HITB SECCONF SIN-2021

Gazing Ahead: What Modern RF Combat Looks Like in the Next Decade

Harshit Agrawal

RF Security Researcher and Graduate Student, Boston University

TRACK 1

/Speaker/Harshit/> whoami

```
USER INFORMATION
----------------------------------------------
Harshit Agrawal
RF Security Researcher
----------------------------------------------
Primary Research area includes:
RF Security, Drone Security, Electronic Warfare,
SIGINT, and IOT Security

Speaker at conferences like RSAC USA, DEFCON USA
HITBSecConf Amsterdam, Cyberweek UAE,
----------------------------------------------

Twitter: @harshitnic
Email: harshit[dot]nic[at]gmail[dot]com
LinkedIn: https://linkedin.com/in/harshitnic
```

To be discussed...

- IoT Has a Transformational Impact across Vertical Sectors
- Internet of Radio Vulnerabilities
- CIA Triad for IoT Security
- IoT Threat Map
- Cyber Electronic Warfare
- Emerging tools of Cyber Reconnaissance
- Internet of Military Things (IoMT)
- Autonomous Weapon Systems

Where CCTV cameras identify & stop excessive force before it turns deadly

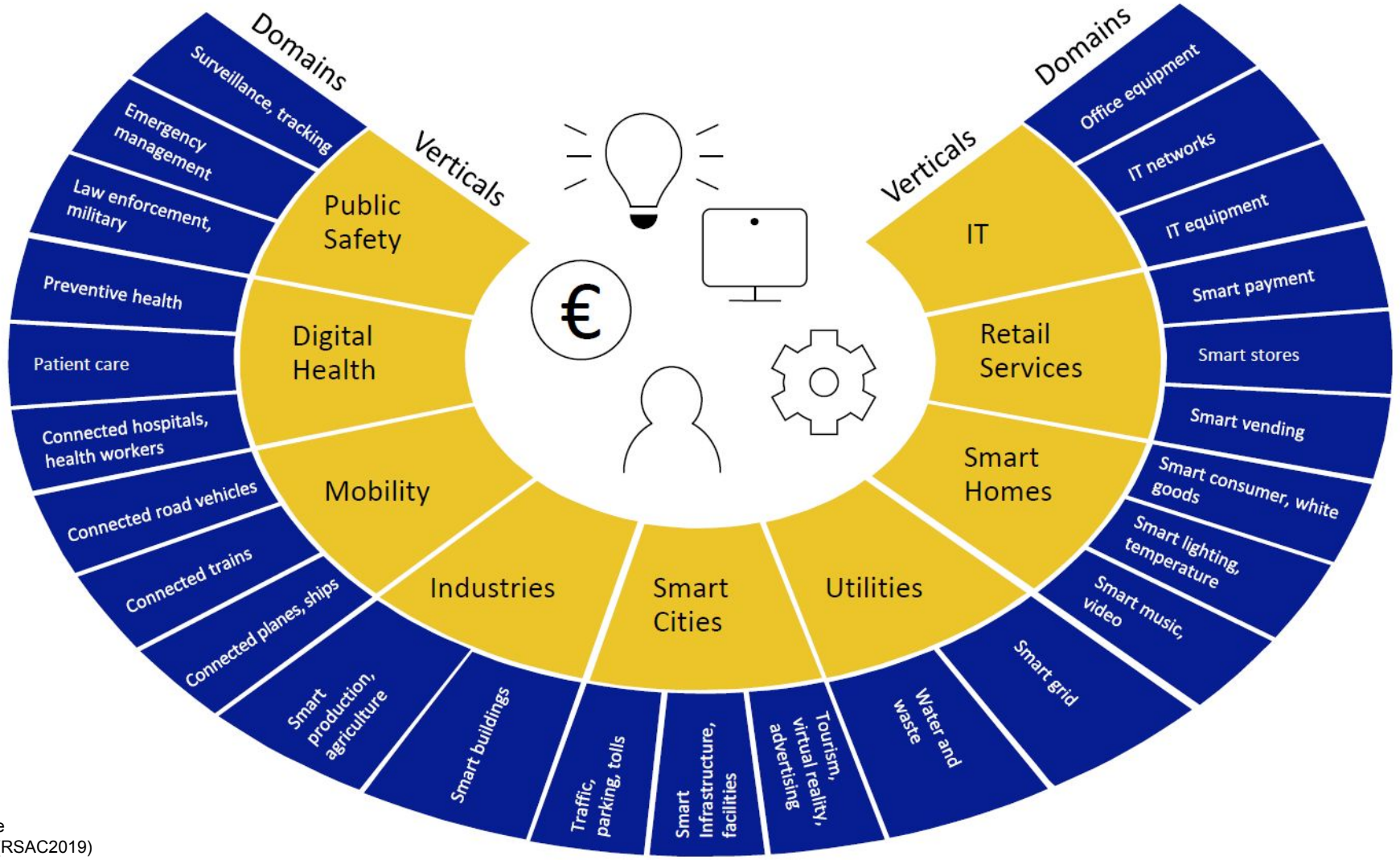
Where wearable sensors alert patients to emergencies before they happen

Credit: https://www.medicaldevice-network.com/

Where drones are used to support first responders

Image Source: Faradair.com

IoT Has a Transformational Impact across Vertical Sectors



Credit: Srinivas Bhattiprolu, Nokia Software
Trends and Best Practices in IoT Security (RSAC2019)

The IoT Environment

- Diverse Types of Devices
- Proprietary IoT Protocols
- Unmanaged and Invisible

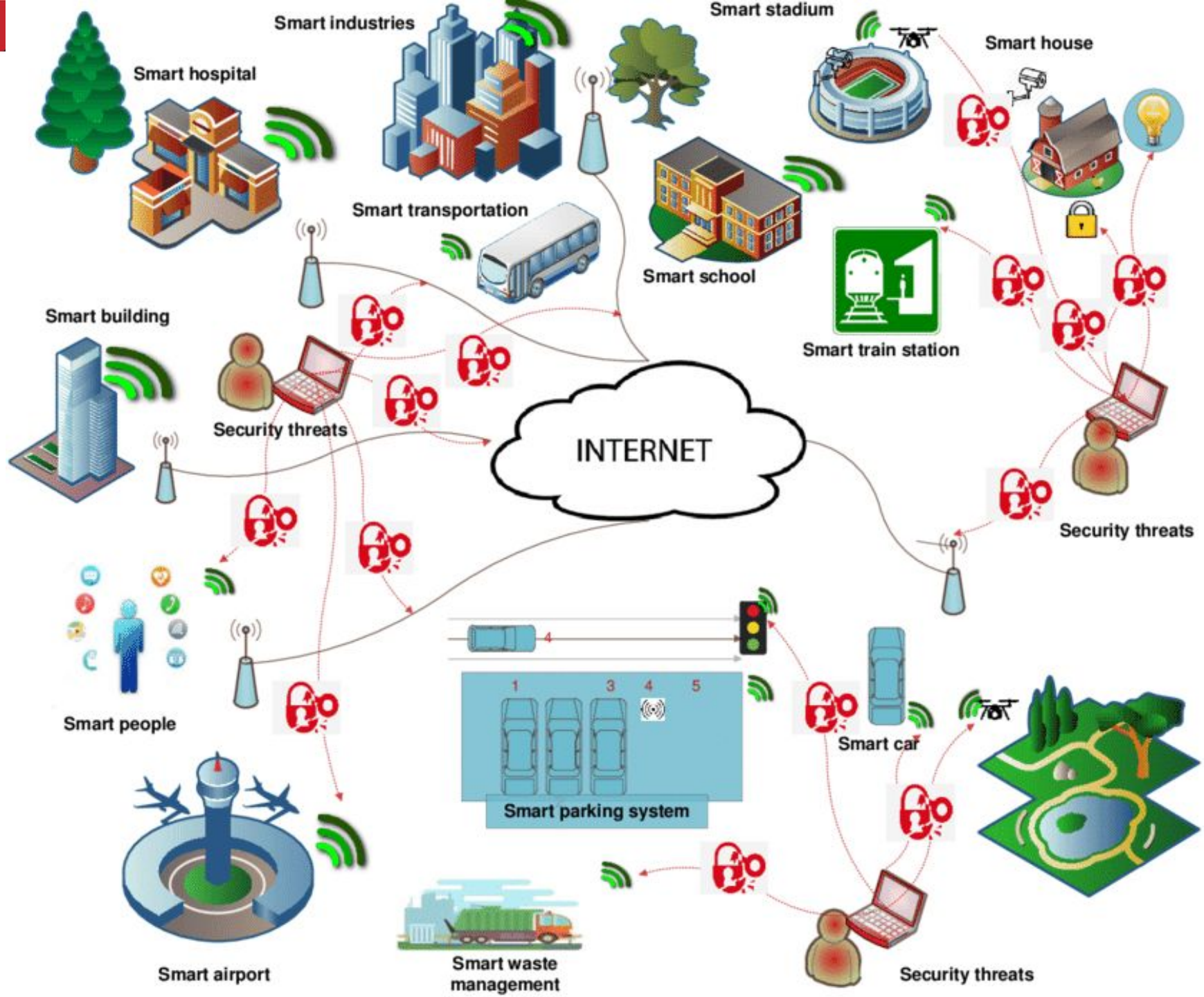


Image Credit: Ibrar Yaqoob, Ejaz Ahmed, DOI:10.1016/j.comnet.2017.09.003

Scanning the Internet for IoT Devices

SHODAN | Explore | Pricing | hetgear

TOTAL RESULTS

1,004,689

TOP COUNTRIES

United States	217,009
Japan	87,579
United Kingdom	48,222
Sweden	47,350
Italy	46,600

More...

TOP PORTS

8443	37,441

View Report | View on Map

New Service: Keep track of what you have connected to the Internet.

13.244.107.128
ec2-13-244-107-128.af-south-1.compute.amazonaws.com
Amazon Data Services South Africa
South Africa, Cape Town
cloud honeypot

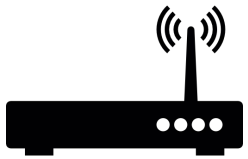
```
HTTP/1.1 200 OK
Date: Tue, 20 Jul 2021 19:44:02 GMT
X-Powered-By: PHP/5.6.20-0+deb8u1
Server: dcv 2wire Gateway 4D_WebSTAR_S/5.0
```

18.183.7.211
ec2-18-183-7-211.ap-northeast-1.compute.amazonaws.com
Amazon Data Services Japan
Japan, Tokyo
cloud honeypot

```
HTTP/1.1 302 Found
Date: Tue, 20 Jul 2021 19:44:02 GMT
X-Powered-By: Express
Server: dcv 2wire Gateway 4D_WebSTAR_S/5.0
```

18.189.16.228
ec2-18-189-16-228.us-east-2.compute.amazonaws.com
Amazon Technologies Inc.
United States, Hilliard
cloud honeypot

```
HTTP/1.1 200 OK
Date: Tue, 20 Jul 2021 19:43:58 GMT
X-Powered-By: ASP.NET
Server: dcv 2wire Gateway 4D_WebSTAR_S/5.0
```



Censys | Hosts | ip camera

Results

Host Filters

Autonomous System:

43.00K	AMAZON-02
20.68K	KIXS-AS-KR Korea Telecom
17.31K	DTAG Internet service provider operations
13.95K	COMCAST-7922
6,653	France Telecom - Orange

More

Location:

72.22K	United States
36.57K	Germany
32.06K	South Korea
20.19K	France
18.56K	Japan

More

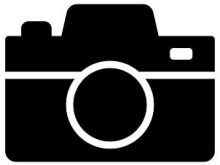
Service Filters

Hosts
Results: 379,861 Time: 1.66s

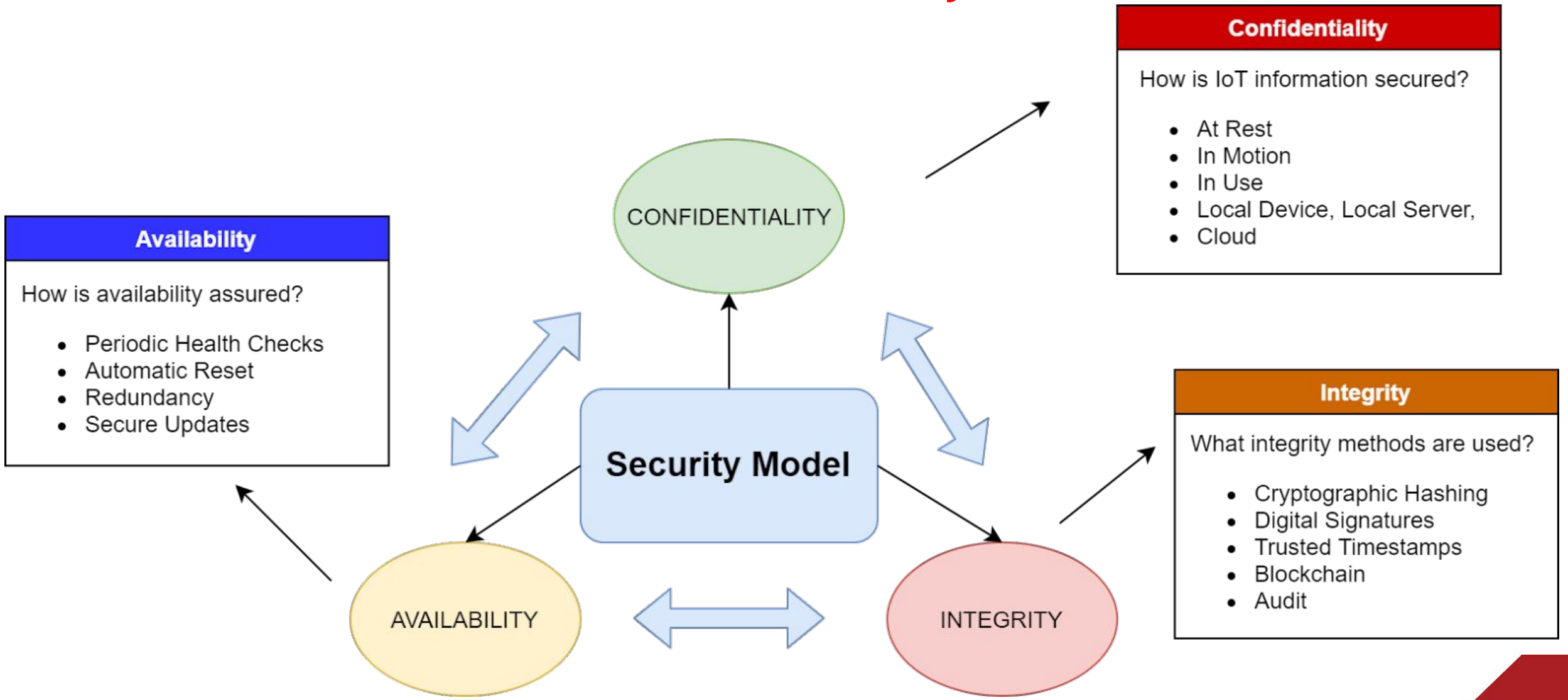
166.130.89.12 (mobile-166-130-89-12.mycingular.net)
ATT-MOBILITY-LLC-AS20057 (20057) United States
443/HTTP 8443/HTTP
services.tls.certificates.leaf_data.subject.common_name: IP Camera
services.tls.certificates.leaf_data.issuer.common_name: IP Camera
services.tls.certificates.leaf_data.subject_dn: C=US, CN=IP Camera
services.tls.certificates.leaf_data.issuer_dn: C=US, CN=IP Camera

166.130.89.123 (mobile-166-130-89-123.mycingular.net)
ATT-MOBILITY-LLC-AS20057 (20057) United States
443/HTTP 8443/HTTP
services.tls.certificates.leaf_data.subject.common_name: IP Camera
services.tls.certificates.leaf_data.subject_dn: C=US, CN=IP Camera
services.tls.certificates.leaf_data.issuer_dn: C=US, CN=IP Camera
services.tls.certificates.leaf_data.issuer.common_name: IP Camera

52.74.239.174 (ec2-52-74-239-174.ap-southeast-1.compute.amazon



CIA Triad for Security



Confidentiality

How is IoT information secured?

- At Rest
- In Motion
- In Use
- Local Device, Local Server,
- Cloud

Availability

How is availability assured?

