Cyber-Physical Coordinated Attacks: The Emerging Complexity of Crisis Management

John C. Checco

MULTI-MODAL THREATS

It is conceivable and probable that today's adversaries have contemplated and recruited for event scenarios in which a physical crisis is pre-ignited by a series of more carefully orchestrated cyber incidents. As extremist groups grow bolder and attract younger more technology-astute prospects, there will be a convergence where both logical and physical attacks methods are used in concert towards a singular goal. These will be much more complex and targeted than the typical diversionary tactics we are prepared for today.

This new breed of threat is **multi-modal**; it takes advantage of the operational silos between organizations, whether those are departments within a corporation, supply chains or competitors across an industry, regional government agencies across a nation, or multiple governing nations across a global coalition. Planning such complex executions requires extremely intimate knowledge of the disparate targets and their relationships.

In every sector there are vulnerabilities with the potential to affect both cyber and physical operations. Attackers are connecting the dots to create complex attacks utilizing multiple disparate tactics, techniques, and procedures (TTPs) to amplify overall impact or create cross-sector ramifications.

Relationship Between Cyber and Physical Attacks

Not all multi-modal attacks are the same in purpose and effect. Several specific categories can be defined where cyber and physical threats intersect:

- **Precursor:** This occurs when a party uses cyber-attacks on the infrastructure to prepare a target for a hostile takeover, as in the case of Russia and Georgia in 2008.[1]

John C. Checco is special advisor to the board of the Wall Street Technology Association, past president of InfraGard's NY Metro Chapter and co-chairs the annual NY Metro Joint Cyber Security Conference & Workshop. John currently resides as Resident CISO in Financial Services for a global security platform provider. Prior to this role, he was SVP for Bank of America's Global Information Security Innovation Group; integral in the establishment of their Zero Trust initiative, Responsible Automation guidelines, the Analysis & Resiliency Center for Systemic Risk, and participated in the DHS Loaned Executive Program. John also served as the Senior Information Security and Risk Advisor for Bloomberg L.P. where he introduced the BISO role to their various lines of business. His past experience encompasses emerging technology research and development at NYNEX, Pitney Bowes and IBM. John is a part-time Fire Instructor and volunteer firefighter with special teams training in extrication and dive rescue.

- **Scaffolding:** Similar to the precursor modus operandi, scaffolding attacks disrupt the supply chain for a larger economic and/or operational attack, which may have been the focus of the Colonial Pipeline attack.[2]
- **Direct Diversion:** As a diversionary tactic, a single party initiates a cyber-attack to redirect remediation resources away from a physical target.[3]
- **Indirect Diversion:** in this scenario, the party that performs subsequent cyber-attacks is exploiting the advantage of another party's conflict, as we currently see with several uninvolved nation states increasing their cyber-attacks during the Russia-Ukraine conflict.[4]

It is important to note that not all multi-modal attacks start with a cyber-attack. In the case study on electromagnetic pulse (EMP), it is the physical attack that cripples many electronic capabilities including communications and internet routing devices.

Case Study: The EMP (Electromagnetic Pulse) Threat

The most simplistic explanation of what an EMP attack is: flooding an air space with electrons, so those electrons overload the capacitors and resistors in any electronics device in its path, rendering them inoperable and, in many cases, irreparable. To be clear, an EMP attack is more complicated than a typical blast wave as it generates both short-term (M1) and long-term (M3) effects. To make matters more complicated, EMPs can travel great distances and are frequently created by solar flares, but are protected by the earth's magnetic shield.

This adversarial threat comes in two form factors: (1) detonating a nuclear device at an altitude high above their target, or (2) using smaller devices, known as EMP cannons, to affect a specific facility. The national risk of a major EMP event created by a nation-state actor is considered extremely high impact but low probability. Groups such as InfraGard's National Disaster Resiliency Council (NDRC), Domestic Electromagnetic Spectrum Operations (DEMSO) and the Energy Information Sharing and Analysis Center (E-ISAC) are focused on electromagnetic pulses as a disruption path to any target dependent on the resiliency of the electrical grid.[5]

Resiliency against EMP events is not simply an energy sector issue. During an EMP attack, the consumers of energy are most likely not protected. Where will power facilities be delivering energy? The prediction is that industries such as agriculture, food supply, transportation, communications will only be able to operate at 10% capacity over an 18-month period.[6] It has been estimated that a power generation facility that has 10% resiliency can still generate about 80% of the power needs it serves.[7] Preparation is key, because the low probability of an attack still includes both man-made upper atmospheric nuclear detonation[8] as well as the natural solar flare, such as the Carrington event of 1859.[9]

Beyond using EMP to disrupt technology and operations, high-value human targets are at risk. There is circumstantial evidence pointing to suspected localized low energy pulse attacks against US government employees both abroad (Cuba,[10] Guangzhou[11]) and domestic arenas.[12]

Cross-Sector Affectation & Scaffolding Dependencies

An attack in any one of these categories would leave the targeted region extremely vulnerable to physical attacks. In many cases, a primary cyber-attack is used to simplify the secondary physical attack methods, as, after a cyber-attack, the normal protectors for minimizing physical damage have been significantly diminished.

Scaffolding dependencies, whereby the success of a high-level complex operation relies on the continued sustenance of one or more lower-level operations, further complicate matters, as indirect and/or collateral damage may far outweigh any direct destruction as direct effects tend to be acute while collateral effects are often long-lasting.

The Roman Empire & Kill Chain

A documentary about the technologies of the Romans[13] shows they were the most advanced civilization of their time. Several distinct innovations, each one dependent on the prior success, were key to their success:

1. The formulation of **marine concrete**.
2. Architectures using **arches and domes** using custom-formed blocks of concrete.
3. Water **aqueducts** built using arches, for irrigation as well as waste removal.
4. Utilizing water flow to power massive **grain milling operations.**
5. Prioritizing **food supply** to keep armed forces healthy.

This combination of innovative technologies that supported each other came about because of astute governing concepts and sustained a highly advanced civilization. If any of these tenets did not exist, or were disrupted, then their society would not have survived.

Eventually, the Roman Empire fell due to what today we call the kill chain, the disruption of an entire operation by simply destroying one of its dependencies.

