threatcasting

2020 Mastercard Threatcasting Report

THE FUTURE OF FRAUD, CYBERATTACKS, AND EMERGING TECHNOLOGIES

Table of Contents

Table of Contents

Threatcasting Overview

The future of fraud, cyberattacks and emerging technologies

In the next decade, the adoption of emerging technology will expose greater vulnerabilities for criminals, nation-states, corporations, organizations, and individuals to capture data (physical, digital, biological) and whole identities to commit fraud. Opportunities for fraud will increase and the motivation to commit this type of crime will grow. Beyond financial gain, the perpetrators of fraud will have political and ideological goals, co-opting criminals, proxy attackers, and unsuspecting combatants as allies.

The 2020 Mastercard Threatcasting project identified two threat futures at the intersection of fraud, cyberattacks, and emerging technologies:

Threat Futures

Hiding in the Complexity – "Old Fraud in New Ways"

Criminals will use the expanding technological landscape to commit traditional fraud by hiding in the complexity and scale of the technology, business, and financial ecosystems.

New Motivations – "New Fraud in Old Ways"

Bad actors will use traditional fraud and broader criminal activities for nontraditional effects, attacking beyond financial systems to adjacent infrastructure. The logic of these attacks will be orthogonal to traditional attacks with expanded goals to destabilize, distract, disrupt, influence, and just to prove it is possible.

Actions

Form Deeper Sharing Relationships

In recognition of the broad implication of these future threats broader industry sharing relationships are needed.

Monitor Threats

Using the Threatcasting indicators and Fraud Assessment Framework, Mastercard's Fusion Center will monitor for emerging threats and work to coordinate their disruption.

Periodic Reporting

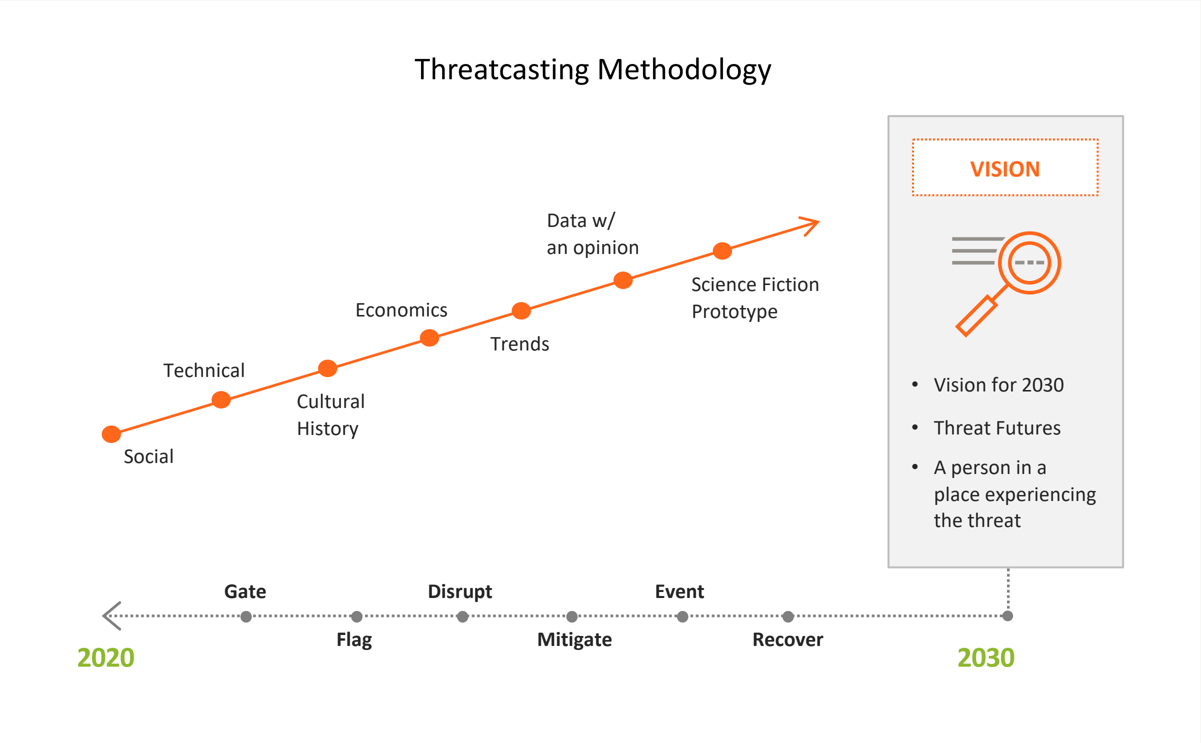
In the coming future periodic reporting is needed on the progression of these threats and the emergence of new ones.

What is Threatcasting?

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

Threatcasting uses inputs from social science, technical research, cultural history, economics, trends and subject matter–expert interviews. These various inputs allow for the creation of potential futures. Some of these futures are desirable, while others are to be avoided.

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



(Figure 1)

Mastercard 2020

Threatcasting Workshop Overview

Workshop purpose

Through our threatcasting workshop, Mastercard sought to identify possible threats 10 years into the future at the intersection of fraud, cybersecurity, and technology. Additionally, the assembled participants determined what organizations and ecosystems could do to disrupt, mitigate, and recover from these possible threats.

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

Workshop process

In February 2020 a cross-functional group of Mastercard practitioners, partners, and customers gathered in a workshop to create models of threat futures.

Drawing research inputs from a diverse data set and subject matter–expert interviews, our groups synthesized the data into workbooks, curated with Johnson specifically for Mastercard's purposes. For this workshop, two different kinds of workbooks were used.

Threatcasting workbooks

The basic threatcasting workbook asks each group to pick one data point from each of the different speakers or areas (social, technical, economic, etc.) then consider all of these points to begin to model 10 years out. In order to do this, the methodology takes a macro to micro approach: Start with the high-level data point (derived from the research inputs) then apply it specifically to a person in a place with a problem. This approach frees the group to imagine and model multiple futures, which we later clustered and aggregated. The clustered results appear in this report.

The second threatcasting workbook we used was the Research Synthesis Workbook, which tasks the group with identifying a data point, exploring its implications, determining if it's positive or negative (or both), and finally, discussing how the implications apply to Mastercard and the broader industry (What "we" should do about it.). The "we" is purposely broad as the input can be personal to the group, the collected team in the room, the entire company, or the entire human race. The goal of the Research Synthesis Workbook is to capture the important data points from the research presentations and the opinions and views of the Mastercard experts assembled in the room.

Together, the group modeled multiple futures centered around a person in a place experiencing the threat. Each of these visions, along with our discussions and secondary research, is covered in this report.

High-Level Findings

In the next decade, the adoption of emerging technology will expose greater vulnerabilities for criminals, nation-states, corporations, organizations, and individuals to capture data (physical, digital, biological) and whole identities to commit fraud. The opportunities for fraud will increase and the motivation to commit the crime will grow. Beyond financial gain, the perpetrators of fraud will have political and ideological goals, co-opting criminals, proxy attackers, and unsuspecting combatants as allies.

Threat Future 1

Hiding in the Complexity – "Old Fraud in New Ways"

Criminals will use the expanding technological landscape to commit traditional fraud by hiding in the complexity and scale of the technology, business and financial ecosystems.