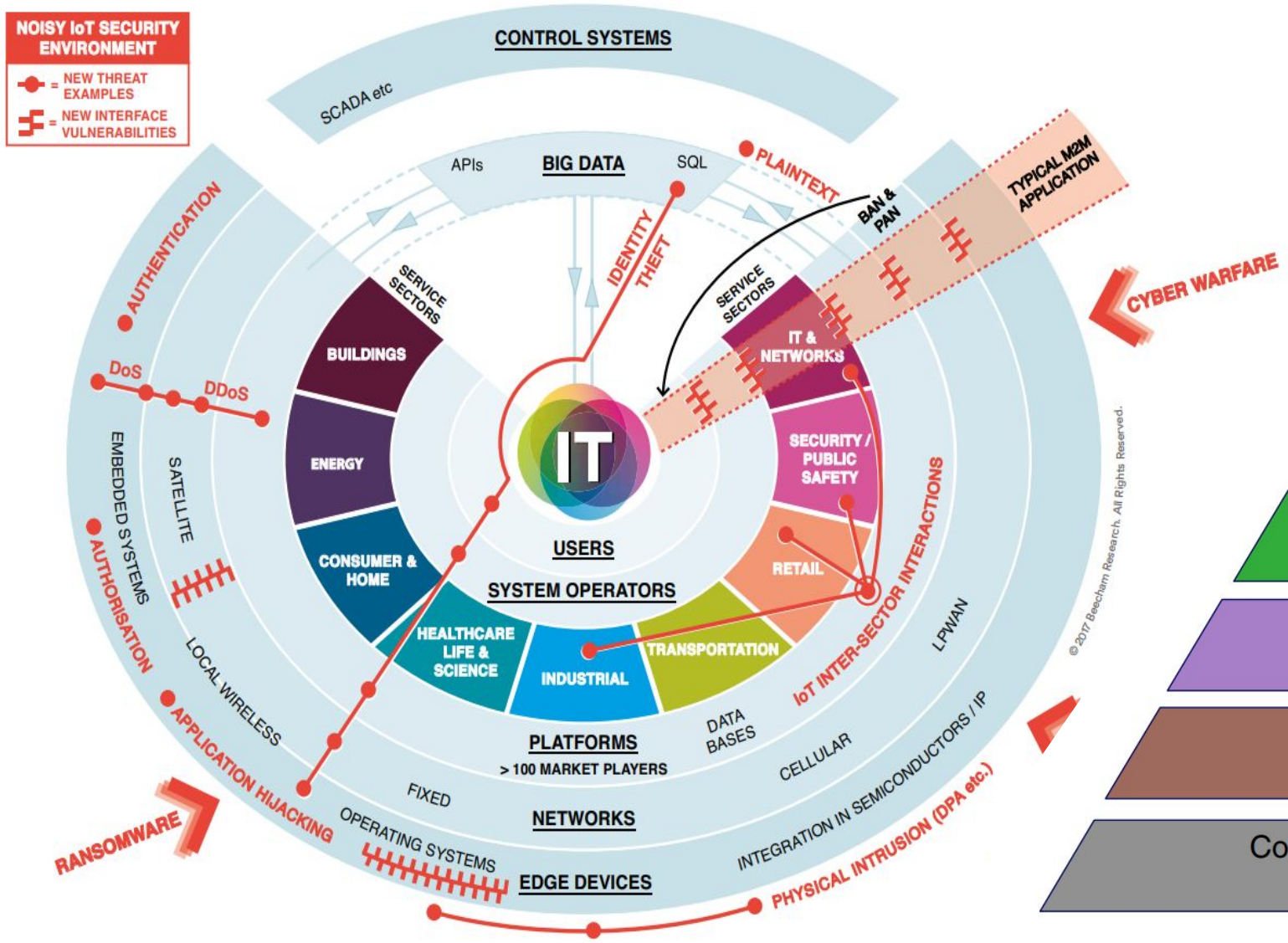
- Periodic Health Checks
- Automatic Reset
- Redundancy
- Secure Updates

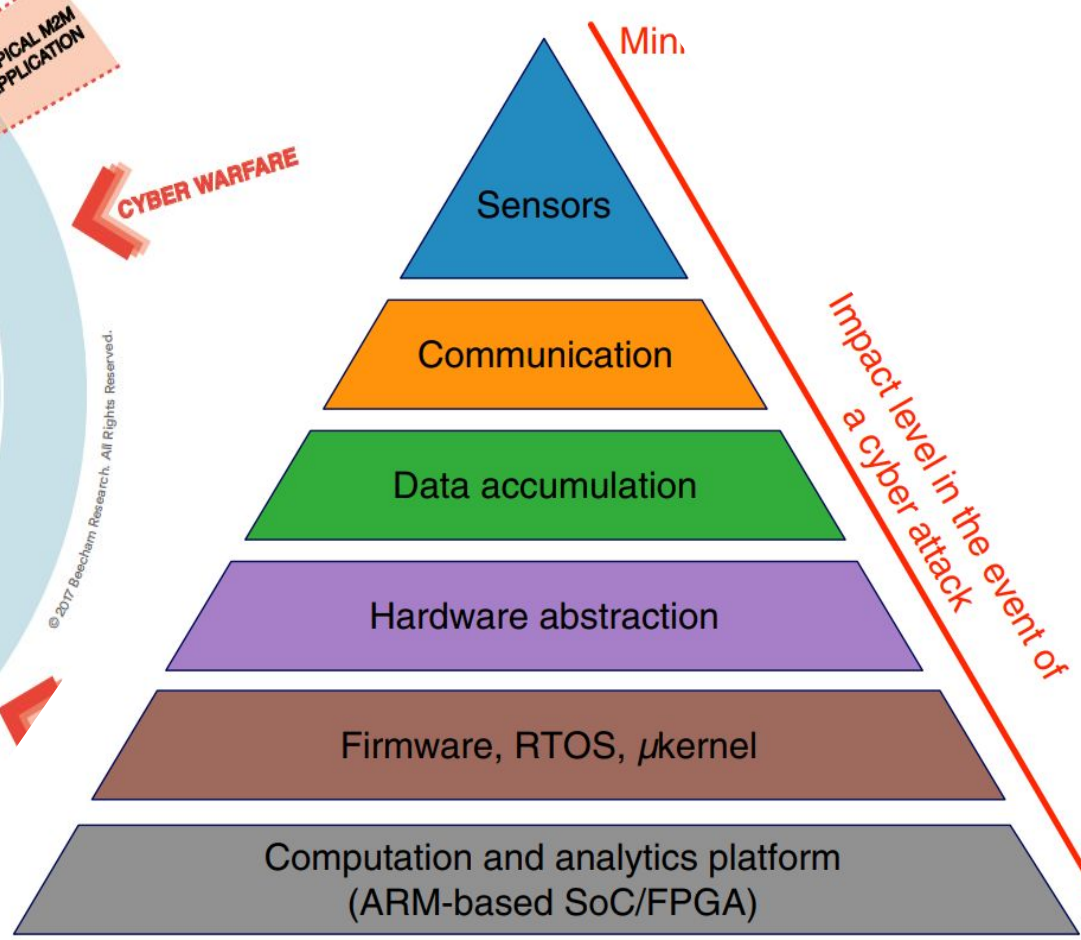
Integrity

What integrity methods are used?

- Cryptographic Hashing
- Digital Signatures
- Trusted Timestamps
- Blockchain
- Audit

IoT Security Threat Map





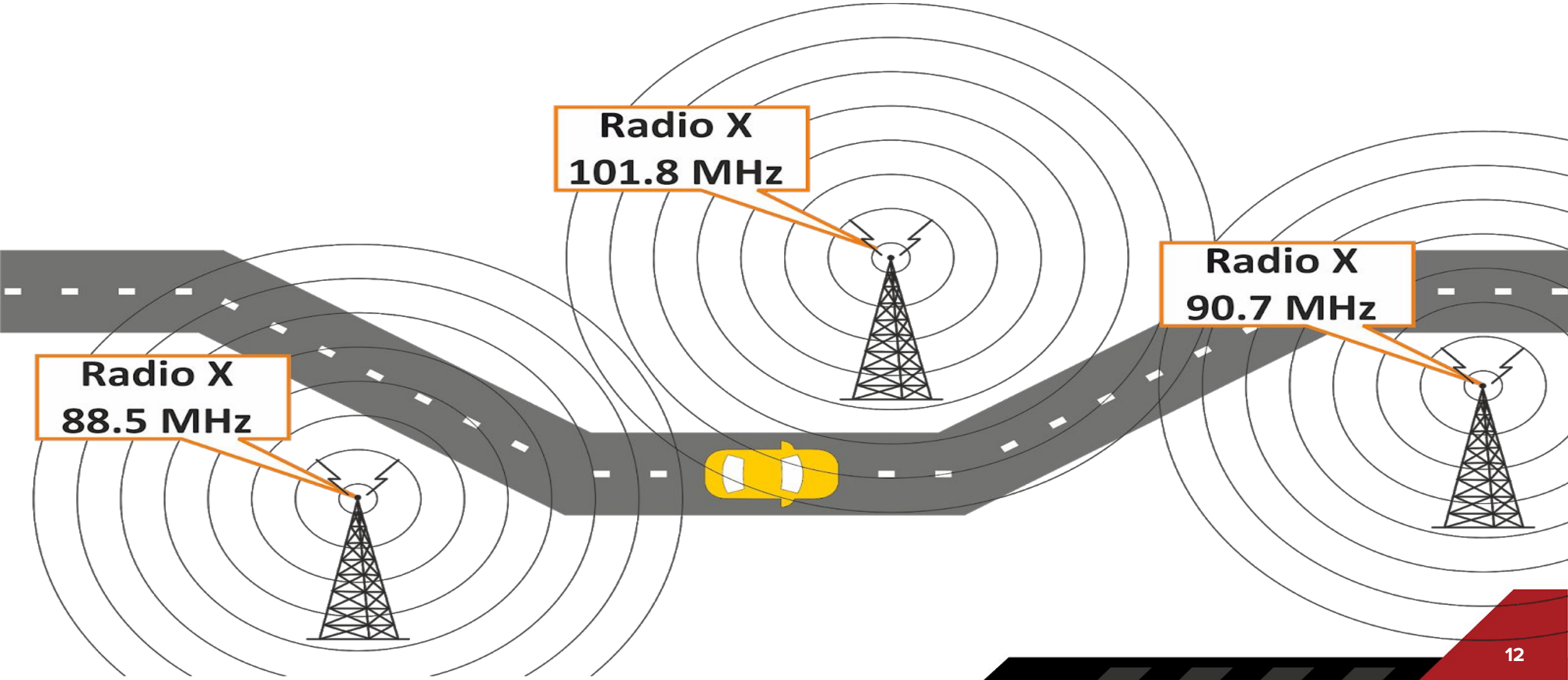
Source: http://www.beechamresearch.com/download.aspx?id=43

DoD Fuel Depot

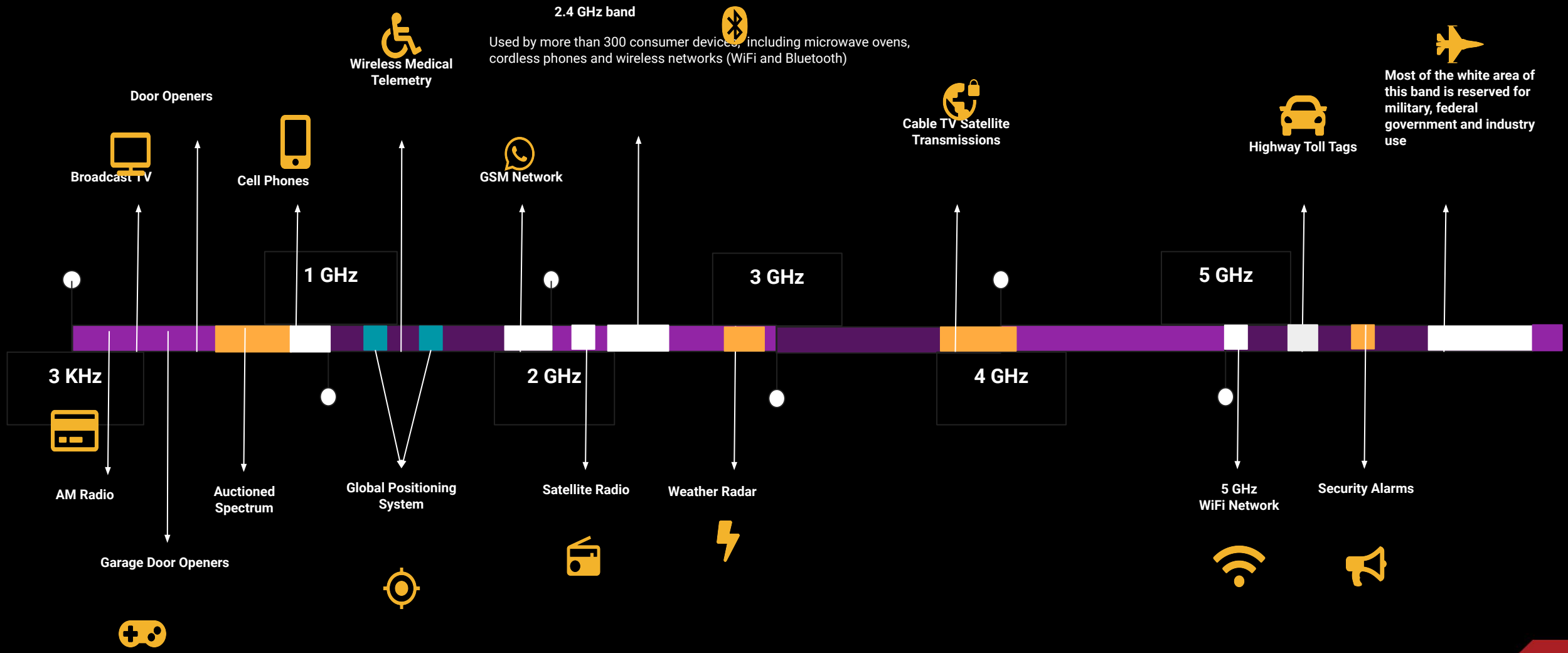
Battlefield Situational Awareness

- **IoT Uses and Potential Benefits**
- **Threats and Vulnerabilities**
- **Recommendations**

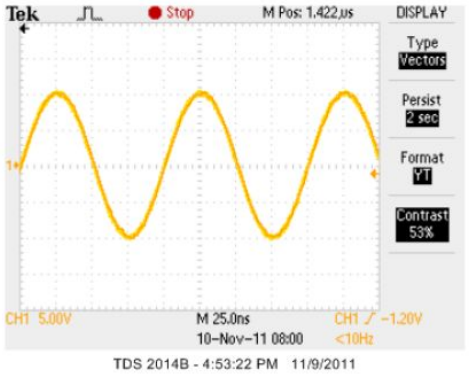
What Is RF?

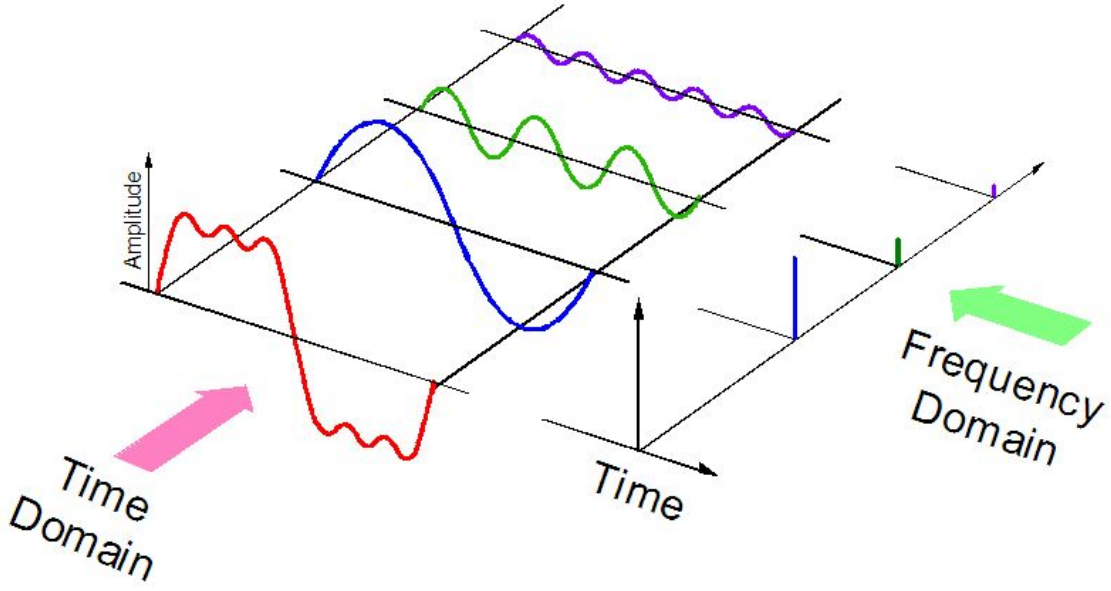


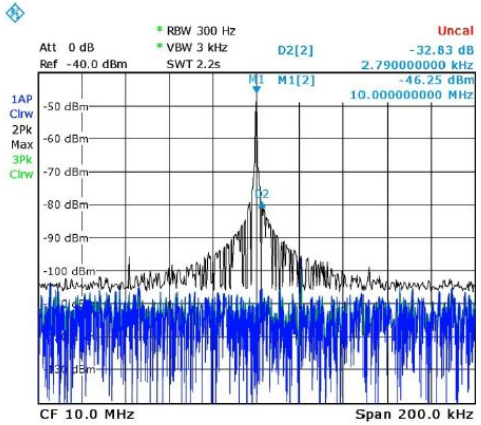
Inside the radio wave spectrum?