Similarly, the Food & Agriculture sector is one of the only sectors that is dependent on the remaining fifteen sectors as defined by the US DHS, as identified by the National Disaster Resilience Council (NDRC).[14]

Industry Vulnerabilities (capable of multi-modal affectation)

In each sector, cyber threats have the potential to affect physical and downstream operations exist. Understanding where these vulnerabilities are and where cyber-attacks can be used for amplifying incidents where cross-sector ramifications are far greater than its parts is crucial.

Banking & Financial Services

The banking and financial services industry experiences persistent direct attacks against components such as consumer bank accounts, ATMs, and institutional payment systems. There are many scenarios where cyber events seek one or more of the following situations: (a) financial gain from playing a series of long or short market positions, (b) retribution against a specific public company or the financial institutions themselves, or (c) disrupting the economy on a national or global scale regardless of any financial gain.

The unintended applications of a technology can lead to more systemic events, whether through intentional misuse (for example, the utilization of cryptocurrency to bypass sanctions[15]) or, exploiting the lack of operational guardrails preventing runaway execution such as automated high frequency micro-trading which resulted in the Flash Crash of 2010.[16] Since this 2010 economic event, regulations have been introduced to automatically halt trading to prevent spiraling of the stock market.

SWIFT Protocol Abuse

According to security threat intelligence vendor F-Secure, SWIFT is characterized as an easily exploited technology:

> Attackers realized that focusing on low profile, calculated, and sophisticated attacks on financial institutions has the potential for a much higher gain and requires less overall effort than continuously targeting individual customers. There have been at least eight high-profile attacks on SWIFT systems over the past five years (among many other lower-profile attacks), all resulting in significant financial loss.[17]

Fake News/Alerts

Fake news, especially rampant across social media channels, has played directly into moving economic markets and allowing threat actors to capitalize on that market response. As CNBC reported:

> The FBI and SEC are to launch investigations after more than £90bn was temporarily wiped off the US stock market when hackers broke into the Twitter account of the Associated Press and announced that two bombs had exploded at the White House, injuring Barack Obama.[18]

Automated (unsupervised) High Frequency Micro-Trading

A noted analyst from JP Morgan warns about the exponential rise of HFMT, the automated technology that caused the Flash Crash of 2010:

> Automated trading strategies are programmed to automatically sell into weakness. Together, index and quant funds now make up as much as two-thirds of assets under management globally, and 90 percent of daily trading comes from those or similar strategies.[19]

Cryptocurrency as a [Financial] Weapon

Morgan Wright, reporting from The Hill, "Iran is doing what every respectable state sponsor of terrorism does when their economy is going down the drain. They turn to bitcoin. Just like North Korea did (and still does)."[20] A senior Iranian official confirmed: "[Crypto]currency would facilitate the transfer of money (to and from) anywhere in the world ... It can help us at the time of sanctions."[21]

Blockchain Weaponization

The [pseudo-]anonymity of cryptocurrencies could also be used by those same nations to financially support and arm terrorist groups, acting as an underground payment system "in plain sight" with attribution capabilities by our cyber-defenses limited to coalescing disparate crypto-wallets;[22] but really having no other actionable remediation.

> National security experts are warning about cold-war type scenarios where the blockchain and cryptocurrencies are weaponized to illicit ends and governments (such as North Korea) can use it to evade sanctions and unleash an era of financial warfare.[23]

Public Utilities / Infrastructure

The utility sectors are similar to banking and finance since they serve the public at large, and most citizens will be affected by downed utilities. We have seen explicit attempts to obstruct energy production, specifically with the advent of StuxNet. Industrial control systems (ICS) are the computer control systems for managing one or more physical devices. Many times, these devices have embedded ICS consoles. The systems that aggregate and maintain large sets of devices via ICS are known as supervisory control and data acquisition (SCADA) systems.

In assessing the risks within ICS/SCADA systems, two characteristics need to be considered: threat type and location sensitivity.

- **Threat Types**
  - **Operational** threats have an immediate impact on business with little to no warning, and should be considered a significant risk to the organization.
  - **Targeted** threats are those that have a specific goal on altering business operations, critical data exfiltration, and/or holding entities at risk by embedding and burrowing until C2 actions are taken.
  - **Indirect** threats are characterized by disrupting ancillary operations, such as disabling the physical access control systems.
- Location Sensitivity
  - **Tier 1** facilities are critical to daily operations of the business.
  - **Tier 2** facilities can sustain short-term outages without affecting critical areas of operations.
  - **Tier 3** facilities do not affect short-term operations, but may have longer-term impacts.

Historically, different reporting lines are responsible for different systems; thus, there are inconsistent levels of protection across these systems.

> Many of the computers controlling industrial systems are old and predate the consumer Internet. Companies, against the advice of hacking gurus, increasingly brought them online in the past decade as a way to add ‘smarts’ to U.S. infrastructure. Often, they are connected directly to office computer networks, which are notoriously easy to breach. America’s power grid, factories, pipelines, bridges and dams—all prime targets for digital armies—are sitting largely unprotected on the Internet.[24]

Transportation

As far back as 2016, a Booz Allen Industrial Cybersecurity Threat Briefing has predicted what we are seeing today, “New targets, including light rail operators, and new tactics such as supervisory control and data acquisition (SCADA) access as a service (SAaaS) and ransomware against ICS, are likely to emerge and expand.”[25]

Water Utilities

Various events have targeted water sources and water treatment plants over the decade:

2013: “Iranian hackers infiltrated the control system of a small dam less than 20 miles from New York City two years ago, sparking concerns that reached to the White House.”[26]

2017: “An unnamed water district, dubbed the Kemuri Water Company (KWC), experienced unexplained patterns of valve and duct movements over at least a period of 60 days.”[27]

2021: "Hackers remotely accessed the water treatment plant of a small Florida city last week and briefly changed the levels of lye in the drinking water, in the kind of critical infra structure intrusion that cybersecurity experts have long warned about."[28]

Electric Grid

James Heyen's research identified increased threats against the electrical grid in times of disruption. "Following the [U.S.] Northeast Blackout of 2003, there was an uptick of scanning by rogue actors for weaknesses in many industrial control systems."[29]

Smart Cities

Even as our traditional city infrastructures are under attack, Smart Cities are gaining national momentum as a playground for technology innovation and experimentation. Yet only a handful of groups are addressing the cyber and physical security needs for protecting these cities' infrastructures which are inevitably an entirely new attack surface for predators. 30

> The increased complexity of city's systems, interdependencies, globally connected social, economic and political sub systems has increased the vulnerability of a city's security. The interface between urban growth, technology, infrastructure and capital requirement presents a unique set of opportunities and challenges to the implementation of Smart cities.[31]

Any one of these scenarios would leave the targeted region extremely vulnerable to physical attacks. In many cases a primary cyber-attack simplifies secondary physical attack methods, as the normal protectors for minimizing physical damage have been significantly diminished: "Los Angeles, Houston, Chicago, and Dallas each had more than 2 million exposed cyber assets that make them vulnerable to exploitation and compromise."[32]

After the financial sector, the energy sector has been the most aggressive industry in the cyber and physical security arena and has focused on many critical infrastructure impacts from EMP (electromagnetic pulses) to better information sharing amongst the various ISACs under the GRF/EASE initiative.

