

Next-Generation Radio-Frequency Monitoring in Secure Environments

Minh Nguyen, Brent Laird, Michael R. Gross

Our world is filled with electromagnetic energy, and we are constantly buffeted with both visible and invisible waves radiating throughout our living environment. Electromagnetic energy can be naturally occurring, such as x-rays from black holes and solar flares, shortwave radiation (ultraviolet, visible, and infrared energy) from the sun on a normal day, longwave (mostly infrared) or thermal radiation emitted from the Earth's atmosphere and surface, and radio waves from galactic sources. Electromagnetic energy can also be human-made. The spectrum of energy ranges from extremely low frequency waves such as those emanating from power lines [60 hertz (Hz) in North America [1]] to extremely high frequencies that are used for medical purposes (e.g., diagnostic x-rays, cancer treatments). In between these opposite extremes are visible light and invisible radio frequency [(RF), 3 kilohertz (kHz) to 300 gigahertz (GHz) [2]] energy emitted in the course of many of our day-to-day activities: waking up to a morning radio show, using the microwave to reheat coffee, logging onto a Wi-Fi network, calling a colleague on a cell phone, pairing a fitness tracker using Bluetooth near-field communications, monitoring a home via internet-of-things devices, using a key fob to enter and start a car, using GPS to navigate, using hands-free technology while driving, listening to a satellite radio station, paying a highway toll via radio frequency identification (RFID) transponder, remotely opening a garage door, watching broadcast television, and on and on. In each of these examples, one or more "radios" are transmitting and/or receiving information through electromagnetic waves in the RF. The ubiquity of RF in today's technology results in a constant complex background of RF signals at any given time and place.

[Photo credit: iStock.com/da-kuk]

Should we be worried about all of these RF waves that surround us? Several US government agencies, including the National Institute of Health's National Institute of Environmental Health Sciences [1], Centers for Disease Control [3], Federal Communications Commission (FCC) [2, 4], and the Environmental Protection Agency [5, 6, 7], have reported on research related to potentially adverse health effects of specific portions of the electromagnetic spectrum. To prevent interference across RF signals, particularly in regard to public safety services, the FCC and the National Telecommunications and Information Administration share regulatory responsibility over the allocation of the spectrum between frequency bands 0 kHz and 275 GHz [8]. However, health risks and public safety are not the only concerns posed by this metaphorical ocean of waves. Across the US government, agencies must also consider our complex RF background when identifying potential security risks and implementing methods to mitigate for them. In order to effectively monitor RF signals, they need a system that can sift through enormous volumes of data, in or near real-time, across a wide frequency range. In order to be actionable, such a system must have the ability to differentiate between what is "normal" (in other words, what they would expect to find in the given environment and can thus ignore), what is "anomalous" (unexpected), and what is "significant" (security threat worthy of further investigation).

This article will focus on the last area of concern: security—why we need to monitor signals and what methods and hardware currently exist to meet our needs. Finally, we will introduce new initiatives, including IARPA's Securing Compartmented Information with Smart Radio Systems (SCISRS) program [9], that aim to develop the next-generation methods to automatically detect and characterize suspicious signals and RF anomalies in complex RF environments.

The need to detect anomalous signals

So why are anomalous RF signals a security problem and why would anybody need a system to monitor them? The simplest answer is that certain facilities house highly classified information and, therefore, must have the most rigorous security measures in place. There are strict standards for the physical and technical security of any sensitive compartmented information facility (SCIF) [10, 11]. These standards create a foundation from which those tasked with

securing a SCIF can deduce what normal signals should look like. Attempts to steal or leak data will then give themselves away through telltale signals such as intentional transmissions from unauthorized or modified wireless devices, unexpected mobile cellular signals, and unintentional emanations that carry compromising information. Each type or category of signal has specific methods that are used to detect them. But, as technology progresses, the overall "normal" RF background in secure environments grows more complex, and these indicators of breaches may become easier to hide and more challenging to discover.

