

Cyber-Physical Attack Using High Power RF in Havana, Cuba

Allyffazzkkamn Argudo and Ghislaine Nasibu Mwana

Marymount University, Alexandria Virginia, USA

ara47724@marymount.edu

gmn64459@marymount.edu

Abstract: Global communications have relied heavily on fiber-optic cables. Satellite communications have become the norm for areas that are not highly populated or easily reached by conventional wires. The availability and use of satellite communications systems have had a limited market; with this limitation, the need for open development of each vendor's software never gained traction. This led to weaknesses not being discovered until a flaw was made public in a systems breach that affected the end users. Wireless communications that rely on microwaves lead to the use of malware to provide an override to normal operations of the equipment. As the issue of Stuxnet would allow for the override of the safety settings of satellite terminals, the malware could even be deployed remotely through a system update. The weaponization of such systems is now a point of concern. Previous studies have shown that naval satellite communications systems can be a weapon by removing the software power limitations (McKay, 2021). As satellite systems on ships can be larger due to being fixed, transmission power generation may be more significant. This study considers the land-based mobile systems deployed against any target and quickly dismantled and removed. Can land-based mobile satellite communication systems affected by Stuxnet or manually altered yield the same power output, and at what range will it affect human tissue? This is believed to be the case with the ongoing investigation. The survey results showed that mobile equipment could be dangerous to human tissue at distances easily achieved by mobile terminals, especially if the target is a fixed location like a building with large glass windows that R.F. power can penetrate easily.

Keywords: Replication Study, Cyber-Attack, SATCOM, VSAT, BGAN, HIRF

1. Introduction

Maritime trade is critical to the global economy. Globally, 90% of the world's traded goods move thru waves (Arampatzis, 2021). Cyber threats in the Maritime industry can seriously affect the national economy due to the digitalization of the infrastructure, which makes it vulnerable. In the U.S., it accounts for a third of the country's economy. The increased dependence on the internet equates to increased vulnerability. Maritime communications between cruise ships or cargo shipping depend mainly on non-terrestrial communication. Terrestrial communications rely on satellite communications to provide access to more remote areas where communications are required. Military, government agencies, and commercial entities must have contacts through reliable means as some of the market locations may not have steady and reliable traditional communication networks.

SATCOM network plays an essential role in global telecommunications systems. They are the roots of various services used on vessels to guarantee safety and security (Caprolu et al., 2020). In the maritime industry, SATCOM is seen as a global WIFI network. "Its core is linked together through network nodes just as a regular office network would be; except, in this case, R.F. energy is used in place of cables, which propagates data payloads throughout great distances in air and space on the backbone of SATCOM devices, satellites and ground nodes" (McKay, 2021). SATCOM network provides reliable communications to cruise ships and maritime vessels. Degraded communication is the major challenge in satellite communication systems. Vulnerabilities, in this case, include design flaws that allow access to the SATCOM by letting remote attackers intercept, manipulate, block, and in some cases, take complete control.

Problem Statement: Compromised satellite communication terminals, whether remotely accessed due to software vulnerabilities or controlled on-site due to a lack of physical safety mechanisms, can yield High-Intensity Radio Fields (HIRF). A by-product of exceeding safety limits can cause harm to human tissue in direct relation to the proximity of the source.

2. Literature review

2.1 Introduction

This research utilizes similar parameters as those provided by McKay (2021). The land-based study of how HIRF is achieved thru smaller mobile terminals that can easily be concealed and aimed at targets of interest was added.

2.2 Defining Cyber-physical attacks

"The rocket worked perfectly except that it landed on the wrong planet" – Werner von Braun stated this when his invention was turned into a weapon of war. As with any new technological development thought to aid humanity, the same concept can then be used to harm. Cyber-physical attacks are such a new development that many possible outcomes have yet to be documented. Cyber-physical attacks have become part of real life; what once was a science fiction idea is now a daily concern as the internet of things (IoT) has grown. The exploitation weaknesses within a physical system connected to the internet are what cybercriminals focus on with the intent to alter or take over the functionality of a physical system. For the scope of this study, cyber-physical attacks will focus on high radiofrequency radiation and the possibility of being able to cause harm to biological specimens through the alteration of energy applied to a system from naval equipment and land-based equipment.

2.3 Satellite Hacking

In his study "Satellite network hacking & security analysis," published in 2016, Adam Hudaib discussed satellite hacking in-depth. One central point that Hudaib made is that most satellites are old and critical infrastructure, and these lapses make them vulnerable to hacking. Huda states that "older satellites might be more vulnerable as defenses may be less stringent, security flaws can be exposed over time, and there are limited means to patch those flaws once it is in orbit" (Hudaib, 2016, p34). Huda has broken-down satellite hacking into four main types: (1) Jamming: refers to flooding or overpowering a signal, transmitter, or receiver so that the legitimate transmission cannot reach its destination. (2) Eavesdropping: allows a hacker to see and hear what is being transmitted. (3) Hijacking: the unauthorized use of a satellite for transmission or seizing control of a signal and replacing it with another. (4) Control: taking control of part or all of the TT&C ground station (Hudaib, 2016, p38). "Last Call for SATCOM Security" springboards off a 2014 white paper, "A Wake-up Call for SATCOM Security. Santamarta (2014) provides insight into how satellite systems for all locations have vulnerabilities that were not addressed, as cybersecurity was a field being developed. Most non-state attackers were not focused on utilizing SATCOM systems to conduct any attack, mainly due to the volatile stability. SATCOM systems are turned off when not in use since satellite systems are charged per hour used, or fuel consumption to power generators would not be efficient when a communications system is not required. The studies' authors provided insight into the significant vulnerabilities of aerial, maritime, military/land, and space systems. The tables below show the information matrix that the authors of the study compiled:

