Resilient Communications Availability

Inverting the Confidentiality, Integrity, and Availability Paradigm

Steve Chan
Decision Engineering Analysis Laboratory, VT
San Diego, USA
e-mail: schan@dengineering.org

Abstract—**Communications networks are subject to degradation due to a variety of factors from the cyber electromagnetic spectrum. Interference may be unintentional and/or intentional, but the consequences are comparable; communications availability may be affected. Although cellular carriers must abide by the Federal Communications Commission's Enhanced 911 (E911) rules, poor radio frequency cellular coverage and intermittent connections remain problematic. As numerous communications networks transition to Internet Protocol-based operations, new service reliability vulnerabilities have emerged for, by way of example, 911 location services, and poor wireless internet network (a.k.a. wi-fi) coverage may cause availability issues for 311 (e.g., reportage of road damage), and 211 (e.g., facilitation for essential community services), among others. As society becomes more dependent upon wireless communications networks, it is vital to maintain acceptable service availability levels under prototypical circumstances as well as amidst incidents, including disruptions emanating from within the cyber electromagnetic spectrum ecosystem. In several cases, public safety systems, which have gone through full acceptance testing, have been adversely affected due to interference stemming from known systems (e.g., as they expand) as well as unknown systems (e.g., unregistered). Dropped calls, garbled messages, and blocked messages have been among the reported effects. Given these known phenomena, it is possible to interfere with both cellular and Voice over Internet Protocol (VoIP) 911 and first responder-related calls by the strategic placement of interfering nodes in the form of misused cellular boosters and/or strategically positioned femtocells, deliberate Bluetooth congestion so as to limit the number of frequency channels available and interfere with wi-fi and cellular network technologies (including spread spectrum), thereby affecting the involved communications paradigm. This string of effects has segued into a potential cyber kill chain (which comprise the phases of a cyberattack from reconnaissance to exploitation) paradigm, which is examined in this paper. Among other items presented, an alarming spike in the prevalence of non-compliant boosters is noted. In addition, the increasing number of incidents as pertains to "incidental radiators" and "unintentional emitters" of Radio Frequency Interference (RFI) is also noted. Overall, as the potential for RFI has increased, the potency of the described cyber kill chain also increases. An outcome of the paper is the recognition of this potential blindspot within current communications architectural paradigms.**

Keywords-Communications networks; Cyber electromagnetic spectrum; Radio frequency cellular coverage; Internet Protocol-based coverage; Signal boosters; Oscillation detection; Oscillation prevention; Spectrum analyzer; Smart auto switching; Non-bonded single channel; Bonded multi-channel; Cyber kill chain.

I. INTRODUCTION

Various government organizations, such as the U.S. Cybersecurity and Infrastructure Security Agency (CISA) Emergency Communications Division (ECD), have provided guidance (e.g., route diversity) for communications resiliency. In essence, it is vital to maximize both the reliability and resiliency of the involved communications network. While reliability represents the ability to continue operating at acceptable service availability levels, resiliency deals with the ability to recover from adversity. This paper will examine the notions of reliability and resiliency for communications networks amidst some known cyber electromagnetic spectrum phenomena, which can readily segue to a cyber kill chain. Indeed, the cyber kill chain described in the abstract has become even more potent amidst COVID-19 times. Misconfigured and/or poorly manufactured boosters can cause extensive interference, and the number of non-compliant boosters has increased dramatically. The Federal Communications Commission (FCC) notes that, "Although signal boosters can improve cell phone coverage, malfunctioning, poorly designed, or improperly installed signal boosters can interfere with wireless networks and cause interference to a range of calls, including emergency and 911 calls." With the increase in mobile phone usage during COVID-19 times, it should be of no surprise that the market demand for boosters has increased dramatically. Along with the COVID-related increase in online purchases, e-commerce sites have been selling a high volume of signal boosters; however, not all of these signal boosters comply with FCC standards. Alarmingly, these non-FCC-compliant boosters have been noted as being top sellers in the signal booster category. To even further fuel this trend, there is an e-commerce tactic utilized, wherein sellers use reviews from other low-cost products to make the boosters appear more popular than they are, thereby inducing even more sales. As a further accelerant, on a related front of goods sold, some of the keiretsu-like structured manufacturers also sell equipment into the electrical grid sector. While the

 ISBN: 978-1-61208-818-1

substantive portion of the Radio Frequency Interference (RFI) noise emanating from the electric utility equipment are construed as emanating from "incidental emitters," it should be noted that there are no specific limits on the conducted or radiated emissions [1]; this represents a potential blindspot.

This section introduced the subject matter. The remainder of this paper is organized as follows. Section II describes cellular and non-cellular communications coverage. Section III presents regulatory compliance and adherence considerations. Section IV discusses communications architectures that endeavor to mitigate against the interference issue and maintain acceptable service availability. Section V features the trend of ongoing societal predilection towards availability. Section VI goes into finer details with respect to some known cyber vulnerabilities within this facet of the communications ecosystem. Section VII presents some preliminary experimentation/simulation. Section VIII puts forth some concluding thoughts and the acknowledgement closes the paper.

