Cyber-Physical Coordinated Attacks:

The Emerging Complexity of Crisis Management

John C. Checco
C|CISO, SDRM, CISSP, CSSLP, CCSK, MBA
President Emeritus, New York Metro InfraGard

(Edited by Anthony Cruz)

SEPTEMBER 2018 / Turning Point Crisis Management USA

Contents

Introduction

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 one 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.

I have been blessed in my career to have worked in a broad spectrum of industries, from pure technology research to telecommunications to health imaging to financial services to government. I have also had the good fortune to be involved in many community organizations that are focused on protecting our critical infrastructures at the local and national levels, encompassing both cyber threats as well as emergency services first responder operations. Being active across both industries and security domains has exposed unique insights into the necessity for due diligence against new paradigms of attack.

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.

Threat Vectors

There are many scenarios in which cyber events predicate one or more of the following objectives: (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 nation or global scale regardless of any financial gain.

Financial Windfalls from Manipulating Market-Moving Data

By way of historical reference, market moving data has been used in a variety of methods.

SWIFT Protocol Abuse

- **Threat Analysis: SWIFT Systems and the SWIFT Customer Security Program** (https://www.mwrinfosecurity.com/assets/swift-whitepaper/mwr-swift-payment-systems-v2.pdf)

Cryptocurrency Thefts

- **$9 Million a Day Is Lost in Cryptocurrency Scams** (https://news.bitcoin.com/9-million-day-lost-cryptocurrency-scams/)
- **Cryptocurrency Theft from 2011 to 2017** (https://bitcoinexchangeguide.com/top-cryptocurrency-theft-hacks/).

Fake News/Alerts

Particularly susceptible through social media, fake news plays directly to the motive of capitalizing on market response:

- **Fake Associated Press (AP) tweet sends stocks briefly plunging** (https://www.cbsnews.com/news/fake-ap-tweet-sends-stocks-briefly-plunging/)
- **'Bogus' AP tweet about explosion at the White House wipes billions off US markets** (https://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html)

Technology Misuse Potentially Triggers a Financial Crisis

Criminal application of technology itself can lead to more systemic material events, whether it be intentional misuse (i.e. cryptocurrency to bypass regulations or bypass taxation authorities) or lack of guardrails on runaway technology (automated high frequency micro-trading).

Automated (unsupervised) High Frequency Micro-Trading

- **JP Morgan's top quant warns next crisis to have flash crashes and social unrest not seen in 50 years** (https://www.cnbc.com/2018/09/04/jpmorgan-says-next-crisis-will-feature-flash-crashes-and-social-unrest.html):

> *"… 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."*

Cryptocurrency as a [Financial] Weapon

- **Iran, North Korea and Venezuela turning to cryptocurrency to bypass US sanctions, experts warn** (http://www.foxnews.com/tech/2018/09/07/iran-north-korea-and-venezuela-turning-to-cryptocurrency-to-bypass-us-sanctions-experts-warn.html):

> *… a senior science and technology official of Iran's Presidential Office said: "… [Crypto]currency would facilitate the transfer of money (to and from) anywhere in the world … It can help us at the time of sanctions."*

- **Blockchain Weaponization, National Security Concerns, and Attacks of the Foreseeable Future** (https://www.linkedin.com/pulse/blockchain-weaponizion-national-security-concerns-attacks-cruz-1/):

> *"A U.S. military officer recently noted that Chinese researchers published an article in National Defense Science and Technology in 2016 highlighting some of the value of the technology as well as some of its security ramifications, especially in the realm of defensive and offensive cyber operations. Additionally, 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. Partly due to these concerns, the U.S. Congress is asking for a Department of Defense study into nefarious use of the blockchain and its implications on national security. Global law enforcement bodies such as Interpol are emphasizing the potential of nefarious actors to deploy, as well as command and control, malware or conduct activities such as the distribution of child pornography. While intelligence services are*

looking at potential use cases, some of the techniques state actors can use in offensive operations are already known and possibly being employed by criminal actors."