Threat Future 2

New Motivations – "New Fraud in Old Ways"

Bad actors will use traditional fraud and broader criminal activities for nontraditional effects, attacking beyond financial systemS to adjacent infrastructure. The logic of these attacks will be orthogonal to traditional attacks with expanded goals to destabilize, distract, disrupt, influence, and just to prove it is possible.

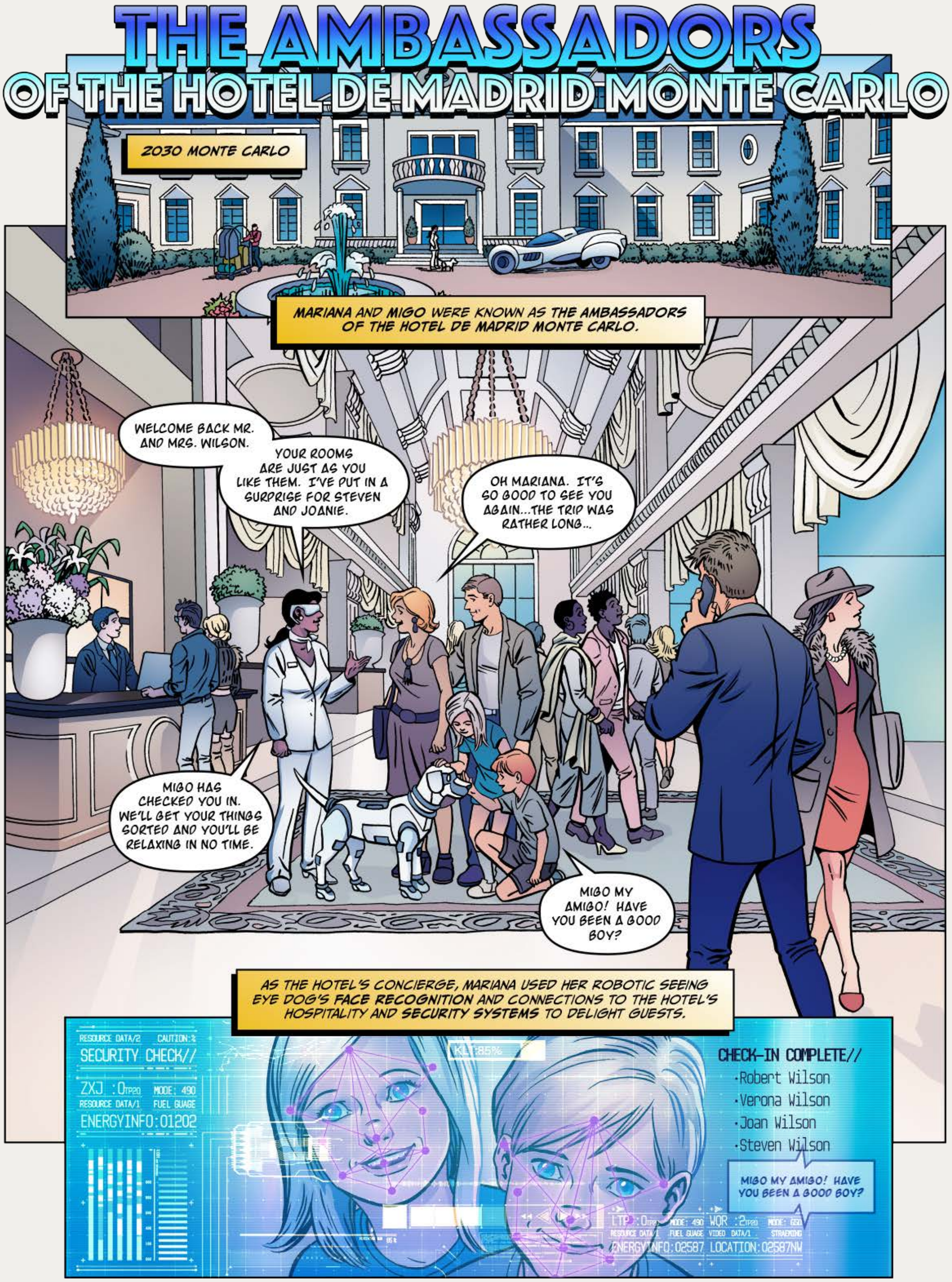
Threat Future 1

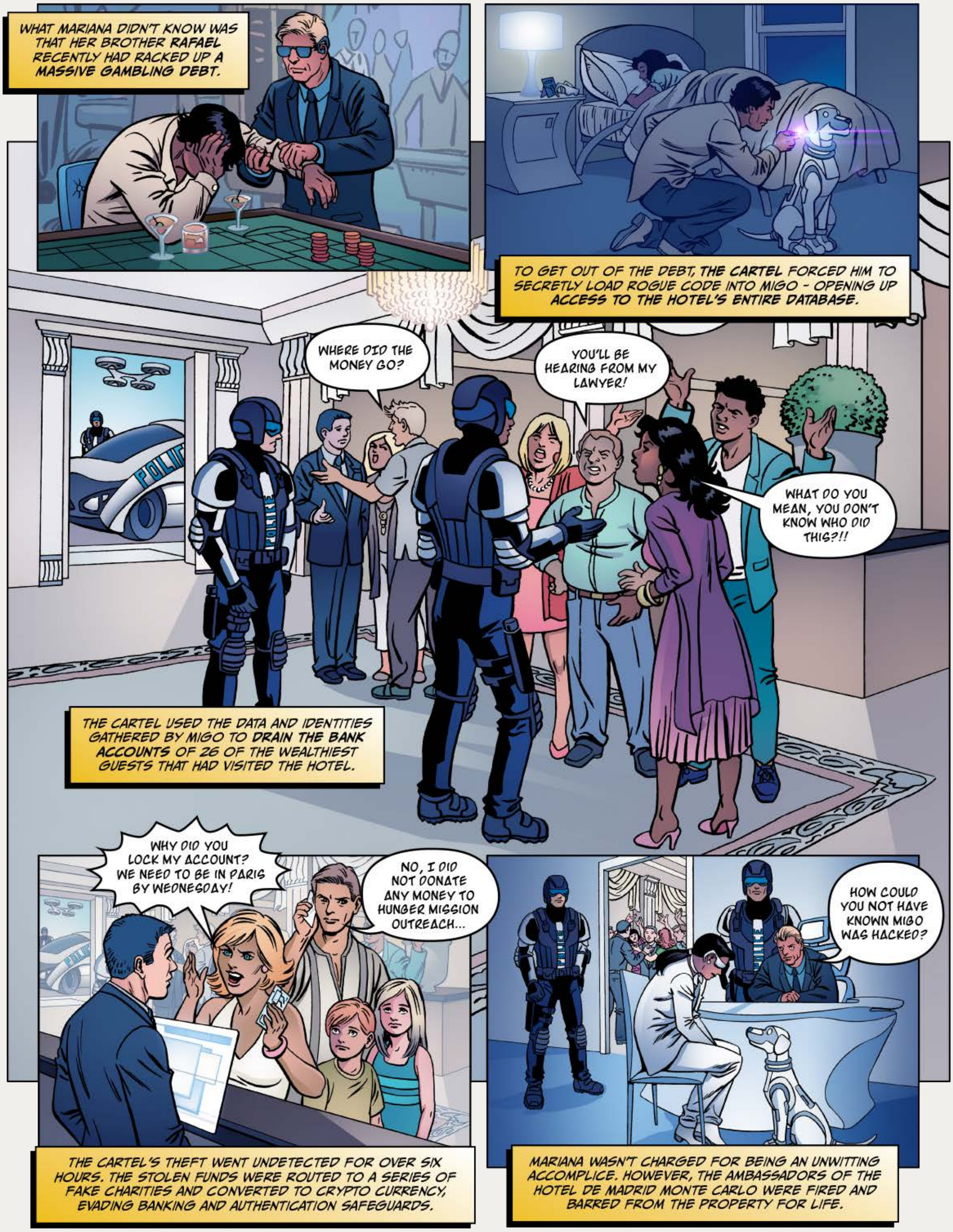
Hiding in the Complexity

Criminals will use the expanding technological landscape (targeted systems and platforms) to commit traditional fraud for financial gain by hiding in the complexity and scale of the technology (hardware, software, 5G connectivity, artificial intelligence (AI), and autonomy) as well as the business and financial ecosystems which will be enabled and expanded by emerging technology and connectivity.