US facilities and federal buildings are governed by standards and physical security policies that restrict ingress and egress of items that can receive, record, transmit, or emit information, thereby imposing a technical threat [12]. But the basic equipment necessary to facilitate day-to-day business activities must also be able to receive, record, transmit, or emit information. The varying answers to the simple question "*what is allowed inside of where?*" result in a significant challenge to those responsible for securing these facilities. For example, official electronic devices, information technology (IT), and associated media are permitted if they are operationally required, they have been approved by their organization, and their introduction complies with all relevant policies and procedures. However, the same types of devices (information storage media, radio transmitters, computers, photographic-/audio-/video-recording equipment, and other personal electronic devices) are not allowed, if they do not meet the criteria for official IT. While most personally owned electronic equipment is not permitted in secure facilities, exceptions are made based on a variety of conditions related to the facility (e.g., its location, the types of information housed and exchanged within it) and the capabilities/features of the equipment itself. These might include items needed by individuals with disabilities or for medical reasons (e.g., motorized wheelchairs, hearing aids, pacemakers, electronic hemoglobin-testers, insulin pumps) which are permitted so long as their introductions comply with applicable policies and procedures. Personal cell phones are never permitted inside a SCIF but may be permitted in other parts of the same building. The nature of the policies governing electronic devices and IT result in highly complex RF environments. Now imagine having to do this in less typical surroundings. Some missions require that information and data be generated, stored, used, transmitted, and received in

environments where there is less control. For example, military operations might require a temporary SCIF in order to meet tactical, emergency, or immediate operational requirements. The RF background and baseline would look very different in a remote location versus an urban location, and data security may be more challenging based on variable factors. In some exceptional circumstances, the mandated standards for a SCIF cannot be met, and additional security measures must be taken to mitigate for the increase risk to data security.

Any malicious actors, those whose intent is to steal data, will try to conceal the signals emanating from their devices and by their activities. They may do this by hiding their signals using methods such as spread spectrum or frequency hopping or by employing short bursts that are less likely to be detected in a system that is scanning through a wide spectrum of frequencies; a rough metaphor would be like security guards watching a video feed that jumps from one camera to another and onward until it has completed the circuit of cameras located throughout a building. Vigilant guards would catch illicit activity if it occurred in the time and location that showed up on their monitor, but there is some probability that they could miss it if the activity were very short and fast and there were a large number of cameras to sequentially scan. Alternatively, data thieves may not try to hide their signals at all; rather, they may use signals that mimic or closely resemble those that you would typically see in the target environment. Finally, an opportunist might simply take advantage of unintended RF emanations that inadvertently carry information.

Existing methods to mitigate risks

What can we do to secure our data? Security risks can be binned into broad categories, for which different mitigation strategies are employed. For some categories, the security monitoring is constant; whereas in others, the mitigations are employed on a case-by-case basis. We'll discuss a few examples in the next section.

Wireless intrusion detection system (WIDS)

Rogue wireless devices pose security risks to US facilities, ranging from the nonapproved devices that are inadvertently brought into restricted facilities to hostile devices that intentionally pass information to adversaries. The most minor violations, such as when

an employee forgets a cell phone in a jacket pocket and unintentionally brings it into a SCIF, can result in significant cost to an organization. A typical smartphone contains multiple transceivers including, but not limited to: cellular, Wi-Fi, near-field communications (e.g., Bluetooth), and GPS. Exploitation of cell phones (i.e., interception and monitoring) can enable an adversary to remotely access these transmitters/receivers as well as the phone's storage, camera, and microphone to gain information about the phone's surroundings. Even if a cell phone has not been exploited, accidental introduction into a secure space results in a cost to the organization: forensic analysis of confiscated devices takes time and manpower and can divert critical personnel from mission-critical security duties. Rogue wireless devices can also be *intentionally* introduced by an insider threat—an individual inside an organization who intends to use their authorized access for espionage, unauthorized disclosure of information, or other means of causing damage to the security of the United States. Adversaries can also hide or implant wireless devices inside hardware. Regardless of the intent, the presence of rogue wireless devices impose threats to US information infrastructure.