II. COMMUNICATIONS COVERAGE

A. Cellular Coverage

While a substantive portion of developed country internet users depend on hard-wired internet connections, the shift to wireless has increased tremendously over the past several years. According to a 12 June 2019 Pew Research Center Internet/Broadband fact sheet, approximately one-in-five American adults is dependent strictly upon smartphones for online access and no longer has traditional home broadband service. This phenomenon had transpired even prior to the advent of the first fairly substantial Fifth Generation (5G) technology standard for cellular network deployments in April 2019. To date, the attractiveness of relying upon smartphone cellular services to connect to the internet is the relative ubiquity of a cellular signal; however, the quality of the cellular signal varies greatly, and this is particularly noticeable with higher bandwidth digital media-related activities (e.g., watching streaming video, uploading pictures for social media, etc.), particularly when only one bar of a Fourth Generation (4G) cellular signal (in terms of the commonly accepted Received Signal Strength Indicator or RSSI, a signal typically ranges from full bars at -50db to no bars/dead zone at -120db) is available.

The degradation in signal strength should be of no surprise. Cellular signals are radio waves, and as with all types of radio frequency waves, they are readily susceptible to interference. Outside Radio Frequency Interference (RFI) can be caused by, among others, mountains, hills, valleys, trees, and tall structures. The transition from an outside to an inside environs also experiences RFI; certain construction materials, which are the primary cause of poor cellular service, include concrete, brick, metal, glass, various energy-efficient materials (e.g., foam board, fiberglass batts, Leadership in Energy and Environmental Design or LEED certified glass), and conductive material (e.g., copper), among others. Internal interference can be caused by wood, plaster, drywall, plywood, electrical devices, and clutter.

In addition to the exemplar cellular signal blocking materials provided, weather also has a tremendous impact on cellular coverage as does distance from a cellular base station (a.k.a. cell tower or cell site). For these cases, a cellular signal booster (a.k.a. amplifier or repeater) can assist matters by amplifying the weak signal. Typically, the Federal Communications Commission (FCC) has no issue with cellular signal repeaters extending the range of a cellular network in areas that, historically, receive poor cellular service [2].

B. Non-Cellular Coverage

In addition to cellular means, non-cellular wi-fi is a method for devices, such as smartphones, to connect wirelessly to the internet via radio frequency waves. Generally speaking, wi-fi is faster than Third Generation (3G) and is sometimes faster than 4G mobile data; typically, bottlenecks stem from bandwidth limitations on the landline internet connection side. In contrast to cellular signals, wi-fi signals can readily pass through many materials (e.g., plywood, plaster, and drywall) that pose a problem for cellular signals. However, for certain cases, some walls are quite thick and may utilize reinforced concrete or other materials that block some of the signals. Hence, similar to cellular, as a radio wave, wi-fi is also susceptible to interference, such as from other wi-fi networks and other usages within the utilized bands. For these cases, a wi-fi repeater or extender can assist matters. As a wi-fi extender makes no use of a cellular signal, there must be an existing wi-fi signal for an extender to work.

III. REGULATORY COMPLIANCE AND ADHERENCE

The FCC has endeavored to ensure that cellular booster equipment does not interfere with the carrier network that it supports, and boosters must undergo a series of tests to be certified by the FCC. Carrier-specific boosters must adhere to a particular set of regulations while carrier-agnostic boosters adhere to a separate set of regulations. By way of example, for carrier-specific boosters, the amplifier gain (e.g., FCC-approved commercial cellular signal boosters are restricted to +70 dB gain), downlink output power (FCC-approved boosters are restricted to 12 dBm) [3], and other technical limits are set by 47 CFR Ch. 1 §20.21. For carrier-agnostic boosters, these characteristics, as well as other technical limits, have also been established. With a surge in the use of boosters, an interesting phenomenon has arisen.

Malfunctioning and misused boosters have posed substantial interference problems for the cell tower sites of cellular carriers as well as the public safety emergency radio traffic that utilize the same frequency bands that signal boosters occupy. For this reason, various cellular carriers have lobbied the FCC so as to curtail the use of boosters and have requested the following constraints: (1) signal boosters

 ISBN: 978-1-61208-818-1

are subject to the wireless licensee's presumptive authorization (i.e., the booster is registered and able to be controlled by the licensee in the form of dynamic control over the booster's transmit power for any reason at any time), (2) signal boosters may only be operated on a channelized basis on the proscribed frequencies utilized by the wireless licensee whose signal is being boosted (i.e., carrier-specific narrowband booster), (3) signal boosters are designed with oscillation detection and will terminate transmission when oscillation occurs, and (4) signal boosters are subject to the FCC's equipment certification process, an industry certification process, and approval by the individual licensee.

