

Critical Infrastructure Security

Lecture 7

Dr. Naveed Anwar Bhatti

Webpage: naveedanwarbhatti.github.io

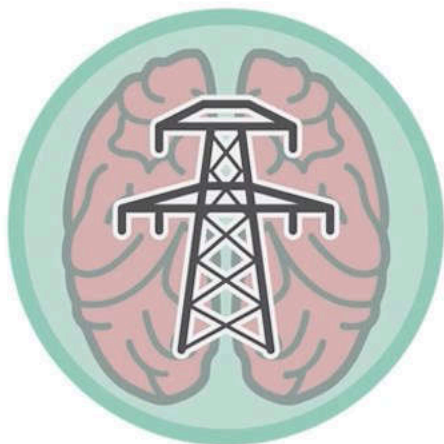


SECURING SMART GRID





The consequences of a cyber attack against the Smart Grid range from espionage to sabotage, and from petty theft to larger privacy concerns



The consequences of a cyber attack against the Smart Grid range from espionage to sabotage, and from petty theft to larger privacy concerns

While no one product or technology is certain to stop all attacks, when used together in a defense-in-depth posture across all areas of the Smart Grid, it is possible to greatly minimize the risk of a successful cyber attack.

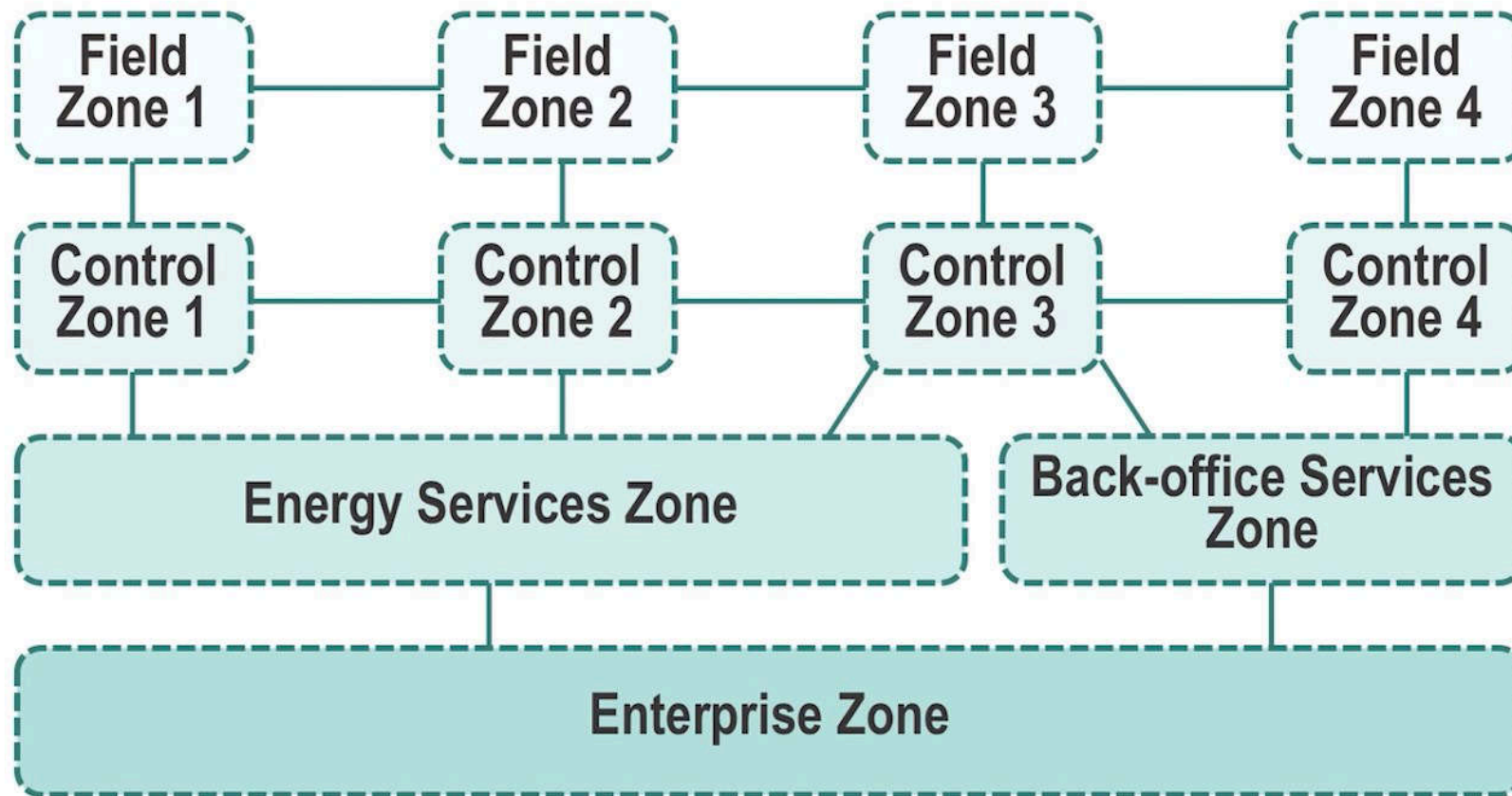
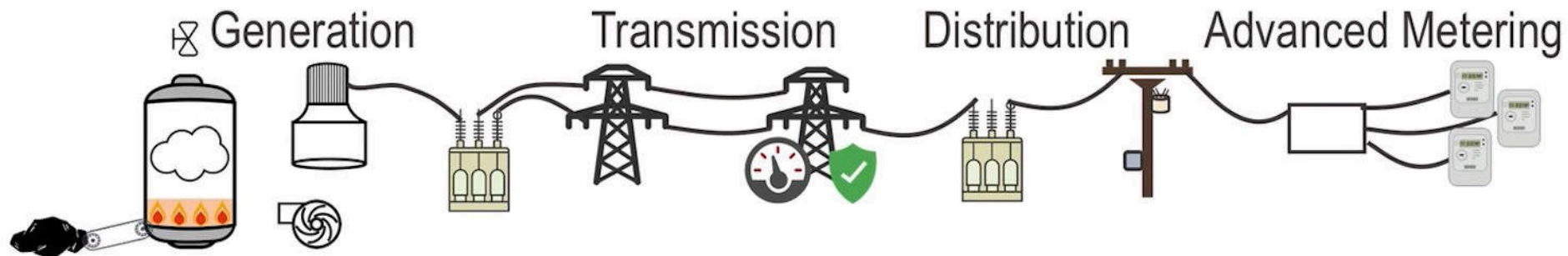