Over the years, mitigations have been developed and evolved to counter known wireless threats. Because wireless technology is based on communication standards, the detection of unbound RF signals can be used to detect rogue wireless devices. Currently, one of the most common security tools is the wireless intrusion detection system (WIDS), a commercial wireless technology that assists with the monitoring of specific parts of the RF spectrum to identify unauthorized wireless transmissions and/or activities. WIDS can be used to detect, identify, and geolocate wireless local area network (WLAN) devices in controlled spaces. Systems that also include active defense capabilities that can prevent unauthorized connection are wireless intrusion *protection* systems (WIPS). Both WIDS and WIPS consist of an RF sensor component (antennas and radios designed to collect specific wireless transmissions), a central controller/analysis component (software developed to distinguish between authorized/normal and unauthorized/anomalous wireless transmissions), and a display component (the user interface/dashboard that reports findings to designated personnel) [13].

WIDS and WIPS use strategically placed sensors and diagnostic software to track known signals such

as those from Wi-Fi, cellular transmissions, and end-user devices. The components and abilities of commercially available WIDS/WIPS vary based on the manufacturer; however, all systems will have sensors and a server. Hardware-based sensors are comprised of strategically placed antennas paired with radios that are used to scan the relevant channels [typically 2.4 GHz and 5 GHz for Wi-Fi, sometimes 800-900 megahertz (MHz) and 1.8-1.9 GHz for cellular], spending a set amount of time (e.g., 100 milliseconds to 1 second) at each channel. The WIDS/WIPS server detects potential threats by analyzing signatures, behaviors, protocols, and RF spectrum collected by the sensors [14].

Department of Defense (DoD) components deploy WIDS solutions to monitor their controlled spaces for WLAN activity and to detect WLAN-related policy violations on unclassified and classified DoD wired and wireless LANs. WIDS that comply with DoD and other US agency policies [12, 13] are capable of monitoring transmissions that fall within the Institute of Electrical and Electronics Engineers (IEEE) 802.11 body of standards in the 2.4, 3.6, 4.9/5, and 60 GHz spectrum bands. They continuously scan for and detect authorized and unauthorized WLAN activities 24 hours a day, 7 days a week, identifying unauthorized devices interfering with authorized devices, identifying authorized devices operating outside the 802.11 protocol, configuration parameters, and identifying the physical location of all 802.11 devices within the controlled space. In addition to the required 802.11 WLAN protocols, WIDS may also have the capability to detect or monitor traffic of cellular protocols, additional 802.11 protocols, 802.14 protocols, other low-latency protocols, and other long-range wireless protocols.

TEMPEST

Originally a cover name selected by an NSA engineer in the early 1950s, TEMPEST has since become a generic word (noun, verb, or adjective) used in relation to the unintentional emanations of classified information from equipment [15]. Any time a machine is used to process classified information electronically, the various switches, contacts, relays, power lines, and other components may emit electromagnetic or acoustic energy [16]. These emissions behave like small radio broadcasts that radiate through free space, or they may be induced even farther on nearby conductors like signal lines,