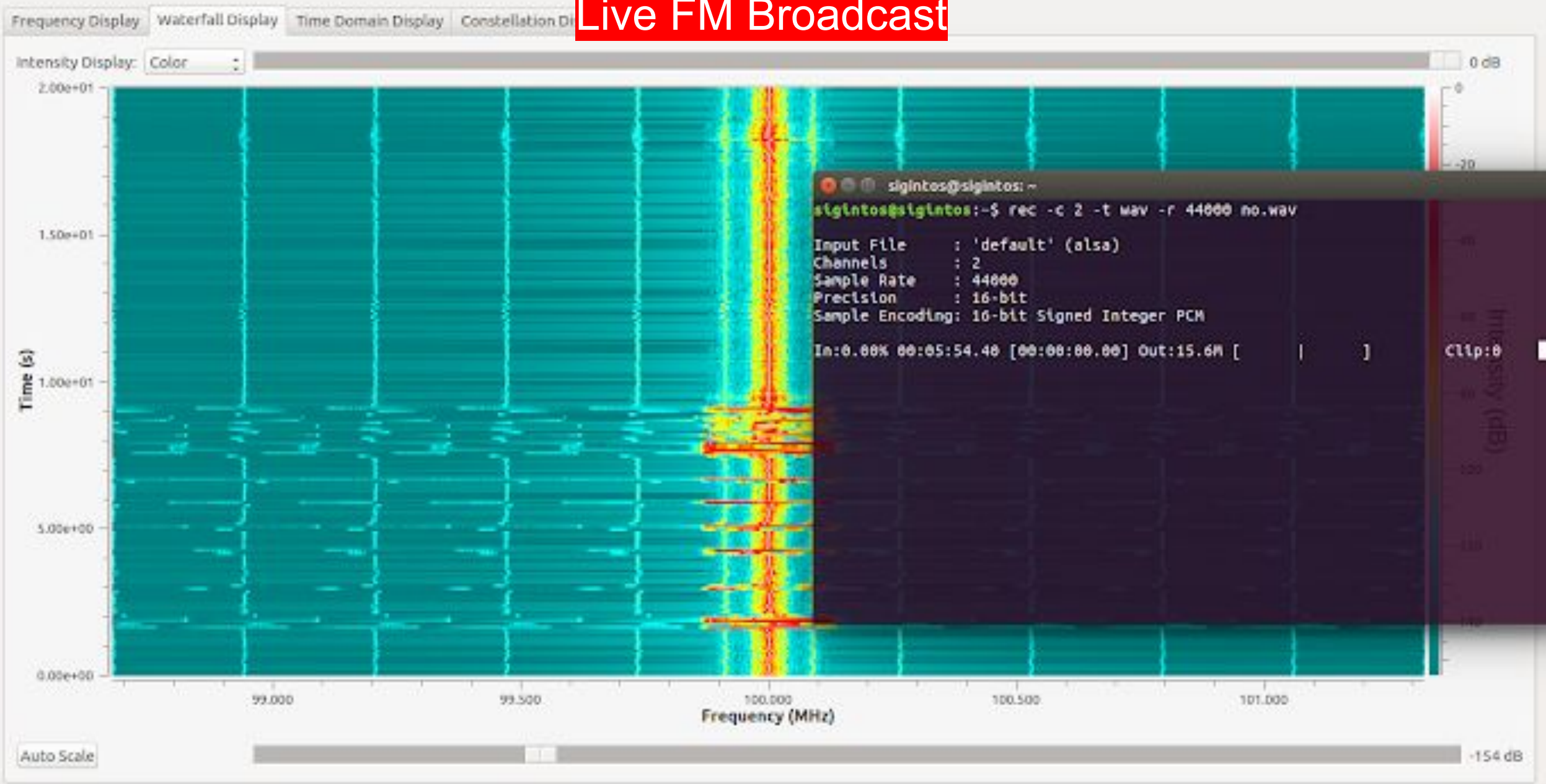
Time domain and Frequency domain







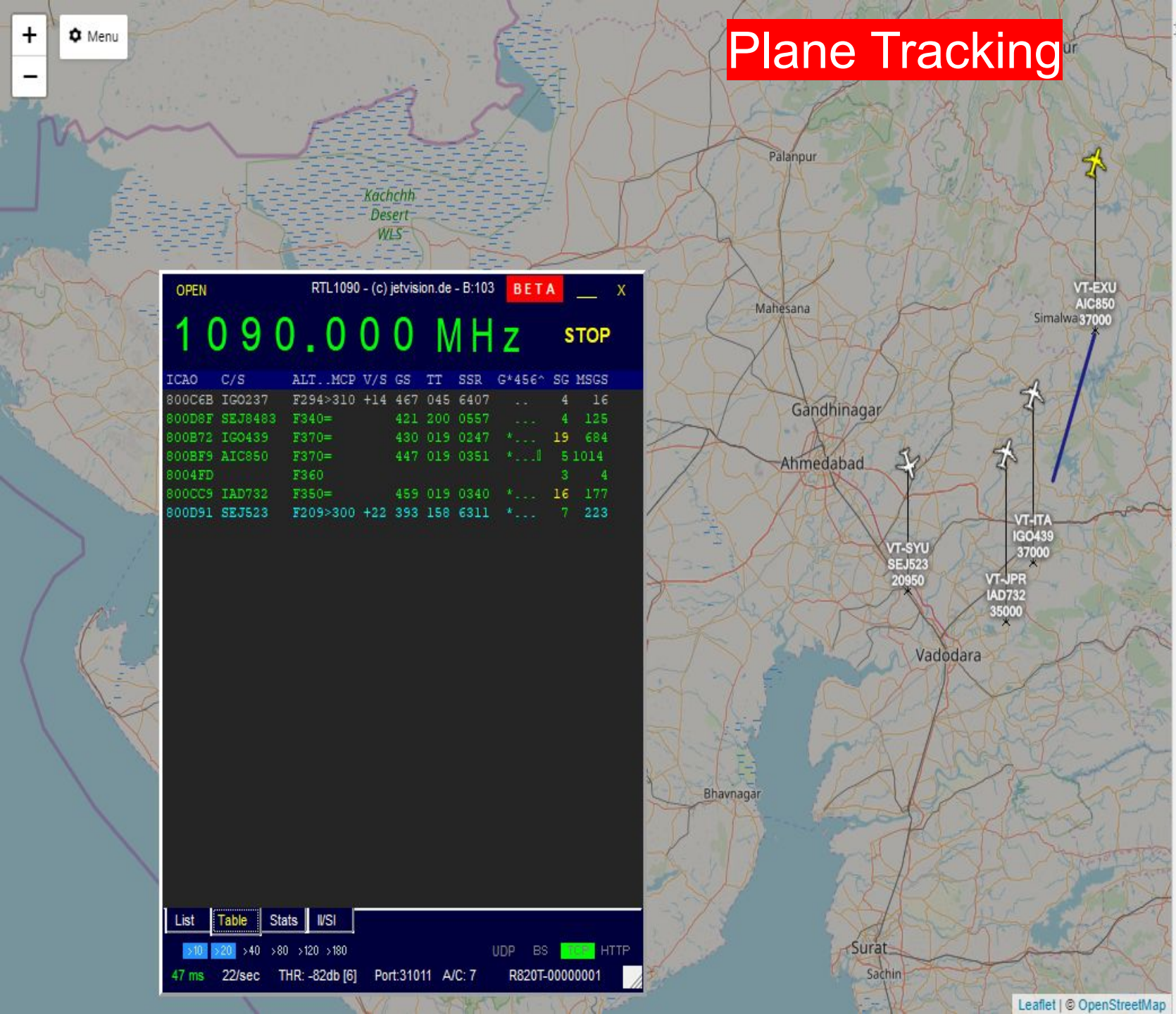
Live FM Broadcast



GPS Spoofing

```
sigintos@ubuntu: ~/GPS_SDR_SIM/gps-sdr-sim
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.0 MiB / 1.001 sec =   5.0 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.2 MiB / 1.000 sec =   5.2 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.0 MiB / 1.001 sec =   5.0 MiB/second
  5.2 MiB / 1.000 sec =   5.2 MiB/second
^X 5.2 MiB / 1.001 sec =   5.2 MiB/second
^Z
[4]+  Stopped                 sudo hackrf_transfer -t gpssim.bin -f 1575420000 -s 2600000 -a 1 -x 0
sigintos@ubuntu:~/GPS_SDR_SIM/gps-sdr-sim$ hackrf_info
hackrf_info version: unknown
libhackrf version: unknown (0.5)
Found HackRF
Index: 0
Serial number: 0000000000000000325866e6229f5e23
Board ID Number: 2 (HackRF One)
Firmware Version: 2018.01.1 (API:1.02)
Part ID Number: 0xa000cb3c 0x00658475b
sigintos@ubuntu:~/GPS_SDR_SIM/gps-sdr-sim$ sudo hackrf_transfer -t gpssim.bin -f 1575420000 -s 2600000 -a 1 -x 0
call hackrf_set_sample_rate(2600000 Hz/2.600 MHz)
call hackrf_set_freq(1575420000 Hz/1575.420 MHz)
call hackrf_set_amp_enable(1)
Stop with Ctrl-C
  5.0 MiB / 1.001 sec =   5.0 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.2 MiB / 1.000 sec =   5.2 MiB/second
  5.2 MiB / 1.000 sec =   5.2 MiB/second
  5.0 MiB / 1.000 sec =   5.0 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.2 MiB / 1.000 sec =   5.2 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.0 MiB / 1.001 sec =   5.0 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.0 MiB / 1.000 sec =   5.0 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.2 MiB / 1.000 sec =   5.2 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
  5.2 MiB / 1.001 sec =   5.2 MiB/second
```

https://cddis.nasa.gov/archive/gnss/data/daily/



OPEN RTL1090 - (c) jetvision.de - B:103 BETA

1090.000 MHz STOP

ICAO	C/S	ALT..MCP	V/S	GS	TT	SSR	G*456^	SG	MSGS
800C6B	IGO237	F294>310	+14	467	045	6407	..	4	16
800D8F	SEJ8483	F340=		421	200	0557	...	4	125
800B72	IGO439	F370=		430	019	0247	*...	19	684
800BF9	AIC850	F370=		447	019	0351	*...	5	1014
8004FD		F360						3	4
800CC9	IAD732	F350=		459	019	0340	*...	16	177
800D91	SEJ523	F209>300	+22	393	158	6311	*...	7	223

List Table Stats W/SI

>10 >20 >40 >80 >120 >180 UDP BS TCP HTTP

47 ms 22/sec THR: -82db [6] Port:31011 A/C: 7 R820T-00000001

VT-EXU 800BF9

Air India AIC850

India Civil

Airbus A320 251NSL A20N

Altitude:	Vertical Speed:	Speed:	Heading:	Distance:	Squawk:	Engines:	Species:
37000 ft	0 ft/m	446.5 kts	19.1°	263.95 nmi	0351	Twin jet	Landplane

Wake Turbulence:
Medium

Route:
PNQ Pune, India
DEL Indira Gandhi, New Delhi, India

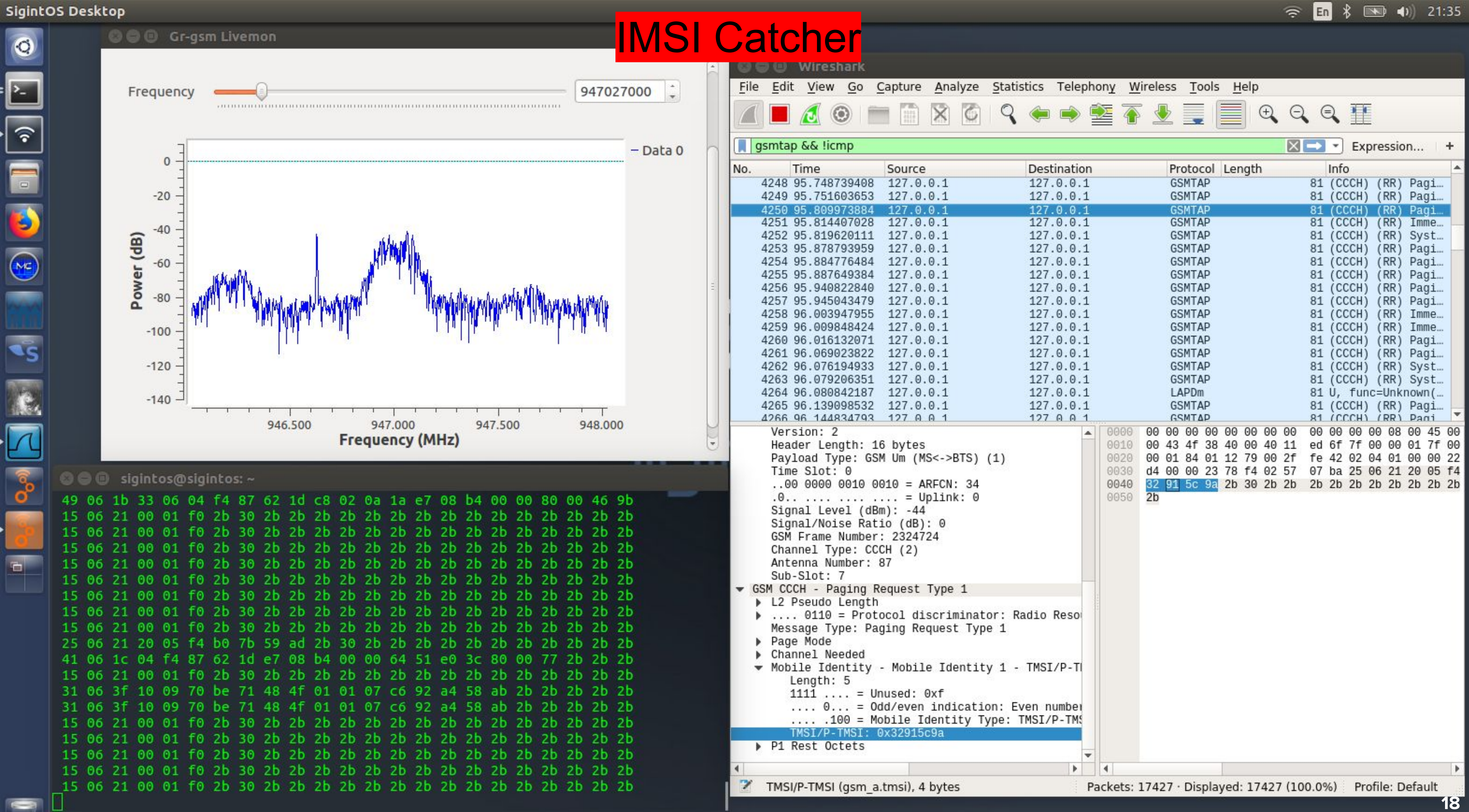
www.airport-data.com : : www.airliners.net : : www.airframes.org
Show on map : : Enable auto-select : : Submit route correction

Tracking 6 aircraft — Pause : : List only visible

Silhouette	Flag	Reg.	ICAO	Callsign	Route	Altitude	Speed
		VT-SCO	8004FD			36025 ft	
		VT-JPR	800CC9	IAD732		35000 ft	458.9 kts
		VT-SYU	800D91	SEJ523	CCU-BLR	20950 ft	393.1 kts
		VT-SYS	800D8F	SEJ8483	DEL-STV	33975 ft	420.8 kts
		VT-ITA	800B72	IGO439	DED-*-DEL	37000 ft	430.4 kts
		VT-EXU	800BF9	AIC850	PNQ-DEL	37000 ft	446.5 kts

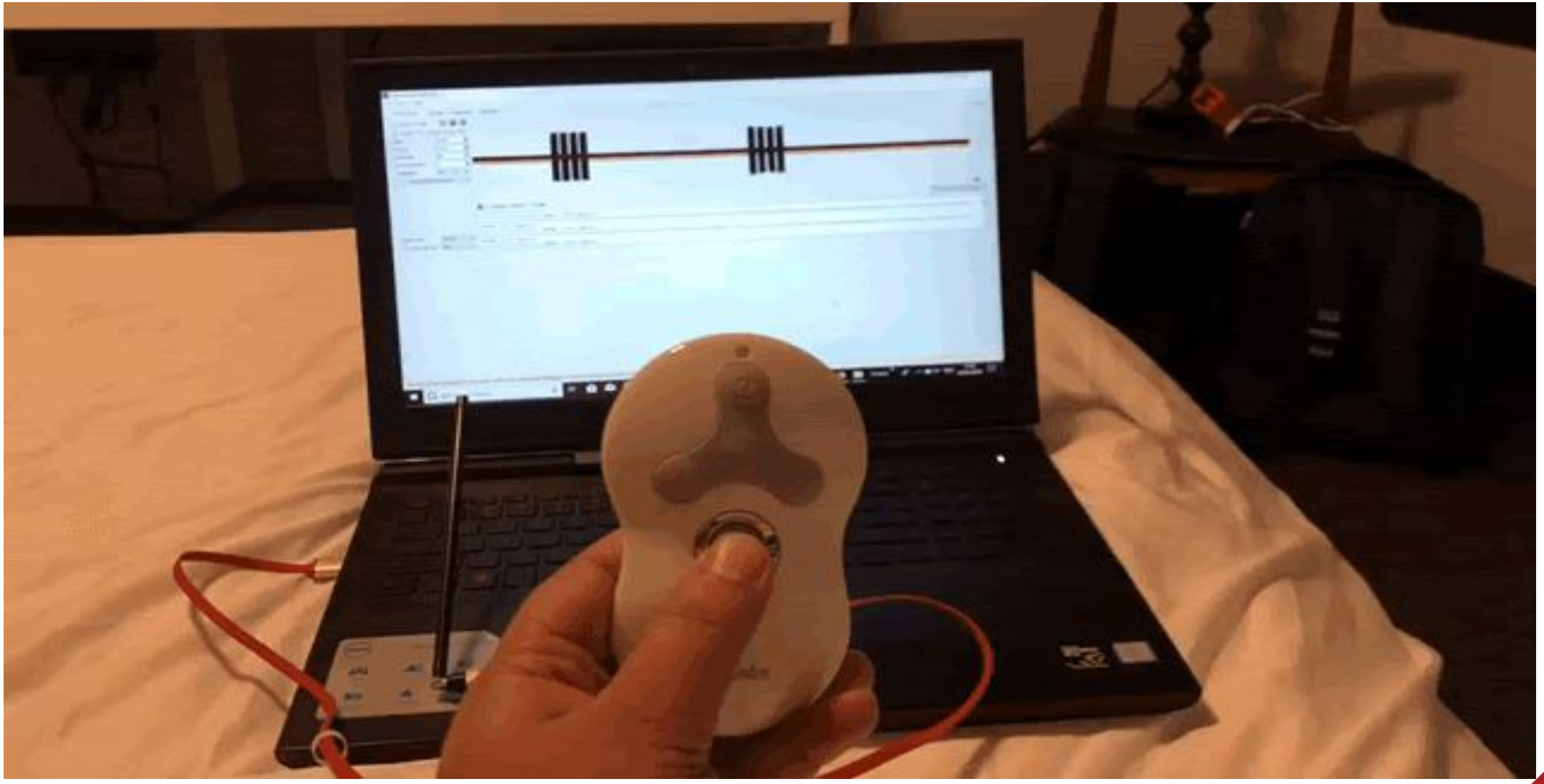
Powered by Virtual Radar Server

IMSI Catcher



Car Key - Replay Attack

Smart Light Demo



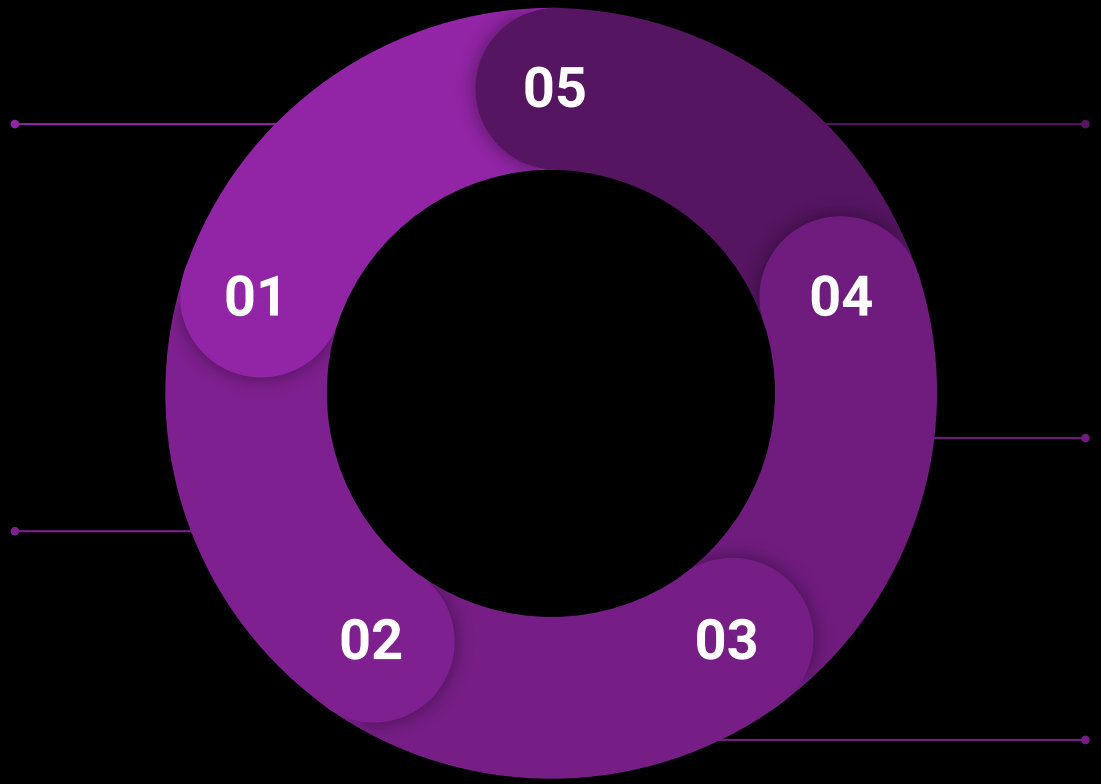
Internet of Radio Vulnerabilities

Rogue Cell Towers

Used to hijack cell phone connections, and to break 2-factor authentication to listen to calls and read texts.

Rogue Wi-Fi Hotspots

Impersonate legitimate Wi-Fi networks, and might be used for MITM attacks to sniff network traffic and steal credentials.



Vulnerable Wireless Devices

Low-end keyboard/mouse dongle can expose to RF attack through keystroke injection, which may expose the larger network to insider attacks.

Eavesdropping/ Surveillance Devices

Voice activated FM & GSM, or other radio bugs

Unapproved IoT Emitters

Sensors often have multiple data radios, 802.11 is known, but what if also transmitting on other frequencies like Zigbee, or LORA.

INTERNATIONAL / COMMENTARY

NATO Designates Cyber as Official Domain for Warfare

Anna Ferrara / David Inserra / @dr_inserra / June 29, 2016 /

Defending our territory and protecting our citizens is NATO's core mission.

We also turned our attention to cyberspace.

We agreed that we will recognise cyberspace as an operational domain.

