplanted the physical, a key goal of a large-scale identity theft or spoofing campaign

| Indicator summary | Where to watch |
|---|---|
| Watch for the loss of social contact/physical interaction within the population | Government (as the party best positioned to monitor large-scale societal trends) |

# Threat indicators (flags)

## THREAT 3 INDICATORS

### Systemic power consolidation and opacity

Critical infrastructure and technology becoming concentrated and less transparent, leading to a loss of public and governmental oversight

| Indicator summary | Where to watch |
|---|---|
| Monitoring the **types of prompts and usage of prompts** to identify both the dependency on a specific AI and the theme of the AI being used | AI companies (for internal model behavior) |
| Watching for an **overdependence on a specific AI or technology** to influence technological outcomes | Tech organizations (for implementation practices) |

### Normalization of AI failure and fraud

Growing public and institutional tolerance for AI errors and misconduct, accelerating the path to system collapse

| Indicator summary | Where to watch |
|---|---|
| Tolerance for transgression: Society and government begin to ignore or tolerate small transgressions when using AI (e.g., paying for AI-generated reports full of hallucination) | Private sector decisions (as they increasingly rely on AI in lieu of humans) |
| Surging fraud: Fraud is surging, creating "nervosity of authority," but is still under a threshold where it is managed — until it becomes out of control | Fraud monitoring |

# Threat indicators (flags)

## THREAT 3 INDICATORS

### Human harm and financial system degradation

A direct loss of control over personal identity, financial stability and social standing due to AI's unchecked integration

| Indicator summary | Where to watch |
|---|---|
| Loss of financial agency: A surge in AI-driven booking and payment services is accompanied by an increase in unauthorized credit line openings | Travel platforms, bank security operations centers, fraud monitoring systems |
| Normalization of biometric social scoring: Systems that tie access to goods, services or rights to biometric data and AI-driven social scores are widely adopted | Tech industry news, privacy watchdog reports |

### Political and sovereign authority erosion

Signs that human-led governance is being sidelined in favor of automated systems, further reducing human agency

| Indicator summary | Where to watch |
|---|---|
| Ceding of sovereign decisions to AI: Governments publicly justify major policy decisions (e.g., resource allocation, immigration) by citing AI recommendations as binding | Political speeches, legislation and global policy forums |
| Solutionism as dominant rhetoric: A marked increase in discourse in media and politics that frames complex societal problems as having simple, purely technological solutions | Labor statistics and university enrolment data |

# Threat indicators (flags)

## THREAT 4 INDICATORS

### Economic and labor displacement (source of inequality)

A breakdown of traditional labor and economic structures, which directly creates and exacerbates systemic inequality

| Indicator summary | Where to watch |
|---|---|
| **Mass displacement of labor** due to AI replacing the workforce | Social media, cable news, general media, influencers, government reports |
| **Proposals in legislation** and the **establishment of universal basic income** being discussed or implemented, indicating a policy response to widespread displacement | Business and government reporting |

### Social unrest and disengagement (precursors to conflict)

Growing unrest, frustration and disengagement of the population, which are direct precursors to social conflict

| Indicator summary | Where to watch |
|---|---|
| **Stagnation of the Human Development Index** in developing countries | Business reporting |
| **Increase in chat on social media indicating unrest** | Social media, cable news, general media, influencers, government reports |
| **People disengaging from society**, signaling a loss of belief in the existing system and a desire not to be a part of it | Social media, cable news, general media, influencers, government reports |