Threat Future Visualization

Science fiction prototypes are visualizations based on research, future models and current activities. These visualizations are purposely not sensationalized depictions of possible and potential threats. They are used to make threats visceral and concrete for the reader. The following visualization explores a future of interconnected technologies, business and financial ecosystems that are left vulnerable to a criminal cartel via an unsuspecting insider threat.


THE AMBASSADORS
OF THE HOTEL DE MADRID MONTE CARLO
2030 MONTE CARLO
MARIANA AND MIGO WERE KNOWN AS THE AMBASSADORS OF THE HOTEL DE MADRID MONTE CARLO.
WELCOME BACK MR. AND MRS. WILSON.
YOUR ROOMS ARE JUST AS YOU LIKE THEM. I'VE PUT IN A SURPRISE FOR STEVEN AND JOANIE.
OH MARIANA. IT'S SO GOOD TO SEE YOU AGAIN...THE TRIP WAS RATHER LONG...
MIGO HAS CHECKED YOU IN. WE'LL GET YOUR THINGS SORTED AND YOU'LL BE RELAXING IN NO TIME.
MIGO MY AMIGO! HAVE YOU BEEN A GOOD BOY?
AS THE HOTEL'S CONCIERGE, MARIANA USED HER ROBOTIC SEEING EYE DOG'S FACE RECOGNITION AND CONNECTIONS TO THE HOTEL'S HOSPITALITY AND SECURITY SYSTEMS TO DELIGHT GUESTS.
RESOURCE DATA/2 CAUTION:%
SECURITY CHECK//
ZXJ :0TP20 MODE: 490
RESOURCE DATA/1 FUEL GUAGE
ENERGYINFO:01202
KL :85%
CHECK-IN COMPLETE//
·Robert Wilson
·Verona Wilson
·Joan Wilson
·Steven Wilson
MIGO MY AMIGO! HAVE YOU BEEN A GOOD BOY?
LTP :0TP20 MODE: 490 WQR :2TP20 MODE: 650
RESOURCE DATA/1 FUEL GUAGE VIDEO DATA/1 STREAMING
ENERGYINFO:02587 LOCATION:02587NW


WHAT MARIANA DIDN'T KNOW WAS THAT HER BROTHER RAFAEL RECENTLY HAD RACKED UP A MASSIVE GAMBLING DEBT.
TO GET OUT OF THE DEBT, THE CARTEL FORCED HIM TO SECRETLY LOAD ROGUE CODE INTO MIGO - OPENING UP ACCESS TO THE HOTEL'S ENTIRE DATABASE.
WHERE DID THE MONEY GO?
YOU'LL BE HEARING FROM MY LAWYER!
POLICE
WHAT DO YOU MEAN, YOU DON'T KNOW WHO DID THIS?!!
THE CARTEL USED THE DATA AND IDENTITIES GATHERED BY MIGO TO DRAIN THE BANK ACCOUNTS OF 26 OF THE WEALTHIEST GUESTS THAT HAD VISITED THE HOTEL.
WHY DID YOU LOCK MY ACCOUNT? WE NEED TO BE IN PARIS BY WEDNESDAY!
NO, I DID NOT DONATE ANY MONEY TO HUNGER MISSION OUTREACH...
POLICE
HOW COULD YOU NOT HAVE KNOWN MIGO WAS HACKED?
THE CARTEL'S THEFT WENT UNDETECTED FOR OVER SIX HOURS. THE STOLEN FUNDS WERE ROUTED TO A SERIES OF FAKE CHARITIES AND CONVERTED TO CRYPTO CURRENCY, EVADING BANKING AND AUTHENTICATION SAFEGUARDS.
MARIANA WASN'T CHARGED FOR BEING AN UNWITTING ACCOMPLICE. HOWEVER, THE AMBASSADORS OF THE HOTEL DE MADRID MONTE CARLO WERE FIRED AND BARRED FROM THE PROPERTY FOR LIFE.

Targeted Systems and Platforms

Smart Infrastructure

National and local governments will use connected smart devices to increase efficiencies and monetization for transportation infrastructure (e.g., roads, tolls, bridges, etc.). These efficiencies will be used not only by citizens but corporations and global supply chains as well.

Buildings and Cities

The proliferation of connectivity, computational power, and sensors will cause uneven implementation of smart cities, buildings, and infrastructure. This interconnectivity will pose a problem for security and policing activities.

Global Distributed Artificial Intelligence Systems

Public and private organizations will implement AI to varying degrees across global commercial infrastructures. Much of this AI will be proprietary and not transparent, meaning decision-making and actions will be difficult, if not impossible, to trace. The level of sophistication will vary based on capital investment, leaving many underfunded organizations and countries vulnerable and at a disadvantage. AI will begin to touch all software.

Robots

Aided by AI, autonomous computational devices (robots) will broaden in use from the factory and warehouse floors to use in healthcare, childcare, security, and consumer usage.

Autonomous Vehicles

Autonomy on land, sea, and air will create a physical network of devices that can be managed, tracked, and attacked by bad actors. The integration of these vehicles into smart infrastructure and cities creates a vulnerable shadowed and high-speed transactional plane.

Transport Systems and Drones

Local governments and global supply chains will use AI and computational power to streamline and create efficiencies for the movement of people and goods. These systems will tie into broader networks of municipal and corporate systems. Many of these systems will travel long distances, crossing borders and even oceans.

Personal and Industrial IoT

The ability to turn any object into a computer that can sense and communicate brings the threat landscape down to a micro level. The rollout of the personal IoT landscape is not leading with security in mind, which is creating massively vulnerable platforms. Industrial IoT's implementation has a higher level of security, but operating inside of closed systems creates a vulnerability after a breach or behind the scenes.

Wearables and Implantables

The ability to turn any object into a computer that can sense and communicate brings the threat landscape down to a personal level, tying transactions to specific people, bodies, and biometrics. New vulnerabilities will arrive for the biological health of consumers and the complexity of biological data.

In the future, criminals will use the complexity and scale of corporate and financial systems to defraud consumers. They will not only operate and hide in this complexity, but they will take advantage of the ambiguously designated responsibilities of governments, corporations, and regulatory bodies.

Complex global corporate ecosystems and the supply chain will provide ample targets for criminals to enter the supply chain, alter hardware and software systems, corrupt data, and hijack AI and other forms of autonomy to cause harm. These attacks will be both immediate and "low and slow," taking place behind the scenes, out of sight, and over an extended period.