Table 1: Attack Vector Identified

Industry	Security Risk	Flight Safety Risk	RF Risk	Likelihood	Attack Vector
Aviation	Yes	No*	No*	Medium	Remote
Maritime	Yes	N/A	Yes	High	Remote
Military	Yes	N/A	No	Medium	Remote

*Based on input received from the Aviation industry through the A-ISAC and our own research

Table 2: Vulnerability Outcome

Industry	Threat
Aviation	<ul style="list-style-type: none"> • Ability to disrupt, intercept or modify non-safety communications such as In-Flight WiFi* • Ability to attach crew and passenger devices. • Ability to manipulate SATCOM antenna positioning and transmissions.
Maritime	<ul style="list-style-type: none"> • Ability to disrupt, intercept or modify onboard satellite communications. • Ability to attach crew's devices. • Ability to control SATCOM antenna positioning and transmissions. • Ability to perform cyber-physical attacks using HIRF.
Military	<ul style="list-style-type: none"> • Ability to pinpoint the location of military units. • Ability to disrupt, intercept or modify satellite communications. • Ability to perform cyber-physical attacks using HIRF.
Space	<ul style="list-style-type: none"> • Ability to disrupt satellite transponders.

* Typically pilot and co-pilot do not use it. In-Flight WiFi is normally used by flight attendants for PAX and PCI transactions. * Configurations may vary the impact. Santamarta 2018, p2. Appendix I

Probable capabilities of state-level entities were not provided. The study showed many vulnerabilities in many commercial systems only. The authors urged the parties whose equipment was studied to fix the deficiencies. However, as most satellite systems are costly to develop, most companies that have spent many resources in developing and deploying these systems have proprietary protocols that are closed source, making them undocumented. While there is something to be said about security thru obscurity, once an adversary can figure out a system, the ability to react or have other entities analyze the system's weaknesses is hindered by the same security thru obscurity. One example of cooperation was INMARSAT when it cooperated with a third party to solve a problem with the marine communications system. A back door was discovered that allowed for remote installation of the unauthorized firmware update (Caprolou, et al., 2020, p4). This kind of action yields the inevitable possibility of being able to remotely program a VSAT dish and other programmable antennas and overriding pre-programmed power transmission and position of antennas. While many systems utilized in maritime and ground operations may have newer hardware as of 2016, there are 1046 satellites in space; most have hardware and programming relevant to the technology of the 1980s. The issue of having ground equipment that meets today's communications standards while still being able to translate the information to older systems creates avenues of attack. About 1.4 million VSAT terminals are connected to satellites at any given time. That sheer quantity of terminals establishes a target of opportunity. Most maritime terminals that are part of this replication study have had known issues. The land terminals need not have any problems as a nefarious actor can purchase a system and aim it at a target manually while overriding safety protocols of the equipment thru physical manipulation or software manipulation.

3. Communications equipment

For this replication study, all BGAN and VSAT terminals are considered relevant. A summary of observed cyber issues for many systems has been provided in the tables 3 and 4 below. By adding newer land systems that have not been tested to have cybersecurity issues, this study assumes that software can be remotely accessed, along with in-person adjustments.


Table 3: HawkEye 3610
HAWKEYE™ 4 LITE
1.3 Meter Flyaway VSAT



ANTENNA			
Aperture	1.3m parabolic		
Optics	Center fed	Auto-Acquire	
Elevation	Manual	5 to 90 degrees	
Azimuth	90 degrees	120 degrees	
LEO/MEO Capable	N/A	Yes	
PACKED SYSTEM WEIGHT (950MP W/AC POWER SUPPLY)			
Weight	Two cases, <84lbs		
Dimensions	All cases: <70 linear in		
RF PERFORMANCE			
RF BAND	X	Ku	Ka
Transmit (GHz)	7.90 - 8.40	13.75 - 14.50	29.0 - 31.0
Receive (GHz)	7.25 - 7.75	10.95 - 12.75	19.20 - 21.20
Polarization	Circular	Linear	Circular
G/T	16.7 dB / K	20.5 dB / K	21.8 dB / K
EIRP (Standard Power)	51.7 dBW	54.8 dBW	56.6 dBW
EIRP (High Power)	54.7 dBW	58.2 dBW	59.9 dBW