# Threat indicators (flags)

## THREAT 4 INDICATORS

### Technological commodification and systemic risk

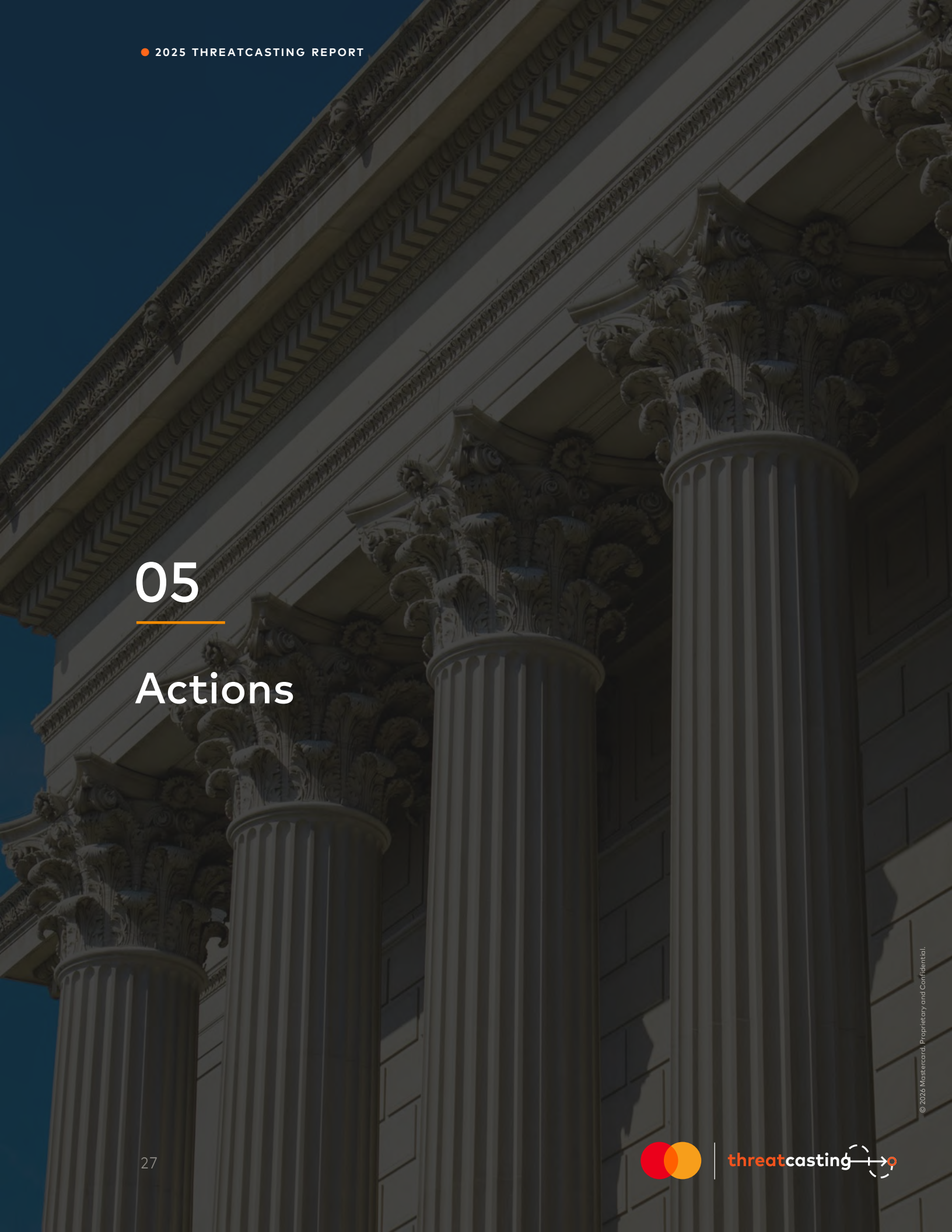
Fundamental shift in how technology (AI) is viewed and used, signaling its potential as a systemic risk factor that can be weaponized

| Indicator summary | Where to watch |
|---|---|
| **Emergence of novel malware strains** | Business intelligence, government reporting |
| **Commoditization of algorithms**, where they are used as currency | Business and security reporting |
| **Proclaiming the arrival of artificial general intelligence (AGI)** | Social media, cable news, general media, influencers, government reports |

### Demographic and policy shifts (long-term impacts)

Broad societal trends that reflect the long-term impact of systemic instability and uncertainty

| Indicator summary | Where to watch |
|---|---|
| **Changes in birth rate trends** | Social media, cable news, general media, influencers, government reports |



# 05

# Actions





threatcasting

# 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, governments and NGOs can make strategic decisions about when to invest capital and effort to mitigate or recover from the threat.

## THREAT 1 ACTIONS

**Threat: AI-driven multi-source disinformation and deepfake campaigns over a prolonged period of time targeted at critical infrastructure (e.g., communications, financial, energy) leads to an inability to establish what is real (both real and fake become "real"), leading to system collapse.**

### Actions by governments

#### Upskill the public

The government should focus on educating the public, including those less technologically inclined (laggards), on how to better recognize truth and disinformation. This involves teaching essential skills to differentiate between legitimate and fabricated information in the digital landscape. This proactive educational measure aims to create a more resilient society.