> ISO/IEC 30182:2017 describes, and gives guidance on, a smart city concept model (SCCM) that can provide the basis of interoperability between component systems of a smart city, by aligning the ontologies in use across different sectors.[33]

Commercial Facilities

Compared to energy and other public infrastructure, risks to commercial facilities ICS/SCADA components exist as well. The attackers' TTPs (Tactics, Techniques and Procedures) are similar, but the risk and response plans are governed by individual private entities—corporations, landlords and/or facility management firms. Threats to commercial facilities fall into two major areas: direct breaches of systems, and exploitation of organization procedure weaknesses.

> One international law enforcement agency estimates that victims lose about $400 billion each year worldwide—making it a bigger criminal enterprise than the global trade in marijuana, cocaine and heroin combined.[34]

Many differing guidelines exist for creating defense-in-depth with such networks, even to the point of isolated network systems separating BMS/SCADA from internet-facing corporate networks. Existing data centers and facilities cannot feasibly migrate to air-gapped isolation as it would require:

- Significant resources in standing up a new network infrastructure;
- Whitelist-based point-to-point routing rules (possibly breaking current operations);
- Separate consoles for accessing BMS and corporate systems;
- Disconnection of BMS data into existing logging/monitoring tools (on the corporate network);
- Disablement of remote manufacturer direct access to BMS systems (perhaps a good thing);

Aviation

The Aviation ISAC (A-ISAC) encompasses six different aspects of the industry: airlines, airports, platforms, satellites, engines, and equipment manufacturers.[35] Regrettably, each operates in its own lane with regards to tabletop exercises and cross-functional potential events. Conversely, there is no overriding authority for managing the entire sector: terminals are owned/operated by the regional authority, logistics (parking, food, et al) are consigned services, airlines rent gate space, airplane manufacturers are not directly involved in daily flight operations, and security (TSA, FAA, or other) is an isolated resource.

The International Air Transport Association (IATA) is a trade association representing ~300 airlines and over 80% of total air traffic.[36] "IATA has a list of recommendations to address present and future aviation threats including a focus on the universal implementation of global security standards, effective information-sharing among governments and with the industry, sustainable risk-based security measures, and emerging risks."[37]

The International Civil Aviation Organization (ICAO) has a Global Aviation Security Plan (GASeP) "provides the foundation for States, industry, stakeholders and ICAO to work together with the shared and common goal of achieving five key priority outcomes: (1) enhance risk awareness and response, (2) develop security culture and human capability, (3) improve technological resources and innovation, (4) improve oversight and quality assurance; and (5) increase cooperation and support." [38]

Many attacks in the air transportation industry were preceded by the ability to physically bypass existing security checkpoint systems. Using cyber-attacks to bypass security checkpoints opens up an entirely new set of attack surfaces.

Passenger/Reservation Systems

The lowest hanging fruit in the air transportation sector is the ability to manipulate the airlines' corporate and operational systems by manipulating flight reservations and passenger identities.

> Air Canada said that it detected unusual login activity … It is possible to use the [exposed] information to obtain genuine documents such as driving licenses and new passports.[39]

Airplane Scheduling Systems

Airlines use the concept of day-bedding for ensuring the maximum number of flights in/out of multiple airports. With the airlines, one's departing flight is directly dependent on another's incoming flight. When operated properly, this prevents the need for any airline to have planes in the hangar thereby reducing costs. However, when it fails, the cascading affects can be global: "Four air carriers now control approximately 85 percent of domestic capacity. All it takes is one airline to experience an outage and thousands of passengers could be stranded."[40]

Baggage Handling Systems

It is surprising to know that not all bags on commercial airlines are scanned. There exists the distinct possibility that the baggage handling systems can be hacked to bypass scanning based on certain tag number formats or baggage attributes.

> The six typical vectors for introducing explosives are: passengers (on person); passenger carry-on baggage; passenger checked baggage; cargo originating from known, unknown, or consolidated shippers; courier bags; and mail. More subversive vectors include crew members (e.g., pilots or flight attendants); an intentional or accidental security bypass; food catering service or meal cart; duty-free items; cleaning crew; and service crew (e.g., mechanics, fuelers, baggage handlers). To prevent the introduction of an explosive, all of these vectors must be secure.[41]

X-Ray / Passenger Inspection Systems

X-Ray passenger inspection systems suffer from a variety of limitations such as the following:

- **Missed identifications** are commonplace due to opaqueness, clutter and similarity of consumer electronics to detonation devices. "No security X-ray system has yet been produced that can make autonomous decisions for acceptable and reliable threat detection. All still heavily depend on human operators to view and interpret the images."[42]
- **Screening Avoidance** such as the recent trend surrounding weapons made of non-detectable materials. "The Liberator, Wilson's plastic pistol, would contain a 6-ounce piece of steel that can be removed, raising the possibility that walk-through metal detectors would not detect the guns."[43]

Healthcare / Medical

The healthcare sector reformed the security system with HIPAA (Health Insurance Portability and Accountability Act) in 1996 and HITECH (Health Information Technology for Economic and Clinical Health Act) in 2009. HIPAA requires better protecting patient information, while the HITECH Act requires that all medical records be in electronic form. Yet, no standard format was defined for electronic health records. Because the electronic data is not normalized, this lack of standardization leads to more cases of medical identity fraud and misdiagnoses. Normalization is the process of restructuring relational data to reduce data redundancy and improve data integrity. Having multiple unsynchronized instances of the same patient and medical data creates a broad attack surface ripe for unauthorized modification and abuse.