This scale and complexity provide a widening attack plane for criminals to reach consumers and the local or national governments that use these systems. These combined factors will make detection and attribution multifaceted and difficult.

Threat Indicators

Threat indicators are meant to give an organization early warning and clear signals that a specific threat is beginning to manifest. They can be used so that organizations do not react too early or too late to global events. Fundamentally, these signals are clear, observable, quantifiable evidence upon which strategies can be built. The post analysis of the threatcasting raw data can be broken down into two categories:

Conditions under which the threat is most likely to take shape.

Specific Occurrences or a moment in time, an action or an observable data point that indicates the threat is beginning to take shape.

Conditions

These conditional areas could be subtle and occur over a long stretch of time. Conversely, they could manifest quickly by swift government of industry actions. They will certainly be unevenly distributed globally, occurring in different locations at varying speeds. The more conditional indicators that occur in this threat area, the more likely it will be that the threat itself will happen.

Technology Advances and Adoption

- Increased general business and consumer reliance and integration of AI
- Widespread usage and proliferation of IoT in homes and cities
- Smart cities encourage dependence on devices
- Increased reliance on IoT devices that circumvent corporate security
- Common acceptance and use of biometric information
- Interoperability of standards and common formats that utilize biometrics
- Technology manufactured by competition or "nonfriendly" actors

Business/Security/Regulatory

- Privatization of identity
- Poor collaboration between technology owners and regulators leads to disparate and inadequate security and regulatory standards
- Inadequate security by peer data custodians
- New regulations that impact future technology advancements
- Inability to completely track stolen funds
- Elimination of humans in customer service positions
- Integration of technology partners into financial networks
- A lack of control over knowledge of transaction end points
- Permissive insider threat environment becomes more common across industry
- Over-reliance on AI-powered banking systems
- Covert and undiscovered system penetration or exfiltration

General

- Natural disasters
- Geopolitical tensions and situations
- Shifts in retirement demographic create rise in use of technology by general population and labor force
- Popularity of fake charities

Specific Occurrences

Specific occurrences are typically late-stage indicators that the threat has manifested or is about to occur. Because of this, organizations must be careful to verify the validity of the information. This will guard against a reaction to a false positive. Also, specific occurrences are vulnerable to disinformation and misinformation.

Attack Activity

- Identification of new or novel hacking techniques and methodologies
- Confirmed cases of AI hacks
- Proof of AI tools that steal IP
- Proof of weaknesses in software development processes
- Increased use of cyberattacks to affect physical outcomes
- Breaks in the infrastructure of security systems

Data/Technology

- Examples of Black-market exchange of information or services
- Identification of advances in targeted data breaches and leaked stolen data sets
- Quantum computing becomes operational and breaks encryption and tokenization[1]
  – See sidebar for flags from previous 2018 threatcasting
- Biometrics data replace passwords
- Consolidation of identity into one source, allowing a single compromised device to transact on behalf of an individual

General

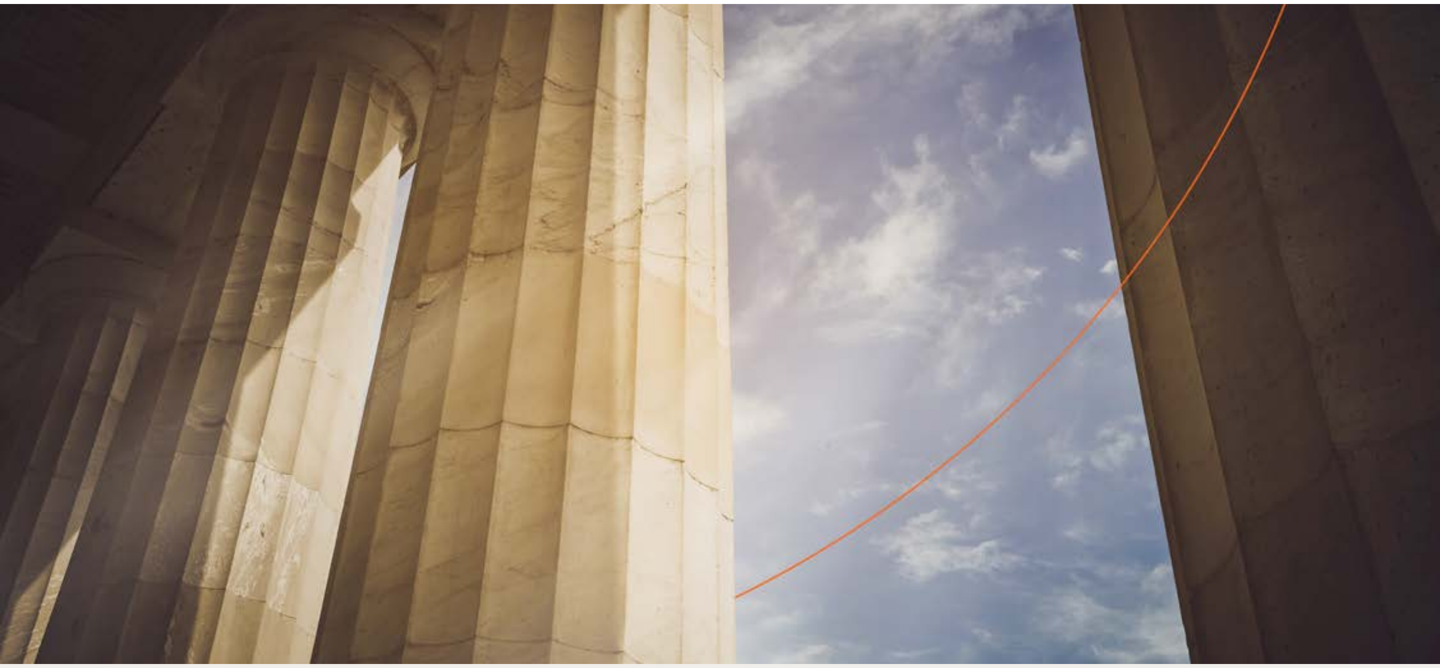
- Remote purchase and delivery of big-ticket items (e.g., cars) become more commonplace
- Increase in violence by people of certain age or in certain demographic with no previous history

Quantum Threat/Reality[1]

(Detailed Actions/Flags)

- Sensing and Monitoring
  – Although quantum computers can break "unbreakable" encryption, they can do little else more effectively than regular computers (speed/cost)
    > "Reading emails, stealing bitcoins, designing molecules" [Flag: Until this is proven wrong]
  – Entanglement is fragile and uptime is essential, "The universe is working against the computer" (decoherence)
    > Need 6 mil qubit computer and current computers run at 55 [Flag]
    > It took two years to go from 47ms to 94ms uptime [Flag]
- Explore "Unknown" Threats
  – "We know what we know until we prove it wrong"

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 happens. An organization can take action to prevent these threat futures. Utilizing the indicators as a signal of a threat's progression, an organization can make strategic decisions for when to invest capital and effort to mitigate or recover from the threat. The post analysis of the threatcasting data showed that there were three types of action that could be taken to disrupt, mitigate, and recover from this threat future.

Technology and Business: Actions that can be taken by a single organization that include both business and technological steps.

Partnerships and Ecosystem: Actions that can be taken by multiple organizations both inside and outside of the industry.

Legal and Regulatory: Actions that would include support for actions taken by legal or regulatory bodies (e.g., government, law enforcement).