Section 510 of the International Code Council's (ICC) 2018 International Fire Code (IFC) affirms these points for signal boosters, such as: (1) Bi-Directional Amplifiers (BDAs) used in emergency responder radio coverage systems shall have oscillation prevention circuitry, and a spectrum analyzer or other suitable test equipment shall be utilized to ensure that spurious oscillations are not being generated by the subject signal booster, as well as (2) signal boosters shall have FCC or other radio licensing authority certification and be suitable for public safety use prior to installation. Despite the actions taken by the FCC and the guidance provided by the IFC, the preference of cellular carriers is to sell/provide femtocells (for use in a home or office) to customers. Interference remains a complex issue, and phenomena, such as inter-cell site and intra-cell site interference, remain problematic. Interference can be caused by a call on the same frequency from a neighboring cell, or a call on an adjacent channel in the same or neighboring cell [4]. For 4G, intra-cell interference is reduced by, among other techniques, Orthogonal Frequency-Division Multiplexing (OFDM) digital modulation and Orthogonal Frequency Division Multiple Access (OFDMA). In comparison, inter-cell interference, which is caused by frequency reuse (the process of utilizing the same radio frequencies at cell sites within a geographic area that are separated by sufficient distance so as to minimize interference) and increased femtocell deployment.

IV. COMMUNICATIONS ARCHITECTURES

As is evidenced, cellular interference is a major issue, thereby necessitating a robust, reliable, and resilient communications architecture. In many cases, a layered approach is employed, and non-cellular wi-fi may be leveraged.

A. Network Topology

Although non-cellular wi-fi, particularly public wi-fi, is not necessarily stable in many cases (this often stems from congestion on the network), most of the time, non-cellular wi-fi tends to be faster than cellular [mobile] data connections. For this reason, contemporary smartphones employ smart auto switching between non-cellular wi-fi and mobile data. This smart network switching (a.k.a. adaptive wi-fi), in essence, connects to a wi-fi network and a cellular network concurrently. In some cases, instead of bonding them into a single channel (i.e., non-bonded single channel), traffic is sent on whichever connection is faster at the moment (i.e., switches back and forth between non-cellular wi-fi and cellular [mobile] data). Alternatively, multi-channel bonding (i.e., bonded multi-channel) can be used, which leverages multiple internet connections (mobile data, wi-fi, Bluetooth, etc.) concurrently for increased throughput and redundancy.

1) Types of Networks Leveraged:

Accordingly, three types of networks are often leveraged: (1) Wireless Personal Area Networks (WPANs), which are short-range networks that utilize Bluetooth technology to connect a smartphone to a device (e.g., desktop computer, which has an Internet Protocol or IP connection); (2) Wireless Local Area Networks (WLANs), which are medium-range networks that typically utilize wi-fi technology and provide wireless access points that are connected to a wired network; and (3) Wireless Wide Area Networks (WWANs), which are long-range networks that typically utilize cellular technology and leverage the backbone provided by cellular service providers.

2) Striving for Reliability and Resiliency:

In addition, contemporary communications architectures might leverage three different layers for reliability and resiliency: (1) Cellular booster layer, which — depending upon the manufacturer — can boost 4G coverage ranging from 50,000 to 200,000 square feet with a potential +70 dB gain (for U.S. carriers) at various levels of signal strength (i.e., 5 bars, 3-4 bars, 1-2 bars) (the coverage will depend on the strength of the original signal, and the commonly accepted inflection point for booster viability is at about -105 dB outside signal); (2) Lorawan Wi-Fi layer, which can provide coverage ranges from the gateway ranging from about 800 meters at 100% data packets received to approximately 1500 meters at 98% data packets received in an urban environment [5]; and (3) 5G layer with three versions of wireless technology: low-band (part of the nationwide coverage), mid-band (faster speeds at longer ranges and limited indoors functionality), and millimeter-wave (mmWave) (for extended indoors functionality, albeit walls, glass, and even a hand can block mmWave signal) [6], as well as spread spectrum technologies (e.g., chaotic sequence) combined with generalized frequency division multiplexing.

B. The Amalgam of Network Layers

Smart switching leverages both non-cellular wi-fi and cellular. Macrocells cover about 30 kilometers (km) radius. Microcells cover about a 2 km radius and lessen the load of the macrocell network as well as provide capacity and in-building penetration. A metrocell covers about a 300 meter radius. A picocell covers about a 200 meter radius, and

 ISBN: 978-1-61208-818-1

femtocells cover about a 10 meter radius (although the AT&T femtocell covers about a 12 meter radius). The irony of carriers preferring femtocells is that they are designed to maintain a connection to the femtocell as much as possible, but risk dropping a call, particularly if the call needs to be switched to a picocell, metrocell, microcell, or macrocell (which can readily occur for callers on the move). Hence, the barrier to entry to disrupt a call is rather low. For example, interfering with the wi-fi would obligate the smart switching to devolve to cellular; then, interfering with the femtocell (as just one example) can induce a dropped call or even prevent a 911 call.

V. PREDELICTION TOWARDS AVAILABILITY

The 9/11 Commission Report, originally published on 22 July 2004, had recommended that the U.S. Congress provide for "the expedited and increased assignment of radio spectrum for public safety purposes," as various blindspots in emergency communications infrastructure were illuminated when first responders from varying jurisdictions were unable to communicate with each other due to differences in equipment [7]. Furthermore, cellular service was quickly overwhelmed from use by both first responders and civilians. In the absence of a dedicated public safety network, first responders predominantly communicated, via Land Mobile Radios (LMRs) (wireless communications systems that support low-speed data communications and voice) and commercial cellular networks (wireless communications systems that support voice and high-speed data communications and access to communications, but cannot substantively deliver the equivalent security standards that LMRs can for "mission critical voice" communications). Traditionally, LMRs have been the most reliable and secure method of voice communications. However, LMRs operate on thousands of different networks, are often not interoperable because they operate on different spectrum frequencies, are encrypted in different ways, are non-standardized (i.e., customized) by vendors and/or agencies, and newer LMRs are often not backwards compatible.