external power lines, telephone lines, or water pipes [16]. The potential for an adversary to capture and reconstruct the electromagnetic radiation makes it a security threat. TEMPEST_n, the noun, refers to the technical threat itself; whereas TEMPEST_v, as a verb, can be used to describe the mitigation to reduce the threat, and TEMPEST_{adj}, as an adjective, is used to describe anything related to the phenomenon [15]. The simplest solution to the TEMPEST_{adj} threat is to quantify the distance the TEMPEST_{adj} emanations are able to travel, and establish the zone required to be controlled, and this is the strategy that was adopted by the US military when the problem was first discovered by Bell Telephone during World War II [17]. By 1955, additional techniques were available to suppress TEMPEST_n, and it became possible to TEMPEST_v equipment to prevent it from radiating. In 1976, NSA created the Industrial TEMPEST Program (ITP), a government-industry partnership to develop TEMPEST_n-suppressed equipment to satisfy the government's growing need and reduce the prohibitively high costs for case-by-case mitigations [17]. A few years later, the North Atlantic Treaty Organization (NATO) agreed to a scheme to have vendors offer approved TEMPEST_{adj} products for catalog and sale to NATO and NATO member nations [18]. Despite the successful development of commercially available TEMPEST_n-suppressed equipment, when faced with the need to protect an entire facility housing a large quantity of intelligence-related equipment, an organization might choose to also apply TEMPEST_{adj} countermeasures to the building's construction to shield it in its entirety from TEMPEST_{adj} radiation. Regardless of risk mitigation security measures, TEMPEST_n is a phenomenon that can still be demonstrated and, therefore, a threat that still exists today.

The current state of the art for TEMPEST mitigations can be separated into two categories: prevention and detection. In the first category, the main countermeasures include shielding (putting shields around the equipment to block acoustic or electromagnetic signals), filtering (putting filters on power lines and other outbound connections), masking (structuring devices to emanate signals that don't distinguish between different data values), attenuation (adjusting devices to use less power, minimizing the signal it can radiate), and zoning (establishing a controlled area between equipment and potential adversaries) [19]. In the second category—detection—hardware is used to detect the emanations that could be used to capture and reconstruct

information-bearing signals. Different instrument sensors would be employed in order to capture the different TEMPEST emanations. For example, an oscilloscope may be used to detect voltage signals. A sound transducer could be used to capture acoustic signals. Various antennas and radios would be used to capture other electromagnetic signals in the RF spectrum. Because the wide variety of emanations that can fall under the TEMPEST umbrella, detection methods are often only deployed if there is a specific suspicion of a TEMPEST risk or threat.

Cell-site simulators

A cell-site simulator (also known as fake cell tower, rogue base station, "IMSI catcher," or by commercially available models such as the StingRay) is essentially made up of two components: a software-defined radio (SDR) for sending and receiving radio waves and a computing device to provide a network backend for simulating a cellular core network. Together, they function by transmitting as a cell tower, fooling nearby cellular devices (e.g., cell phones) into identifying the simulator as the best cell tower in the area and subsequently connecting to it. The cell-site simulator receives the unique identifying numbers [international mobile subscriber identity (IMSI)] of those connected devices. When used for criminal justice purposes, law enforcement will use the IMSI to identify its target and obtain signaling information related only to the particular phone that is being targeted [20]. More nefarious actors may connect to any phone, and subsequently perform man-in-the-middle attacks, placing malware between the device and their cellular network, to remove the phone from the real network, clone the target's identity, track location, extract or intercept data, and in some cases deliver spyware [20]. Specialized sensors can be used to detect cell-site simulators. In 2017, the Department of Homeland Security's National Protection and Programs Directorate conducted a limited pilot project that deployed sensors in the National Capitol region in order to identify and better understand potential IMSI catcher activities, and anomalous activity was observed that appeared consistent with IMSI catcher technology including at locations near the White House [22].

Wireless devices, TEMPEST, and cell-site simulators are only a few examples of RF security risks. While current mitigations provide a reasonably high level of confidence in the security of data in

US facilities, these and other threats still exist. Additionally, US data in mobile or temporary environments is more challenging to secure. All of the threats that are described in this article have common elements (signals that are anomalous or unexpected) and similar challenges (their ability to hide in a complex RF background environment).