> A hospital employee snooped on patients' information for 14 years before the breach was discovered. The breach affected 1,100 patient records and remained undetected until one of the patients called in with a complaint.[44]

Misdiagnosis/Death from Patient Identities Fraud

There are two serious scenarios that occur from such disarray:

- **Medical Identity Theft**

  Some (mostly low-income) families or communities will reuse the identities of family members who have health insurance to piggyback on their insurance plans. This is unhealthy to all patients using the same identity, as the medical history does not accurately reflect any single patient and a rogue patient may be subject to undue medications and treatments.

- **Misdiagnosis/Mistreatment Against a Target**

  This more nefarious scenario would be a cyber-attacker altering the medical history of a target to create a situation where an improper medication/treatment is given to the target, resulting in death. The number of healthcare data breaches have been growing exponentially annually.[45]

Death from Manipulating Devices

Similar to the scenarios above, medical devices can be directly hacked to achieve a similar outcome. Medical devices including pacemakers, heartrate monitors, MRIs, and Insulin pumps have been found to be exploitable with potentially deadly results. 46 As new exploits are found in medical devices, a volunteer group known as I Am the Cavalry works to identify, address, and assist medical device manufacturers/facilities in remediating issues.[47]

> Every single medical device that is connected to a network is a breach opportunity. Put another way, every single medical device that can be operated remotely presents unthinkable possibilities.[48]

Healthcare is a fragile target, as there is an imbalance between keeping critical medical devices secure (patched) versus keeping them operational.[49]

Telecommunications/Internet

There are espionage cyberattacks on many of our legacy communications systems to garner information about operations and targets for further attacks. These include, but are not limited to:

SS7 Vulnerabilities

Signaling System 7 (SS7) was developed in the 1970s as a method to coordinate and route calls across the Public Switch Telephone Network (PSTN). The notion of secured communications was not a concern in the 1970s, and SS7 is vulnerable. Even as more varieties of newer technologies (ISDN, xDSL, Ethernet) were invented, SS7 remained the primary one in use and securing communications that happen on this platform is inconceivable due to the sprawl and impact area for changing (breaking) the protocol. What we are left is a legacy protocol that was never meant for arbitrary inline inspection as it runs over transports that are designed to allow unrestricted and anonymous tapping of information flow almost anywhere in the communication flow.

> Cyber criminals exploited SS7 flaws to intercept two-factor authentication codes (one-time passcode, or OTP) sent to online banking customers and drained their bank accounts.[50]

SIP Abuse

Session Initiation Protocol (SIP) is one of the modular capabilities added onto SS7 to allow customer premise equipment (CPE) such as PBX systems to provide endpoint identification to the switch network. Prior to this, switching systems relied on massive telecommunication databases to convert complex circuit numbers and trunking information to be translated to actual phone numbers.

As originally designed, SIP allowed arbitrary injection of metadata into the signaling layer, without any consideration for misuse; the engineering assumption was that all endpoint devices (CPE) would properly identify themselves. Although SIP was created to fill a deficiency in SS7, it is now widely used for cellular networks as well as internet traffic; allowing indiscriminate devices to identify themselves without any endpoint authentication or verification.

As a result, we are in a situation today where phone number spoofing is rampant, and call-blocking does not prevent the true call originators. More disturbing is how internet providers are utilizing SIP for VoIP protocols.

> Because VoIP is not inherently tied to a particular location and often provides access to multiple phone numbers, it provides a level of anonymity that allows subscribers to mask their identities as well as the physical locations. The relative ease of access to and the ability to veil location and identity through VoIP networks provides ample opportunity for misuse and furtherance of illegitimate goals.[51]

Border Gateway Protocol (BGP) Hijacking

BGP routers are the road signs that allow internet traffic to find the shortest open path to its destination. However, if the communication stream were diverted to take an alternate route—one that allows the traffic to be captured and analyzed without the knowledge of either the sender or receiver—then even encrypted sessions (prior to TLSv1.3) could be decrypted offline and its information used for future cyber and physical attacks.52 Such is the case in a BGP attack, and it is not as uncommon as it first may seem.

> Routers rely on the BGP to puzzle out the best route between two IP addresses; when one party advertises incorrect routing information, routers across the globe can be convinced to send traffic on geographically absurd paths.[53]

BGP hijacking has been an ongoing attack vector resulting from conflicts, espionage, and misconfigurations. Some of the most notable incidents are: 2022 (Ukraine[54]), 2019 (EU/China[55]), 2018 (Nigeria/China[56]), 2017 (US/Russia[57]), 2015 (Malaysia[58]), 2014 (Russia/China[59]), 2013 (Iceland/Belarus[60]), 2010 (Worldwide/China[61]).

Telecommunication Security

Unfortunately, little effort exists to provide technology protections to areas such as SS7 and SIP. All efforts have been limited to laws enacted against fraudulent identity activity or misrepresentation[62]. But this has an obvious conundrum: How does one report a fraudulent identity? Reporting the false SIP information (i.e. Caller-ID) does not provide any attribution towards the true actor – especially if the SIP being used is your own phone number.[63]

Internet Communication Security

There have been many efforts to secure internet communications:

- **DNSSEC** *"DNS data itself is [cryptgraphically] signed by the owner of the data."*[64]
- **BGPSEC** *"Each hop in the [routing] path now protected with a signature."*[65]
- **TLSv1.3** *"Renegotiation is not possible in a TLSv1.3 connection."*[66]

As a matter of reference, DNSSEC has been around since 1997; BGPSEC was introduced in 2000 and yet neither has a significant adoption rate.[67]

MANAGING THE COMPLEX THREAT LANDSCAPE

The most common issue in organizations is a gap in proper delineation of responsibilities, which leaves them vulnerable to internal and external threats. This will culminate in the orchestration of cyber and physical tactics for a single terrorist objective. It is the precursor to more advanced and complex threats; some scenarios even seemingly unfathomable. Make no mistake; multi-modal attacks are certainly in our future. The end goal here is to gain situational awareness and prepare for any invocation of these complex threats.