MODEM INTEGRATION	
Supported Modems	iDirect 950mp (Evolution and Velocity)
	ViaSat CBM-400 (Linkway and EBEM)
	L3Harris MPM-2500 (NCW)
	External Modem
Future Modems	iDirect450 mp
	Comtech 5650C
	L3Harris Protected Anti-Jam Tactical Satcom (PATS)

Table 4: Star Win, 2021



Technical Specification:	
Type of antenna panel	Flat array antenna
Frequency Range	Tx 13.75 ~ 14.50 GHz Rx 10.95 ~ 12.75 GHz
Polarization	Linear polarization
VSWR	≤ -15dB
Cross Polarization Isolation	≥ 35dB
Tx/Rx Polarization Isolation	≥ 85dB
Satellite Searching Mode	Satellite parameter presetting GPS/Inclinometer guiding
Tracking Time	<120 S
BUC mounted panel	2\3\4\8\16W
Antenna Power Resistance	≥ 100W
Power Supply	AC 90-240V (DC optional)
Antenna Panel Size / Weight	540 x 570 x 34mm / 5Kg x 2
Total Antenna Weight	24KG

4. Harm to Biological Tissue

Published scientific literature on possible biological harm from animal or human exposure to R.F. energy. For many years now, it has been known that radio energy of sufficient intensity can produce heating in substances with finite conductivity, such as biological tissue. High R.F. levels can harm biological tissue due to the human body's inability to cope with or dissipate the excessive heat it generates. In other words, the specific physical reactions associated with R.F. field exposure are generally related to the energy absorption rate or the intensity of currents and internal electric fields. The FCC has conducted studies that show biological tissue's specific absorption rate of radio wave energy. The Specific Absorption Rate (SAR) is usually expressed as watts/kilogram. The safe rate of abortion for a human body is considered to be 0.04 W/kg OET, 56 [20] within a given period, reflected as 30 minutes. Table 5 below has specific information on absorption rates at different frequencies (Rooker, 2008) within a given period, reflected as 30 minutes. The table below has detailed information on different absorption rates at different frequencies. Some examples of physical harm come from the attacked that happened to the Indian army with the utilization of microwave pulses (Marlatt, 2005). Furthermore the National Academies of Science has concluded that the attack on the embassy in La Habana Cuba utilized radio frequency waves (Santamarta, 2014).

Table 5: Limits for Localized Exposure

Table 2. FCC Limits for Localized (Partial-body) Exposure	
Specific Absorption Rate (SAR)	
Occupational / Controlled Exposure	General Uncontrolled / Exposure
(100 kHz - 6 GHz)	(100 kHz - 6 GHz)
< 0.4 W/kg whole-body	< 0.08 W/kg whole-body
<8 W/kg partial-body	< 1.6 W/kg partial-body

Table 6: Limits for Maximum Permissible Exposure

Table 1. FCC Limits for Maximum Permissible Exposure (MPE) (A) Limits for Occupational / Controlled Exposure				
Frequency Range (MHz)	Electric Field Strength (E) (V/m)	Magnetic Field Strength (H) (A/m)	Power Density (S) (mW/cm ²)	Averaging Time E ² , H ² or S (minutes)
0.3 - 3.0	614	1.63	(100)*	6
3.0 - 30	1842/r	4.89/r	(900/f ²)*	6
30 - 300	61.4	0.163	1.0	6
300 - 1500	-----	-----	f/300	6
1500 - 100,000	-----	-----	5	6
(B) Limits for General Population / Uncontrolled Exposure				
Frequency Range (MHz)	Electric Field Strength (E) (V/m)	Magnetic Field Strength (H) (A/m)	Power Density (S) (mW/cm ²)	Averaging Time E ² , H ² or S (minutes)
0.3 - 1.34	614	1.63	(100)*	30
1.34 - 30	824/r	2.19/r	(180/f ²)*	30
30 - 300	27.5	0.073	0.2	30
300 - 1500	-----	-----	f / 1500	30
1500 - 100,000	-----	-----	1.0	30

f = frequency in MHz

*Plane-wave equivalent power density

Note 1: Occupational / controlled limits apply in situations in which person are expose as a consequence of their employment provided those persons are fully aware of the potential for exposure and can exercise control over their exposure. Limits for occupational / controlled exposure also apply in situations when an individual is transient through a location where occupational / controlled limits apply provided he or she is made aware of the potential exposure.

Note 2: General population / uncontrolled limits exposures apply in situations in which the general public may be exposed, or in which persons that are exposed as a consequence of their employment may not be fully aware of the potential for exposure or cannot exercise over their exposure.

5. Deployment

The studied systems have already been placed within ships, aircraft, and land. Many commercial entities have heavily relied on maritime systems for communications to shore anywhere in the world. The Intellian GX60TM is a system installed in large cruise ships with antennas capable of handling large data transmissions. Intellian GX 100TM is another approach utilized in maritime activities such as cruise ships. The capacity for voice and data is more significant and can be used with different size antennas. The L3Harris Hawkeye 4TM lite is a system that can be rapidly deployed on land and provided with concealment inside larger structures that allow radio waves to travel through. Starwin flat panel system, meant for fast deployment and easy setup and tear down due to the shape. Only the tripod has to be removed for transport. The body alone allows for easier concealment from buildings and can even be placed within a vehicle to make it mobile and concealable. One major issue with these systems is the antenna size and distance for the field of effect. The smaller the antenna, the closer the target

needs to reach the necessary levels to cause harm due to the antenna's limitations of energy concentration and focal point.