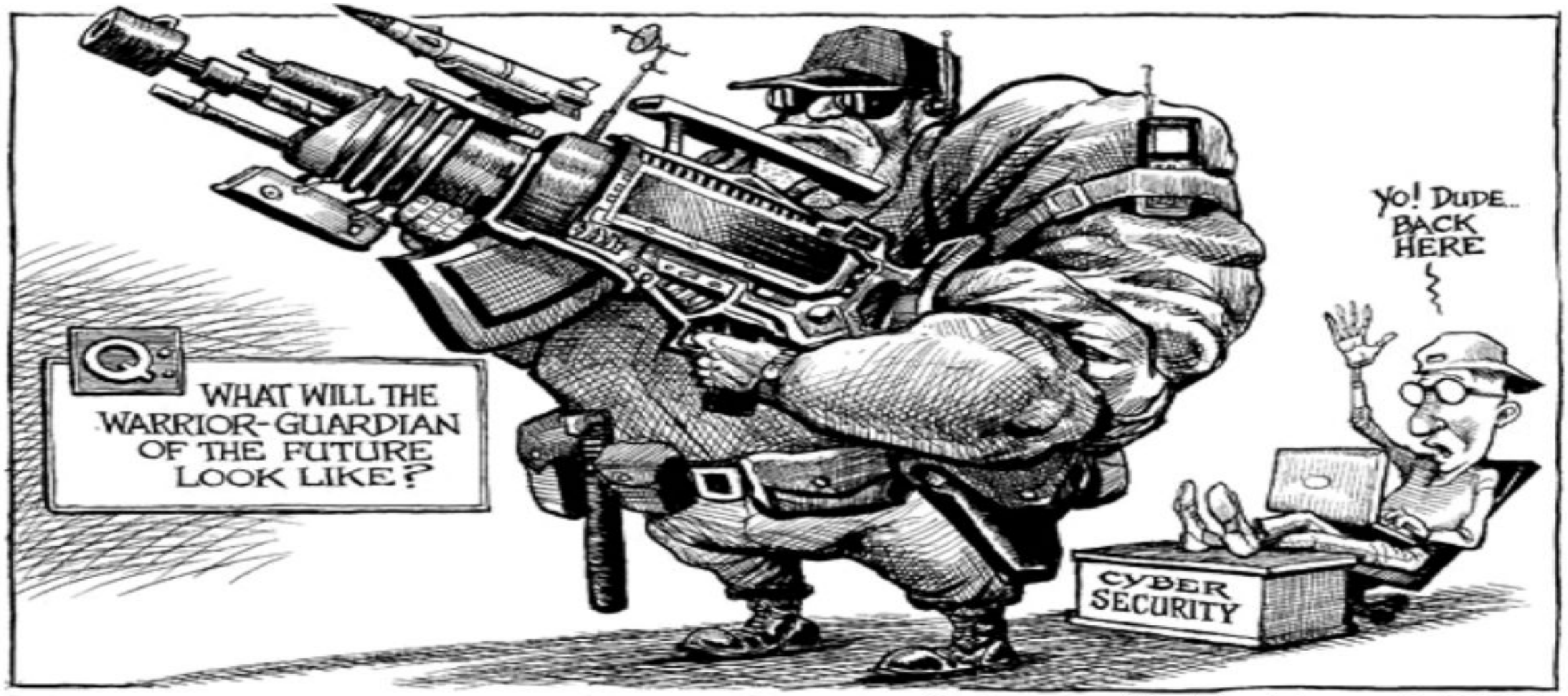
Just like air, sea and land.

Cyber defence is part of collective defence.

Most crises and conflicts today have a cyber dimension.

So treating cyber as an operational domain would enable us to better protect our missions and operations.

Source: https://www.dailysignal.com/2016/06/29/nato-designates-cyber-as-official-domain-for-warfare/



Cartoon credits: The Economist 2009

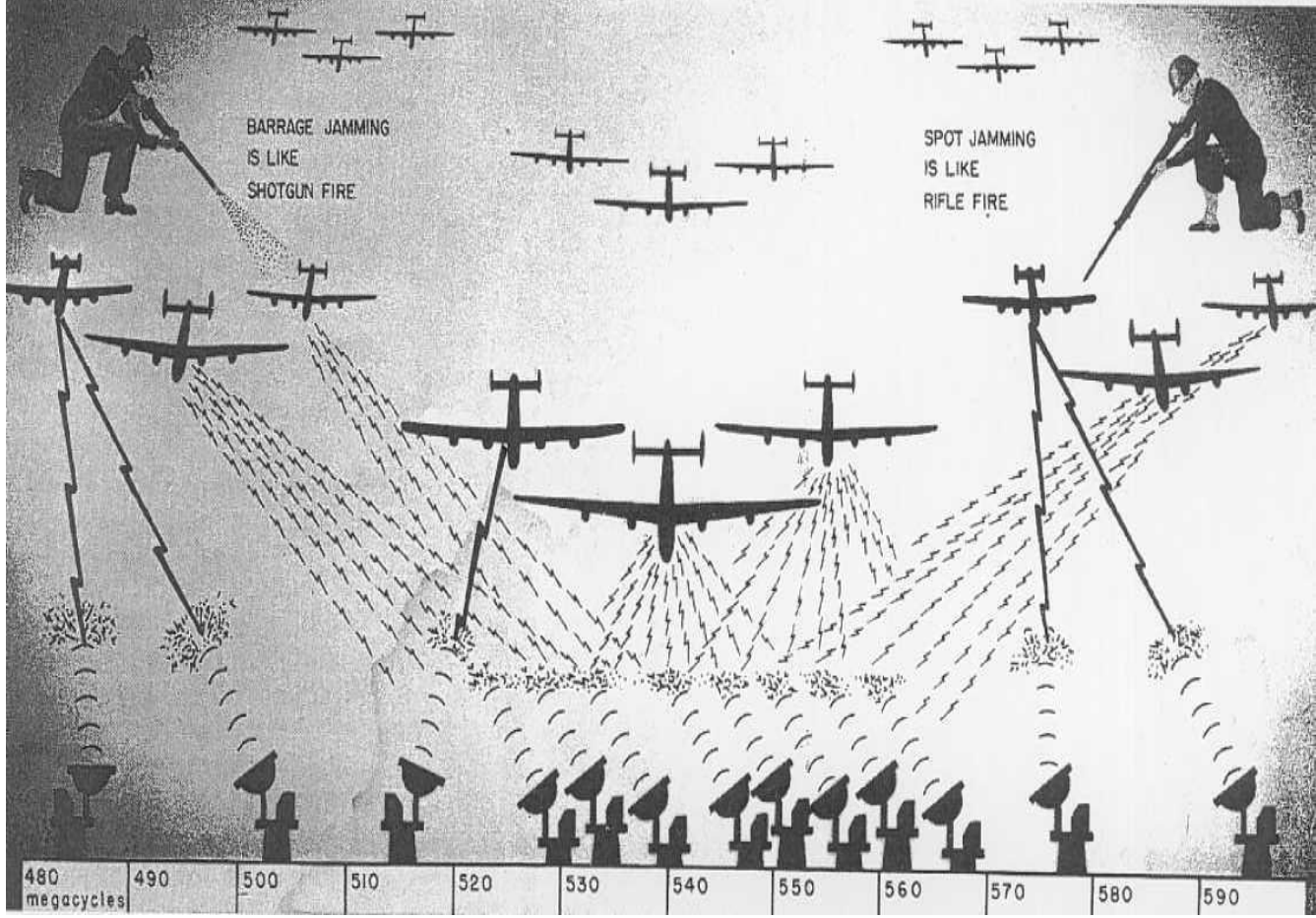

Airborne


Ground


Space


Naval


Cyber



A Brief History of EW

The Origins of Electronic Warfare

By Wing Commander M. T. THURBON, RAF (Retd)

Men who ignore the past are doomed to relive it.
Santayana

There is a widespread belief that Electronic Warfare (EW) originated early in World War II with the British jamming of the German blind bombing aids Knickebein, X-Gërat and Y-Gërat. In fact what is now called EW has a surprisingly long history and many of the earliest examples of its application still, I believe, hold important lessons for us today. Excellent accounts of the development of electronic warfare in World War II can be found in Alfred Price's books.[1,2] My aim is to retrace the evolution of this subject backwards from 1939.

1919–1939

The years between the two world wars saw many conflicts but the scope and nature of most of these precluded the use of EW. Perhaps only in the Spanish Civil War, a proving ground for a wide range of the most modern weapons of the day, were there opportunities for the limited application of counter-measures against communications, although the available references fail to reveal any such operations. This apparent lack of EW activity between 1918 and 1939 does not mean that the subject was completely forgotten. In Great Britain the designers of the early radar systems were, from the very beginning, keenly aware of the possibility of enemy counter-measures. As early as 9 September 1935, less than seven months after the feasibility of radar was first demonstrated, Sir Robert (then Mr) Watson-Watt, in a progress report to the Committee for the Scientific Study of Air Defence, proposed the establishment of what became known as the Chain Home system. His scheme included provision for minimising the effects of interference, especially deliberate jamming. Sir Robert suggested that planning should proceed on the assumption that the anti-jamming design would be effective but he recognised that this hope might be disappointed and that a means of rapidly changing wavelength might have to be provided, although this solution might be expensive. By 1937 the use of multiple wavelengths had become accepted. On 19 October 1935, he was asked by the Committee whether radio-location (as radar was then called) could be defeated by deliberate jamming. In reply Sir Robert defined the conditions that would have to be fulfilled if jamming were to be effective and he discussed the extent to which those conditions might be met by direct jamming from, for example, sites on the Belgian coast. He also considered the possibility of indirect jamming via the ionosphere (these early radars operated in the HF band). He concluded that provided the cover was limited to 0 to 30 degrees in elevation, jamming from ground stations in enemy territory could not defeat the system. It was recognised that airborne jamming could be effective but it was thought that the aircraft could be located by direction finding (DF) and, at least by day, intercepted by fighters. Other suggestions made at the time were for the provision of a reserve and secret frequency for each RDF station and the use of a narrow rotating beam scan. Such was the concern about the vulnerability of RDF to jamming that in 1937 a Jamming Section was set up at Bawdsey to provide various types of jamming to the Anti-Jamming Group and to conduct experiments to assess the effectiveness and probable use of these types of jamming. The work of this section "had the desired result of bringing out many anti-jamming suggestions". In 1938 ground and airborne jammers were used in trials against a number of RDF sites.[3]

ECCM

Work was also in progress elsewhere during this period. An interesting example, because it must be one of the earliest applications of electronic counter-counter measures (ECCM) to a weapon system, occurred in Germany. In 1916 a German, Franz Drexler, had unsuccessfully attempted to convince the authorities of the case for unmanned aircraft controlled by a system of auto-pilot and radio control (the radio control of a model airship had been demonstrated by a German school teacher, Wirth, in 1913). In 1926 the German Army Air Staff was interested in unmanned aircraft for photographic reconnaissance and strategic bombing. Drexler resubmitted his idea and this time to a more receptive audience. Circumventing the terms of the Treaty of Versailles, which prohibited the Germans from operating unmanned aircraft but which said nothing about research, Drexler and a radio expert Max Diekmann, were set to work on the design of a guided missile. Their preferred solution appears to have been a form of command guidance and someone, probably Diekmann, showed a remarkable awareness of the vulnerability of any radio link to jamming. The missile carried a "telemetry" device and signals were transmitted to a control post having two spaced aerial systems with goniometers. The instantaneous position of the vehicle was continuously indicated on a map and the loop must have been closed by a ground transmitter. The problems of protecting the radio signals from jamming had been given much thought throughout and a chain of what were described as selective traps was interposed at both ends.[4] (A wave trap was a circuit placed in series with the aerial of the receiver so as to reject strong interfering signals.) By using a chain of these traps Diekmann ensured that any jammer would

- Russo-Japanese War, 1904: The birth of signals intelligence
- Battle of Britain, 1940: Turning the tide with RADAR
- Cold War, 1952: Industrial scale jamming
- Cuban missile crisis, 1962: Deceptive drones

- Battle of Latakia, 1973: electronic warfare goes to sea
- US invasion of Panama, 1989: Stealth aircraft attack
- Gulf War, 1991: GPS at war
- Stuxnet, 2005: Weaponizing cyberspace
- 2018: Quantum Superpower

Electronic Warfare (EW)

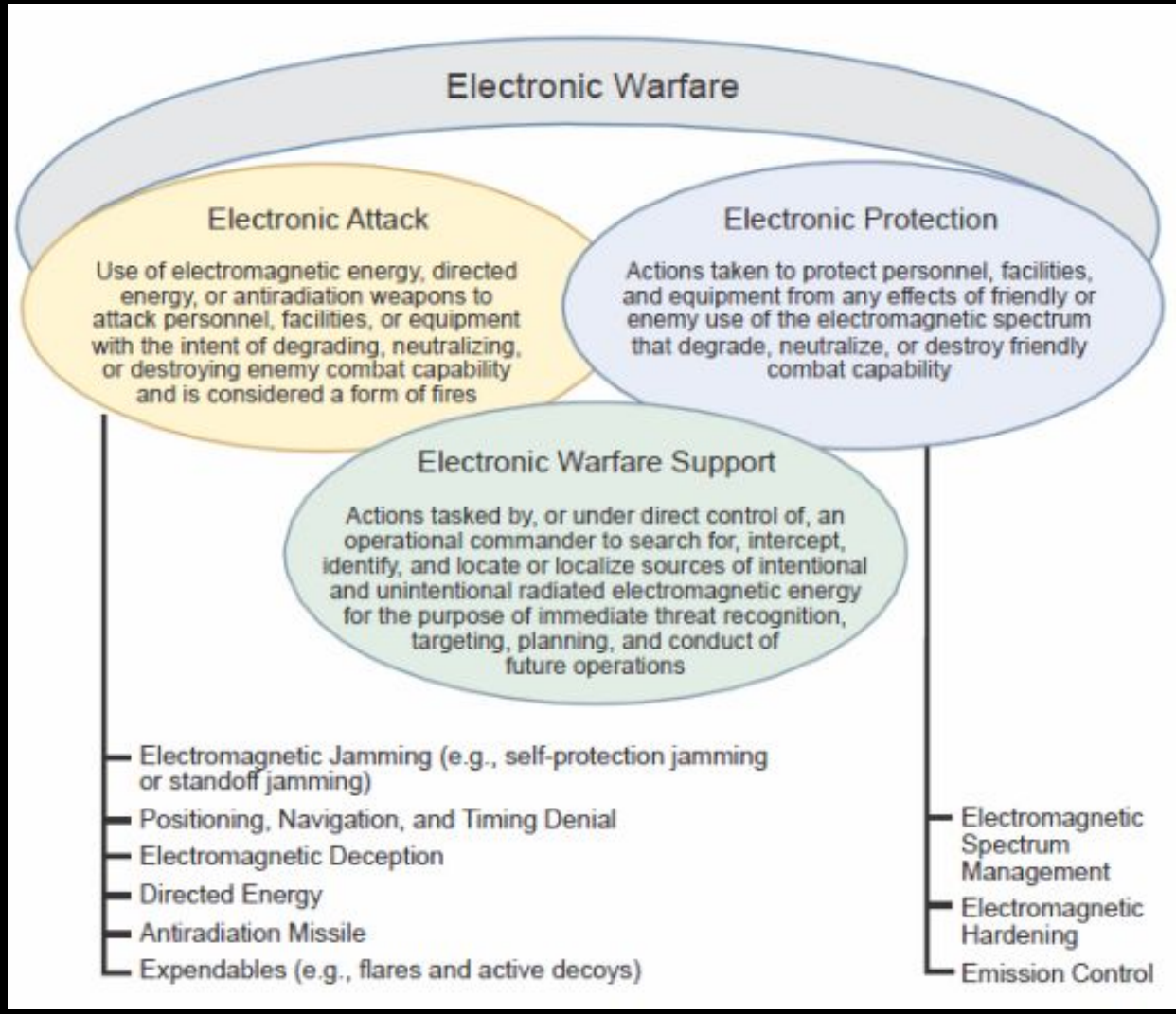
the ability to use the electromagnetic spectrum signals such as radio, infrared or radar to sense , protect , and communicate

Electronic Warfare

Electronic Warfare: is military action using electromagnetic and directed energy to control the electromagnetic spectrum or at attack the enemy (JP 3-51/FM 3-13).