The next generation of securing information

How do we improve our methods for safeguarding information and data? We know that attempts at data breaches might produce unexpected signals in our known RF environments. The seemingly obvious answer would be to scan all RF signals and analyze them for those that might come from or be used by bad actors. In reality, it would be impractical to install all of the hardware necessary to scan every possible frequency range constantly, and it would be computationally impossible to analyze all of the resulting terabytes of data per second in or near real-time. And our monitoring systems must remain agile to adapt to new evolutions in technology and new signals in our expected RF environment (e.g., 5G millimeter waves). An ideal solution would rely on a balance of efficient algorithms and affordable hardware to reduce the likelihood that an anomalous signal would go undetected.

Let's start with hardware. If the signals of interest are hidden within the expected overt signals and ambient signals that exist normally in the environment, then we need radio receivers to detect all of those signals to analyze. But what kinds of radios? A traditional radio is designed to transmit and/or receive signals in a specific range of frequencies, and the range of frequencies is mainly dependent upon the bandwidth of the radio's antenna and its analog components. For example, that radio in your car most likely receives signals between 540 kHz to 1700 kHz for AM stations and 88 MHz to 108 MHz for FM stations. Remember that the RF spectrum ranges from 3 kHz to 300 GHz (in other words: 3,000 Hz to 300,000,000,000 Hz) which is a very broad range, and suspicious signals may range over several orders of magnitude. If you were limited to traditional analog radios in order to receive signals across the entire RF spectrum, you would need a lot of radios. However, "cognitive radios" or "smart radios" allow us to expand the functionality of radio devices by increasing their frequency spectrum and sampling rates. The FCC has

defined cognitive radio as “a radio that can change its transmitter parameters based on interaction with the environment in which it operates” and cites SDR as an implementation strategy [22]. The FCC goes on to say that “cognitive radio can be viewed as a combined application of SDR and intelligent signal processing with functional elements of radio flexibility, spectral awareness, and the intelligence of decision-making.” SDR uses a small receiver to tune in and listen to radio signals at various frequencies and software to reconfigure itself as needed [24]. SDR is not the radio in and of itself; rather, it is a device that contains a tunable circuit that allows the user, through a software-based tuner, to sample only energy at the desired frequency and sampling rate and ignore all other signals [25]. Much like traditional radios, SDRs rely on antennas, and their utility is limited by the abilities of the antennas they are paired with. Higher-end SDR devices can monitor multiple channels, each providing bandwidth across extended frequency ranges. For example, the Ettus N320 is a networked SDR that has four channels, each providing up to 200 MHz of bandwidth, covering the frequency range from 3 MHz to 6 GHz [26]. Beyond SDRs, we can also use spectrum analyzers to digitize input signals and capture more of a frequency spectrum. The Signal Hound SM200C spectrum analyzer operates in two modes: 1) as a receiver providing in-phase/quadrature phase (I/Q)^a real-time samples with 40 MHz or 160 MHz bandwidth that can be tuned over a 100 kHz to 20 GHz range, or 2) as a spectrum analyzer that sweeps across 100 kHz to 20 GHz at 1 terahertz (THz) per second [27]. Given the right combination of antenna, software, and smart radios, we can receive signals from far more of the RF spectrum with less hardware. And less hardware means less expense.

Assuming we are able to capture a meaningful subset of the RF signals using smart radios, we would need to analyze data at rates approaching terabytes per second. It is a foregone conclusion to say that any analysis at this scale must be automated and most likely will need to employ advanced signal processing (e.g., statistical analysis, analysis of cyclostationary features, machine learning techniques) to be effective. Additionally, because the goal is not only to identify the suspicious signal but to also determine any bad intent and capture the perpetrator, the analysis would need to be completed in near real-time to be actionable. So who is developing this next generation of software algorithms? A number of academic, industry, and government groups are focused on RF