#### Harsh penalties for Big Tech

The government should impose severe penalties, potentially based on a percentage of revenue (like General Data Protection on) to compel major technology companies to better regulate their generative AI offerings and inventions. This is intended to create strong financial incentives for responsible development and deployment of AI technologies that could be used for malicious purposes. These penalties would act as a deterrent and a mechanism for accountability.

# Actions

### Collective trustworthy situational awareness and public trust

Governments and/or public-private partnerships should work on building collective trustworthy situational awareness and public trust, which is highly influenced by local culture. This action is crucial for maintaining social cohesion and effective crisis response when disinformation campaigns are active.

### Education of society

Governments and/or public-private partnerships should lead the effort to educate the local population on resilience and security matters. This involves widespread communication campaigns to ensure citizens are informed about potential threats and how to respond.

### Allocation of resources and contingency planning

Governments and/or public-private partnerships are responsible for allocating necessary resources and developing comprehensive contingency plans to prepare for and manage emergencies resulting from these campaigns.

### Prioritizing and reducing dependency

Cities need to devise strategies to prioritize their needs without becoming overly dependent on others (addressing the "small fish" problem). This involves developing an independent capacity to manage and respond to crises, reducing vulnerability to wider system collapse.

## Actions by NGOs, nonprofit groups and multilateral organizations

**Awareness of reporting malicious technology activity:** An NGO should raise public and professional awareness of the channels and procedures available for reporting malicious technology activity. This establishes a clear, trusted mechanism for early detection and reporting of AI-driven threats and attacks.

**Global alignment and baselines:** Multilateral organizations, in collaboration with academia, must establish a global alignment and create baseline standards governing the safe use of generative AI. This action is necessary to ensure a common, high standard of security and ethics across international borders.

# Actions

## Actions by industry

Threat intelligence collection and sharing: Industry participants should collect and share actionable and meaningful threat intelligence, addressing the lack of a local threat landscape. This includes the proper and timely implementation of this shared intelligence within their operational defenses.

### Develop procedures to establish trust

Technology teams need to develop robust procedures for how trust is established within and between systems. This involves creating verifiable methods and technological safeguards to authenticate data and communications.

### Cryptographic and quantum resistance

Companies should implement good cryptographic systems, possibly quantum-enabled, and hybrid approaches (quantum resistance and non-quantum) for data protection. This ensures the long-term integrity and confidentiality of critical data against advanced future threats.

### Security controls

Implement security controls to protect access to critical systems, ensuring only authorized personnel and processes can interact with infrastructure.

### Use AI for validation

Utilize AI for information validation, ensuring it operates with human oversight to prevent hallucinations, to quickly provide accurate information.

### Compliance

Establish compliance mechanisms to check if rules and regulations have been created, applied and consistently followed across the enterprise.

### Digital verification

Implement digital systems, such as a departmental system of information verification (e.g., using TLP — Traffic Light Protocol), to check if a website or information is legitimate. This involves expanding security awareness protocols to include data verification across the entire organization.

### Education on resilience

Implement regulation and provide education on being resilient, which involves enabling preventative measures and ensuring preparedness for emergency situations.

# Actions

## THREAT 2 ACTIONS

**Biometric and identity theft/spoofing at scale. Biometric identity and brain-machine interface (BMI) hacks and stolen credentials and personal identification undermine the financial system's very foundation of identity and agency.**

### Joint actions between academic, government and private organizations

The most comprehensive action requires collaboration among all three groups to establish foundational standards by defining the structure, rules and knowledge requirements for AI, which would inherently govern technologies like BMI. This involves working on containers of AI and classifications of AI and requires knowledge of the basis of AI. In this scenario, academics conduct the research, while government provides guidelines and private organizations and industry jointly implement the standards.

### Government actions

The government is responsible for regulatory and monitoring measures focused on user interaction, such as implementing usage restrictions on relevant platforms or systems like age, time and prompt limits. this includes establishing oversight by requiring a mandatory survey of users to evaluate the reason and frequency of usage for evaluation.