In 2008, the FCC auctioned licenses for segments of the 700 MHz Band for commercial purposes. Carriers began using these segments of the spectrum to offer mobile broadband internet access services for smartphones, tablets, laptop computers, and other mobile devices. On 22 February 2012, the U.S Congress enacted the Middle-Class Tax Relief and Job Recovery Act of 2012 (a.k.a. Spectrum Act), which directed the FCC to allocate the D-Block (758-763 MHz/788-793 MHz) for a public safety nationwide broadband network. Title IV of the Spectrum Act formed the First Responder Network Authority (a.k.a. FirstNet) (an independent authority charged with establishing "a nationwide, interoperable public safety broadband network") within the National Telecommunication and Information Administration (NTIA), an agency of the U.S. Department of Commerce.

Initially, public safety officials endeavored to have a "dedicated public safety network" that was distinct and disparate from any commercial provider. However, while the U.S. Congress had allocated USD $7 billion to build a network, it turned out to be insufficient funding for the construction of a distinct and disparate network [8]. The estimated cost for constructing a new nationwide 4G network for the FirstNet system ranged up to USD $40 billion, as infrastructure, such as cell towers, had to be built not only in dense urban areas, but also across all of rural America [9]. The magnitude of the project hinted at the need for public-public and/or public-private partnerships. In March 2017, FirstNet formed a public-private partnership with AT&T and awarded AT&T a 25-year contract to build out the network. Pursuant to this public-private partnership, AT&T obtained access to the 20 MHz segment of the Band 14 spectrum (758–768 MHz/788–798 MHz) (a highly desirable segment of spectrum in the 700 MHz band that facilitates good propagation in urban/rural areas as well as penetration into buildings) allocated to FirstNet and can receive up to USD $6.5 billion by operationalizing network deployment milestones in a timely fashion; in turn, AT&T agreed to provide access to its existing infrastructure and to "spend about $40 billion over the life of the contract to build, deploy, operate and maintain the network" [10]. Please refer to Figure 1 below.

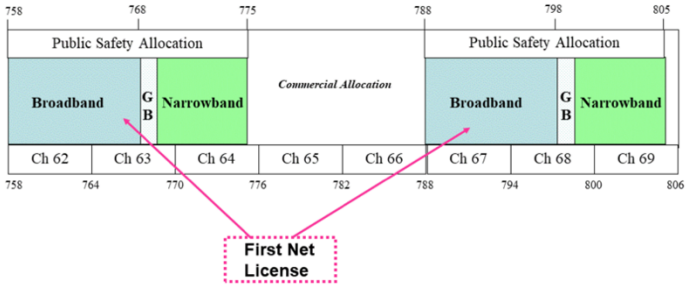

Figure 1. FirstNet Licensed Portions of the 700 MHz Spectrum [11]

As the main backbone of AT&T's Long-Term Evolution (LTE) network (which has substantial nationwide coverage) previously consisted of a superset of Band 17 and Band 12 (699-716 MHz/729-746 MHz), AT&T's FirstNet cellular network soon comprised both Bands 12 and 14.

First responders have priority on AT&T's FirstNet cellular network, but the underlying legislation that created FirstNet allows for much more pervasive usage; any government user and certain commercial entities, under specific circumstances, have priority usage. According to the National Institute of Standards and Technology (NIST), "public safety practitioners utilizing the forthcoming Nationwide Public Safety Broadband Network will have smartphones, tablets, and wearables at their disposal" … "although these devices should enable first responders to

 ISBN: 978-1-61208-818-1

complete their missions, any influx of new technologies will introduce new security vulnerabilities" [12]. Near the turn of the year, NIST had noted that there were 163 FirstNet-ready (capable of accessing the private core FirstNet network running on Band 14) and FirstNet-capable devices (designed to share wireless space with AT&T's commercial customers, whereby FirstNet users receive priority and preemption access over non-FirstNet users). According to NIST and cyber practitioners, the preference towards availability and the looming vulnerabilities of having Band 14 in so many devices (e.g., iPhone, iPad, Samsung Galaxy, Dell, etc.) constitutes a large attack surface area. Also, if the network is overloaded with public-safety use, it would not be available for citizen 911 calls or alerting by citizens, such as in accordance with "If You See Something, Say Something" [13]. Historically, high-profile networks have been subject to such cyberattacks. For example, Romanian hackers took over 123 of the 187 Washington D.C. police department's outdoor surveillance cameras from 12-15 January, just days before the U.S. presidential inauguration on 20 January 2017 [14].

For modern society, availability is central. For example, customers are increasingly influenced by the availability and Quality of Service (QoS) of high-speed wi-fi. Several studies shows that about two thirds of businesspeople assert that they would refuse to return to a location with sub-standard wi-fi, and the dependencies upon availability seem to persist across the enterprise, small medium businesses (SMB), industrial, residential sectors, etc. Providing free wi-fi service also has the complications of contending with squatters (people that "camp out" to gain access to the free wi-fi, but purchase very little, if anything), who impact the bandwidth; there is even the further complication of having squatters that may be infringing/downloading illegal content (albeit there are certain "safe harbor" provisions under §512 of the Digital Millennium Copyright Act or DMCA for the provider of the free wi-fi) and even launching cyberattacks from the wi-fi network.