research for varying purposes. The NSA’s Laboratory for Telecommunication Sciences (LTS) is home to an RF research team that investigates, develops, and tests antenna designs and addresses critical challenges, including the detection of RF anomalies [28]. The US DoD’s Defense Advanced Research Projects Agency (DARPA) has invested in RF initiatives in recent years, including, but not limited to: Radio Frequency Machine Learning Systems (RFMLS) to address performance limitations and DARPA Advanced RF Mapping to provide situational awareness which includes the Distributed RF Analysis and Geolocation on Networked System (DRAGONS) project [29, 30]. Other collaborative efforts have been forged between DoD and academia, such as the RF Challenge at the Massachusetts Institute of Technology (MIT), in which the US Air Force has partnered with MIT to fund responses to its challenges, included a Cyber-RF Anomaly Detector Challenge [31]. More specifically to the purposes described in this article, the Intelligence Advanced Research Projects Activity (IARPA) has started a multi-year research effort aimed at developing smart radio techniques that can automatically detect and characterize RF signals potentially associated with attempted data breaches [32].

IARPA, the research and development arm of the Office of the Director of National Intelligence, is the corporate research and development resource for the intelligence community (IC) at large, and it invests in high-risk, high-payoff research programs to tackle some of the most difficult challenges of the agencies and disciplines in the IC. Through its Securing Compartmented Information with Smart Radio Systems (SCISRS) program, IARPA seeks to elevate the IC’s abilities to safeguard information and data that is generated, stored, used, transmitted, and received in secure facilities and beyond [33]. In the fall of 2021, IARPA awarded funding to five performers to develop smart radio techniques to detect and characterize suspicious/anomalous signals in complex RF environments [33]. Over a three-phase 42 month period, the SCISRS performers will develop methods to detect and characterize background and low-probability-of-intercept (LPI) signals such as direct sequence spread spectrum, frequency-hopping spread spectrum, smugglers, and burst (Phase I); altered and mimicked signal anomalies which are signals that resemble known overt signals in frequency, bandwidth, and pulse shape but are unrecognizable to the protocols established to receive them (Phase II); and unintended emissions such as anomalies in

a. In-phase/quadrature phase (IQ) is a mathematical model/representation of a modulated signal.


the emanation baseline arising from microprocessors or other electronics (Phase III) [34].

SCISRS performers will demonstrate the effectiveness of their methods in two test-bed laboratories established and managed by IARPA's collaborative partners. Each test bed houses an operating network, electronic equipment commonly found inside a secure office environment, and other real or synthesized sources required to contribute to both the overt signals and the incidental/unintended RF emissions typically found in an operational environment. While the test beds are located in different geographic areas (Pacific Northwest coast and Mid-Atlantic East coast), their proximity to urban settings, major international airports, radio stations, and other offices provide additional background noise that reflect real-world RF considerations in the two respective geographic locales. In addition to this, anomalous signals (including LPI signals, altered or mimicked signals, and abnormal unintended emissions), with frequencies ranging over several orders of magnitude, will be surreptitiously introduced by the test-bed teams. During the testing periods, performers will be expected to demonstrate their ability to command and control the onsite collection hardware, detect and characterize the ambient signals that make up the RF baseline in the test bed, and perhaps most importantly, characterize and detect anomalous signals that have been added to the ambient baseline.

SCISRS has just begun, and the first phase of testing is anticipated to occur in late 2022/early 2023, with the second and third phases to follow in subsequent 12 month periods. With the completion of each phase, the performers will deliver software to SCISRS repositories. If successful, the initiative will produce the next generation of software algorithms to analyze the massive amounts of data that can be streamed by smart radio systems.

Conclusion

Wired and RF communications systems have faced security threats since the interception of wired telegraph communications during the US Civil War and the later interception of wireless RF communications during the Russo-Japanese War. More recent security risks described in this article continue to persist through the present day. As telecommunications technologies advance, the introduction of more and/or novel signals will present new opportunities

for adversaries. And as the geopolitical landscape changes, new temporary mission-specific secure facilities may be needed. All of these factors, separately or in combination, contribute to the need to grow our abilities to monitor and detect anomalous RF signals. The SCISRS project is poised to deliver novel or improved software solutions to analyze more challenging signals, automate command and control, and potentially provide the means to identify previously undetectable threats. As long as researchers continue to stay vigilant towards future unknown risks, developers target today's known threats, and leaders are open to supporting and adopting new methods, we can continue to secure our nation's most classified information. 