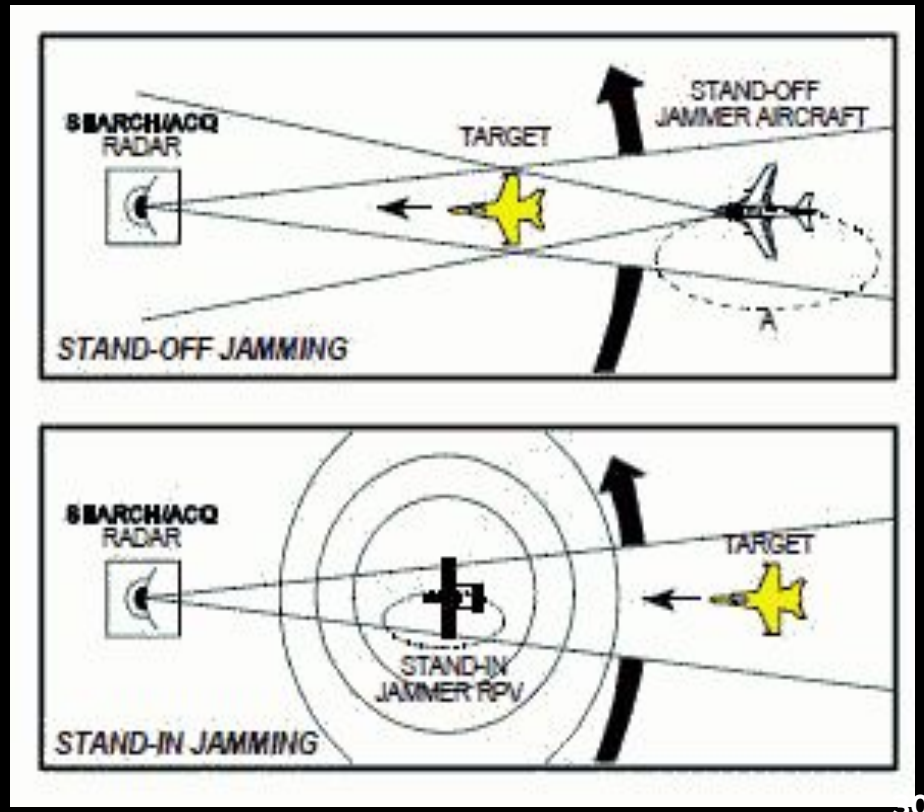
The three major subdivisions of EW are:

- Electronic Warfare Support (ES) *ESM
- Electronic Attack (EA) *ECM
  Electronic Protect (EP) *ECCM



Electronic Attack (EA)

- Passive surveillance of the EM spectrum to detect the enemy's position, strength, and intention, and warning of targets
- Preventing or reducing the enemy's use of the EM spectrum (capabilities) and promoting uncertainty
- "Black boxes" that jam or deceive the enemy
- Radar or communications "jamming"



Electronic Protection (EP)

- Protection of friendly combat capability against undesirable effect of friendly or enemy employed EW
- Types
  –Passive EW
  –Active EW
- Three ways to defend from enemy
  –Modify radar
    - Make it more complex
    - Make it harder to jam
  –Modify the Medium
    - Chaff
    - Torch
  –Modify the platform

ELECTRONIC PROTECTION (EP) TECHNIQUES

Angular Resolution	Compressive IF Amplifier	Jamming Cancellation Receiver	Pulse-To-Pulse Frequency Shift (RAINDOW)
Automatic Gain Control (AGC)	Constant False Alarm Rate (CFAR)	Mainlobe Cancellation	Random-Pulse Blanker
Autocorrelation Cancellation of Extended Targets (ACET)	Cross Correlation Signal Processing	Matched Filtering	Range Gating
Automatic Threshold Variation (ATV)	CW Jamming Canceller	Mainlobe Cancellation	Range Gate Memory
Automatic tuner (SNIFFER)	Dicke Fix	Monopulse Tracker	Sidelobe Blanker
Automatic Video Noise Leveling (AVNL)	Diplexing	Multifrequency Radar	Sidelobe Canceller
Bistatic Radar	Frequency Agility	Moving Target Indication (MTI)	Sidelobe Suppression (SLS)
Coded Waveform Modulation	Frequency Diversity	Phased Array Radar	Staggered PRF
Cross-Polarization	Guard Band Blanker	Polarization Diversity	Transmitter Power
Jittered PRF	High PRF Tracking	PRF Discrimination	Variable Bandwidth Receiver
	Instantaneous Frequency Correlator	Pulse Coding and Correlation	Variable Scan Rate
	Inter-Pulse Coding	Pulse Compression, Stretching (CHIRP)	Velocity Tracker
	Logarithmic Receiver	Pulse Edge Tracking	Video Correlator

Source:Republic of Singapore Air Force

±Burnthrough: Increase signal strength to overpower jammer noise (ECCM)

CYBER DEFENSE

Army electronic warfare technology attacks and disables tank

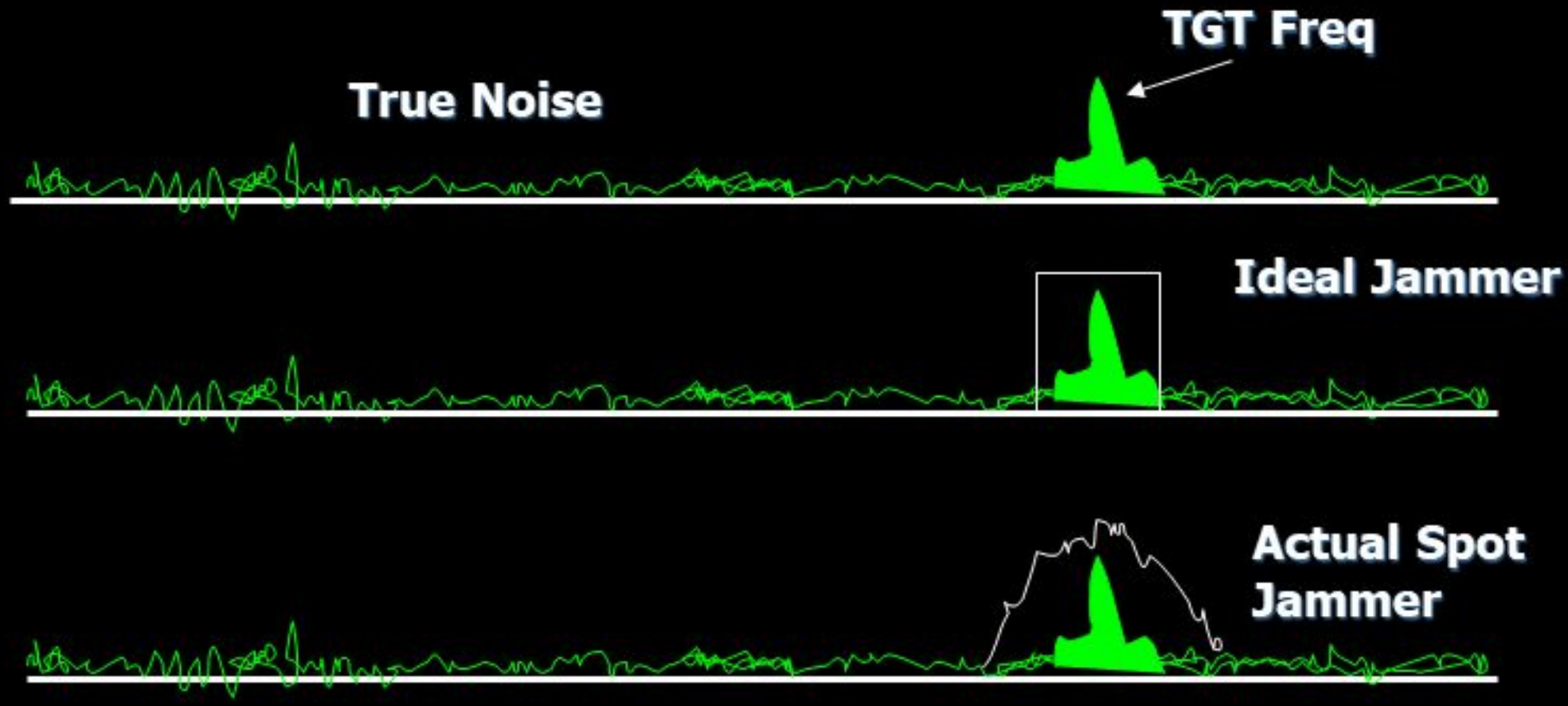
BY KATHERINE OWENS • JUN 05, 2017

Army trainers successfully used cyber weapons and electronic warfare (EW) technology to thwart a simulated tank assault at a training exercise conducted at the Army National Training Center at Fort Irwin, Calif. The exercise reinforced the need for the EW and cyber protection technology that is under development by entities such as the Army Rapid Capabilities Office (RCO) and U.S. Cyber Command.

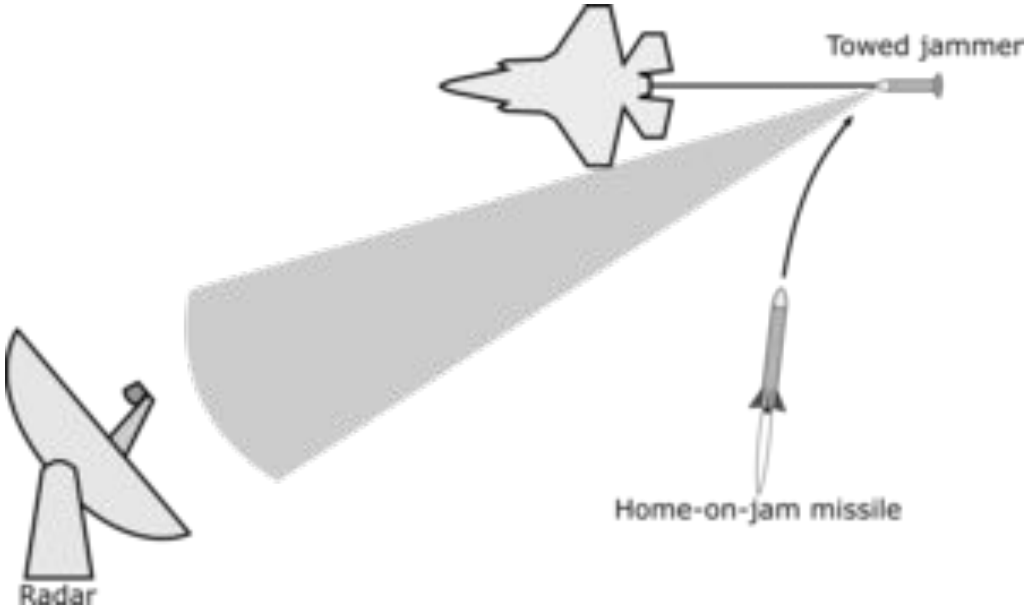
"These tanks had to stop, dismount, get out of their protection, reduce their mobility," said Capt. George Puryear, an Irregular Operations Officer at Fort Irwin. As a result, they were easily defeated.

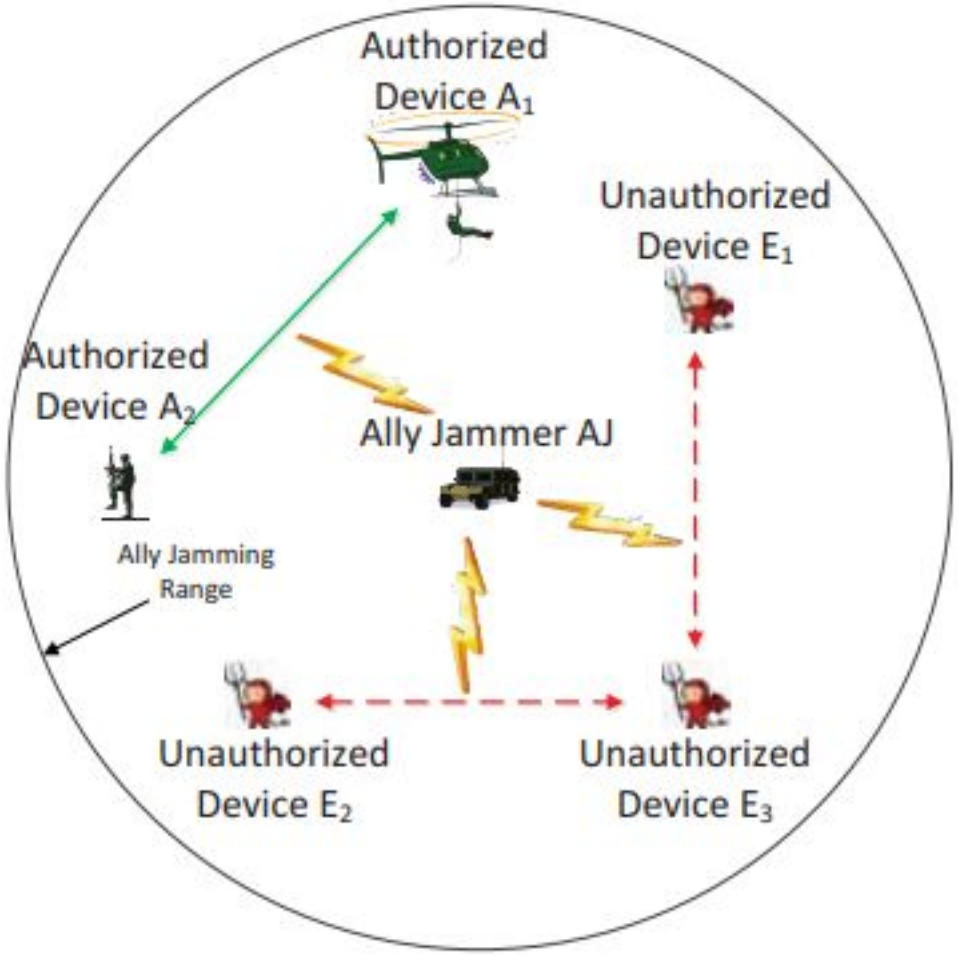
DEFENSE SYSTEMS

Jamming

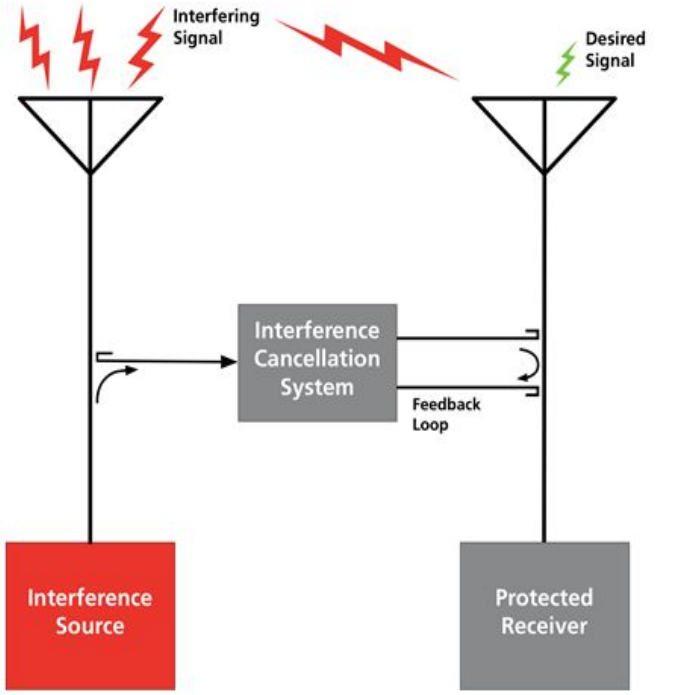


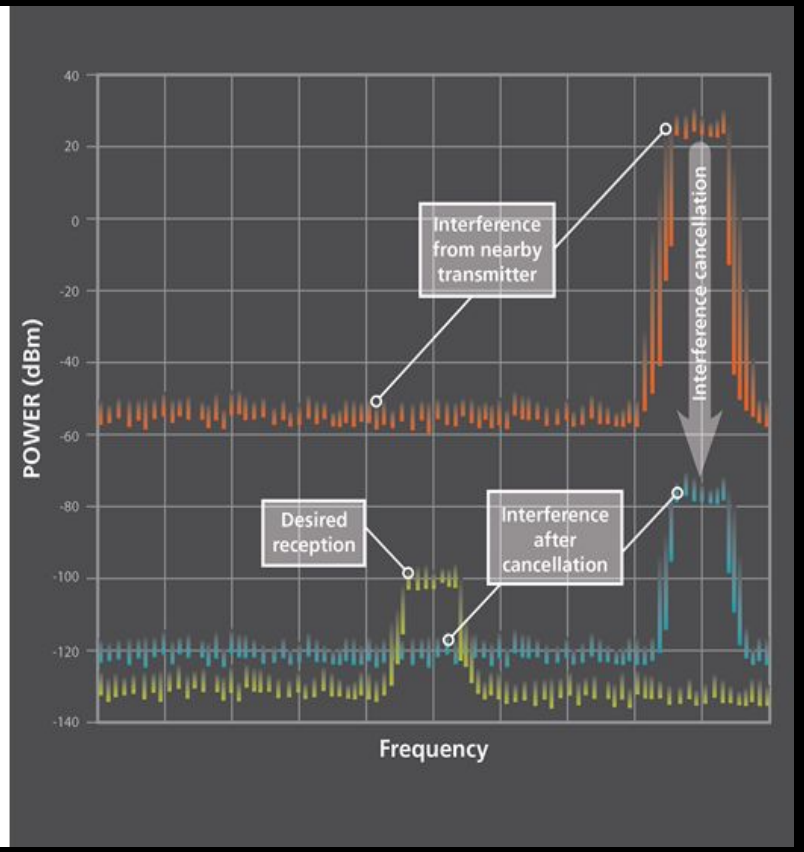
How do we communicate while Jamming?





How do we communicate while Jamming?





EA-18G Interference Cancellation System (INCANS)

A question of power

P: Transmitter power (100 kW) wavelength λ

Power reaching aircraft at range r: $\frac{GP}{4\pi r^2}$

Reflected power: $\frac{GPA}{4\pi r^2}$

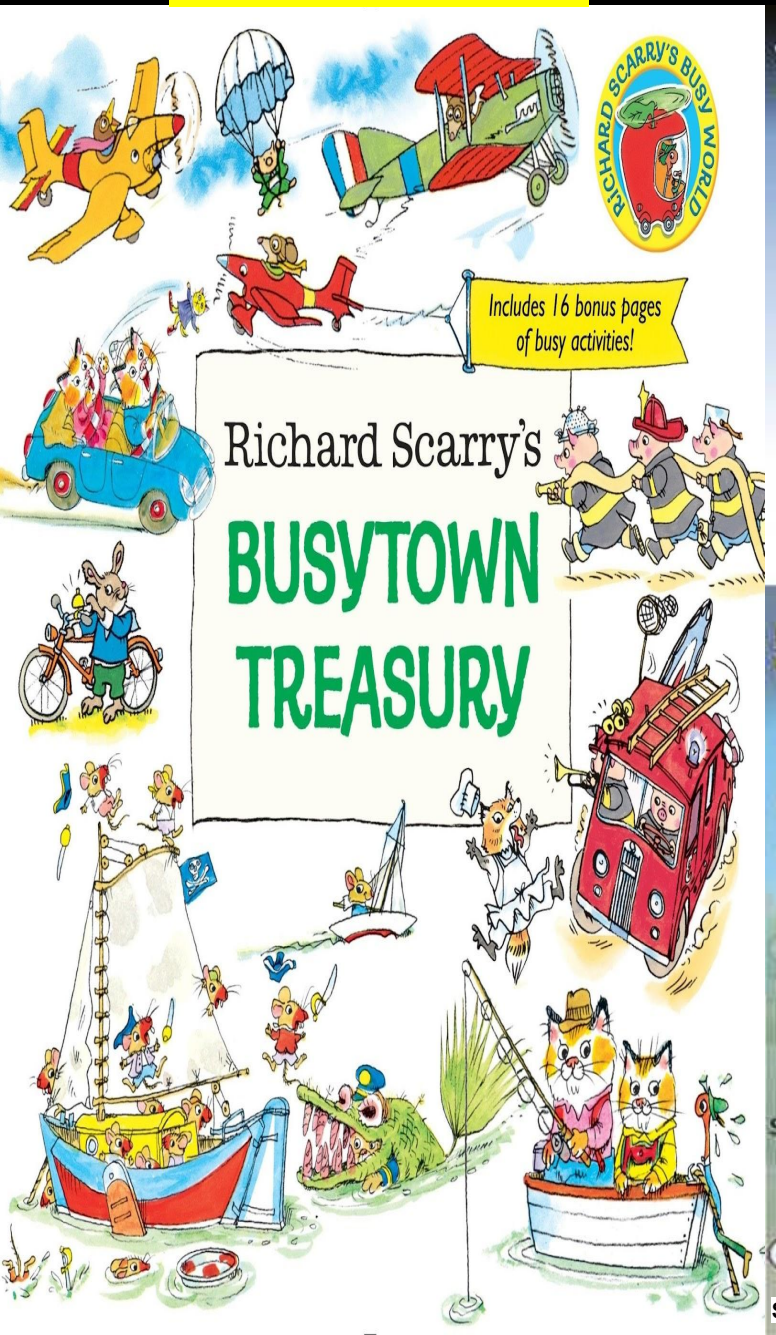
Power reaching receiver: $\frac{GPA}{16\pi^2 r^4}$