It is therefore necessary to—above all else—establish appropriate monitoring of all Smart Grid systems to obtain situational awareness.

By looking at the entirety of a system's digital behaviors, areas of risk can be identified, attacks can be detected, and suspicious or dangerous trends can be identified.



Securing Smart Grid





FIELD ZONE PROTECTION

Field devices are often embedded systems.

Low cost and low power consumption

Smart grid owner is unable to alter these devices, or install any commercially available cyber security countermeasure.





FIELD ZONE PROTECTION

Field devices are often embedded systems.

Low cost and low power consumption

Smart grid owner is unable to alter these devices, or install any commercially available cyber security countermeasure.

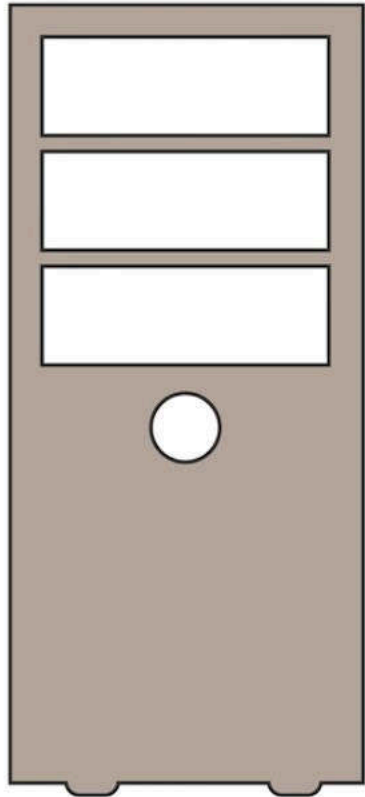
Onus falls to the device manufacturer to build cyber security.

Application whitelisting is one of the more popular software security solutions for embedded devices.





CONTROL ZONE PROTECTION



As we move further in from the field and into the substations, we see more sophisticated devices (e.g., SCADA servers, measurement and data management servers, AMI headends, and similar server-based systems).



CONTROL ZONE PROTECTION

Technologies deployed:



Application whitelisting

Antivirus

Configuration management



CONTROL ZONE PROTECTION

Technologies deployed:

Full system hardening

Separation of services (either to dedicated hardware or to individual virtual machines if virtual data centers are utilized)

Host IDS or Host IPS

Host data loss prevention (DLP)

Event logging





SERVICE ZONE PROTECTION AND BACK-OFFICE SYSTEMS

As we get to centralized SCADA systems, historians, data concentrators, and back-office systems, the capabilities of the servers increase, as does the value of the data.