References

- [1] National Institute of Environmental Health Sciences. "Electric and magnetic fields associated with the use of electric power," 2002 Jun. Available at: https://www.niehs.nih.gov/health/materials/electric_and_magnetic_fields_associated_with_the_use_of_electric_power_questions_and_answers_english_508.pdf.
- [2] Federal Communications Commission. "RF safety FAQ frequently asked questions about the safety of radio frequency and microwave emissions from transmitters and facilities regulated by the FCC." Available at: <https://www.fcc.gov/engineering-technology/electromagnetic-compatibility-division/radio-frequency-safety/faq/rf-safety>.
- [3] Centers for Disease Control and Prevention. "Health effects of radiation." 2021. Available at: <https://www.cdc.gov/nceh/radiation/health.html>.
- [4] Federal Communications Commission. "Wireless devices and health concerns." 2020. Available at: <https://www.fcc.gov/consumers/guides/wireless-devices-and-health-concerns>.
- [5] United States Environmental Protection Agency. "Non-ionizing radiation from wireless technology." 2021. Available at: <https://www.epa.gov/radtown/non-ionizing-radiation-wireless-technology#:~:text=Wireless%20technology%20uses%20radiofrequency%20energy,low%2Dlevels%20of%20radiofrequency%20energy>.
- [6] United States Environmental Protection Agency. "Non-ionizing radiation used in microwave ovens." 2021. Available at: <https://www.epa.gov/radtown/non-ionizing-radiation-wireless-technology#:~:text=Wireless%20technology%20uses%20radiofrequency%20energy,low%2Dlevels%20of%20radiofrequency%20energy>.
- [7] United States Environmental Protection Agency. "Electric and magnetic fields from power lines." 2021. Available at: <https://www.epa.gov/radtown/electric-and-magnetic-fields-power-lines>.