6. Research methodology

Our study's methodology tried to reproduce McKay (2021) wherever possible. We used the same measures and identical treatment statistics as the original author's study, a quantitative observational simulation depicted by formulaic-driven simulations. The concern of the study is the possibility of thermic damage to a human or other biological tissue fluids.

6.1 Data Collection Set

The data collection will focus on the maritime systems with end frequencies due to the power needed to produce such frequencies. The GX60 system will provide the methodology for replicability. GX 100 is limited by propagation's possible power output at 10 watts. V80G system is built with varying power ranges; however, it provides this ability at lower frequencies. Yet the variable wattage of 4W, 6W, 8W, and 16W. For this study, the power level will be raised to 100 watts as it can override systems to this output level. To include newer land-based systems than can easily be assembled, hidden, and manually aimed at a specific target. The propagation of radiofrequency radiation can be calculated by the Far-Field Region formula as described in the FCC OET 65 Bulletin. The formulas below would provide the distance from which each antenna may propagate the radiofrequency radiation.

$$S = \frac{PG}{4\pi R^2}$$

where: S = power density (in appropriate units, mW/cm²)

P = power input to the antenna (in appropriate units, e.g., mW)

G = power gain of the antenna in the direction of interest relative to an isotropic radiator

R = distance to the center radiation of the antenna (appropriate units, e.g., cm)

or:

$$S = \frac{EIRP}{4\pi R^2}$$

Where: EIRP = equivalent (or effective) isotropically radiated power

Another factor to consider comes from the second hypothesis. The ability to calculate radiofrequency radiation exposure from multiple frequencies. As satellite communication systems can broadcast more than one frequency. The formulas come from the International EMF project, which has studied this health issue and environmental factors of static radiofrequency radiation.

SIMULTANEOUS EXPOSURE TO MULTIPLE FREQUENCY FIELDS

It is important to determine whether in situations of these exposures are additive in their effects. Additivity and electrical stimulation, and the basic restrictions below should be met. The formulae below apply to relevant frequencies under practical exposure situations. For electrical stimulation, relevant for frequencies up to 10 MHz, induced current densities should be added to

$$\sum_{i=1 \text{ Hz}}^{10 \text{ MHz}} \frac{J_i}{J_{L,i}} \leq 1,$$

For thermal effects, relevant at 100kHz, SAR and power density values should be added according to:

$$\sum_{i=100 \text{ kHz}}^{10 \text{ GHz}} \frac{SAR_i}{SAR_L} + \sum_{i>10 \text{ GHz}}^{300 \text{ GHz}} \frac{S_i}{S_L} \leq 1$$

where:

J_i = the current density induced at frequency i;

$J_{L,i}$ = the induced current density restriction at frequency i as a given in Table 4;

SAR_i = the SAR caused by exposure at frequency i ;

SAR_L = the SAR limit given in Table 4;

S_L = the power density limit given in Table 5; and

S_i = the power density at frequency i .

Calculating the near and far-field of an antenna, the formulas that the FCC published on OET bulletin 65 are shown in the table below.

For this study, the near-field energy is not being measured as it would have the biological matter close to the antenna. The far field is of interest as it is outside what most persons would consider a safe range, making it the ideal place to deliver an attack to those not suspecting. While distance calculations show that the area with the highest effect is considered near-field, as shown in the formula below OET, 65 (White House Trump Administration, 2020). For this study, the far-field effect will be observed and measured.

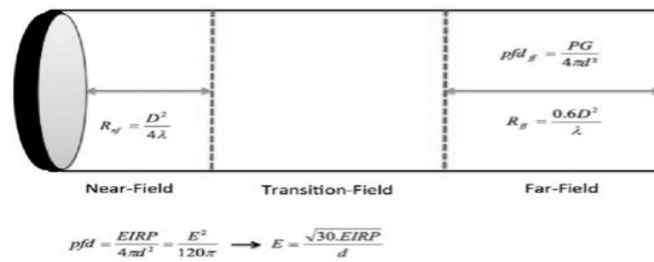


Figure 1: Energy Field

6.2 Tools to measure the results of the study

EIRP calculator (Effective Isotropic Radiated Power) is the measured radiated power of an antenna in a specific direction. It is also called Equivalent Isotropic Radiated Power. It is the output power when the Antenna concentrates a signal into a smaller area. The EIRP can consider the losses in the transmission line and connectors and includes the antenna's gain represented in dB. Entering the transmitted power, cable loss, and antenna gain to calculate the EIRP (Effective Isotropic Radiated Power) R.F., 2018 (National Academies of Sciences, 2020).