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 (https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/); but really having no other actionable remediation.

State of the Sector

In 2016 a collaborative organization known as the Financial Systemic Analysis & Resiliency Center (FSARC) was formed as a subsidiary of the FS-ISAC specifically to focus towards a more global emphasis of attacks on the financial ecosystem. FSARC has been well supported by both the private firms and the public sector agencies.

Public Utilities / Infrastructure

The utility sectors are similar to banking and finance since they serve the public at large, and not many citizens are exempt to the effects of downed utilities. We've 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.

To exemplify the difference between ICS and SCADA systems: a house alarm, central air conditioning control panel, home heating thermostats, television and light switches are considered ICS whereby a home automation system is considered a type of SCADA. Most individual devices (i.e. alarm systems) are accessible from inside the premises. However, in the age of technology, home automation systems offer remote consoles on many high-end automobiles as well as smartphone apps. Consequently, the weakest point of entry is no longer at the physical location (the house), but at the remote interface (smartphone).

In assessing the risks within ICS/SCADA systems, two characteristics need to be considered:

- Threat Types
  - **Operational** Threats have an immediate impact on the business – i.e. there is little to no warning -- and should be considered 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 operation outages without affecting the critical areas of the business.
- **Tier 3** facilities do not affect short-term operations, but may have longer-term impacts.

Threat Vectors

Historically, different operational groups are responsible for different systems; there are inconsistent levels of protection procedures across the various ICS/SCADA systems. The current propensity to place new devices' managed ports (ICS) on the corporate network – due to the history behind this process – increases an organization's risk exponentially.

Many of the systems/subnets are not explicitly prohibited access to the internet. The most likely exploitation/attack vector will be from a failure of corporate security protocols i.e. inadvertent disclosure of sensitive information, rogue insider, or threat actor remote access through a managed/third-party service provider (https://dragos.com/adversaries.html).

Finally, many organizations exhibit multiple gaps in protection from read-only access to full control of HVAC, PDUs and communications.

Equipment Destruction from Manipulating SCADA/ICS

Scenarios with SCADA/ICS range from control over Dams, Liquified Natural Gas pipeline shutdowns, target blackouts using the Electric Grid, as well as more nefarious motivations to compromise Nuclear facilities.

- **Booz Allen Industrial Cybersecurity Threat Briefing** (https://www.slideshare.net/BoozAllen/booz-allen-industrial-cybersecurity-threat-briefing)
- **Honey, I Hacked The SCADA! - Industrial CONTROLLED Systems!** (https://www.youtube.com/watch?v=QAI2GkhT4Jg)
- **U.S. Water Utility Breach and ICS Cyber Security Lessons Learned** (https://www.belden.com/blog/industrial-security/u-s-water-utility-breach-and-ics-cyber-security-lessons-learned)
- **Electric Grid inter-dependency issues** (https://en.wikipedia.org/wiki/List_of_major_power_outages)
- **Cities Exposed in Shodan** (https://www.trendmicro.com/vinfo/sg/security/news/internet-of-things/cities-exposed-in-shodan)

Smart Cities: The next cyber playground

Even as our traditional city infrastructures are under attack, **Smart Cities** are gaining national momentum (https://www.forbes.com/sites/civicnation/2018/09/04/these-midshipmen-are-catalyzing-a-culture-change-on-college-campuses). 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.

- **Securing Smart Cities** (https://securingsmartcities.org/)
- **Cyber Security: A necessary pillar of Smart Cities** (http://www.ey.com/Publication/vwLUAssets/ey-cyber-security-a-necessary-pillar-of-smart-cities/$FILE/ey-cyber-security-a-necessary-pillar-of-smart-cities.pdf)

- **How Can We Make Smart Cities Even Smarter? Start with Security Intelligence** (https://securityintelligence.com/how-can-we-make-smart-cities-even-smarter-start-with-security-intelligence/)
- **Future challenges for smart cities: Cyber-security and digital forensics** (https://www.sciencedirect.com/science/article/pii/S1742287617300579)
- **ANSI Network on Smart and Sustainable Cities** - *Inactive* (https://www.ansi.org/standards_activities/standards_boards_panels/anssc/overview)

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.