Power received: $P_r = \frac{G^2 P A \lambda^2}{64\pi^3 r^4}$

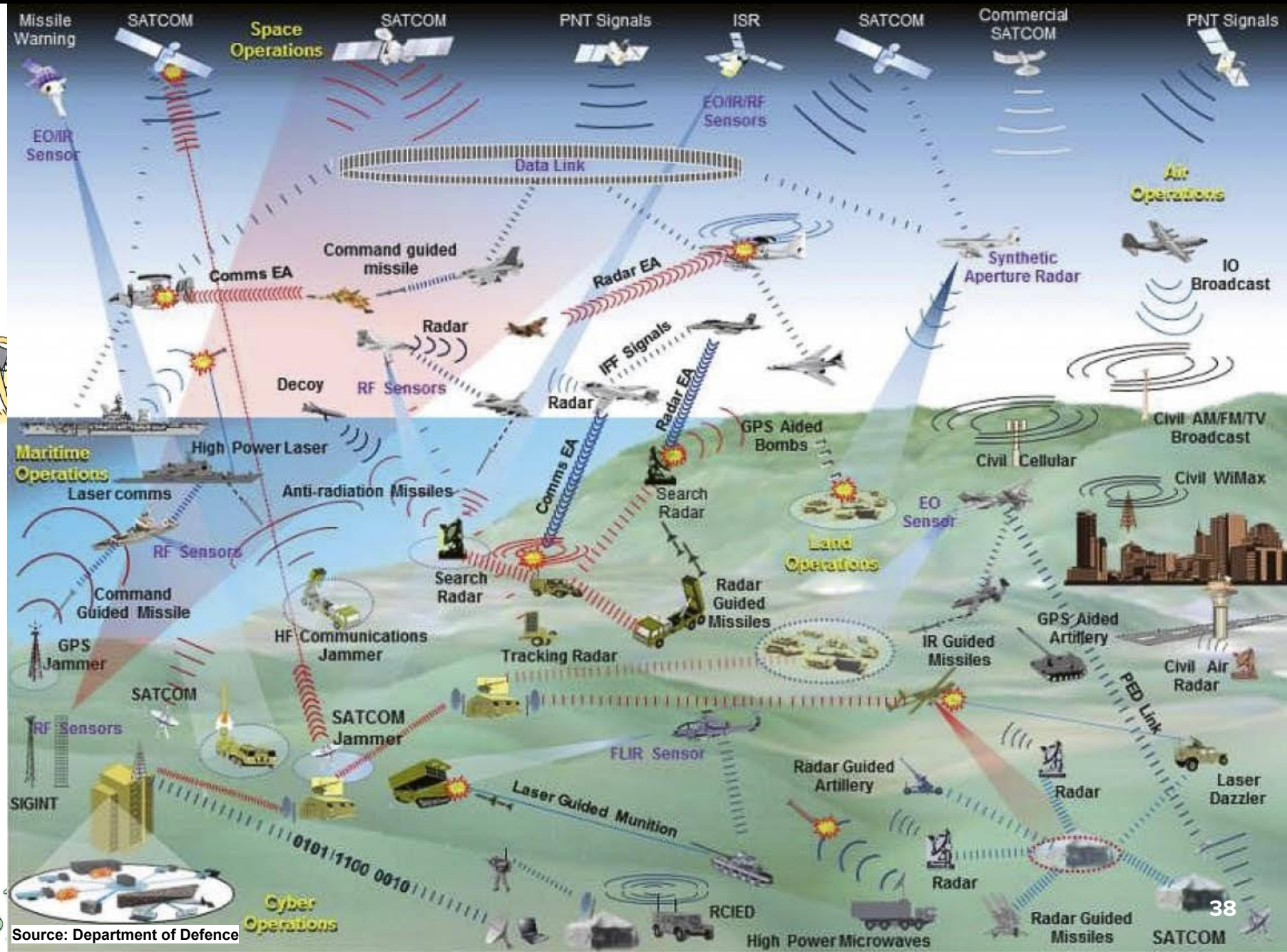
If r = 10km then received power is in pico Watts!

Target	RCS (m2)
Navy cruiser (length 200m)	14000
B-52 Stratofortress	100 –125
C-130 Hercules	80
F-15 Eagle	10–25
Su-27 Flanker	10–15
F-4 Phantom	6–10
Mig-29 Fulcrum	3–5
F-16A	5
F-18 C/D Hornet	1–3
M-2000	1–2
F-16 C (with reduced RCS)	1.2
T-38 Talon	1
B-1B Lancer	0.75–1
Sukhoi FGFA prototype	0.5
Tomahawk TLAM	0.5
Exocet, Harpoon	0.1
Eurofighter Typhoon	0.1 class
F-18 E/F Super Hornet	0.1 class
F-16 IN Super Viper	0.1 class
Rafale	0.1 class
B-2 Spirit	0.1 or less
F-117A Nighthawk	0.025 or less
bird	0.01
F-35 Lightning II	0.0015 –0,005
F-22 Raptor	0,0001–0.0005
insect	0.00001

How it started..

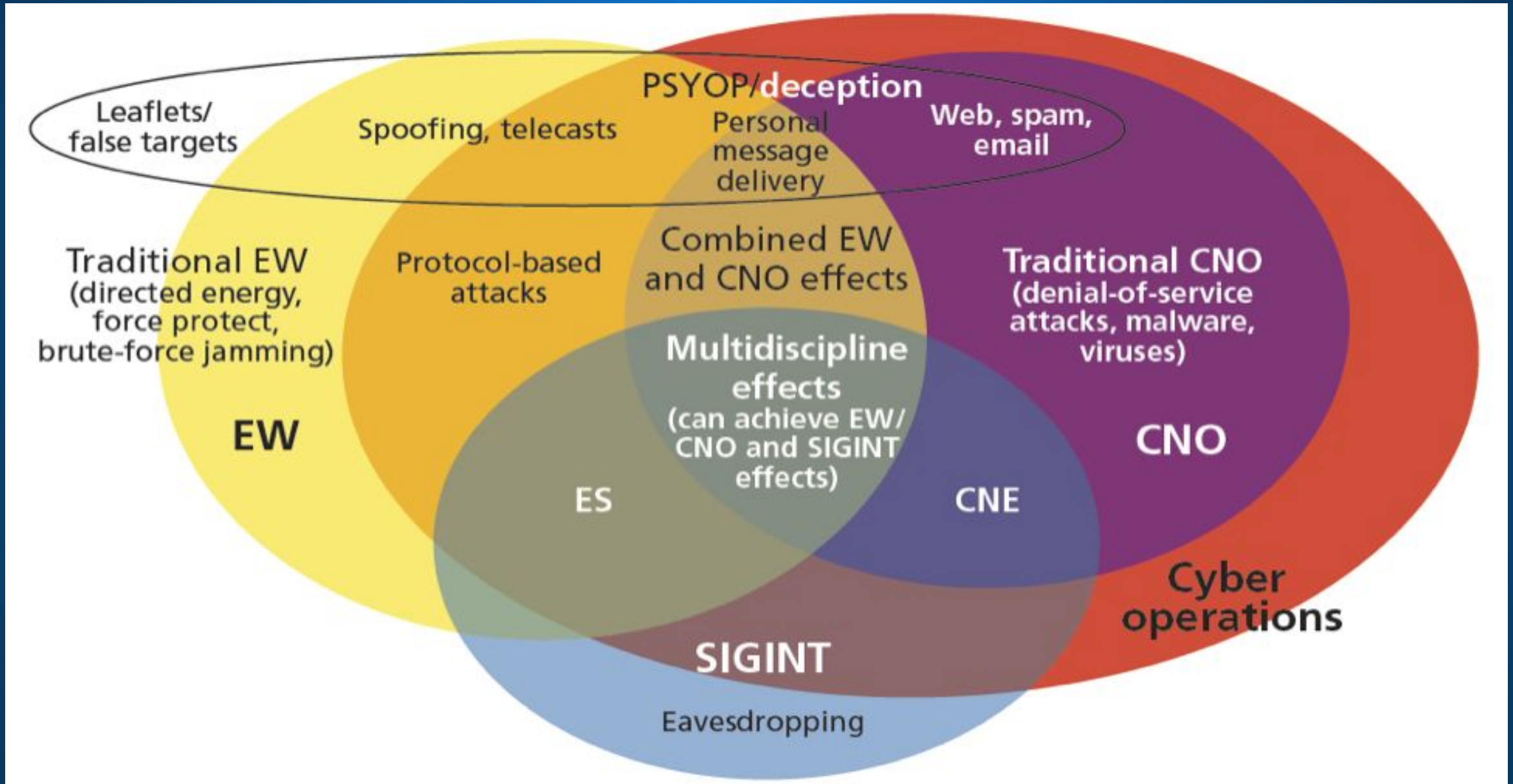


How it's going..

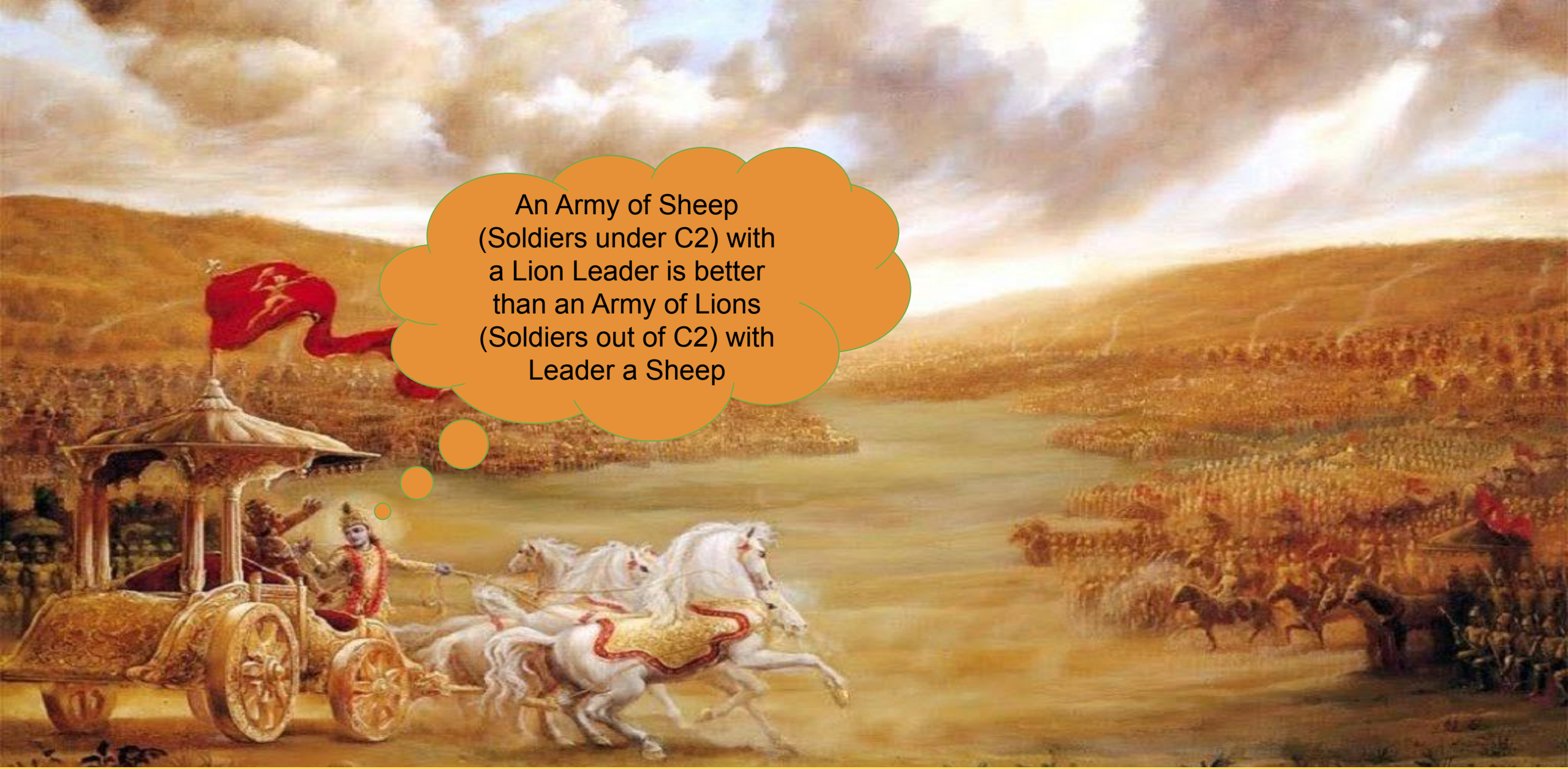


Source: Department of Defence

The Era of Convergence..

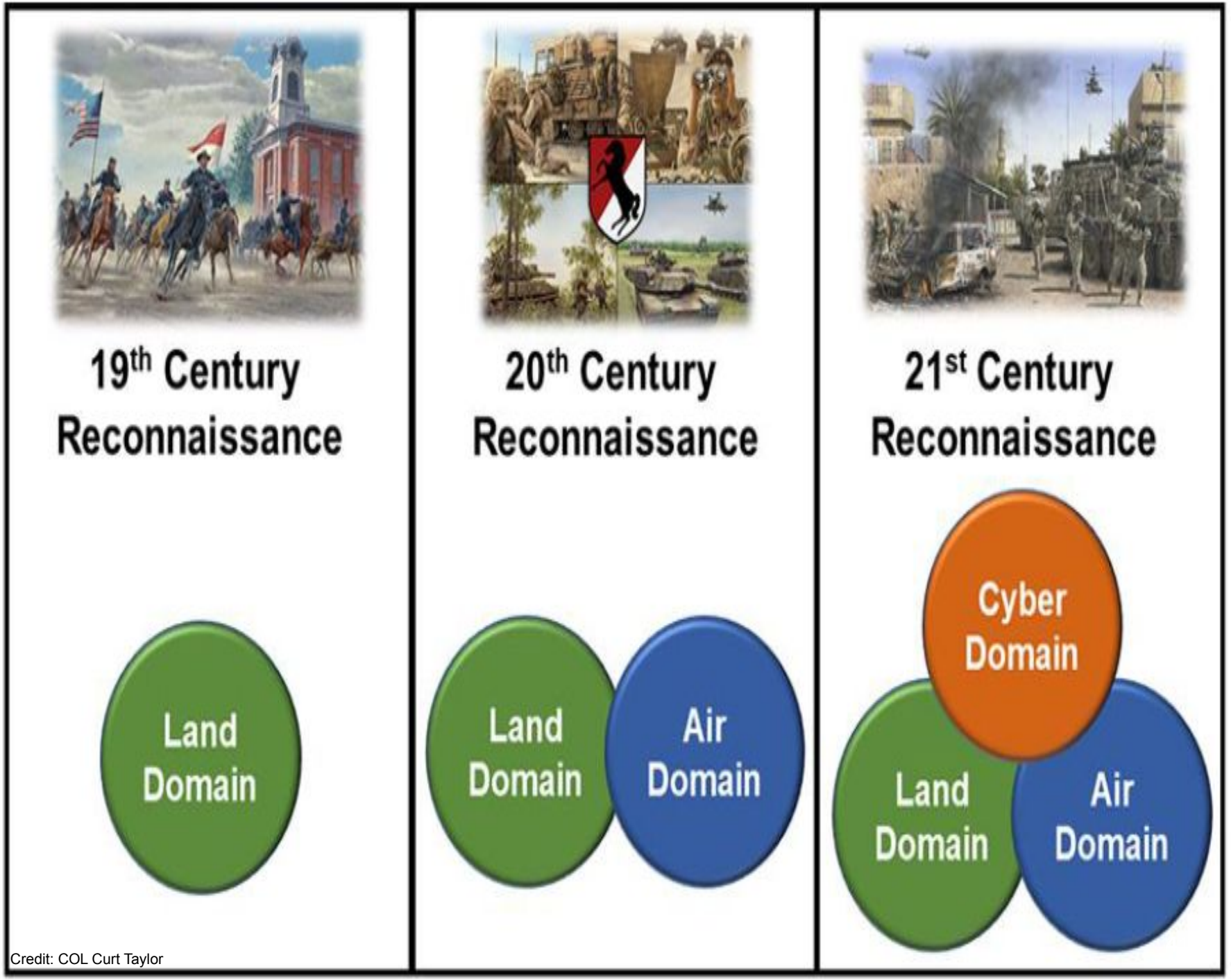


Source: Porche, et al., "Redefining Information Warfare Boundaries for an Army in a Wireless World," p.51



Lord Krishna was the First who understands the Important of “C2”, Implementing successfully C2 & EW Tactics in the Battle of Mahabharat

As warfare expands into more domains, our concept of reconnaissance operations must expand with it.



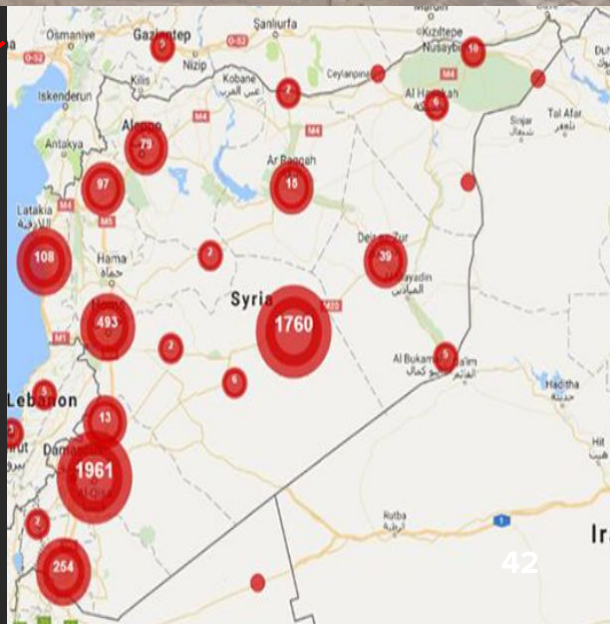
Case Studies: ISR&T

A Russian soldier's post on social media following the invasion of Ukraine.
(Photo accessed at https://www.vox.com/2015/6/17/8795235/russia-ukraine-troops)

Fitness tracking app Strava gives away location of secret US army bases
(Photo accessed at https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases)

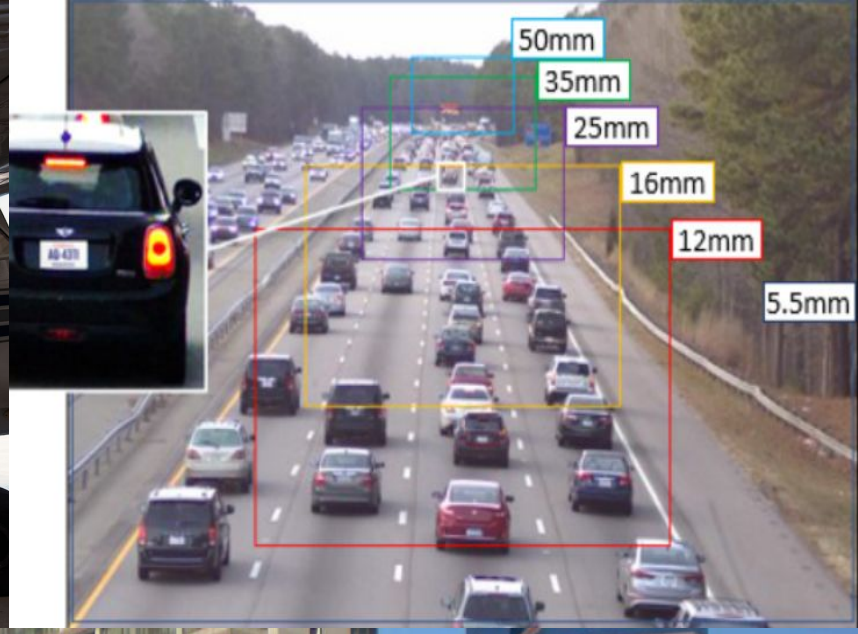
Using this photograph posted on a Russian social-media site, Bellingcat established that Buk 332 had transited Russia prior to shooting down Malaysian Flight 17.
(Photo accessed at https://www.bellingcat.com/news/uk-and-europe/2015/07/16/russias-colin-powell-moment-how-the-russian-governments-mh17-lies-were-exposed)

Ushahidi Syria tracker provides real world situational awareness of battlefield activity based entirely on social-media posts.
(See https://www.ushahidi.com/case-studies/syri -tracker, accessed May 27, 2018)



Emerging tools of Cyber Reconnaissance

- Situational understanding through social-media analysis
- Route reconnaissance using Global Positioning System-enabled device-pattern analysis.
- Near-real-time commercial-satellite imagery.