Antenna Factor and Gain Calculator

The antenna factor provides the ratio of the incident Electromagnetic Field to the output voltage from the antenna and the output connector. The Gain factor is the ratio of the signal received or transmitted by a given antenna compared to an isotropic or dipole antenna. Antenna gain can only be achieved by making an antenna directional, with better performance in one direction than in others Systems, 2018 (Marlatt, 2005).

7. Findings / Results

The values have been converted from voltage to watts as calculations for radio waves are compiled in wattage.

The study considers the average size of a human and weight to be about 150 lbs, based on the calculations conducted by the FCC. It should be noted that specific body parts /organs, due to their more direct exposure to the environment and greater volume of water per cm², may be affected faster than organs further inside the body. The conductivity of the human body is set at 0.6 s/m, and parts of the body can conduct at a higher rate, such as the cerebral spinal fluid at 1.79 s/m Baumann (1997). Calculating the Specific Absorption Rate (SAR), the density of a 150lbs person will be set at the standard 1010 kg/m³. The electric field calculation from EIRP will be multiplied by 0.6 s/m divided by the density of 1010 kg/m³.

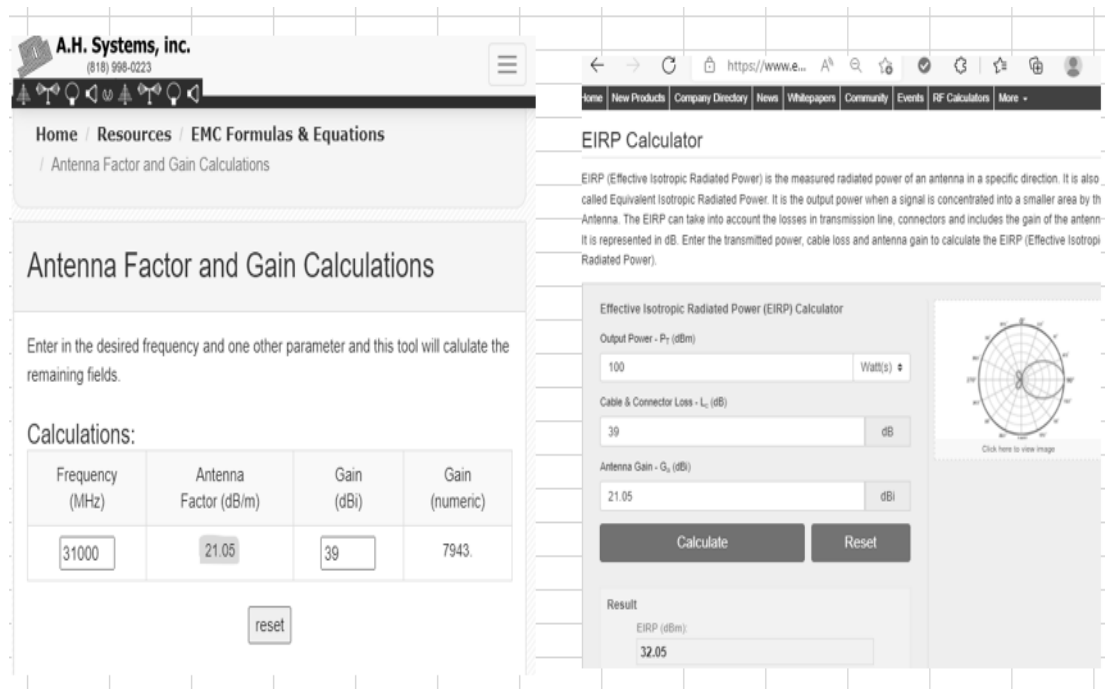


Figure 2: Calculations for L3Harris Hawk 4 Lite

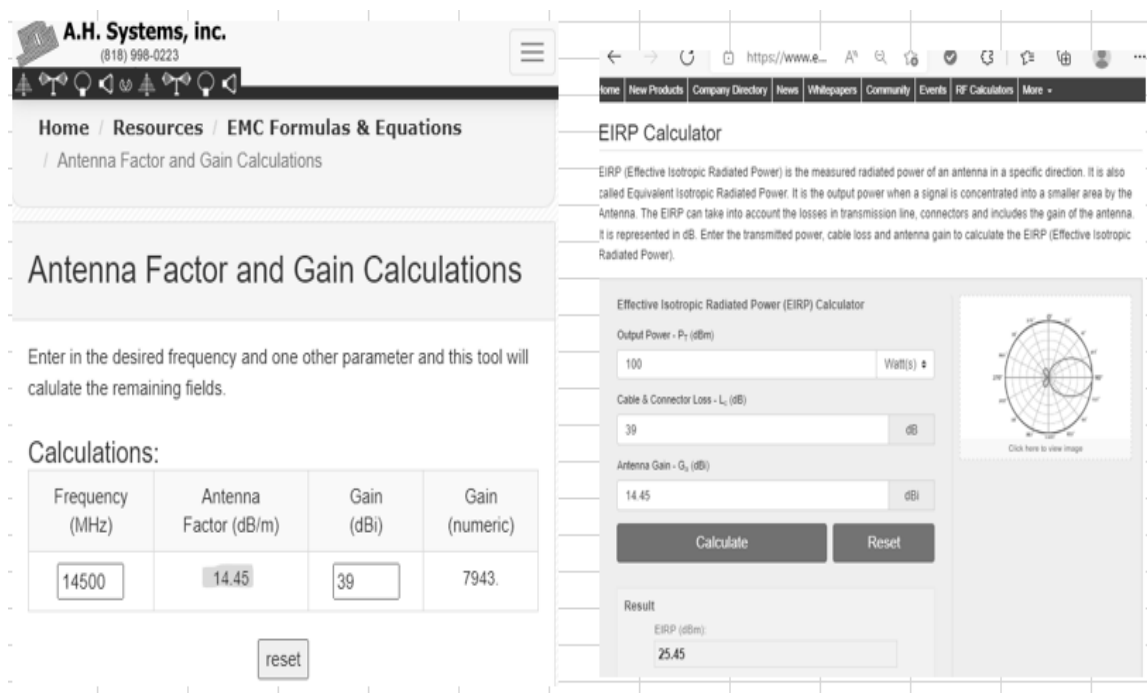


Figure 3: Calculations for Starwin High Gain Portable

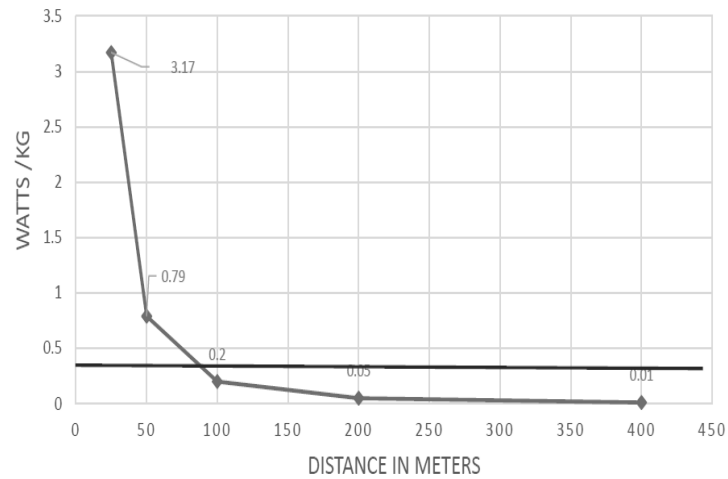


Figure 4: GX 60 SAR W/KG

Hypothesis H_a , the value of SAR, is met at a distance of fewer than 100 meters. This value provides validation while showing that a cruise ship could become a significant area target where people can be radiated.

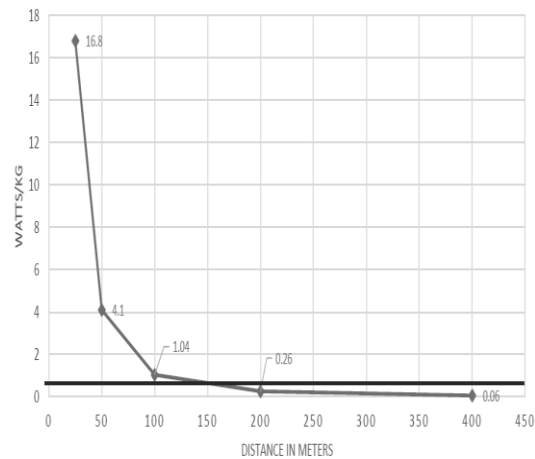


Figure 5: GX 100 SAR W/KG

Hypothesis H_a , the value of SAR, is met at a distance of fewer than 160 meters. This value provides validation while showing that a cruise ship could become a prominent area target where people can be radiated.

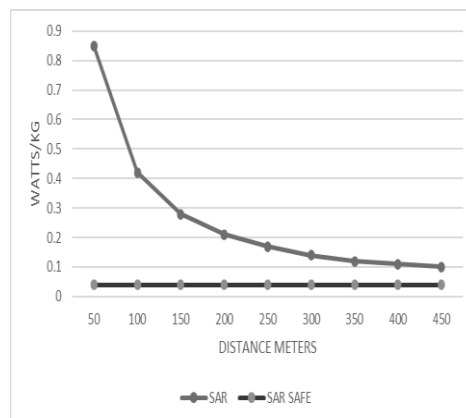


Figure 6: L3Harris HackeyeTM 4 Lite

Hypothesis H_a , the value of SAR, is met at a distance of fewer than 400 meters. This value provides validation while showing that a land-based system could be used to target specific areas.