State of the Sector

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

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.

Threat Vectors

Threats to commercial facilities fall into two major areas: direct breaches of systems, and exploitation of organization procedure weaknesses.

Brute Force Cyberattack

Brute force cyberattacks on local Building Management Systems (BMS/SCADA) can be used for creating many types of operational disruptions. Two simplistic scenarios where this can endanger life are:

Remotely Disabling Alarm Systems

This simple tactic can cause a significant delayed reaction to a building event, such as a fire or release of toxic chemicals into the building's air recirculation systems. This delayed reaction is twofold; (a) evacuation of occupants, and (b) response by emergency personnel, law enforcement and/or other first responders.

Remotely Activating Alarm Systems

Slightly more complex, this approach can be used for three types of motivations: (a) uncontrolled/unfettered access to the building and its contents, (b) attacks on vulnerable employees corralled at muster point, or (c) attacks on emergency personnel, law enforcement and/or other first responders.

Endangerment by Gaps in Emergency Response Processes

The most common issue I have seen with most organizations I have worked with over the past 20 years is a **gap in proper delineation of responsibilities**.

Recall the incident back in 2017 where a car crashed into a crowd at Times Square, NYC (https://www.cnn.com/2017/05/18/us/new-york-times-square-car-pedestrians/). At that moment, I was working in the DC area, and was alerted to the incident by a peer who saw it on the news. Having my main office in NYC just one block away from the incident, I was curious why my organization's Employee Emergency Notification System had not contacted me. So, I made a few calls to confirm/deny the following:

- ✓ How were my peers in the NYC office notified? Short answer: they weren't.
- ✓ Were the office security personnel notified? They were not aware of any incident; but directed the inquiry to the facility management firm.
- ✓ Had the building's facility management firm been aware of the event? They did confirm the incident reported directly to them by NYPD; but stated they were not responsible for notifying the tenants, as that was the responsibility of the tenants' own corporate communications.
- ✓ Were corporate communications (based outside of NY state) aware (through monitoring news feeds)? Yes, but stated it was the regional office's responsibility.
- ✓ Was the NY regional office head – a front-line business unit, not an emergency or communications support group – apprised of the situation? They were not aware except for what they saw on the news, but stated it was not a terrorist event (as *it was now 2 hours after the incident*).
- ✓ Could the organization approximate how many local employees from our three offices within that area could have been outside the building at lunch during the time of the incident? The estimation was an astounding 7500 potential employees!
- ✓ Then came the obvious question: "**Since at the time of the incident we did not know if this was a terrorist event, shouldn't we be notifying our local employees that may be in harm's way?**"

Update: The regional office head did send out an email notification 4 hours after the incident, and the regional playbooks were updated to (1) be in the direct line of notification by both the building landlord and the facility management firm, and (2) activate the Employee Emergency Notification System in the event of a similar incident.

State of the Sector

Robust guidelines exist for creating isolated network systems (http://www2.schneider-electric.com/documents/support/cybersecurity/WP-BESTPRAC-securing-intelligent-building-management-system.pdf) separating BMS/SCADA from internet-facing corporate networks.

My experience has shown that most existing data centers and facilities cannot adopt such guidelines 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 sector has a myriad of attack surfaces, but in the same vein, aviation protection and security has the most mature attention by agencies as well as topics of research (https://www.nap.edu/search/?topic=284&rpp=20&ft=1&term=aviation+security).

One of the main issues in the aviation sector is that 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 Aviation ISAC (A-ISAC) encompasses six different aspects of the industry: airlines, airports, platforms, satellites, engines, and equipment manufacturers. But each operates in its own "swim lane" with regard to table top exercises and cross-silo potential events.