Credit: Persistent Surveillance's Cessna.

Internet of Military Things (IoMT)

The ‘B’ in IoBT - Internet of Battlefield Things:

- Adversarial and hostile environments
- Extreme and wide ranging weather and physical environment
- Often not retrieved or not safe to retrieve
- Service calls for malfunctioning or compromised device are not a phone call away
- Time constraints are critical to the success of a mission but a device needs to be able to remain dormant and functional until then.

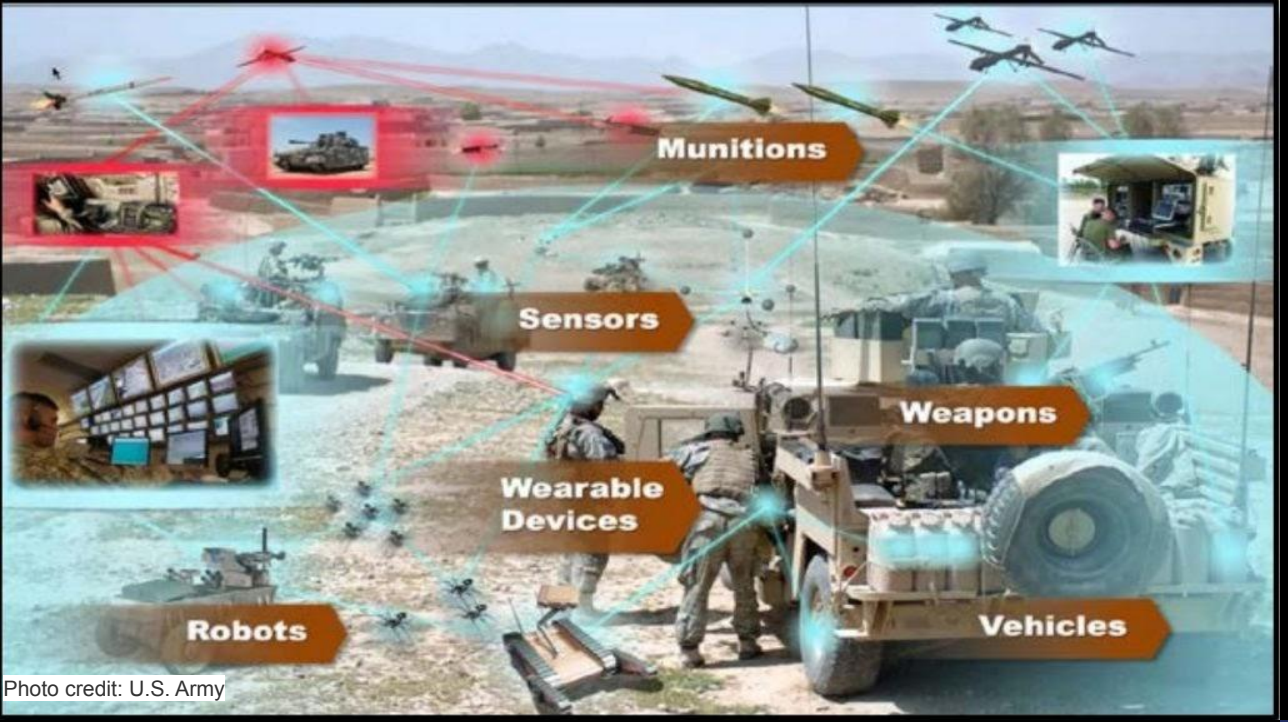


Photo credit: U.S. Army

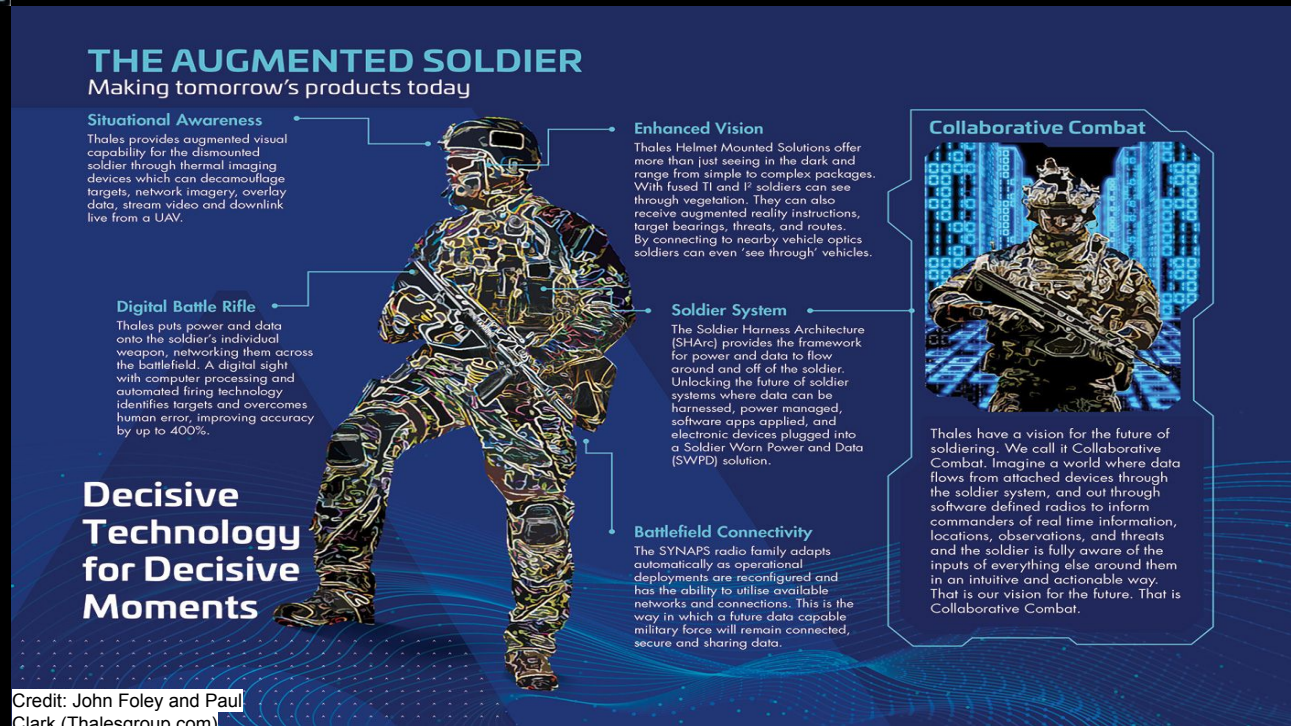
Internet of Battlefield Things - Key Properties

- ➔ Diverse ownership:
  - Friendly (BLUE)
  - Neutral/Civilian (GREY)
  - Enemy (RED)
- ➔ Growing variety of devices
- ➔ Dynamic asset + environment conditions
- ➔ Potential for degraded compromised networking infrastructure

Key Technology trends impacting IoBT:

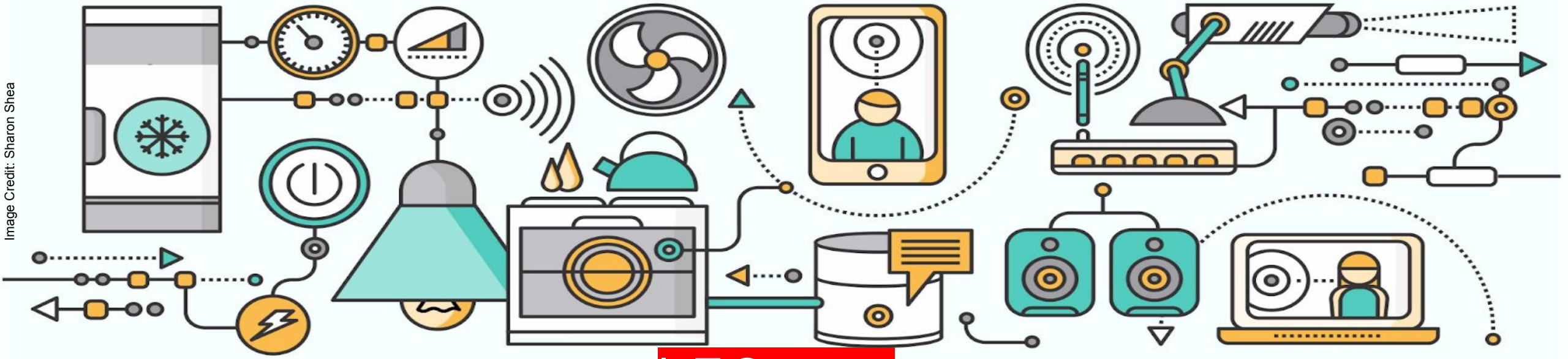
- AI and Analytics
- Sensors
- Health Monitoring Systems
- Processors and Transmitters
- Data Storage
- Security

Gazing Ahead: What Modern RF Combat Looks Like in the Next Decade | Harshit Agrawal



Credit: John Foley and Paul Clark (Thalesgroup.com)

Image Credit: Sharon Shea

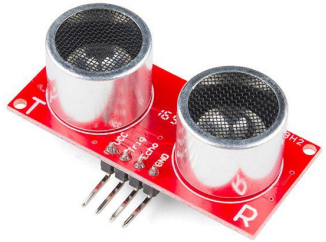


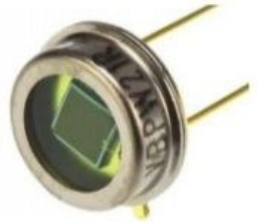
IoT Sensors

Temperature Sensor

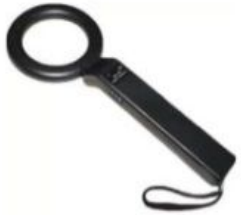
Humidity Sensor

Proximity Sensor

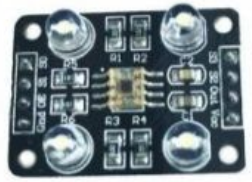




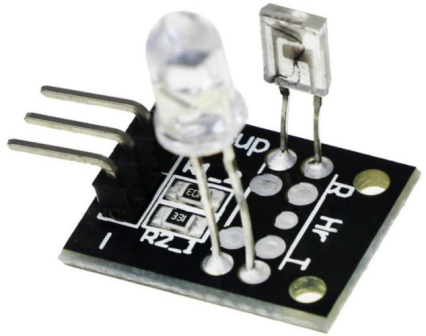
Light Sensor



Metal Sensor



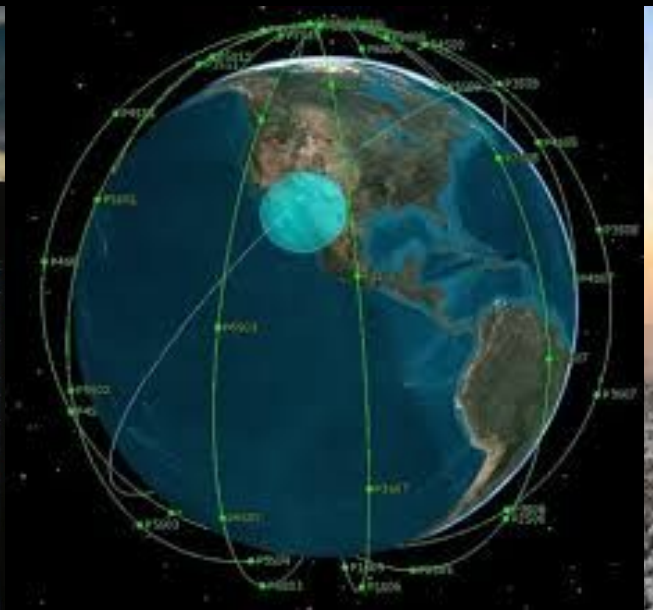
Color Sensor



Credit: Harris Corporation

Credit: https://www.soldiermod.com/volume-25/thales-2020-2.html

Autonomous Weapon Systems




NY
AF
85 500

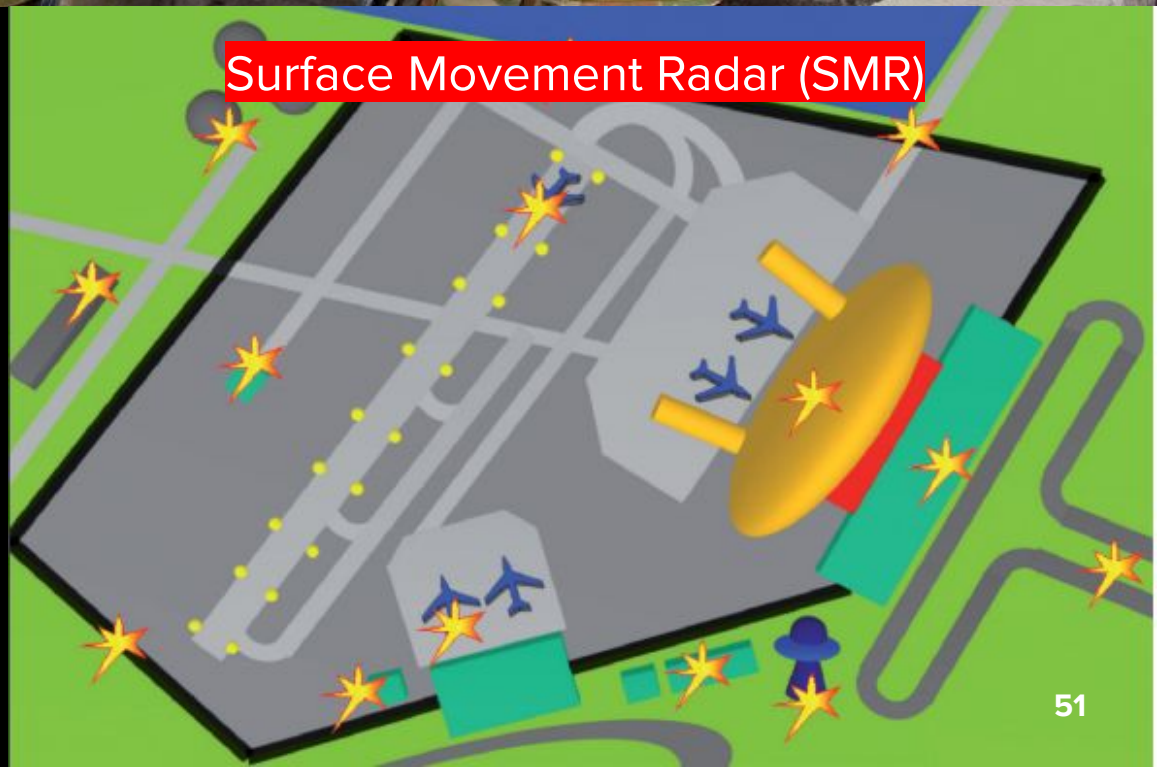

SELF DRIVING MODE
40


OPENTOTEX

Drone is hard to be detected by naked eye.

- Technological reasons:
  - Small size ➔ small RCS signal buried in many noisy environments.
  - Slow-moving ➔ moving target detector sets a higher threshold.
    - Ground/Sea clutters.
    - Related to drone pulses, PRF, RPI, CPI design etc.
  - Earth geometry and landscape blockage.
  - Too many similar targets for be tracked.
- Trade-offs between:
  - “false alarm” versus “missed targets”
  - “cost” and “performance”.

Radars need to be tailored to be able to detect drones.