Technology and Business

Organizations have the most control over these technology and business actions. The following activities will help to mitigate or nearly disrupt the threat.

Data Handling and Security

- Special priority given to the protection of collected data
- More diligence for the protection of data through backups and encryption
- Increased distribution of identification data and decentralized data
- A focus on migration from legacy systems
- Increased identification and management of dormant accounts
- Developing and implementing fraud AI behavior detection rules
- Increased use of multifactor authentication
- Including an extra security handshake between apps and financial institutions before transaction completion
- Adoption of layered security protocols to ensure single breach points not sufficient (layered AI)
- Mandate that all players “know your inventory” (e.g., What endpoints are on your networks?)
- Explore deception capabilities (e.g., effective measures to confuse adversary)
- Continued exploration and implementation blockchain technology

Corporate Initiatives

- Gather intelligence on threat areas and start monitoring indicators
- Conduct wargaming and preparation exercises that update the organization’s threat response “playbook”
- Conduct exercises that address IP theft
- Practice defense in depth to prevent future attacks
- Work with the wider industry to monitor AI and IoT-driven device activity
- Explore organization software development lifecycle integrity
- Enable legal team knowledge and advocacy of current and future issues

Insider Threat Prevention

- Improve background checks for employees in critical roles
- Explore employee vetting tools that are active and adaptive; however, caution is needed, as these tools could be seen as invasive and might be used improperly

Partnerships and Ecosystem

The nature of this threat is the complexity of the technology and the business relationships that it will afford organizations. Broadly, this threat cannot be thwarted by a single organization alone. It will be a whole-of-industry, whole-of-nation and most probably a whole-of-society problem. Because of this, organizations must review their partnerships and ecosystem strategies in new ways.

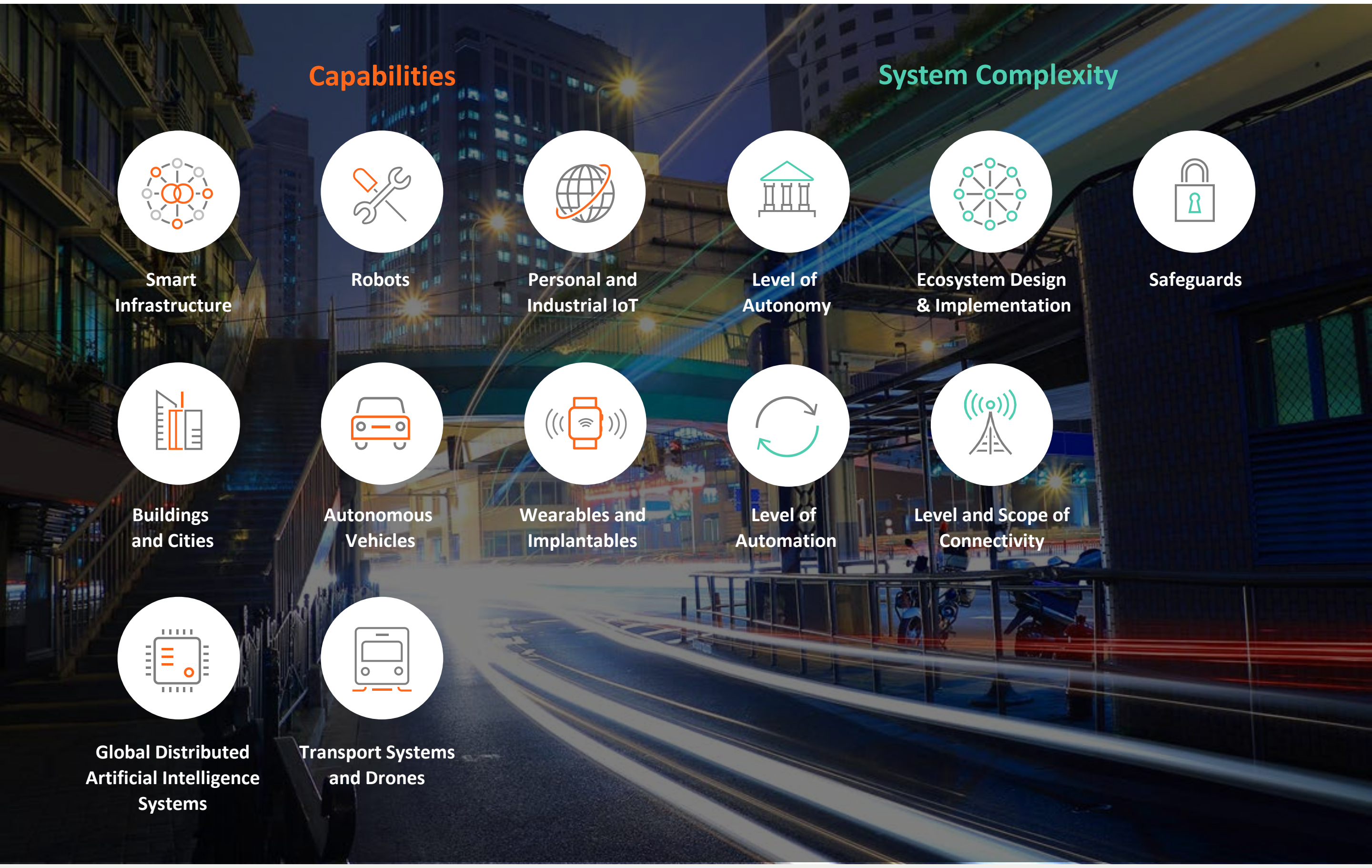
- Engage in wider information sharing across industry groups and government
- Foster closer cooperation between technology or enabling companies and government
- Enable information sharing between financial institutions to identify fraudulent activity across institutions
- Encourage intelligence sharing with law enforcement agencies
- Minimize usefulness of these stolen data sets by finding new ways to authenticate users during transaction flows

Legal and Regulatory

Many aspects of this threat fall outside the jurisdiction and influence of private industry. Just as the partnerships and ecosystems need to be readdressed, so too does an organizational or industry approach to legal and regulatory bodies. Because these bodies can be complex and deliberate by design, a much more long-term approach will be required.

- Encourage informed regulations and privacy law that
  – Safeguard personal data
  – Report breaches of data and sharing of data
  – Enact regulation that requires the verification of AI-driven transactions by another third-party AI
- Encourage more control over basic cybersecurity hygiene and common best practices
- In-state basic security protocols for governments
- Enforce data separation requirements
- Encourage transparency on current and emerging threats on AI and IoT-driven devices
- Support public education campaigns on information that should and should not be shared with financial apps and services

Fraud Assessment Framework



Capabilities

Smart Infrastructure

Robots

Personal and Industrial IoT

Buildings and Cities

Autonomous Vehicles

Wearables and Implantables

Global Distributed Artificial Intelligence Systems

Transport Systems and Drones

System Complexity

Level of Autonomy

Ecosystem Design & Implementation

Safeguards

Level of Automation

Level and Scope of Connectivity

The Fraud Assessment Framework is a series of questions and classifications that are meant to identify weak points in the complexity of new products, emerging technologies as well as business partnerships and ecosystems. The framework investigates the following:

System Capabilities

- What are the base technological capabilities of the device or system?

System Complexity

- What is the level of complexity of the system?
  - – Connectivity
  - – Automation/Autonomy
  - – Safeguards
- Ecosystem Mapping

System Capabilities

What are the base technological capabilities of the device or system?