Threat Vectors

Preemptive Access Bypassing Security Checkpoint Systems

Air transportation has been used by terrorists as both a conduit (hijackings as far back as 1931) and as a weapon for carrying out nefarious, highly visible, and psychologically damaging activities (the coordinated 9/11 attacks). Many of these attacks are preceded by the ability to bypass existing security checkpoint systems. With the growing trend of cyber-attacks, bypassing security checkpoints can open 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. Traditionally, this was a single outsourced monopoly (SABRE) run on a legacy mainframe platform. Being able to manipulate flight reservations and passenger identities at this level can go unnoticed (and may only be discovered AFTER an incident has occurred and its origins investigated).

- **Air Canada app data breach involves passport numbers** (https://www.bbc.com/news/technology-45349056)

Airplane Scheduling Systems

For the seasoned traveler, it is well known that airlines use the concept of "day-bedding" for ensuring the maximum number of flights in/out of multiple airports. The concept of day-bedding is the ability to use the same resource for multiple uses – originated with the use of the same bed for alternating night workers and day laborers. 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" thus reducing costs. However, when it fails, the cascading affects can be global.

- **How Airlines Are Susceptible to Cyber Attacks** (https://cyberscout.com/education/blog/how-airlines-are-vulnerable-to-cyber-attacks)

Now that 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.

To date, most of these groundings have been attributed to weather and technical "glitches"; but it is fathomable (and even suggested) that a cyber-attack can do even more damage to the air transportation system.

Baggage Handling Systems

It is surprising to know that not all bags on commercial airlines are scanned; although I suspect most of us accept that not all packages are scanned on cargo planes. Even assuming that at some point we can gain the expediency to automatically scan all baggage, there exists the possibility that (either programmatically or via a hack) the baggage handling systems can be altered to bypass scanning based on certain tag number formats or baggage attributes. Such modification could allow explosives or nerve agents to be placed on board. A good synopsis of existing baggage handling security issues can be found here:

- **Assessment of Technologies Deployed to Improve Aviation Security: Baggage Handling** (https://www.nap.edu/read/9726/chapter/6)

X-Ray / Passenger Inspection Systems

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

- Missed identifications are common place due to opaqueness, clutter and similarity of consumer electronics to detonation devices.
    - **X-Ray Limitations** (https://www.x-rayscreener.co.uk/?xray=x-ray-limitations)
    - MSA Security (which offers X-Ray screener training) publishes a monthly newsletter containing an X-Ray puzzle, "Can you Identify This?"
- Screening Avoidance such as the recent trend surrounding weapons made of non-detectable materials.
    - **A judge ruled that a website has to suspend downloads for 3D gun plans. But they're already out there** (https://www.cnn.com/2018/07/31/us/3d-guns-downloaded-plans-states)

In-Flight Navigation Systems

Security researcher Chris Roberts claimed to have accessed a plane's navigation system through a USB port connected to its infotainment system (https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane). Whether true or not, similar access breaches have been reported in the automotive industry; and it is conceivable that Roberts' claims are all too accurate.

- **More on Chris Roberts and Avionics Security** (https://www.schneier.com/blog/archives/2015/05/more_on_chris_r.html)

State of the Sector

My research in the past year has not seen any major updates in aviation security other than constantly changing TSA screening rules (https://www.dallasnews.com/business/airlines/2017/10/25/new-airline-security-measures-starting-thursday-may-include-interviews-us-bound-passengers).

This lack of progress in itself should be setting off alarms, although an explicit need to collectively address aviation security exists:

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

  > *The GASeP addresses the needs of States and industry in guiding all aviation security enhancement efforts through a set of internationally agreed priority actions, tasks and targets.*
  >
  > *The 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.*

- **Aviation Security; More Collaboration is the Only Way!** (https://www.iata.org/about/worldwide/ame/industry-gazette-summer-2017/Pages/Aviation-Security.aspx

Healthcare / Medical

The healthcare sector has aimed for security reform with the advent of HIPAA (Health Insurance Portability and Accountability Act) in 1996 and HITECH (Health Information Technology for Economic and Clinical Health Act) in 2009.