VI. KNOWN CYBER VULNERABILITIES

To demonstrate how Distributed Denial of Service (DDoS) or Telephony Denial of Service (TDoS) attacks could affect 911 call systems (and putting aside the known vulnerabilities of TeleTYpewriter or TTY services), researchers created both a detailed simulation of North Carolina's 911 infrastructure as well as general simulation of the U.S. 911 infrastructure; the researchers reported that with only 6,000 infected phones, it was possible to effectively block 911 calls from 20% of the state's landline callers, half of the mobile customers, and per the simulation, although people called back four or five times, they still could not reach a 911 operator [15].

By way of background information, when 911 is called, via a landline or mobile phone, the carriers facilitate the connection to an appropriate call center. Over time, to increase the capacity and avoid bottlenecks, carriers have transitioned from circuit-switched 911 infrastructure to packet-switched Voice over Internet Protocol (VoIP) infrastructure, which is referred to as Next Generation 911 (NG911). Within the NG911 paradigm, load balancing among the approximately 6,200 public-safety answering points (a.k.a. Public-Safety Access Points) (PSAPs) improves reliability, and callers can also transmit text, images, video, and other data to the PSAPs. While the NG911 can indeed help mitigate against the DDoS problem by dynamically connecting to PSAPs around the country, the rate at which callers give up trying to call 911 (a.k.a. the "despair rate"), amidst a TDoS attack, is significant [15].

Beyond being vulnerable to DDoS attacks, there are other attack vectors. For example, for those areas, wherein Band 14-related towers for the FirstNet system are not viable to be deployed, it is envisioned that satellite systems will be deployed for the "last mile" [16]. However, satellite vulnerabilities have been of concern for quite some time. The issue of Assured Positioning, Navigation and Timing (A-PNT) (related to Global Positioning System or GPS/location spoofing) had been raised in the National Defense Authorization Act (NDAA) for Fiscal Year 2019 and prior. Indeed, one of the central features of Enhanced 911 (E911) (for Basic 911 service, the caller must inform the emergency operator as to the location, whereas for E911, the location is automatically displayed on the emergency operator's screen) is location-determination. Yet, phenomenon, such as swatting (a tactic of deceiving emergency services to respond to a particular location via location spoofing) have been prevalent for quite some time. Typically, swatting involves calling 911 with a non-serviced "burner" or anonymous pre-paid phone; the burner phones are neither enabled nor linked to any account. Yet, under federal law, these Non-Service Initiated (NSI) devices (with no service plan) are still able to call 911. The popularity of VoIP has segued to an interesting vulnerability for the 911 system; VoIP users manually provide their address (e.g., billing address) so as to populate the database of the VoIP service provider (VSP). When a 911 call is placed, the call is sent to an Emergency Services Gateway (ESG). Automatic Number Identification (ANI), and for some cases a pseudo-ANI (pANI) is involved, processes the number, and the ESG performs a search of the VSP database to ascertain the assigned PSAP. The call is forwarded to the assigned PSAP, which receives the location information provided by the VSP database. Automatic Location Information (ALI) returns an address (which might be false) that is associated with the number. Compromising location-determination systems (e.g., modifying the VSP, ANI, or ALI records) could lead to first responders being directed to the wrong location. Altering the VSP, ANI, and/or ALI databases or denying service to the databases could also increase the credibility of the swatting call [17]. By misdirecting resources, swatters could delay first responders to a planned physical attack; in addition, a swatter could

 ISBN: 978-1-61208-818-1

create an incident, which concentrates first responders in a specific location for the purposes of an ambush [18].

As an alternative to calling 911, the swatter could simply call one of the approximately 4,000 PSAPs (of the approximately 6,200), which serve as primary 911 call centers, whereby operators dispatch first responders directly [15]. Calls made directly to the PSAP do not use the VSAP, ANI, and/or ALI databases; rather, the operator simply asks the caller for the address. Please refer to Figure 2 below, which summarizes some of the described attack vectors.