- **Connectivity**
  - What systems does the device or broader system connect to?
- **Computational power**
  - How much computational power does it have?
  - How much computational power does it need to perform the task?
- **Personal and payment data**
  - How does the system receive, use, store, and share personal and payment data?
- **Biometric**
  - How does the system receive, use, store, and share biometric data?
- **Software**
  - Who developed the device or system and where was it developed?
  - How does it interface with consumers? (Optional)

System Complexity

What is the connectivity to

- Other devices
- Businesses and ecosystems
- Systems (technological)

What are the safeguards?

- What are the levels of transparency, checks and balances, audit?
- When is other technology brought in?
  - – e.g., AI audit of other AI actions and processes
- When is a human brought in?
  - – Human in the loop

What is the level of automation and Autonomy?

- How much of the device's/system's tasks are automated?
  - – Process data = take preset actions
- How much of the device's/system's tasks are autonomous?
  - – Process data + make decision = act

How is the ecosystem designed and implemented?

- Who is involved in the system?
- Who is partnered with the system?
  - Where are they located?
- What are the networks for holding detection, attribution, and accountability?
- Who is responsible for policing and regulation?

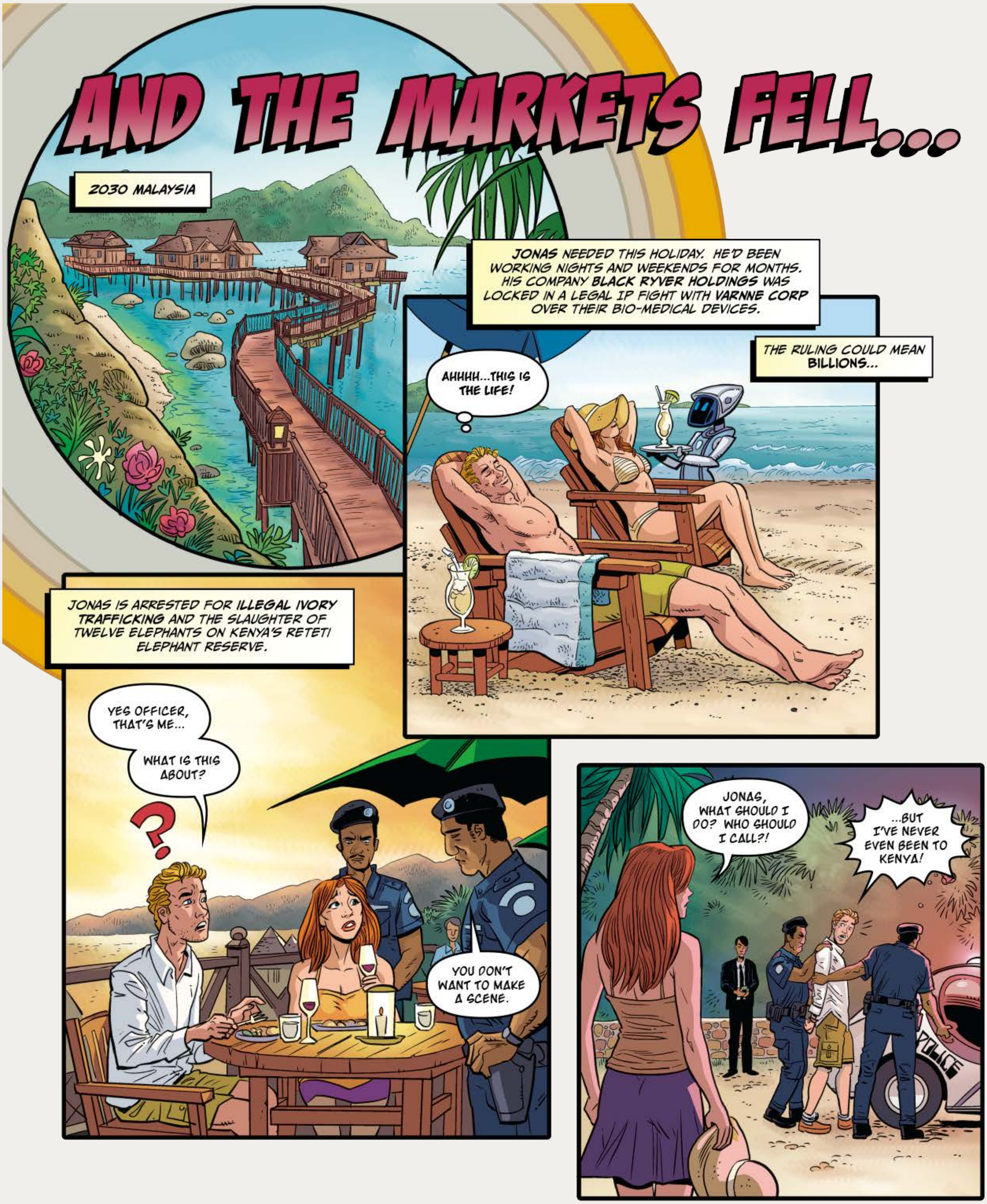
Threat Future 2

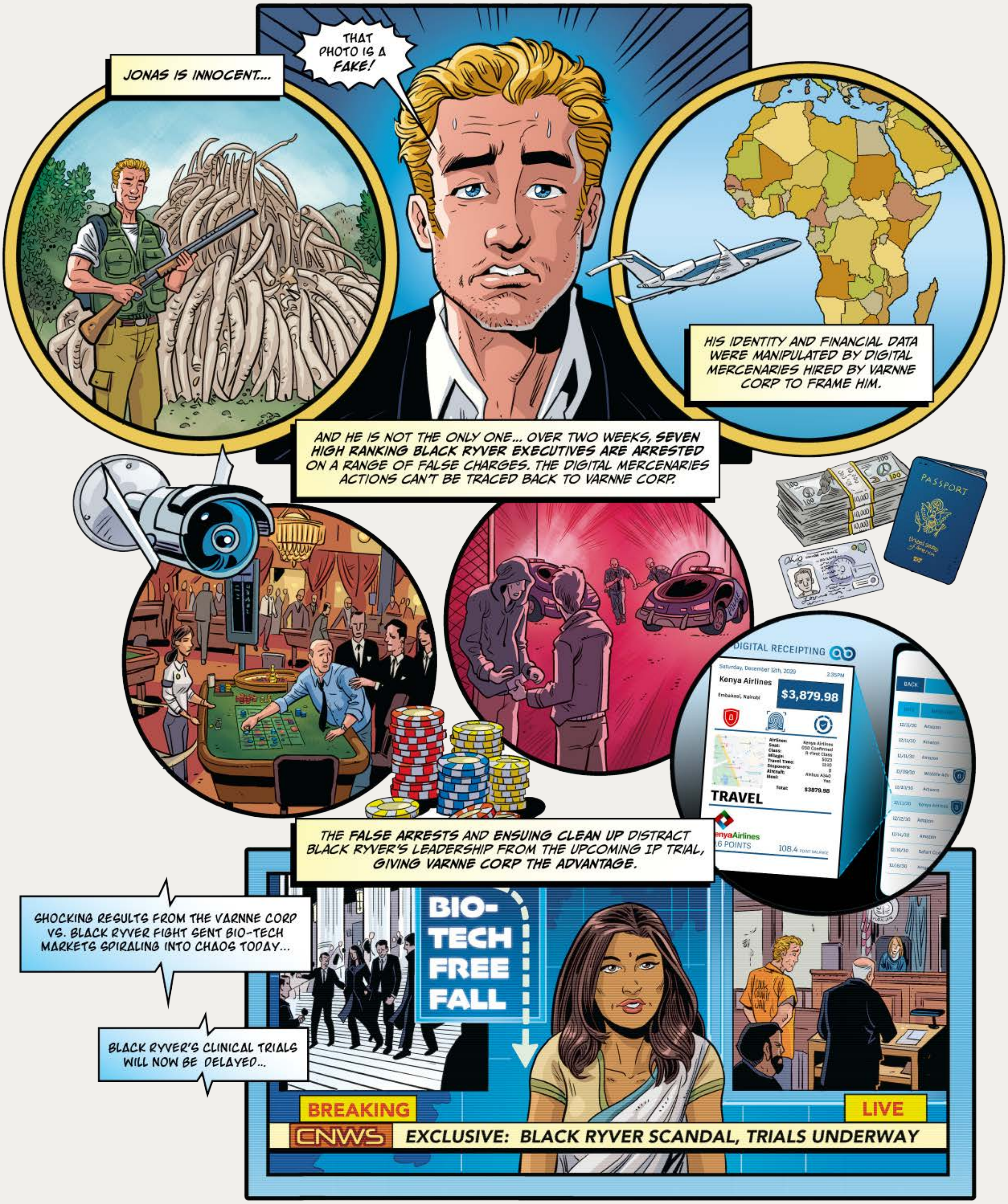
New Motivations

Bad actors will use traditional fraud and broader criminal activity for non-traditional effects, attacking beyond financial systems to adjacent infrastructure. The logic of these attacks will be orthogonal to traditional attacks with the extended goals of destabilizing, distracting, disrupting, influencing as well as just proving it is possible.

Threat Future Visualization

Science fiction prototypes are visualizations based on research, future models and current activities. These visualizations are purposely not sensationalized depictions of possible and potential threats. They are used to make threats visceral and concrete for the reader. The following visualization explores a future where corporations use fraud and criminal activity to target individuals in rival organizations to gain strategic business advantage.


AND THE MARKETS FELL...
2030 MALAYSIA
JONAS NEEDED THIS HOLIDAY. HE'D BEEN WORKING NIGHTS AND WEEKENDS FOR MONTHS. HIS COMPANY BLACK RYVER HOLDINGS WAS LOCKED IN A LEGAL IP FIGHT WITH VARNNE CORP OVER THEIR BIO-MEDICAL DEVICES.
AHHHH...THIS IS THE LIFE!
THE RULING COULD MEAN BILLIONS...
JONAS IS ARRESTED FOR ILLEGAL IVORY TRAFFICKING AND THE SLAUGHTER OF TWELVE ELEPHANTS ON KENYA'S RETETI ELEPHANT RESERVE.
YES OFFICER, THAT'S ME...
WHAT IS THIS ABOUT?
?
YOU DON'T WANT TO MAKE A SCENE.
JONAS, WHAT SHOULD I DO? WHO SHOULD I CALL?!
...BUT I'VE NEVER EVEN BEEN TO KENYA!
POLICE


JONAS IS INNOCENT....
THAT PHOTO IS A FAKE!
HIS IDENTITY AND FINANCIAL DATA WERE MANIPULATED BY DIGITAL MERCENARIES HIRED BY VARNNE CORP TO FRAME HIM.
AND HE IS NOT THE ONLY ONE... OVER TWO WEEKS, SEVEN HIGH RANKING BLACK RYVER EXECUTIVES ARE ARRESTED ON A RANGE OF FALSE CHARGES. THE DIGITAL MERCENARIES ACTIONS CAN'T BE TRACED BACK TO VARNNE CORP.
PASSPORT
DIGITAL RECEIPTING
Saturday, December 12th, 2029
2:35PM
Kenya Airlines
Embakasi, Nairobi
$3,879.98
TRAVEL
Total: $3879.98
BACK
108.4 POINT BALANCE