Threat Vectors

Of particular interest was the requirement of HIPAA for better protected handling of patient information, followed by the HITECH Act requirement that all medical records be in electronic form.

But there are no standard requirements for the electronic format of medical records (although the DICOM SR format is adopted by many medical imaging companies). Three new industries arose from these acts:

- Companies that **convert paper records** to some type of electronic format (mostly PDF);
- Companies that **create electronic systems** for entering new patient/medical data (customized and proprietary data stores);
- Companies that are hired to **convert formats** from one system to another (usually a third XML/JSON format that can be exported or ingested by other proprietary systems);

This lack of standardization – and at least three (3) potential levels of outsourcing – actually leads to more cases of medical identity fraud and misdiagnoses because the electronic data is not *normalized* – 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.

- **1.13M Records Exposed by 110 Healthcare Data Breaches in Q1 2018** (https://healthitsecurity.com/news/1.13m-records-exposed-by-110-healthcare-data-breaches-in-q1-2018)

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 those members with health insurance – wittingly or unwittingly – to piggyback on their insurance plans. This is unhealthy to both all patients using this one identity, as the medical history is not accurately reflecting any single patient; and a rogue patient may be subject to undue medications and treatments.

- **Misdiagnosis/Mistreatment Against a Target**: This more nefarious scenario plays to the fact that a cyber-attacker could alter the medical history of a target to create a situation where an improper medication/treatment is given to the target, resulting in death. Although this sounds like science fiction, but the number of breaches with healthcare data has been growing exponentially every year (https://www.healthcareitnews.com/projects/biggest-healthcare-data-breaches-2018-so-far).

Death from Manipulating Devices

Similar to the "Misdiagnosis/Mistreatment Against a Target" scenario above, medical devices can be directly hacked to achieve a similar outcome. This has been written about ad-nauseum, but is best succinctly addressed and demonstrated by a group called "I Am the Cavalry" (https://www.iamthecavalry.org/domains/medical/).

- The Lack of Medical Device Security -- Accidents Waiting To Happen (https://www.forbes.com/sites/paulmartyn/2018/07/11/the-lack-of-medical-device-security-accidents-waiting-to-happen)
- **The changing face of medical-device design** (https://www.mckinsey.com/industries/pharmaceuticals-and-medical-products/our-insights/the-changing-face-of-medical-device-design)
- **AHA, other groups call for medical device security guidance, financial support** (https://www.healthcareitnews.com/news/aha-other-groups-call-medical-device-security-guidance-financial-support)

State of the Sector

And yet, similar to our discussion above about progress in the area of aviation security; **we should be setting off mayday alarms** with the increasing request for medical device security stymied by the lack of response by medical device manufacturers.

Telecommunications / Internet

Society's reliance on technology, especially analog and digital communications, was inspired by visionaries in the world science fiction.

- 1976: Popular science-fiction writer Arthur C. Clarke spoke at MIT about the future capability for interconnected devices, including satellite communications. (https://www.cnet.com/news/arthur-c-clarke-describes-the-21st-century-in-detail-in-1976/)
- Late 1960s: Television shows such as Star Trek and Twilight Zone envisioned many of the devices we use today. An engineer at Motorola even credits "Star Trek" for inspiring the mobile phone. (http://www.destination-innovation.com/how-startrek-inspired-an-innovation-your-cell-phone/)
- 1964: Renowned science-fiction author Isaac Asimov predicted many everyday advancements such as satellite communications, alternative energy production, smart appliances, video calls, autonomous vehicles, and even mundane items such as frozen food and hue lighting. (https://www.digitaltrends.com/cool-tech/10-predictions-isaac-asimov-got-right-50-years-ago-5-botched/)
- 1946, the comic strip Dick Tracy showed law enforcement using smart watches. (https://www.smithsonianmag.com/smart-news/how-dick-tracy-invented-smartwatch-180954506/)
- 1914: H.G. Wells explored ideas surrounding atomic/nuclear power in the novel "*The World Set Free.*" (https://www.smithsonianmag.com/science-nature/ten-inventions-inspired-by-science-fiction-128080674/)