Improvised Explosive Device (IED)

Counter IED Techniques

Initiation mode	Initiation system	Remarks
Timed	Chemical decay	
	Clockwork	
	Electronic timer	
Command-initiated	Suicide	PBIED Can also be timed
	Radio-controlled (RCIED)	
	Command wire (CWIED)	
	Passive infrared	
	Active infrared	
	Projectile-controlled (PCIED)	Uses a rifle bullet to connect a circuit from a distance
Victim-operated (VOIED)	Booby traps	
	Pressure pads	
	Pull switches	

Source: Adrian Wilkinson, James Bevan, and Ian Biddle

Space Warfare: Strategy and Principles

There are several potential objectives for an attacking force in a space war:

1. Deceive an enemy so that they react in ways that hurt their interests

2. Disrupt, deny, or degrade an enemy's ability to use a space capability, either temporarily or permanently

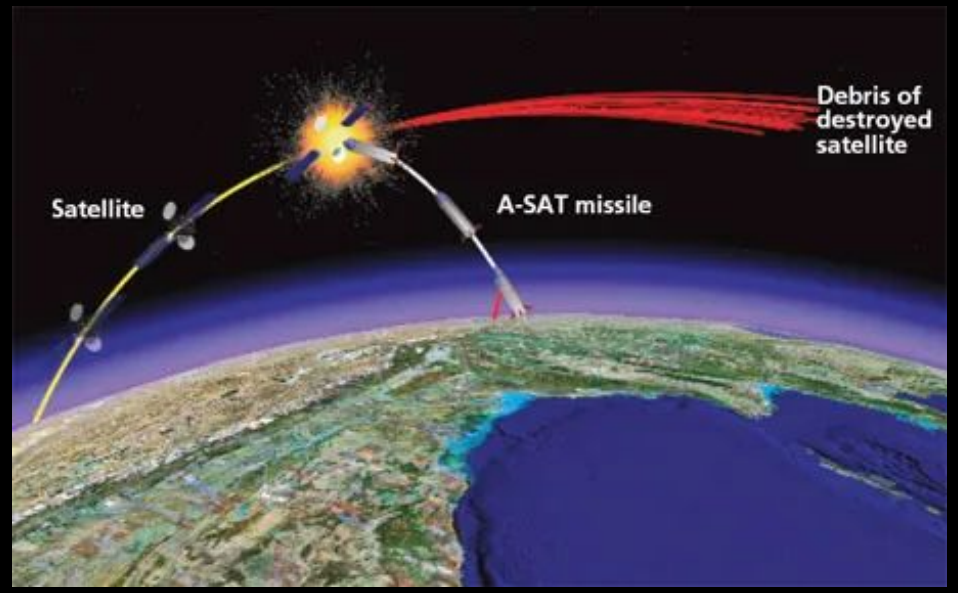
3. Destroy completely a space-based capability

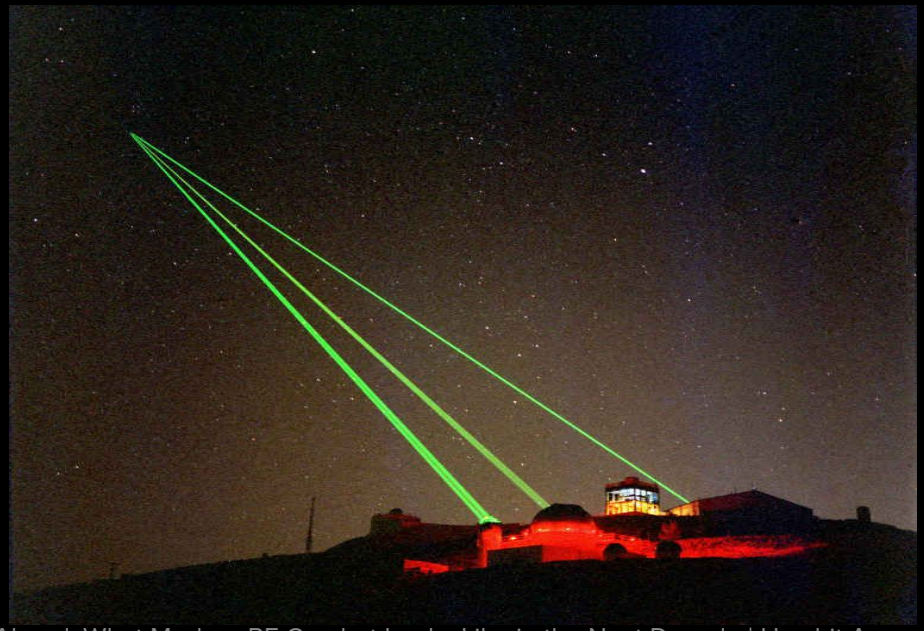
4. Deter or defend against a counter attacking adversary, either in space or on Earth

Counterspace Weapons

Kinetic Physical Attack

- Direct Ascent-SAT
- Co-Orbital ASAT
- Ground Station Attack





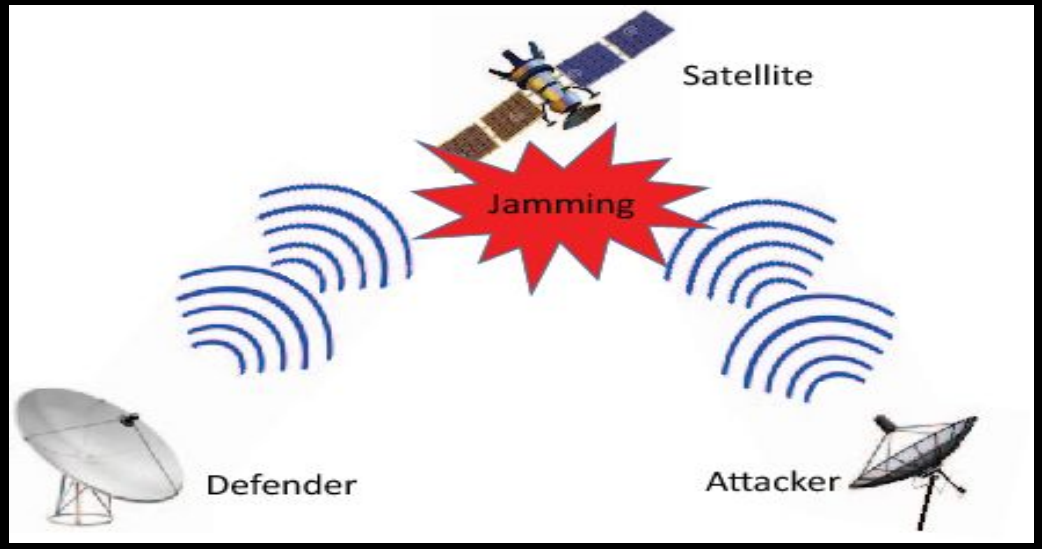
Non-Kinetic Attack

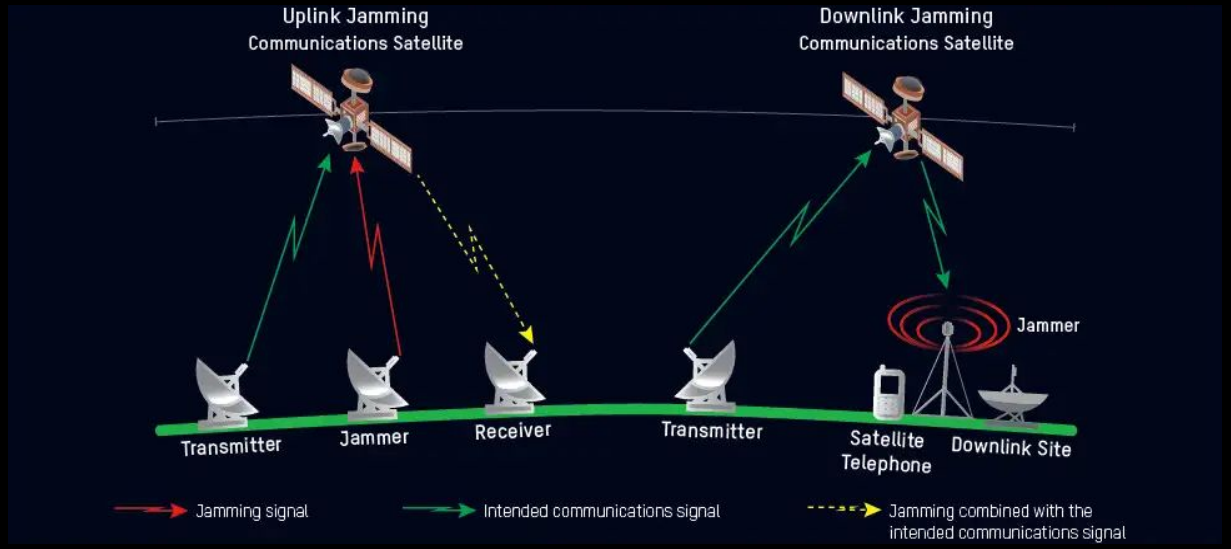
- Electromagnetic Pulse Attack
- High-Powered Laser
- High-Powered Microwave

Counterspace Weapons

Electronic Warfare

- Jamming
- Spoofing





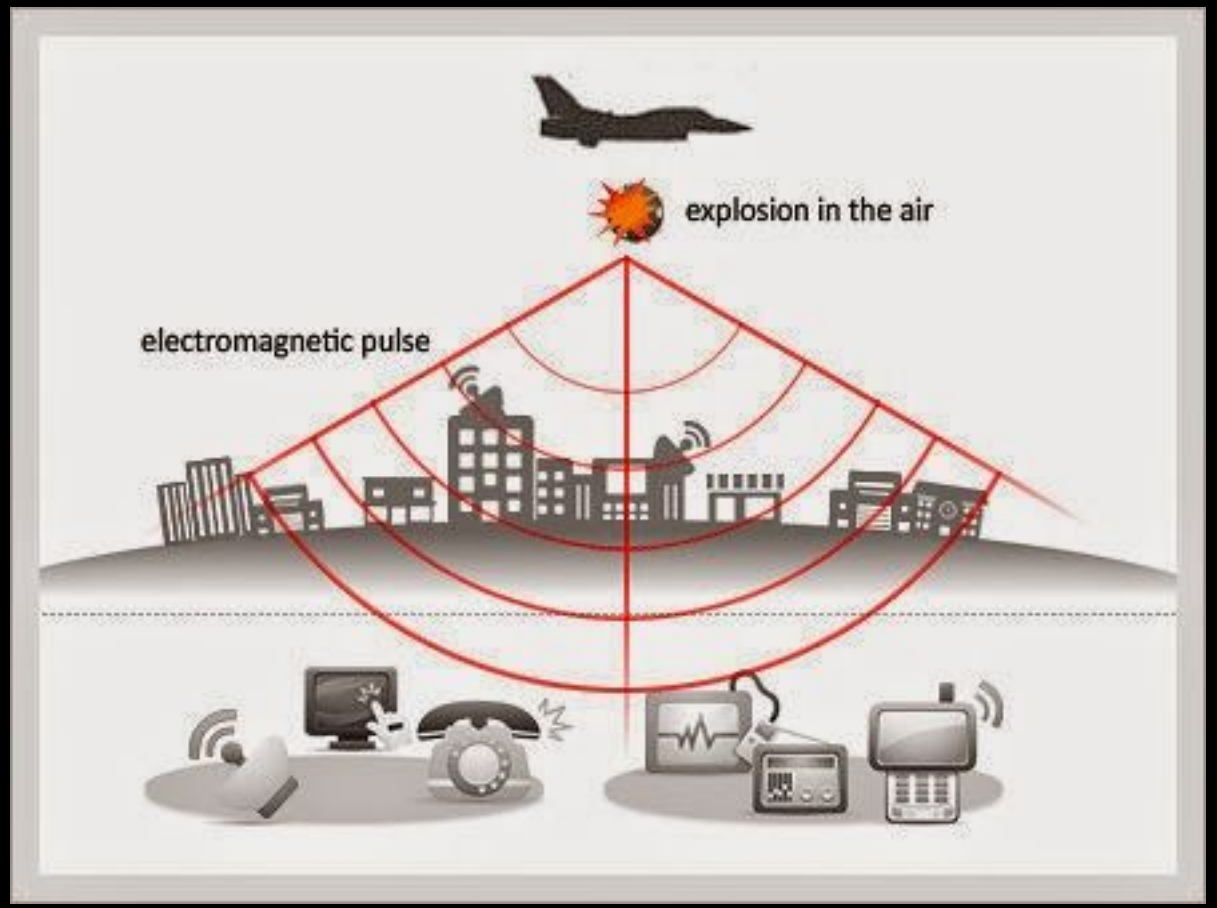
Cyber Attack

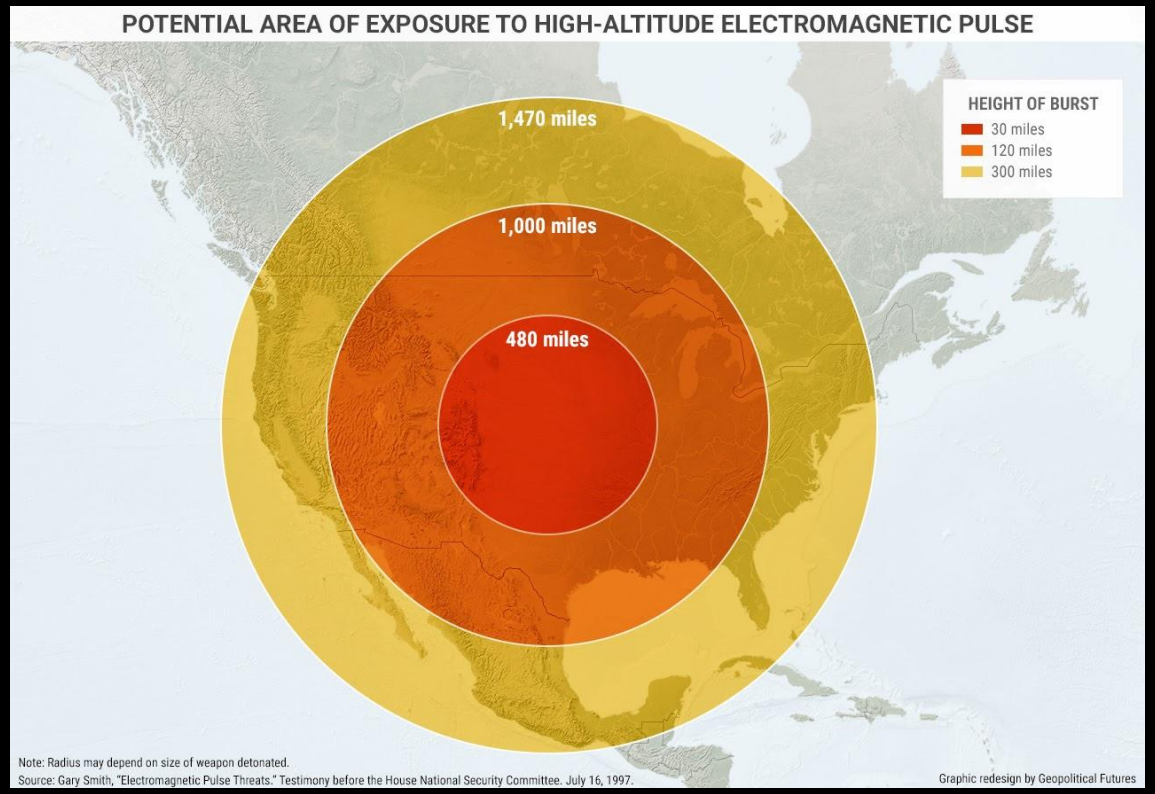
- Data Intercept / Monitoring
- Data Corruption
- Seizure of Control

Space Warfare

- Electronic Warfare, Directed Energy, and Cyberattacks
  - Intensity Dissipation
  - Precision
    - Frequency
    - Polarization
    - Signal Strength

The EMP Threat: Examining the Consequences





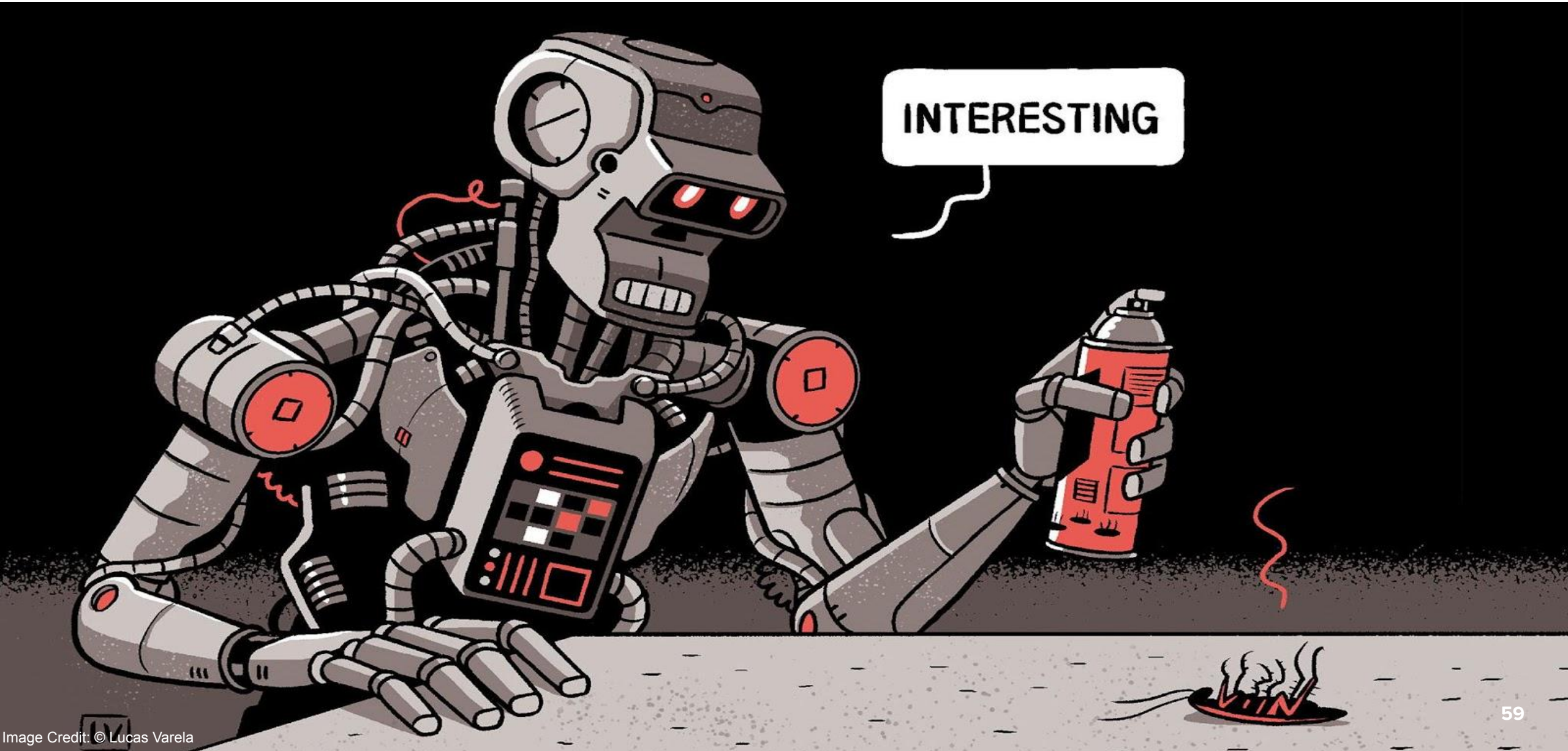


Image Credit: © Lucas Varela

References (academia, standards, reports)

- Andrew Toth, Dan Rapczynski, and Jason A. Wampler "Lightweight hardware monitoring of IoT devices", Proc. SPIE 10630, Cyber Sensing 2018, 106300H (3 May 2018); https://doi-org.ezproxy.bu.edu/10.1117/12.2305254
- Hardware Security in IoT Devices with Emphasis on Hardware Trojans Simranjeet Sidhu 1 , Bassam J. Mohd 2 and Thaier Hayajneh 1,*
- Venugopalan, V., Patterson, C.D. Surveying the Hardware Trojan Threat Landscape for the Internet-of-Things. J Hardw Syst Secur 2, 131–141 (2018). https://doi.org/10.1007/s41635-018-0037-2
- Ibrar Yaqoob, Ejaz Ahmed, DOI:10.1016/j.comnet.2017.09.003
- Beth Stackpole, (ANSYS)
- https://www.digitalengineering247.com/article/keeping-the-connected-soldier-connected-with-simulation/
- Harris Corporation
- Porche, et al., “Redefining Information Warfare Boundaries for an Army in a Wireless World,” p.51
- https://www.dailysignal.com/2016/06/29/nato-designates-cyber-as-official-domain-for-warfare/
- http://www.beechamresearch.com/download.aspx?id=43
- Department of Defense, USA
- North Atlantic Treaty Organization (NATO)
- L3Harris Corporation
- Persistent Surveillance Cessna.
- IoBT Reign, University of Illinois at Urbana-Champaign
- Venugopalan, V., Patterson, C.D. Surveying the Hardware Trojan Threat Landscape for the Internet-of-Things.

Conclusions:

- War Fighting Environment will continue to change, & be more reliant on Spectrum for operations
- Spectrum is a critical manoeuvre(sp) space – one can make a difference by advancing there tradecraft
- To Counter current and evolving threat: EW, Cyber, Spectrum Operations, Spectrum Manoeuvre is required
- Airborne EW must include Multi-function Weapons
- Rapid Threat detection, Cooperative Systems, Coherent Effects, Cognitive and Autonomous Systems

Thank You For Attending My Talk. ☺️

Harshit Agrawal

Security Researcher

harshit.nic@gmail.com

Twitter: @harshitnic

https://www.linkedin.com/in/harshitnic/