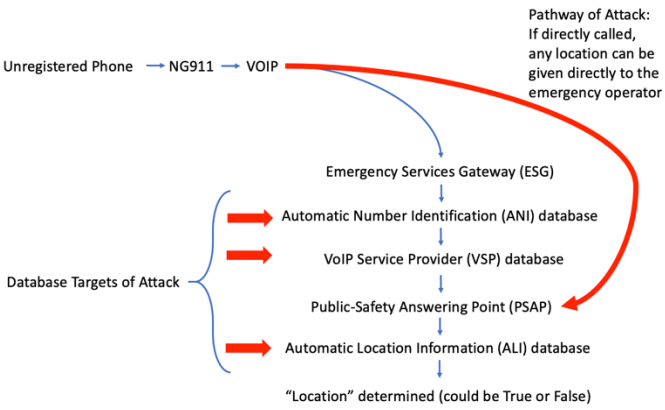

Figure 2. Potential Attack Vectors to Spoof Location

Generally, the phone numbers for PSAPs are closely held information. However, recorded 911 calls obtained by Freedom of Information Act (FOIA) or the relevant public records act (e.g., for a particular state) contain the Dual-Tone Multi-Frequency (DTMF) tones for the number of the PSAP when a call is transferred [19]. There are various DTMF decoders available on GitHub and other open source repositories to determine the numbers for the PSAPs. The National Emergency Number Association (NENA), an organization that serves as a public safety committee with regards to 911, is endeavoring to have the PSAP numbers protected (i.e., redacted) and non-extractable for 911 recordings. In any case, the Confidentiality, Integrity, and Availability (CIA) triad must be carefully considered. A disclosure of previously private information or communications to unauthorized parties is a breach of confidentiality (e.g., the VSP, ANI, and/or ALI databases are compromised). A violation of the intended function of a system by unauthorized parties is a breach of integrity (e.g., misdirecting of emergency services by swatters). An attack (e.g., DDoS or TDOS) that leads to an unavailability issue (e.g., PSAPs being made unavailable to handle 911 calls) is a breach of availability, which seems to be of the highest concern amidst contemporary times.

VII. Experimentation/Simulation

Beyond the described attack vectors, limiting the frequency channels available for use also creates honeypot observational space opportunities for a potent cyber kill chain, and this notion is shown in Figure 3 and 4 below.

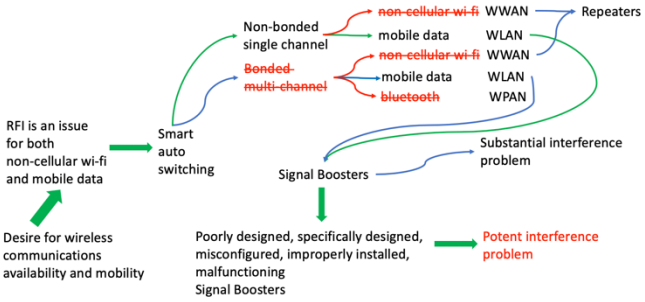

Figure 3. Limiting the channels available for use to create a more potent honeypot observational space cyber kill chain

The described scenario was simulated on a GNU Octave platform, which is a numerical computation platform that is mostly compatible with MATLAB. However, as GNU Octave is released under a GNU GPLv3 license, the source code was modified so as to take advantage of Compute Unified Device Architecture (CUDA) multi-threaded parallel computing accelerants for the utilized Semi-Definite Programming (SDP) solver so as to quickly address the involved convex optimization problems.

A. Cyber Kill Chain

The simulation involved Bluetooth Adaptive Frequency-Hopping (AFH) spread spectrum on twenty collocated WPANs. The Bluetooth usage engaged in changing channels up to 1600 times per second among 79 channels on the 2.4 GHz band. The simulation also involved wi-fi networks on twenty collocated WLANs. With the 2.4 GHz band heavily congested with Bluetooth traffic, the wi-fi networks were constrained to only a single channel on the 2.4 GHz band (e.g., Channel 40) and the 5 GHz band. The emulated FirstNet-capable devices (which share wireless space with commercial customers) included cellphones (which generally have very weak Wi-Fi radios to maximize battery life and small antennas to minimize device size), tablets (compared to cellphones, they have have stronger Wi-Fi radios and better antennas), and laptops (compared to tablets, they have stronger Wi-Fi radios and better antennas). The specified effective range for the devices were as follows: 200 meters from a hub for cellphones, 400 meters from a hub for tablets, and 900 meters from a hub for laptops. The effective range between a hub to another hub (i.e., remote hub) was established as 3 km. At 1.5 km, the bandwidth was 10 Million bits per second (Mbps); at 3 km, the bandwidth is < 5 Mbps. Every "hop" across a remote hub cut the available bandwidth in half (single radio hubs were emulated, and these cannot send and receive at the same time). More than three hops resulted in a bandwidth < 1 Mbps. The urban/rural demarcation was set at 1.5 km. As the "urban" area was congested with Bluetooth traffic, the

 ISBN: 978-1-61208-818-1

wi-fi avoided the 2.4 GHz and endeavored to utilize the 5 GHz band. However, with twenty WLANs competing for the 5 GHz band, the lower portion of the Unlicensed National Information Infrastructure (U-NII-1) and upper portion (U-NII-3) quickly became congested. For the simulation, the remaining U-NII-2 was congested with portable weather radar (IEEE channel numbers 120, 124, 128). IEEE channel numbers 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, and 144 of U-NII-2 was congested (at spreading factor 7, no packets were received, and even at spreading factor 12, no packets were received) so that communications, via smart auto switching, devolved to cellular mobile data, such as described in Figure 3.