Sector-Independent Coordinated Collaboration

One aspect that should be addressed globally is the inter-dependencies of sectors. Each sector has its own Information Sharing & Analysis Center (ISAC),[68] but they are not perfect in sharing IOCs (indicators of compromise) or attack TTPs (tactics, techniques, and procedures). The issue of sharing data in an ISAC is not always the same. Some examples of disparate sharing are:

- The **Energy Sector** is divided into several distinct ISACs: Electricity (E-ISAC,[69] Oil & Natural Gas (ONG-ISAC,[70] Downstream Natural Gas (DNG-ISAC),[71] Nuclear Energy Institute (NEI, [72] and Energy Analytic Security Exchange (GRF/EASE[73]). The Multi-State ISAC (MS-ISAC[74]) attempts to resolve this issue by sharing data from across these other ISACs.
- The **Aviation Sector** ISAC (A-ISAC[75]) combines several disparate sub-industries under the same umbrella: airlines, airports, platforms, satellites, engines, and equipment manufacturers. Many times, the data presented is not relevant to more than one of those six categories thus, it inadvertently creates a high noise-to-signal ratio, making focused analysis very difficult.
- The **Financial Sector** ISAC (FS-ISAC[76]) has a slightly different issue; the ISAC consists of many major financial firms as well as a myriad of much smaller financially focused organizations. Although IOCs and TTPs are shared, it is usually latent reporting. In some cases, an organization would not report the attack at all, except for legal notification, as it may bring undue attention to reputational risks and regulatory audits.
- The **Analysis & Resilience Center for Systemic Risk**[77] has been one successful model for a multi-sector targeted mission to identify systemic risks to any critical infrastructure.
- **InfraGard**, an FBI outreach program through their Office of Private Sector, focuses on both cyber and physical threats across U.S. critical infrastructures.[78]
- **ASIS International**, traditionally a physical security organization, expanded its focus in 2016 to include cybersecurity.[79]
- **DHS/CISA** created a shared collaboration space in 2018 for their NCC physical security watchdogs to work alongside the CISA cyber security watchdogs.[80]

Crisis Resource Management & Cybersecurity Frameworks

The FAA, in response to the crash of United Airlines Flight 173 on December 28, 1978, developed one of the first critical thinking guidelines for crisis management. Originally known as Cockpit Resource Management, this process is integrated by many emergency services into their Incident Command System.[81] One aspect of this guideline that applies to any group of decision-makers is the use of the three decision outcome avenues.[82]

- **Avoid:** plan to prevent possibilities of a crisis.
- **Trap:** recognize bad decisions and fix potential problems before a crisis.
- **Mitigate**: minimize the negative effect during a crisis.

It is important to note that whenever an unexpected/unplanned event occurs that requires the use of this catch-all activity, an investigation post-crisis is necessary to review and codify the event handling procedures for future possible incidents.

This concept of "decision outcome avenues" applies directly to information security planning. It has been expanded by the National Institute of Standards and Technology (NIST) into the formal Cyber Security Framework (CSF) as: Identify, Protect, Detect, Respond and Recover. The NIST CSF paradigm has advanced in several ways; most significantly to include the Cyber Defense Matrix [83] authored by security researcher Sounil Yu. Although originally designed to assess the security coverage provided by technology, it can also be used to assess potential scaffolding impacts. To augment the NIST CSF tenets, I would boldly venture to add a far left tenet of **Preempt** as a security strategy positioned to the leftmost pillar. The concept of Preempt would be to remove the attack surface itself, thus eliminating the capability of a threat actor to operate.

An example of preempt is the use password compromise. In the Identify stage, one can list a myriad of vulnerabilities and weaknesses with their organization's password policies and technologies. Consequently, a Protect plan would define password controls, such as stronger patterns or shorter password rotations. The Preempt principle, however, would take an alternate approach by implementing passwordless authentication using FIDO/2, transferring first-stage biometric authentication to the verified end-user device. [84] Organizations should utilize both the crisis management plan and defense framework in concert to build a more holistic preplan of managing the unexpected multi-modal incident.

Managing [Crisis] Without Authority

Marine Corps LtCol (Ret.) Robert J. Darling has defined a crisis management roadmap, which was originally designed for smaller organizations, for building resiliency plans against both physical and cyber threats. [85] Promoted as the mnemonic: **Start, Doing, More, To, Live!**™. This method breaks down crisis management into five distinct actions that can be performed by anyone at any level of the organization.

- **Sensing:** refers to one's situational awareness to recognize an unfolding crisis. Examples of this are communication loss, erratic operational performance, upstream issues, or proximal events where proximity refers to either physical (locale) or logical (technology stack).
- **Decisioning:** defines the crucial initial steps once a crisis event has been recognized. This unfolds into two stages: Assuming Leadership and Triaging the immediate situation.
  - **Assuming Leadership:** requires the mindset of preparing to take control as well as ensuring you can display the proper demeanor that allows you to take control.
  - **Triage**: implements initial short-term actions to address the immediate dangers, with a focus on four specific aspects: Prioritization, Control Awareness, Direction, and Response.
    - a) ***Prioritization:*** is the foremost activity for triage determining the order of operations, coarsely categorized as: Life, Safety, Property and Exposures. Life can be further broken down into concentric circles of preservation: self, team, affected victims, clients/customers, bystanders and finally everyone else.
    - b) ***Control Awareness:*** is identifying which attributes of the situation can be controlled and which are out of your control.
    - c) ***Direction:*** defines the guardrails for a proposed action plan.
    - d) ***Response:*** is coalescing all the information gathered up to this point into a structured plan of action, addressing a priority which you can control, understanding any ramifications of decisions. Note that, although you want to focus on things directly within your control, you never discard what is out of your control but rather park it as observe-and-report.
- **Making:** is the act of moving forward with purpose. This is the outward display of assuming leadership, but to be effective, you also need to be very structured in your approach:
  - **Know Your People:** Take the time to determine their capabilities and expertise as well as their willingness to assist. Assigning the right people to the right task is as important as the task itself.
  - **Define a series of RPOs (Recovery Point Objectives):** Break down any large plan into a series of smaller achievable milestones. Bystanders who are inadvertent participants[86] can achieve better results without being overwhelmed by the enormity of the situation.
  - **Scale In-Band Operations (Business Continuity):** Among any response is to work within your control, which typically means to focus on what the team knows best within their existing roles.

- **Implement Out-of-Band Operations (Emergency Response):** For those tasks that are outside of the normal working roles, a leader must determine and convince the most capable persons to assist in handling those non-traditional tasks. This is never an easy decision. Sometimes the best person for an out-of-band task is also the best person for an in-band task. Other times, someone with the expertise does not have the willingness to step out of their comfort zone.
- ***If All Else Fails*** ... Apply the tenets of Avoid/Trap/Mitigate. Control what you can; minimize the impacts of what you cannot. Do not try to focus on what you cannot affect.