However, in the frenzy that pushed companies to create the technology and communications advancements from the science fiction world, they did not foresee the possibly for misuse of these technologies, nor the ramifications of such abuse. The exception to this being Isaac Asimov's "Three Laws of Robotics" (http://www.cs.bham.ac.uk/research/projects/cogaff/misc/asimov-three-laws.html) – actually there is a fourth law known as "Zeroth Law of Robotics."

Threat Vectors

Espionage from Manipulating Legacy Communication Protocols

Cyberattacks on most communications systems are positioned for espionage – i.e. 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). There have been previous versions of signaling systems, most of which relied on analog tones for communication, but SS7 brought the first major updates to allow flexible layers to support modular digital signaling. This allows SS7 to operate uniformly over a variety of transport mechanisms (ATM, MPLS, Frame Relay, SONET, PBX).

However, the notion of secured communications was not a concern in the 1970s; and as SS7 proliferated over more varieties of newer technologies (ISDN, xDSL, Ethernet), any thoughts on securing the

communication plane is inconceivable due to the sprawl and impact area for changing (breaking) the protocol.

What we are left with today is a legacy protocol not meant to arbitrary inline inspection, yet running over transports that are designed to allow unrestricted and anonymous tapping of information flow almost anywhere in the communication flow.

- 2014: **Hackers Can Read Your Private SMS and Listen to Phone Calls** (https://thehackernews.com/2014/12/hackers-can-read-your-private-sms-and.html)
- 2017: **Real-World SS7 Attack — Hackers Are Stealing Money from Bank Accounts** (https://thehackernews.com/2017/05/ss7-vulnerability-bank-hacking.html)

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 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; still without any endpoint authentication or verification.

- **Criminal Activity Through VoIP: Addressing the Misuse of your Network** (http://www.tmcnet.com/voip/1205/special-focus-criminal-activity-through-voip.htm)
- 2010, **SIP Abuse – Amazon EC2** (https://aws.amazon.com/security/security-bulletins/sip-abuse/)
- 2011, **3 Simple Reasons VoIP Abuse Will Grow** (https://www.csoonline.com/article/2127420/malware-cybercrime/3-simple-reasons-voip-abuse-will-grow.html)
- 2014, **Analysis of SIP-Based Threats Using a VoIP Honeynet System** (https://ieeexplore.ieee.org/document/6857088/)

BGP Hijacking

Whereas Domain Name Services (DNS) is akin to a phonebook for internet URLs, Border Gateway Protocol (BGP) is the navigation system. BGP routers are the road signs that allow internet traffic to find the shortest open path to its destination.

Most hacking uses a man-in-the-middle (MitM) attack to hijack a targeted internet session, and much of the internet traffic is still open. Secure protocols such as SSL/TLS make reading internet traffic infeasible to do in real-time as the entire communication session is encrypted using a mutually defined shared key.

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. (https://www.noction.com/blog/bgp-hijacking)

Such is the case in a BGP attack, and it is not as uncommon as it first may seem (https://en.wikipedia.org/wiki/BGP_hijacking).

- 2010: **How China swallowed 15% of 'Net traffic for 18 minutes** (https://arstechnica.com/information-technology/2010/11/how-china-swallowed-15-of-net-traffic-for-18-minutes/)
- 2013: **Someone's Been Siphoning Data Through a Huge Security Hole in the Internet** (https://www.wired.com/2013/12/bgp-hijacking-belarus-iceland/)
- 2014: **Chinese Routing Errors Redirect Russian Traffic** (https://dyn.com/blog/chinese-routing-errors-redirect-russian-traffic/)
- 2017: **BGP hijackers: 'This traffic is going to Russia!'** (https://blog.vectra.ai/blog/bgp-hijackers-this-traffic-is-going-to-russia)

State of the Sector

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 (https://www.fcc.gov/consumers/guides/spoofing-and-caller-id). 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* (https://community.verizonwireless.com/thread/941600).