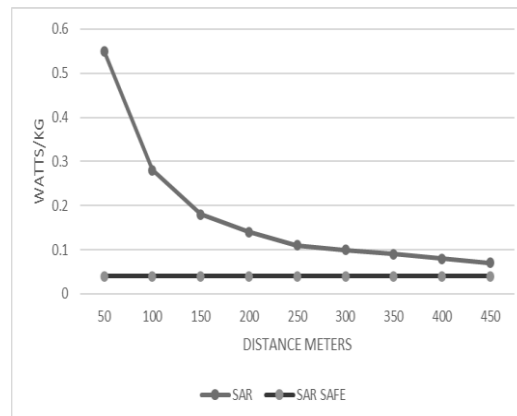


Figure 7: Starwin High Gain Terminal

Hypothesis H_a , the value of SAR, is met at a distance of fewer than 150 meters. This value provides validation while showing that a land-based system could be used to target specific areas.

The results of this replication study corroborate what the original author provided as a hypothesis for the dangers of specific absorption rates (SAR). All the systems studied in this virtual environment provided feedback of power that shows serious harm can come to biological tissue; in most cases, human beings, due to the high SAR, at times, the values were hundreds of times higher than the safe limit of exposure. Further adds to the theory that satellite communication equipment can be turned into a weapon given enough knowledge of radio wave theory, cybersecurity, the location of the attack, and the intended target. Static locations such as ships, buildings, or open recreational areas can be flooded with radio wave radiation that can, over time, cause illness to those that are continuously exposed. One example of this attack was conducted at the United States Embassy in Habana, Cuba. As per the image below, the distance from the embassy to other buildings is less than 38 meters, well within the highest output radius of all tested systems. If an antenna is pointed at the facility for a prolonged period, personnel assigned to that embassy can start showing symptoms related to radio wave radiation.

United States Embassy, La Habana Cuba



Figure 8: map calculator, 2022



Figure 9: google maps, 2022

8. GAP / Limitations

There are some limitations to this replication study. While our replication study attempted to address the gaps and build on the authors' recommendations McKay (2021), this study had notable limitations. First, just like in the author's original work, we could not conduct a physical test of the SATCOM equipment. Studies like this should be extended from simulation to field testing. Second, due to the software's proprietary nature, we cannot thoroughly test the hardening of the software of each system. Third, manufacturers did not provide the maximum tolerance for the high-power amplifiers, thus making it unknown if the equipment could withstand an overload before becoming inoperable. In these scenarios, most attackers do not concern themselves with how

long equipment may operate. However, when long-term overt and denial actions are taken, the need to ensure the viability of higher-end tolerance is required.

9. Conclusion

In conclusion, our primary goal in conducting this replication study was to evaluate the robustness of cyber-physical attacks using high-intensity radiated fields. Our replication shows that the results of McKay (2021) study are exciting and helpful for future research. After completing our study, we feel that it is evident that there is much scope for research on cyber-physical attacks. It is paramount to be aware that the satellite system's cybersecurity challenges are enormous in cybersecurity and human defense. Furthermore, the maritime or aerospace industry has also developed a lot so have the risks that weigh on them. This replication study reinforces the argument that further studies are needed on this matter and greater cooperation between manufacturers and cybersecurity analysts.

Definition of Terms

- Decibel (dB). Ten times the logarithm to the base ten of the ratio of two power levels (OET 65 (1997), pp.2-5).
- EIRP (Effective Isotropic Radiated Power) is the measured radiated power of an antenna in a specific direction
- Gain (of an antenna) is a ratio that is usually expressed in decibels of the power required at the input of a loss-free reference antenna to the power supplied to the input of the given antenna to produce, in a given direction, the same field strength or the same power density at the same distance. When not specified otherwise, the gain refers to the direction of maximum radiation. Gain may be considered for a specified polarization. Gain may be referenced to an isotropic antenna (dBi) or a half-wave dipole (dBd) (McKay (2021), pp 44; OET 65 (1997), pp.2-5).
- Hertz (Hz). The unit for expressing frequency, (f). One hertz equals one cycle per second. Magnetic field strength (H). A field vector equals the magnetic flux density divided by the medium's permeability (OET 65 (1997), pp.2-5).
- High-Intensity Radiated Fields (HIRF) are those that can produce, within the frequency domain from 10kHz to 40 GHz, an electromagnetic field strength sufficient to cause a SAR rating of 0.4 w/kg or above (McKay, 2021).
- SATCOM: a global Wi-Fi network, the roots of various services used on vessels to guarantee safety and security (Caprolu et al., 2020).
- Specific absorption rate (SAR) measures the energy absorbed by (dissipated in) a total mass contained in a volume element of dielectric materials such as biological tissues. It is usually expressed in watts per kilogram (W/kg) or per gram (mW/g). Human exposure to RF fields is based on SAR thresholds where adverse biological effects may occur. When the human body is exposed to an RF field, the SAR experienced is proportional to the squared value of the electric field strength induced in the body (McKay (2021) , pp 48; OET 65 (1997), pp.2-5).