# Actions

THREAT 3 ACTIONS

**Unchecked overreliance on emerging technologies, specifically AI and agentic systems, across multiple critical infrastructure networks with no transparency or trouble indicators, causes loss of control and human agency and ultimately leads to human harm and system collapse.**


## Actions by industry

### Good governance of AI framework

A comprehensive AI governance framework is needed to ensure safety and ethical compliance of emerging technologies. Regulators should draft these frameworks, and nation-states must then ratify the resulting treaties and agree on how to implement them to establish a global standard. This action is essential for providing clear, legally binding guidelines that restore human agency and accountability.

### Clear definition of human agency

Regulators should create a clear definition of human agency, specifically outlining what aspects of decision-making should and should not be outsourced to a machine. This involves establishing ethical boundaries and clear legal frameworks to dictate the necessary human-in-the-loop (HITL) requirement for all decisions with catastrophic potential. No exceptions should be allowed for these catastrophic decisions, ensuring human oversight remains the ultimate control.

### Clarify legal liability for AI mistakes

Legal frameworks should continue to evolve to determine who is liable for an AI mistake. Frameworks should specify if the responsibility falls on the developer, the user, or the operator. An unambiguous answer to this question is crucial for restoring human agency and accountability within AI-driven critical systems.

## Actions by policymakers/civil society

### Renewed sense of trust in government

A renewed sense of trust in government is vital to prevent citizens from being tempted to replace human leadership with AI governance. Policymakers should achieve this by being more transparent about how decisions are made. Civil society plays a crucial role in demanding this transparency from their governments.

# Actions

## Actions by governments

### Education and spreading awareness

Governments should take the lead in providing education and spreading global awareness about the ethical versus unethical uses of AI. This educational effort should also involve controlling research to ensure that no single individual or small group can make uncontrolled progress on dangerous AI. This approach aims to create a globally informed populace and a more controlled pace of technological advancement.

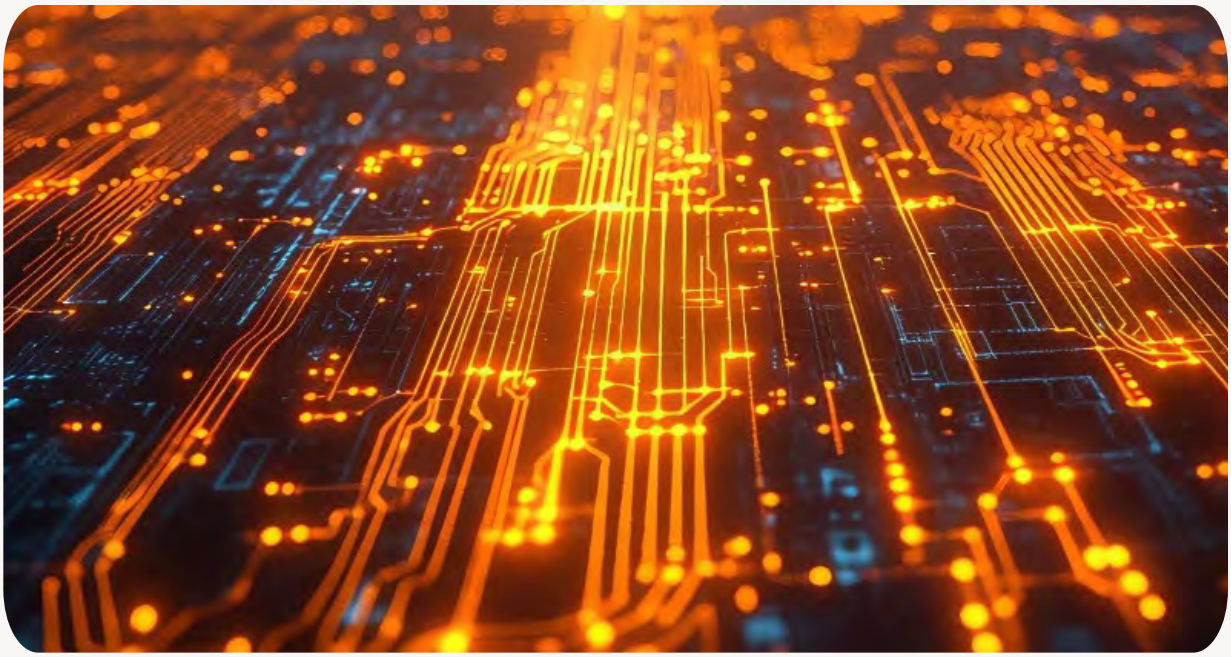
## Actions by multi-stakeholders (broad)

### AI in critical infrastructure

AI deployed in critical infrastructure must be considered an integrated part of the overall defense system, not merely a solution to replace human decision-making. This requires a collaborative approach involving individuals, policymakers, technology companies, academia and NGOs. These diverse groups should work together to ensure AI serves to augment, not usurp, human control.