- **Terminating:** includes understanding the conditions where emergency operations can be concluded. Similar to Sensing where situational awareness is used to define abnormal conditions a leader needs to use that same awareness to: (1) establish criteria for **Normalcy,** (2) determine conditions that warrant an **RTO** (return to operations), (3) specify tasks for **Salvage** and cleanup, and (4) take explicit actions to demonstrate that they **Relinquish Leadership.**
- **Learning:** is the continuous iterative process of review during and after the incident. It is comprised of: (1) interim debriefing sessions, (2) introspection as well as peer evaluation, (3) improvement of the decision-making processes, and (4) commitment to instantiate changes.

This method has proven effective for many types of multi-modal events (cross-sector, cyber-physical and scaffolding).

Non Sequitur

We should also be aware of three pitfalls with this topic: tunnel vision, apophenia, and bias.

- **Tunnel Vision:**

  Most enterprise security professionals focus on affectations and impacts to their operations and rightly so. Due to the sheer volume of signals that our SOC (security operations center) analysts must attend to, there is neither the time nor resources to identify systemic attacks.

  Focused impact analysis is the normal modus operandi for many organizations, and will not change. For all intents and purposes, it should not change, but be augmented by a small team responsible for looking above the water line.

- **Apophenia:**

  At the other end of the gamut, there are organizations teams solely looking for patterns; they interpret every problem in the context of a multi-modal threat. This swing of the pendulum is counterproductive as it could lead to unnecessary actions and expenditures. The Analysis & Resilience Center for Systemic Risk[87] is a textbook example of an organization built to look for systemic threats yet, they have an SOP which defines criteria to characterize and park seemingly non-systemic events, along with the ability pull them back into the fold if there is a correlation.

- **Bias, Preference or Expertise?**

  The prevalence of bias has historically contributed to a myopic behavior in every industry, and effectively working within the constraints of each sector's risk culture may be an effort upon itself. Risk assessment calculations are skewed by two key biases: motivational bias and cognitive bias.

  - **Motivational Bias** (predisposed by reward/punishment):

    Reputational risks are rated as high as other risk areas, as consumer/institutional confidence directly affects their market value;

  - **Cognitive Bias** (distortion of conscious beliefs):

    Although cyberattacks may cause fiduciary losses directly, indirect collateral damage to the larger financial ecosystem may not be felt for some time afterwards, which may cause firms to underestimate the residual risks after such an attack has been mitigated;

SUMMARY

Multi-modal capabilities will be the **point of inflection for all future attacks**, and we must be prepared. Organizations need to stop artificially treating cyber from other types of threats but must correlate both logical and physical risks as equal attributes in the same threat model. Collectively, we need to focus more efforts on identifying global cross-sector disruptions. The global economy has experienced the effects of our own indiscretions with regard to the mortgage crisis in 2008, resulting in a wholesale lack of trust in both the financial and real estate sectors as well as our regulators. And this was our own doing!

We must be careful of over-stepping the bounds of sanity. This can happen by confusing our highly advanced technical capabilities with bias and hubris, such as with the ludicrous suggestion (by a former senior advisor to the U.S. State Department Antiterrorism Assistance Program) that our response to potential threats should be a preemptive cyber-attack.

I leave you with one final excerpt:

Those wishing to do us harm have no state allegiance; they cross borders to share information and collaborate to refine their methods of causing chaos and destruction. The focus of governments must be on protecting people. And that cannot be done with insular thinking.[88]

NOTES

1. "Russia's Cyberattack on Georgia," Human Events Archive, August 15, 2008, https://archive.humanevents.com/2008/08/15/russias-cyberattack-on-georgia/.
2. R. Virani, "The Supply Chain Is the Next Big Cyberattack Target," Supply & Demand Chain Executive, March 16, 2022, https://www.sdcexec.com/safety-security/article/22118933/alliant-cybersecurity-the-supply-chain-is-the-next-big-cyberattack-target.
3. "Cyber-warfare, cyber diversions and cyber terrorism," https://book.cyberyozh.com/cyber-warfare-cyber-diversions-and-cyber-terrorism/.
4. Audrey Conklin, "Chinese cyberattacks on NATO countries increase 116% since Russia's invasion of Ukraine: study," Fox Business News, March 26, 2022, https://www.foxbusiness.com/technology/chinese-cyberattacks-nato-increase-ukraine.
5. InfraGard, "INFRAGARD EMP RESOURCE CENTER," https://www.empcenter.org.
6. T. Ahasan, "Preparing for the crash: The threat of an electromagnetic pulse," March 26, 2018, https://globalresilience.northeastern.edu/2018/03/preparing-for-the-crash-the-threat-of-an-electromagnetic-pulse/.
7. InfraGard NDRC, "Chapter VI: Resilient Communities using an Island Concept," in Powering Through "From Fragile Infrastructures To Community Resilience, Curtis 1000, 2016.
8. J. Stavridis, "North Korea's Secret Weapon: A Huge Electromagnetic Storm," April 25, 2018, https://www.bloomberg.com/view/articles/2018-04-25/north-korea-s-secret-weapon-an-electromagnetic-storm.
9. P. Dockrill, "Here's What Would Happen if a Solar Storm Wiped Out Technology as We Know It," June 21, 2018, https://www.sciencealert.com/here-s-what-would-happen-if-solar-storm-wiped-out-technology-geomagnetic-carrington-event-coronal-mass-ejection.
10. P. Martin, "American diplomats in Cuba were targeted with microwave weaponry," September 2, 2018, http://revolutionradio.org/2018/09/02/american-diplomats-in-cuba-were-targeted-with-microwave-weaponry/.
11. B. M. Farmer, "Is an invisible weapon targeting U.S. diplomats?" CBS News 60 Minutes Overtime, June 27, 2021, https://www.cbsnews.com/news/is-an-invisible-weapon-targeting-u-s-diplomats-60-minutes-2021-06-27/.
12. J. Herb, "US investigating possible mysterious directed energy attack near White House," CNN, April 29, 2021, https://www.cnn.com/2021/04/29/politics/us-investigating-mysterious-directed-energy-attack-white-house/index.html.
13. History Channel, "Ancient Impossible," 2014, https://play.history.com/shows/ancient-impossible/season-1/episode-8.
14. InfraGard NDRC, "Chapter 5," in Powering Through: Building Critical Infrastructure Resilience, Bowker, 2021.
15. D. Dudley, "Iran Dabbles In Crypto For Cross-Border Trade, In Effort To Bypass Sanctions," Forbes, August 10, 2022, https://www.forbes.com/sites/dominicdudley/2022/08/10/iran-dabbles-in-crypto-for-cross-border-trade-in-effort-to-bypass-sanctions/?sh=4d4a50704776.
16. Andrei Kirilenko, "The Flash Crash: The Impact of High Frequency Trading on an Electronic Market," CFTC, 2010.
17. F-Secure, "Threat Analysis: SWIFT Systems and the SWIFT Customer Security Program," https://www.f-secure.com/content/dam/f-secure/en/business/common/collaterals/f-secure-threat-analysis-swift.pdf.
18. P. Foster, "'Bogus' AP tweet about explosion at the White House wipes billions off US markets," April 23, 2013, https://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html.
19. H. Son, "JP Morgan's top quant warns next crisis to have flash crashes and social unrest not seen in 50 years," CNBC, Sep 4, 2018, https://www.cnbc.com/2018/09/04/jpmorgan-says-next-crisis-will-feature-flash-crashes-and-social-unrest.html.
20. M. Wright, "As Iran turns to Bitcoin and its own cryptocurrency to avoid sanctions, maybe it's time to build another Stuxnet," *The Hill*, August 19, 2018, http://thehill.com/opinion/technology/402477-as-iran-turns-to-bitcoin-and-its-own-cryptocurrency-to-avoid-sanctions.
21. Fox News, "Iran, North Korea and Venezuela turning to cryptocurrency to bypass US sanctions, experts warn," FOX News, September 7, 2018, https://www.foxnews.com/tech/2018/09/07/iran-north-korea-and-venezuela-turning-to-cryptocurrency-to-bypass-us-sanctions-experts-warn.html.
22. *MIT Technology Review*, "Bitcoin Transactions Aren't as Anonymous as Everyone Hoped," August 23, 2017, https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/.
23. A. Cruz, "Blockchain Weaponization, National Security Concerns, and Attacks of the Foreseeable Future," May 18, 2018, https://www.linkedin.com/pulse/blockchain-weaponizion-national-security-concerns-attacks-cruz-1/.