THE FALSE ARRESTS AND ENSUING CLEAN UP DISTRACT BLACK RYVER'S LEADERSHIP FROM THE UPCOMING IP TRIAL, GIVING VARNNE CORP THE ADVANTAGE.
SHOCKING RESULTS FROM THE VARNNE CORP VS. BLACK RYVER FIGHT SENT BIO-TECH MARKETS SPIRALING INTO CHAOS TODAY...
BLACK RYVER'S CLINICAL TRIALS WILL NOW BE DELAYED...
BIO-TECH FREE FALL
BREAKING
LIVE
CNWS
EXCLUSIVE: BLACK RYVER SCANDAL, TRIALS UNDERWAY

Threat Future 2

New Motivations

Bad actors will use traditional fraud and broader criminal activities for non-traditional effects, attacking beyond financial systems to adjacent infrastructure. The logic of these attacks will be orthogonal to traditional attacks with the extended goals of destabilizing, distracting, disrupting, influencing as well as just proving it is possible.

Because the motivation for the fraudulent activity isn't primarily financial, how we monitor, disrupt, mitigate, and recover can be different.

Defining the New Threat Actors:
Who is committing the fraud or criminal activity?

Watching for the **Location**:
Where is the fraud or criminal activity being committed?

Observing the Desired Effects:
Why is the fraud or criminal activity being committed?

Defining the New Threat Actors

Who is committing the fraud or criminal activity?

These conditional areas could be subtle and could occur over a long stretch of time. Conversely, they could manifest quickly by swift government of industry actions. They will certainly be unevenly distributed globally, occurring in different locations at varying speeds. The more conditional indicators that occur in this threat area, the more likely it will be that the threat itself will happen.

State-Sponsored Threats

Nation-state actors begin to use fraud and criminal activity as a means to attack adversaries and gain advantage.

Criminal and Political Proxies

State actors and private organizations tap into criminals, cartels, and like-minded politically motivated organizations to carry out activities that cannot be attributed.

International Digital Mercenaries

A shadow industry of private for-hire actors who solicit “fraud as a service” or “crime as a service” emerges.

Activist Organizations, Extremists, and Terrorists

Enabled by the proliferation of technology and complex ecosystems, traditional activists, extremists, and terrorists amplify their goals using financial systems.

Insider Threats

A leading and persistent threat to organizations, the impact and vulnerability of insider threats become a tool for gaining access and amplifying effects.

Corporation-on-Corporation Attacks

Corporations and private organizations begin to use fraud and crime to gain market advantage over competitors. This activity will cross borders and will make attribution difficult.

Observing the Desired Effects

Why is the fraud or criminal activity being committed?

The observed fraudulent or criminal activity's effect will not be for financial gain but for a different outcome. The motivation for the fraudulent or criminal activity for nonfinancial gain will be the initial identifying factor that the threat is real and that the bad actor is active.

Widespread Destabilization

Destabilizing existing political, commercial, social or civil entities for specific gain or to sow chaos and doubt. A single sector might not be the target, as the effect is a broad-based destabilization in order to accomplish adversarial goals. Attribution may be difficult or completely transparent as the threat actor might want to show their power to effect destabilization as an end unto itself.