References

- Arampatzis, A., 2021. U.S. national cybersecurity plan to SAFEGUARD Maritime Sector
<https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/us-national-cybersecurity-plan-safeguard-maritime-sector/>
- Baumann, S., et al., 1997. The electrical conductivity of human cerebrospinal fluid at body temperature. IEEE Transactions on Biomedical Engineering, 44(3), 220-223. doi:10.1109/10.554770
- Caprolu, M., et al., 2020. Vessels Cybersecurity: Issues, Challenges, and the Road Ahead. IEEE Communications Magazine, 58(6), 90-96. doi:10.1109/mcom.001.1900632
- Cleveland, R. F., Jr., 2001. Evaluating Compliance with FCC Guidelines for Human Exposure to Radiofrequency Electromagnetic Fields https://transition.fcc.gov/Bureaus/Engineering_Technology/Documents/bulletins/oet65/oet65.pdf
- Electromagnetic Fields (EMF)., 2016. Retrieved from <https://www.icnirp.org/cms/upload/publications/ICNIRPrfgdl2020.pdf>
- FCC. Radio Frequency Safety., 2017. Retrieved from <https://www.fcc.gov/general/radio-frequency-safety-0#block-menu-block-4>
- Giri, D., 2004. High-Power Electromagnetic Radiators: Nonlethal Weapons and Other Applications. Harvard University Press. Cambridge, Massachusetts. 2004
- Greenburg, M. and Chalk, P., 2006. Maritime Terrorism: Risk and Liability. RAND Center for Terrorism and Risk Management Policy. Arlington, Virginia

- Gurevich, V., 2005. Electromagnetic Terrorism: New Hazards. Israel Electric corp., Central Electric Laboratory. Haifa, Isreal.http://repository.kpi.kharkov.ua/bitstream/KhPI-Press/11280/1/EE_2005_4_Gurevich_%D0%95lectromagnetic.pdf
- Hudaib, A. A., 2016. Satellite Network Hacking & Security Analysis. International Journal of Computer Science and Security, 10(1), 8-55.
- Livingston, D. and Lewis P., 2016. Space the Final Frontier for Cybersecurity. Chatham House. Retrieved from <https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-Livingstone-lewis.pdf>
- Loukas, G., 2015. Cyber-Physical Attacks: A Growing Invisible Threat. Butterworth-Heinemann. Oxford, United Kingdom
- Marlatt, G., 2005. Directed Energy Weapons (DEWs): A Bibliography. Calhoun NPS.https://calhoun.nps.edu/bitstream/handle/10945/6980/Oct05-DEW_biblio.pdf?sequence=1
- Manz, B., 2017. RF Energy Is Finally Cooking. Retrieved from <https://www.mwrf.com/community/article/21848854/rf-energy-is-finally-cooking>
- McKay, R. W., 2021. Cyber-Physical Attack Using High-Intensity Radiated Fields (Doctoral dissertation, Marymount University).
- National Academies of Sciences, Engineering, and Medicine., 2020. An assessment of illness in U.S. government employees and their families at overseas embassies. Washington, DC: The National Academies Press. <https://doi.org/10.17226/25889>
- National Post Staff., 2020. China used 'microwave' pulse weapon to Force Indian soldiers Off HIMALAYAN hilltops: Report. Retrieved from <https://www.msn.com/en-ca/news/world/china-used-microwave-pulse-weapon-to-force-Indian-soldiers-off-Himalayan-hilltops-report/ar-BB1b5QtW>
- OET 56, Federal Communications Commission., 1999. Questions and Answers about Biological Effects and ... Retrieved from https://transition.fcc.gov/Bureaus/Engineering_Technology/Documents/bulletins/oet56/oet56e4.pdf
- OET 65, Federal Communications Commission., 1997. Evaluating Compliance with FCC Guidelines for Human Exposure to Radiofrequency Electromagnetic Fields. Retrieved from <https://transition.fcc.gov/bureaus/oet/info/documents/bulletins/oet65/oet65.pdf>
- Rooker, JW., 2008. Satellite Vulnerabilities. Defense Technical Information Center. Retrieved from <http://www.dtic.mil/docs/citations/ADA507952>
- Santamarta, R., 2018. Last Call for SATCOM Security - ioactive.com. Retrieved from <https://ioactive.com/wp-content/uploads/2018/08/us-18-Santamarta-Last-Call-For-Satcom-Security-wp.pdf>
- Santamarta, R., 2014. A Wake-up call for SATCOM Security – ioactive.com. Retrieved from https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf
- Santamarta, R., 2014. SATCOM Terminals Hacking by Air, Sea, and Land –ioactive.com. Retrieved from <http://blackhat.com/docs/us-14/materials/us-14-Santamarta-SATCOM-Terminals-Hacking-By-Air-Sea-And-Land-WP.pdf>
- United States Navy. Radio frequency-radiation. Retrieved from https://www.public.navy.mil/navsafecen/pages/acquisition/radio_frequency-radiation.aspx
- White House Trump Administration., 2020. National archives and Records Administration. Retrieved from <https://trumpwhitehouse.archives.gov/briefings-statements/statement-national-security-advisor-Robert-c-Obrien-regarding-national-maritime-cybersecurity-plan/>
- National Academy of Sciences and Medicine., 2020. National Academy of Sciences and Medicine', Retrieved from Front Matter | An Assessment of Illness in U.S. Government Employees and Their Families at Overseas Embassies |The National Academies Press