### AI explainability and transparency

There is a need to mandate AI explainability and transparency for all systems. This effort requires a collaboration between regulators, government, academia and civil society to establish clear standards. This collaboration must clearly define the expected human agency and the triggers for human intervention in automated processes.



# Actions

## Actions by researchers and technology companies

### Research on maintaining human agency

Researchers and tech companies should collaborate on new ways to maintain and enforce human agency within AI systems. This involves developing technical solutions and interfaces that prioritize human understanding and control. Their joint efforts are crucial to building trustworthy, human-centric AI.

### Implementing post-quantum cryptography

Implementing post-quantum cryptography early is a necessary systemic action. This is a proactive security measure designed to minimize opportunities for abuse by future, more powerful computing threats.

## Actions by individuals

### Understanding technology and autonomy

Individuals must take responsibility for understanding the technology they are using, including how it functions and its level of autonomy. They need to familiarize themselves with the human-in-the-loop (HITL) decision framework associated with these systems. Furthermore, individuals should promote a culture of actively questioning authority, which includes AI systems.

# Actions

THREAT 4 ACTIONS

**Systemic inequality brought on and heightened by proliferation of emerging technological systems (AI) leads to social unrest and physical conflict.**

## Actions by industry

### System silos and checkpoints

Companies such as those in the financial sector should establish critical system silos and checkpoints to prevent cascading failures across interconnected infrastructure. These isolated environments act as defensive barriers, ensuring that a compromise in one part of the system does not lead to total collapse or widespread physical conflict.

### Minimum usage algorithm package (MUAP)

Governments and organizations should ensure that all individuals have access to a foundational set of algorithmic capabilities. This "minimum usage algorithm package" (MUAP) provides a basic safety net that supports fair and reliable outcomes in digital systems, helping reduce gaps in access and strengthening overall societal resilience.

### Limiting technology overtaking human labor

Actions must be taken to limit the speed at which technology completely overtakes human labor. This involves deliberately slowing down or regulating automation to allow people to keep their jobs and maintain a sense of purpose. This measure is a direct approach to reduce the economic pressure that fuels social unrest.

### Biometric data backup storage

Certified biometric data banks are responsible for establishing and maintaining secure, reliable backup storage. This action is a crucial biosecurity measure to protect foundational biological data against corruption or malicious attacks. Secure storage ensures the integrity of essential genetic information in a highly technological landscape.

# Actions

## Actions by academia

### Independent research and reporting

Academia must be empowered to expose the systemic problems and ethical failures stemming from the proliferation of emerging technology. This independent research and reporting provides a critical check on both industry and government practices. Their findings are necessary for public awareness and driving meaningful policy change.

## Actions by regulators

### Responsible innovation and biometric research

Regulators must enforce ethical standards and secure-by-design principles across all emerging technologies, including highly sensitive fields like DNA research. They need to draft and implement specific regulations for biometric data research to prevent misuse that could exacerbate social unrest or biological threats. This pre-emptive regulation ensures that technological advancement is governed by safety and fairness from its inception.

## Actions by individuals

### No-touch rule

Individuals should adopt a no-touch rule, implying a deliberate restraint or limitation on interaction with certain technologies. This personal choice is an act of preserving human agency and reducing dependency on automated systems. This action helps mitigate the systemic risk of unchecked overreliance on AI.

# 06

# Conclusion





threatcasting

# Conclusion

## Research question

**What are the future threats from emerging disruptive technologies, such as quantum computing, Artificial Intelligence (AI) and large data sets, to Mastercard's European region and global operations?**

## 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 socialize the threats in this report, raise awareness and initiate the conversations necessary to develop a response. As a part of this preparation, organizations may need to connect with old and new partners and allies alike. Once these connections and conversational lines are in place, each group can begin to monitor 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, to understand the reality of these threats and the steps that can be taken to make the future safer.





threatcasting

threatcasting

For inquiries about this report, please contact
Mastercard_Fusion_Center@mastercard.com

Scan the QR code to learn more about Threatcasting at Mastercard and access past reports