Erosion and Loss of Consumer Trust

This loss of trust with the consumer or average citizen will stretch across multiple sectors and markets. These sectors and markets include:

Financial Systems

Political System

Healthcare and Medical Systems

Security
– Personal
– National

Business
– Specific organization or company
– General business infrastructure

Data and Privacy
– Religious and community organizations

Why is the fraud or criminal activity being committed? (continued)

Infrastructure Disruptions

Infrastructure disruptions will go beyond traditional critical infrastructures to systems that consumers and governments have grown dependent on for the smooth operation of business, civic, and personal activities. The motivation for this kind of attack is confusion, fear, and chaos. The following are examples of the broad range of systems that could be disrupted; however, they do not cover all possibilities. An organization should consider any system that is depended upon by a large collection of people as a potential target.

Transportation

Power

Telco

Sanitation

Medical

Supply Chain

Food

Goods

Data

Corporation on Corporation Attacks for Business Advantage

This will see the expansion of corporate espionage and legal actions. Specific attacks will happen on individuals, groups, or business infrastructure that provides an organization with an advantage over a competitor or market.

Location

Where is the fraud or criminal activity being committed?

The location where the fraudulent or criminal activity is occurring will be of key significance in indicating the threat's progression. Early fraudulent or criminal attacks for nonfinancial gain may occur in markets or countries where the local infrastructure and security practices are not as hardened as other countries and markets. These early attacks will signal that the attack is now technically possible.
It may also serve as an indicator that the bad actor is testing or rehearsing the attack for another more advanced target.

- **Inside the United States**
- **Inside broader markets**
- **Across foreign borders**
- **Emerging geographies**

Indicators

Threat indicators are meant to give an organization early warning and clear signals that a specific threat is beginning to manifest. They can be used so that organizations do not react too early or too late to global events. Fundamentally, these signals are clear, observable, and quantifiable evidence upon which strategies can be built. The post analysis of the threatcasting raw data can be broken down into three categories:

"The Effects": Indicators identify the desired effect that the threat actor is looking to achieve. The specific crime or event may not be observable, but its effects highlight areas for future investigation and research.

Conditions: Indicators that a broader, referencing a landscape or conditions under which the threat is more likely to take shape.

Specific Occurrences: Indicators that reference a specific moment in time, action or observable data point that the threat is beginning to take shape.

"The Effects"

The observed fraudulent or criminal activity's effect will not be for financial gain but for a different outcome. Organizations will need to develop the capability and research to understand that what is observed is not as it seems. The motivation for the fraudulent activity for nonfinancial gain will be the initial identifying factor that the threat is real and that the bad actor is active.

- **Widespread destabilization**
- **Erosion and loss of consumer trust**
  - Financial systems
  - Healthcare and medical systems
  - Business
    - Specific organization or company
    - General business infrastructure
- **Infrastructure disruptions**
  - Transportation
  - Power
- **Personal and payment data**
  - Corp-on-corp attacks for business advantage

Conditions

These conditional areas could be subtle and could occur over a long stretch of time. Conversely, they could manifest quickly by swift government of industry actions. They will certainly be unevenly distributed globally, occurring in different locations at varying speeds. The more conditional indicators that occur in this threat area, the more likely it will be that the threat itself will happen.

- Dominance of one country in a specific technology space
- Single vendor dominating the market space
- Lack of control over external pressures and influencers
- Lack of control over privacy laws, which impedes investigations
- Widening inequality, global exploitation of thought labor in developing countries
  - Use of biometrics as a sole factor for authentication and adoption of policies
- Use of embedded devices to authenticate
- Divergence of privacy rules and standards globally, creating a fragmented enforcement environment
- Offshore vendor ownership is based in a country that has geopolitical differences

Specific Occurrences

Specific occurrences are typically late-stage indicators that the threat has manifested or is about to occur. Because of this, organizations must be careful to verify the validity of the information. This will guard against a reaction to a false positive. Also, specific occurrences are vulnerable to disinformation and misinformation.

- Successful attacks using AI solutions in various parts of the world
- Observing that a similar system or product is compromised
- General news of activity similar to an organization’s products or services
- Specific security breaches of input data
- Repeated data leaks and compromises in specific location
- Reports of stolen embedded devices
- Financial irregularities
  - Actuals out of sync with projections with no apparent justification
  - Gaps in financial reconciliations

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 happens. An organization can take action to prevent these threat futures. Utilizing the indicators as a signal of a threat's progression, an organization can make strategic decisions for when to invest capital and effort to mitigate or recover from the threat. The post analysis of the threatcasting data showed that there were three varieties of actions that could be taken to disrupt, mitigate, and recover from this threat future.

Disruption

Actions that can be taken and organization to disrupt the threat from developing.

Mitigate and Recover

Actions that can be taken by an organization to mitigate or recover from the threat once it has begun to develop or once it occurs.

Advocacy

An action that can be taken by an organization to advocate for changes that are outside of their control.

Actions (continued)

Disruption

Begin monitoring and early detection across identified vectors

- Defining the New Threat Actors: Who is committing the fraud?
- Observing the desired Effects: Why is the fraud being committed?
- Watching for the Location: Where is the fraud being committed?

Work to implement AI/autonomous/complex systems safeguards such as

- Checks and balances that keep a “human in the loop”
- Audits
- Anomaly monitoring
- Integration of security functions across ecosystems

Develop and expand vendor/tool/product selection process

- Safeguard process to prevent malicious code and hardware

Increase insider threat safeguards

- Employee and vendor screening
- Resilient ecosystem training with input from subject matter–experts like the U.S. Department of Defense and U.S. Secret Service

Mitigate and Recover

Prepare

- Conduct exercises for conditions and effects of attacks
- Research and explore better understanding of new threat actors and their motivations

Develop

- Strong ecosystem and extended network for mitigation and recovery

Advocacy

Laws & regulations

- Advocate for increased laws, regulation and norms against corporation-on-corporation attacks and activity threatcasting

About the analyst

Brian David Johnson:

The future is Brian David Johnson's business. As a futurist he works with organizations to develop an actionable 10 -15 year vision and what it will feel like to live in the future. His work is called futurecasting, using ethnographic field studies, technology research, cultural history, trend data, global interviews and even science fiction to provide a pragmatic road map of the future. As an applied futurist Johnson has worked with governments, trade organizations, start-ups and multinational corporations to not only help envision their future but specify the steps needed to get there. Johnson is currently the futurist in residence at Arizona State University's Center for Science and the Imagination, a professor in the School for the Future of Innovation in Society and the Director of the ASU Threatcasting Lab. He is also a Futurist and Fellow at Frost and Sullivan.

Johnson speaks and writes extensively in ongoing columns for IEEE Computer Magazine and Successful Farming where he is the "Farm Futurist". He has contributed articles to publications like The Wall Street Journal, Slate, and Wired Magazine. Johnson holds over 40 patents and is the best-selling author of both science fiction and fact books (WaR: Wizards and Robots, 21st Century Robot and Science Fiction Prototyping). He was appointed first futurist ever at the Intel Corporation in 2009 where he worked for over a decade helping to design over 2 billion microprocessors. Johnson appears regularly on Bloomberg TV, PBS, FOX News, and the Discovery Channel and has been featured in Scientific American, The Technology Review, Forbes, INC, and Popular Science. He has directed two feature films and is an illustrator and commissioned painter. In 2016 Samuel Goldwyn released "Vintage Tomorrows" a documentary based upon Johnson's book of the same name.