NOTES

24. D. Yadron, "Iranian Hackers Infiltrated New York Dam in 2013," *The Wall Street Journal*, December 20, 2015, https://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559?cb=logged0.9423363890964538.

25. Booz Allen Hamilton, "Industrial Cybersecurity Threat Briefing," June 16, 2016, https://www.slideshare.net/BoozAllen/booz-allen-industrial-cybersecurity-threat-briefing.

26. D. Yadron, 2015.

27. K. Brocklehurst, "U.S. Water Utility Breach and ICS Cyber Security Lessons Learned," February 22, 2017, https://www.belden.com/blog/industrial-security/u-s-water-utility-breach-and-ics-cyber-security-lessons-learned.

28. N. Perlroth, "'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town," February 2021, https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html.

29. J. Heyen, "Honey, I Hacked The SCADA! : Industrial CONTROLLED Systems!" March 19, 2016, https://www.youtube.com/watch?v=QAl2GkhT4Jg.

30. P. Vuppuluri, "Investing In Innovation: The Rise Of The Smart City," December 3, 2020, https://www.forbes.com/sites/forbesfinancecouncil/2020/12/03/investing-in-innovation-the-rise-of-the-smart-city/?sh=47f008395ba6.

31. EY, "Cyber Security: A necessary pillar of Smart Cities," November 18, 2016, https://web.archive.org/web/20180218234603/http://www.ey.com:80/Publication/vwLUAssets/ey-cyber-security-a-necessary-pillar-of-smart-cities/$FILE/ey-cyber-security-a-necessary-pillar-of-smart-cities.pdf.

32. Trend Micro, "Shodan Reveals Exposed Cyber Assets," November 28, 2017, https://www.trendmicro.com/vinfo/sg/security/news/internet-of-things/cities-exposed-in-shodan.

33. ANSI, "Smart and Sustainable Cities," https://webstore.ansi.org/industry/smart-cities.

34. D. Paillet, "Defending Against Cyber Threats to Building Management Systems," January 3, 2019, https://www.se.com/ww/en/download/document/998-2095-12-08-15AR0_EN/.

35. "Aviation ISAC," https://www.a-isac.com/.

36. "AITA," https://www.iata.org/en/about/.

37. M. Garcia, "IATA Warns Of Aviation Security Risks, Calls For Better Collaboration With Governments," February 27, 2019, https://www.forbes.com/sites/marisagarcia/2019/02/27/iata-warns-of-aviation-security-risks-calls-for-better-collaboration-with-governments/?sh=3c9d344e36e2.

38. "ICAO GLOBAL AVIATION SECURITY PLAN (GASeP)," 2017, https://www.icao.int/Security/Pages/Global-Aviation-Security-Plan.aspx.

39. BBC News, "Air Canada app data breach involves passport numbers," August 29, 2018, https://www.bbc.com/news/technology-45349056.

40. B. Sullivan, "How Airlines Are Vulnerable to Cyber Attacks," August 19, 2016, https://cyberscout.com/en/blog/how-airlines-are-vulnerable-to-cyber-attacks.

41. *National Academies Press*, "Assessment of Technologies Deployed to Improve Aviation Security: First Report (1999) - Chapter 4 Baggage Handling," 1999, https://www.nap.edu/read/9726/chapter/6.

42. X-Ray Screener, "X-Ray Limitations," https://www.x-rayscreener.co.uk/?xray=x-ray-limitations, accessed December 3, 2020.

43. S. Almasy, "A judge ruled that a website has to suspend downloads for 3D gun plans. But they're already out there," August 1, 2018, https://www.cnn.com/2018/07/31/us/3d-guns-downloaded-plans-states.

44. F. Donovan, "1.13M Records Exposed by 110 Healthcare Data Breaches in Q1 2018," May 7, 2018, https://healthitsecurity.com/news/1.13m-records-exposed-by-110-healthcare-data-breaches-in-q1-2018.

45. Healthcare IT News, "The biggest healthcare data breaches of 2018 (so far)," October 25, 2018, https://www.healthcareitnews.com/projects/biggest-healthcare-data-breaches-2018-so-far.

46. K. Harris, "Hacking medical devices: Managing and bolstering MedTech cybersecurity defenses," August 19, 2021, https://www.hologram.io/blog/medical-device-hacking.