Internet Communication Security

There have been many efforts to secure internet communications:

- **TLSv1.3** protecting end-user communications at a granular level (https://wiki.openssl.org/index.php/TLS1.3);
- **DNSSEC** protecting the internet phonebook (https://www.icann.org/resources/pages/dnssec-qaa-2014-01-29-en);
- **BGPSEC** protecting internet traffic navigation (https://www.noction.com/blog/bgpsec_protocol);

DNSSEC has been around since 1997, BGPSEC was introduced in 2000; yet neither has a significant adoption rate (https://blog.apnic.net/2017/12/06/dnssec-deployment-remains-low/ and https://queue.acm.org/detail.cfm?id=2668966).

Cross-Sector Collateral Damage

Any one of these scenarios would leave the targeted region extremely vulnerable to physical attacks. In many cases a primary cyber-attack is purposeful in simplifying the secondary physical attack methods, as the normal protectors for minimizing physical damage have been significantly diminished.

Adding to the complexity of cyber and physical attack methods, is the issue of **scaffolding** dependencies, where indirect/collateral damage may far outweigh any direct destruction – as direct effects are acute in nature (immediate effects) whilst collateral is more chronic (long-term residual effects).

Scaffolding Vulnerabilities

A documentary about the technologies of the Romans shows they were the most advanced civilization of their time. Several distinct innovations are key to this discussion:

1. The formulation of concrete, specifically **marine concrete** (which cures even under saltwater).
2. The ability to create new and **stable architectures using arches and domes** through the use of custom-formed blocks of concrete. This is the fore-running of modern day truss construction; whereby loads are transferred to the outermost pillars of the structure.
3. Their **complex aqueduct and irrigation systems**. Again, building on the use of concrete arches, the Romans were able to build long aqueducts to supply fresh water to the main metropolitan areas as well as reach remote areas for farmers to sustain the demand for agricultural needs of the population.
4. The **use of water as energy** to power massive grain milling operations.
5. Grain milling operations played a major role in **keeping civilizations and their armed forces well fed**.
6. By maintaining a **healthy population**, civil unrest was minimized.
7. By maintaining a **health army**, they were able to outlast any attack, conquer new lands, control trade routes and expand their empire.

This combination of innovative technologies with astute governing concepts – each one scaffolding from the other – sustained a highly-advanced civilization. If any of these tenets did not exist, or were disrupted, then their society could not survive.

And so it came to be. The Roman Empire eventually fell due to what we call today the “kill chain”.

EMP: Today’s Scaffold

Our collective inter-dependency on the energy sector, in particular, has ramifications more serious than first blush.

There is a lot of activity focused at electromagnetic pulses as a global disruption path (https://www.empcenter.org). There is a definite need to address this, especially the higher probability effect from a localized attack against a single power plant or small population (http://revolutionradio.org/2018/09/02/american-diplomats-in-cuba-were-targeted-with-microwave-weaponry/). The national risk to a major EMP event by a nation-state actor is considered **extremely** high impact but low probability.

The word “**extreme**” is used with a large scale EMP because the calculated effects will be both a long-term lack of power generation as well as lack of capability for power consumption by multiple industries. In short, it is a true cross-sector event.

It has been estimated that a power generation facility having 10% resiliency can still generate about 80% of the power needs it serves. What most of our politicians fail to realize is that during an EMP attack, the consumers of energy are most likely not protected. This begs the question: who will power facilities be delivering energy to? 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 (https://globalresilience.northeastern.edu/2018/03/preparing-for-the-crash-the-threat-of-an-electromagnetic-pulse/).