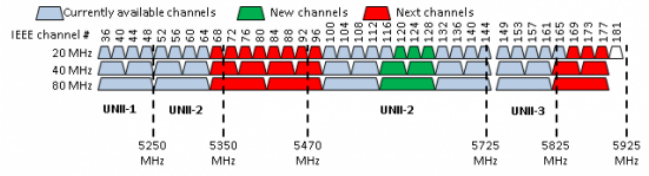

Figure 4. Unlicensed National Information Infrastructure (U-NII) Segments and IEEE Channels on the 5GHz Wi-Fi Spectrum [20]

Co-tier interference (between neighboring femtocells) and cross-tier interference (among different tiers of the network, such as between femtocell and picocell, metrocell, microcell, or macrocell) were also emulated so as to force the communications to return to Channel 40 (between 5170 and 5250 MHz) on U-NII-1. The Berkeley Packet Filter (BPF) was utilized to monitor the channels, specifically Channel 40. Hence, the cyber kill chain was complete.

B. *An Even More Potent Cyber Kill Chain*

Industrial Systems (IS) are heavily dependent upon communications so as to be "smart." As many IS are in remote areas, the communications is sparser and infrastructure deployment can be costly. Hence, signal boosters have been utilized to bridge the gap for this "last mile" paradigm. Ironically, these boosters can readily interfere with the existing communications used by system operators and linemen, who are servicing the involved critical infrastructure. It should also be noted that, in some cases, the keiretsu-like structured manufacturers of the non-FCC-compliant are some of the more predominant purveyors of equipment into the electrical grid sector in certain locales. The ensuing risk is that these represent nodes/clusters of potential interference; two types are discussed briefly.

1) Incidental Emitters: Generally speaking, the substantive portion of the noise emanating from electric utility equipment stems from incidental emitters. Yet, there are no specific limits on the conducted or radiated emissions. There are guidelines for these unlicensed emitters of Radio Frequency (RF) energy to not deliberately cause harmful interference [21], and the Federal Communications Commission (FCC) has mandated that utility companies rectify powerline-related interference problems within a reasonable time, particularly if the interference is caused by faulty electric utility equipment. Under FCC rules, most powerline and electric utility-related equipment are classified as "incidental radiators [22]," as the RF energy or noise created is simply an incidental part of its intended operation. However, historically, a number of electric utility chief executive officers have received letters from the FCC Enforcement Bureau pertaining to this type of violation [22].

2) Unintentional Emitters: A portion of the noise emanating from electric utility equipment stems from unintentional emitters; while this type of emitter intentionally generates an internal radio signal, it does not intentionally radiate/transmit it. Examples include some types of switched-mode power supplies (an electronic power supply that incorporates a voltage switching regulator — which transforms the incoming power supply into a pulsed voltage that is then smoothed, via the utilization of capacitors, inductors, and other elements — to convert electrical power efficiently) as well as microprocessors utilized within some of the electric utility equipment.

Depending upon the locale, the RFI emitters from the electrical grid can constitute a substantive source of interference and is clearly discernible, via a spectrum analyzer. Taking just one example of a potential impact, according to the FCC, location information must be available for at least 70% of wireless emergency assistance 911 calls or location information must be accurate to within 50 meters for 2020, and the requirements increase for 2021 [21]. Yet, given the vulnerabilities and cyber kill chain described, the true operationalization of this mandate needs to be further explored, particularly as the simulated interference precluded this.

VIII. CONCLUSION

Modern communications architectures have shifted to accommodate the societal predilection for availability. The prototypical techniques for reliability (e.g., bonded multi-channel communications) is well understood. The resiliency pathways (e.g., frequency hopping to available frequency channels) are also well understood. An attack (e.g., DDoS) that leads to PSAPs being made unavailable to handle 911 calls is a breach of availability for emergency services, which seems to be of paramount importance in modern society. Yet, the bur availability architectures has not slowed; indeed, the architectures have greatly increased in number, and the described privatization of communications backbones has fueled the use of privately-owned signal boosters. Although boosters should adhere to a set of regulations (e.g., +70 dB gain, 12 dBm downlink output power), it is possible for rogue boosters to ignore these regulations, effectuate communications interference, and

 ISBN: 978-1-61208-818-1

wreak havoc during emergencies. Likewise, congesting channels would rate limit the channels available/utilized for non-bonded single channel and bonded multi-channel communications alike. In particular, while the intent of NG911 is to facilitates 911 callers reporting incidents and the conveying of information (e.g., text, images, video) to the PSAPs, disruption of such communications networks would create a large blindspot for first responders. While the described preliminary experimentation/simulation involved WPANs and WLANs, future work will build upon the described experimentation/simulation by congesting WWANs as well. In this way, the notion of available for the various simulated resilient communications architectures can be better explored and examined.

Overall, given the situation that communication networks are subject to degradation due to a variety of factors, it is possible to interfere with both cellular and voice over Internet Protocol (VoIP) 911 and/or first responder-related calls by the strategic placement of interfering nodes in the form of misused cellular boosters and/or strategically positioned femtocells, deliberate Bluetooth congestion so as to limit the number of frequency channels available and intentionally interfere with wi-fi and last-mile communications technologies, thereby affecting the communications paradigm.

ACKNOWLEDGMENT

This research is supported by the Decision Engineering Analysis Laboratory, an Underwatch initiative, which has previously supported the FTA Program under the Assistant Secretary of Defense for Research and Engineering, via participation at certain venues (e.g., IARIA). This is part of a VT white paper series on 5G-enabled defense applications, via proxy use cases, to help inform Project Enabler.