47. IAmTheCavalry.org, "Medical," November 4, 2020, https://iamthecavalry.org/issues/medical/.

48. P. Martyn, "The Lack of Medical Device Security -- Accidents Waiting To Happen," July 11, 2018, https://www.forbes.com/sites/paulmartyn/2018/07/11/the-lack-of-medical-device-security-accidents-waiting-to-happen.

NOTES

49. J. Davis, "AHA, other groups call for medical device security guidance, financial support," July 5, 2018, https://www.healthcareitnews.com/news/aha-other-groups-call-medical-device-security-guidance-financial-support.y 5.
50. S. Khandelwal, "Real-World SS7 Attack: Hackers Are Stealing Money From Bank Accounts," May 4, 2017, https://thehackernews.com/2017/05/ss7-vulnerability-bank-hacking.html.
51. R. Koch, "Criminal Activity Through VoIP: Addressing the Misuse of your Network," December 2005, http://www.tmcnet.com/voip/1205/special-focus-criminal-activity-through-voip.htm.
52. Noction, "BGP Hijacking overview. Routing incidents prevention and defense mechanisms," April 14, 2018, https://www.noction.com/blog/bgp-hijacking.
53. N. Anderson, "How China swallowed 15% of 'Net traffic for 18 minutes," November 17, 2010, https://arstechnica.com/information-technology/2010/11/how-china-swallowed-15-of-net-traffic-for-18-minutes/.
54. A. Siddiqui, "Did Ukraine suffer a BGP hijack and how can networks protect themselves?" MANRS, March 4, 2022, https://www.manrs.org/2022/03/did-ukraine-suffer-a-bgp-hijack-and-how-can-networks-protect-themselves/.
55. D. Goodin, "BGP event sends European mobile traffic through China Telecom for 2 hours," ARS Technica, June 8, 2019, https://arstechnica.com/information-technology/2019/06/bgp-mishap-sends-european-mobile-traffic-through-china-telecom-for-2-hours/.
56. Reuters, "Nigerian Firm Takes Blame For Routing Google Traffic Through China," Slashdot, November 13, 2018, https://tech.slashdot.org/story/18/11/13/2142249/nigerian-firm-takes-blame-for-routing-google-traffic-through-china.
57. C. Morales, "BGP hijackers: 'This traffic is going to Russia!'," December 14, 2017, https://blog.vectra.ai/blog/bgp-hijackers-this-traffic-is-going-to-russia.
58. A. Toonk, "Massive route leak causes internet slowdown," Cisco, June 12, 2015, https://bgpmon.net/massive-route-leak-cause-internet-slowdown/.
59. D. Madory, "Chinese Routing Errors Redirect Russian Traffic," November 6, 2014, https://blogs.oracle.com/internetintelligence/chinese-routing-errors-redirect-russian-traffic-v3.
60. K. Zetter, "Someone's Been Siphoning Data Through a Huge Security Hole in the Internet," December 5, 2013, https://www.wired.com/2013/12/bgp-hijacking-belarus-iceland/.
61. N. Anderson, 2010.
62. FCC, "Caller ID Spoofing," September 23, 2020, https://www.fcc.gov/consumers/guides/spoofing-and-caller-id.
63. Verizon Wireless, "What can be done - my number is being used in a caller ID spoofing scam," December 18, 2017, https://community.verizonwireless.com/thread/941600.
64. ICANN, "DNSSEC – What Is It and Why Is It Important?" March 5, 2019, https://www.icann.org/resources/pages/dnssec-qaa-2014-01-29-en.
65. Noction, "BGP security: the BGPsec protocol," April 30, 2015, https://www.noction.com/blog/bgpsec_protocol.
66. "TLS1.3," October 7, 2018, https://wiki.openssl.org/index.php/TLS1.3.
67. T. Chung, "Why DNSSEC deployment remains so low," December 6, 2017, https://blog.apnic.net/2017/12/06/dnssec-deployment-remains-low/.
68. "Information Sharing and Analysis Organization Standards Organization (ISAO SO)," UTSA Center for Infrastructure Assurance and Security, https://www.isao.org/information-sharing-groups/.
69. "Energy ISAC (Information Sharing & Analysis Center)," https://www.eisac.com/.
70. "Oil & Natural Gas ISAC (Information Sharing & Analysis Center)," https://ongisac.org/.
71. Ibid.
72. "Nuclear Energy Institute," https://www.nei.org.
73. "Energy Analytic Security Exchange (EASE)," Global Resilience Federation, https://grf.org/ease.
74. "Multi-State ISAC (Information sharing & Analysis Center)," https://www.cisecurity.org/ms-isac/.
75. "Aviation ISAC (Information Sharing & Analysis Center)," https://www.a-isac.com/.
76. "Financial Services ISAC (Information Sharing & Analysis Center)," https://www.fsisac.com/.
77. Business Wire, October 30, 2020, https://www.businesswire.com/news/home/20201030005462/en/Announcing-the-Formation-of-the-Analysis-Resilience-Center-ARC-for-Systemic-Risk.

NOTES

78. "Federally-Defined Critical Infrastructure Sectors," US DHS CISA, https://www.cisa.gov/critical-infrastructure-sectors.
79. ASIS International, "ASIS International Strategic Plan 2016-2021," January 23, 2017, https://www.asisonline.org/globalassets/about-asis/strategic-plan/asis-strat-plan-final-april-2017.pdf.
80. DHS/CISA, "NIPP Supplemental Tool: Connecting to the National Infrastructure Coordinating Center (NICC) and National Cybersecurity and Communications Integration Center (NCCIC)," 2018, https://www.cisa.gov/publication/connecting-nicc-and-nccic.
81. D. Rubin, "Crew Resource Management," *Firehouse Magazine,* 2006.
82. FAA, "CRM Error Management," https://www.hf.faa.gov/webtraining/TeamPerform/TeamCRM013.htm.
83. Sounil Yu, "Cyber Defense Matrix," https://cyberdefensematrix.com/.
84. "FIDO Alliance," https://fidoalliance.org/fido2/.
85. Lt. Col. (Ret) Robert J. Darling, "Turning Point Crisis Management," https://tpcm-usa.com.
86. D. Keltner, "We Are All Bystanders," *Greater Good Magazine,* September 2006, https://greatergood.berkeley.edu/article/item/we_are_all_bystanders.
87. *Business Wire,* October 30, 2020.
88. M. Garcia, "IATA Warns Of Aviation Security Risks, Calls For Better Collaboration With Governments," 2019.