Preparation is key, because the low probability includes both man-made upper atmospheric nuclear detonation (https://www.bloomberg.com/view/articles/2018-04-25/north-korea-s-secret-weapon-an-electromagnetic-storm) as well as the natural solar flare as such as the Carrington event of 1859 (https://www.sciencealert.com/here-s-what-would-happen-if-solar-storm-wiped-out-technology-geomagnetic-carrington-event-coronal-mass-ejection).

Holistic Risk Awareness (or Lack Thereof): Expertise, Preference or Bias?

We [collectively] 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!

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 tolerance calculations are skewed by two key biases:

- **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;

Structured Sector-Independent Collaboration Needed

One aspect that has yet to be addressed globally is the inter-dependencies of sectors. Each sector has its own Information Sharing & Analysis Center (ISAC), but they are not perfect in sharing IOCs (indicators of compromise).

- The energy sector is divided into several ISACs: E-ISAC (Electricity), ONG-ISAC (Oil & Natural Gas), DNG-ISAC (Downstream Natural Gas), NEI (Nuclear energy Institute), and GRF/EASE (Energy Analytic Security Exchange).

- The aviation sector ISAC (A-ISAC) combines six disparate industries under the same umbrella: airlines, airports, platforms, satellites, engines, and equipment manufacturers.

The FSARC has been one successful model for a targeted mission. Can and should it be replicated for other sectors? Both the Energy and Aviation ISACs are looking to build out their own versions of the xSARC, albeit for entirely different purposes – whereas the Energy sector needs to align multiple ISACs into a uniform mission, the Aviation ISAC needs better focus than its current six-dimensional objectives.

Still missing is an overall goal of cross-sector collaboration. Should there be a National Council of xSARCs much like there is a National ISAC Council? Unfortunately, there is no simple answer to this.

State of the Union

This style of cyber-physical attack will be the **point of inflection for all future attacks**; 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.

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 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.

- **As Iran turns to Bitcoin and its own cryptocurrency to avoid sanctions, maybe it's time to build another Stuxnet** (http://thehill.com/opinion/technology/402477-as-iran-turns-to-bitcoin-and-its-own-cryptocurrency-to-avoid-sanctions)

Thankfully, there are more rational efforts in the public and private sectors – albeit in various stages of maturity:

- InfraGard, the FBI outreach program originating from their cyber security division back in 1996, revamped its mission after the 9/11/2001 attacks to focus on both physical and cyber; and was eventually reorganized in 2016 under the general directorate focusing on both cyber and physical threats across 16 national critical infrastructures.

- Physical security organization ASIS International included a focus on cyber in 2016 (https://www.asisonline.org/globalassets/about-asis/strategic-plan/asis-strat-plan-final-april-2017.pdf).

- Earlier this year (2018), DHS created shared collaboration space for their NCC physical security watchdogs to work alongside the NCCIC cyber security watchdogs (https://www.us-cert.gov/nccic/realignment-announcement).

- Other grassroots efforts exist amongst private sector entities, such as the IFSEC Global 2018 conference (https://www.ifsecglobal.com/converged-security-centre-at-ifsec-2018/)

Conclusion

The orchestration of cyber and physical tactics for a single terrorist objective is happening today. It is the precursor to more advanced and complex threats; some scenarios even seemingly unfathomable.

From a threat perspective, we need to treat our adversaries as still in their “tweens” … They are more mature than just using script kiddies, but not yet able to fully harness emerging technologies –

Artificial/Augmented Intelligence, HPC/Parallel computing, Quantum Computing, Containerization or Network Function Virtualization.

Make no mistake. Those days are certainly in our future. The end goal here is to gain situational awareness and prepare for those multi-faceted threats that are certainly coming in our future.

Turning Point Crisis Management provides advisory services for smaller organizations to support the collaboration between similar organizations, promote participation in the grassroots and various outreach groups, and assists in building a roadmap for becoming resilient against both physical and cyber threats.

Be aware. Be safe.

Start, **D**oing, **M**ore, **T**o, **L**ive! ™