- [8] Federal Communications Commission. "Equipment authorization—RF device." Available at: <https://www.fcc.gov/oet/ea/rfdevice#:~:text=The%20FCC%20regulates%20radio%20frequency,9%20kHz%20to%203000%20GHz>.
- [9] Intelligence Advanced Research Projects Agency. SCISRS: Securing Compartmented Information with Smart Radio Systems. Available at: <https://www.iarpa.gov/research-programs/scisrs>.
- [10] Office of the Director of National Intelligence. "Intelligence community standard number 705-1, Physical and technical security standards for sensitive compartmented information facilities." 2010. Available at: <https://www.dni.gov/files/NCSC/documents/Regulations/ICS-705-1.pdf>.
- [11] U.S. General Services Administration. "1025.4 ADM sensitive compartmented information facility use (SCIF) policy." 2020. Available at: <https://www.gsa.gov/directive/sensitive-compartmented-information--facility-use-%28scif%29-policy>.
- [12] Department of Defense. "Department of Defense issuance # DoDI 8420.01 Commercial wireless local-area network (WLAN) devices, systems, and technologies." 2017. Available at: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/842001_dodi_2017.pdf.
- [13] National Security Agency. "Wireless intrusion detection system/wireless intrusion prevention system annex. | version 1.0." 2021. Available at: https://www.nsa.gov/portals/75/documents/resources/everyone/csfc/capability-packages/WIDS-WIPS%20Annex%20v1_0.pdf?ver=u0qF4d82XbjNg8-dNuUuA%3D%3D.
- [14] Coleman DD, Westcott DA, Harkins BE. *CWSP Certified Wireless Security Professional Study Guide: Exam CWSP-205, 2nd Edition ed.* John Wiley & Sons; 2016. ISBN: 978-1-119-21108-2.
- [15] Donahue TM. "Static magic or the wonderful world of TEMPEST or one man's static is another man's treasure!" *Cryptolog*. 1983;10(11). Available at: https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologs/cryptolog_84.pdf.
- [16] "TEMPEST: A signal problem. The story of the discovery of various compromising radiations from communications and Comsec equipment." *Cryptologic Spectrum Articles*. 1972;2(3). Available at: <https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-spectrum/tempest.pdf>.
- [17] "TEMPEST for every office." *Cryptolog*. 1983;10(11). Available at: https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologs/cryptolog_84.pdf.
- [18] NATO. "TEMPEST equipment selection process." Available at: <https://www.ia.nato.int/niapc/tempest/certification-scheme>.
- [19] Smith R. *Elementary Information Security, 2nd Edition ed.* Jones & Bartlett Learning Pub; 2015. ISBN-13: 978-1284055931.
- [20] Department of Justice. "Department of Justice policy guidance: Use of cell-site simulator technology," 2015 Sep 3. Available at: <https://www.justice.gov/opa/file/767321/download>.
- [21] Fong M. "Protecting high-level personnel from IMSI catchers." *Security Magazine*. 2020 Feb 21. Available at: <https://www.securitymagazine.com/articles/91767-protecting-high-level-personnel-from-imsi-catchers>.
- [22] Krebs C. Correspondence to Senator Wyden from Christopher Krebs. Available at: <https://www.wyden.senate.gov/imo/media/doc/Krebs%20letter%20to%20Wyden%20after%20May%20meeting.pdf>.
- [23] Federal Communications Commission. "Cognitive radio for public safety," [Online]. Available at: <https://www.fcc.gov/general/cognitive-radio-public-safety>. [Accessed December 2021.]
- [24] Donat W. *Explore Software Defined Radio*. Raleigh (NC): The Pragmatic Bookshelf; 2021. ISBN-13: 978-1680507591.
- [25] Wuff A. *Beginning Radio Communications: Radio Projects and Theory*. Cambridge (MA): Apress; 2019. ISBN-13: 978-1484253014.
- [26] Ettus Research. USRP N320. "Products." Available at: <https://www.ettus.com/all-products/usrp-n320>.
- [27] Signal Hound. "SM200A/B/C spectrum analyzer product manual." 2020. Available at: <https://signalhound.com/sig-downloads/SM200A/SM200-User-Manual.pdf>.
- [28] Laboratory for Telecommunication Sciences. "Research areas." Available at: <https://www.ltsnet.net/research>.
- [29] Davies J. "Radio frequency machine learning systems (RFMLS)." Defense Advanced Research Projects Agency. Available at: www.darpa.mil/program/radio-frequency-machine-learning-systems.
- [30] Rondeau T. "Advanced RF mapping (radio map) (archived)." Defense Advanced Research Projects Agency. Available at: <https://www.darpa.mil/program/advance-rf-mapping>.
- [31] Massachusetts Institute of Technology. "RF Challenge at MIT: Cyber RF anomaly detector challenge." Available at: <https://rfchallenge.mit.edu/challenge-3/>.
- [32] Intelligence Advanced Research Projects Activity. "IARPA announces launch of SCISRS program." 2021 Oct 26. Available at: www.iarpa.gov/newsroom/article/iarpa-announces-launch-of-scisrs-program.
- [33] Office of the Director of National Intelligence. "ODNI news release no. 36-21. IARPA announces launch of SCISRS program." 2021 Oct 26. Available at: <https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2021/item/2257-iarpa-announces-launch-of-scisrs-program>.
- [34] Intelligence Advanced Research Projects Activity. "IARPA-BAA-20-03." 2020 Sep 28. Available at: <https://iarpa.gov/index.php/research-programs/scisrs/scisrs-baa> and <https://sam.gov/opp/f2e9128015684101b2021e04d37516c7/view>.