REFERENCES

[1] S. Chan, "Detecting Powerline Noise with Low-Cost Noise Sensors for Power Outage Mitigation," 2020 IEEE Sensors Applications Symposium, Kuala Lumpur, Malaysia, 2020, pp. 1-6, doi: 10.1109/SAS48726.2020.9220027.

[2] Federal Communications Commision. *Indoor Location Accuracy Benchmarks.* [Retrieved September 10, 2020] from: https://www.fcc.gov/wireless/bureau-divisions/mobility-division/signal-boosters/signal-boosters-faq

[3] Federal Communications Commision. *Indoor Location Accuracy Benchmarks.* [Retrieved September 10, 2020] from: https://www.fcc.gov/document/use-and-design-signal-boosters-report-and-order

[4] Y. A. Adediran, H. Lasisi, and O. B. Okedere, "Interference management techniques in cellular networks: A review," Cogent Engineering, 4:1, DOI: 10.1080/23311916.2017.1294133

[5] Smartmakers. *LoRaWAN Range Part 2: Range and Coverage of LoRaWAN in Practice (Updated).* [Retrieved September 10, 2020] from: https://smartmakers.io/en/lorawan-range-part-2-range-and-coverage-of-lorawan-in-practice/

[6] M. Yoshida, "MWC: Are Your 5 Fingers Blocking Your 5G?" EE Times. [Retrieved September 10, 2020] from: https://www.eetimes.com/mwc-are-your-5-fingers-blocking-your-5g/#

[7] National Commission on Terrorist Attacks Upon the United States. *The 911 Commission Report.* [Retrieved September 10, 2020] from: https://www.9-11commission.gov/report/911Report.pdf

[8] National Telecommunications and Information Administration. *Public Safety*. [Retrieved September 10, 2020] from: https://www.ntia.doc.gov/category/public-safety

[9] A. Loh, "The State of FirstNet, America's Public Safety Broadband Network," Lawfare [Retrieved September 10, 2020] from: https://www.lawfareblog.com/state-firstnet-americas-public-safety-broadband-network

[10] U.S. Government Accountability Office. *Public-Safety Broadband Network.* [Retrieved September 10, 2020] from: https://www.gao.gov/assets/710/704058.pdf

[11] Federal Communications Commision. *700 MHz Public Safety Spectrum.* [Retrieved September 10, 2020] from: https://www.fcc.gov/700-mhz-public-safety-narrowband-spectrum

[12] J. Franklin, G. Howell, S. Ledgerwood, and J. Griffith, "Security Analysis of First Responder Mobile and Wearable Devices," NIST, pp. ii, May 2020, doi:10.6028/NIST.IR.8196

[13] Federal Emergency Management Agency. *Integrated Public Alert & Warning System*. [Retrieved September 10, 2020] from:https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning- system.

[14] R. Weiner, "Romanian hackers took over D.C. surveillance cameras just before presidential inauguration, federal prosecutors say," *The Washington Post*, December 28, 2017. [Retrieved September 10, 2020] from: https://www.washingtonpost.com/local/public-safety/romanian-hackers-took-over-dc-surveillance-cameras-just-before-presidential-inauguration-federal-prosecutors-say/2017/12/28/7a15f894-e749-11e7-833f-155031558ff4_story.html

[15] M. Goebel, C. Dameff, and J. Tully, "Hacking 9-1-1: Infrastructure Vulnerabilities and Attack Vectors," J Med Internet Res. 2019 Jul; 21(7), Jul. 2019, doi: 10.2196/14383

[16] Senate Hearing 115-153. Investing in America's Broadband Infrastructure: *Exploring Ways to Reduce Barriers to Deployment.* [Retrieved September 10, 2020] from: https://www.govinfo.gov/content/pkg/CHRG-115shrg28640/html/CHRG-115shrg28640.htm

[17] 2019 Michigan State Law Review 1133. *Combatting the Swatting Problem: The Need for a New Criminal Statute to Address a Growing Threat.* [Retrieved September 10, 2020] from: https://digitalcommons.law.msu.edu/cgi/viewcontent.cgi? article=1251&context=lr

[18] Director of National Intelligence, *Persistent Threat of Terrorist Ambush Attacks on First Responders.* [Retrieved September 10, 2020] from: https://www.dni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/81_NCTC_DHS_FBI_-_Ambush_Attacks.pdf

[19] Federal Communications Commision. *Task Force on Optimal PSAP Architecture.* [Retrieved September 10, 2020] from: https://docs.fcc.gov/public/attachments/DA-16-179A2.txt.

[20] C. Spain, "Winning Back the Weather Radio Channels Adds Capacity to 5GHz Wi-Fi Spectrum," [Retrieved September 10, 2020] from: https://blogs.cisco.com/networking/winning-back-the-weather-radio-channels-adds-capacity-to-5ghz-wi-fi-spectrum

[21] "Part 15-Radio Frequency Devices § 15.3," [Retrieved September 10, 2020] from: https:// www.ecfr.gov/cgi-bin/text-idx?node=pt47.1.15&rgn=div5

[22] M. Marcus, J. Burtle, B. Franca, A. Lahjouji, N. McNeil, "Federal communications commission spectrum policy task force," E&UWG, 2002.

 ISBN: 978-1-61208-818-1