There is an increased reliance upon the integrity of data and less on availability since we are moving away from real-time control to more transaction-based information.

Data integrity and information assurance tools, including database security solutions, database auditing, and data loss prevention tools in these areas.

SIEM or Log Management Tool

NETWORK FORENSICS



Drones and Critical Infrastructure

Understanding the DRONE Threat Space



Drone as target

Critical law enforcement or data collection missions using drones could be undermined by cyberattacks on these platforms

Drone as Vector

Drones in the hands of adversaries could present novel avenues for cyberattacks, with drones themselves serving as “cyber weapons” intended to deliver malicious content or kinetic impacts



Drones as a threat

DIY Spy Drone Sniffs Wi-Fi, Intercepts Phone Calls

What do you do when the target you're spying on slips behind his home security gates and beyond your reach? Launch your personal, specially-equipped drone to fly overhead and sniff his Wi-Fi network, intercept his cellphone calls, or launch denial-of-service attacks with jamming signals.

- Flying computers. (1)
- Custom payloads:
 - Sniffers
 - Jammers
 - Network Analyzers
 - 3d mapping, cameras.
 - Physical attacks, explosives.
 - ...



Drone as target

Critical law enforcement or data collection missions using UAS could be undermined by cyberattacks on these platforms

Threat

Vulnerability

Attack

Drone as Vector

UAS in the hands of adversaries could present novel avenues for cyberattacks, with UAS themselves serving as “cyber weapons” intended to deliver malicious content or kinetic impacts



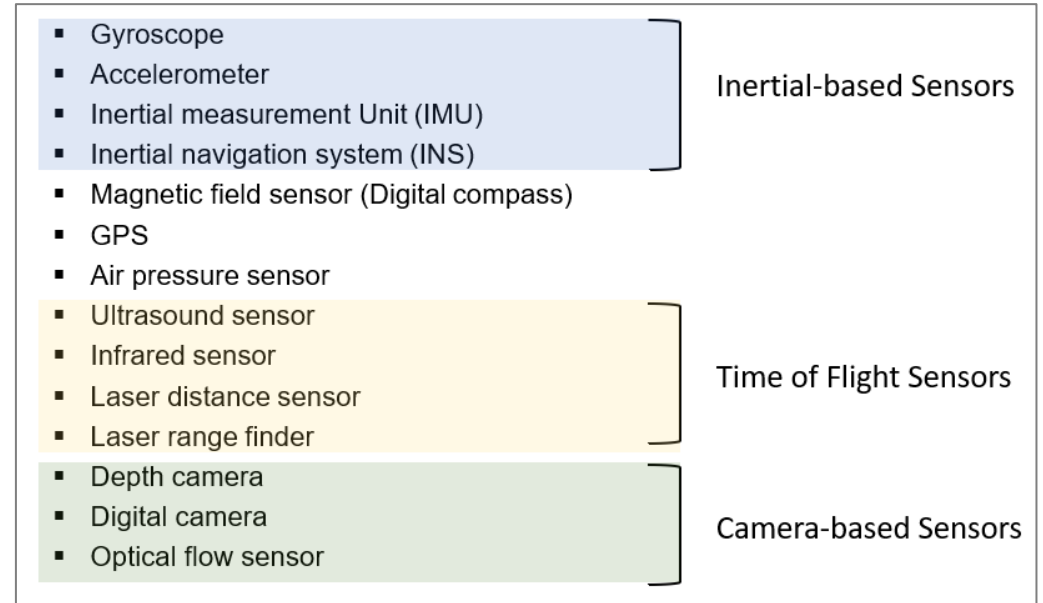
Drone-Related Attack Surfaces

- Sensors
- Navigation
- Air Traffic Control
- Fault Handling
- Application Layer
- Physical Layer
- Link Layer
- Network Layer
- AI

Sensors (+ Navigational Sensors)

- Drones are data-driven systems
 - Sensors: Eyes and Ears of the pilot

- Example of Sensors



- Spoofing/Tempering: Exploiting the limitation of sensors

- Manipulation of visual inputs
- Manipulation of EM in sensors
- Manipulation of auditory/physical inputs

- Jamming:

- Saturation of sensory limits (e.g. laser light on Camera CCDs)
- EM disruption

GPS Jamming and Spoofing

- Global Navigation Satellite System (GNSS)
 - constellation of satellites transmit position and timing data to receivers

Jamming



Spoofing/Tampering



GPS Jamming and Spoofing

- Global Navigation Satellite System (GNSS)
 - constellation of satellites transmit position and timing data to receivers

Jamming

Spoofing/Tampering

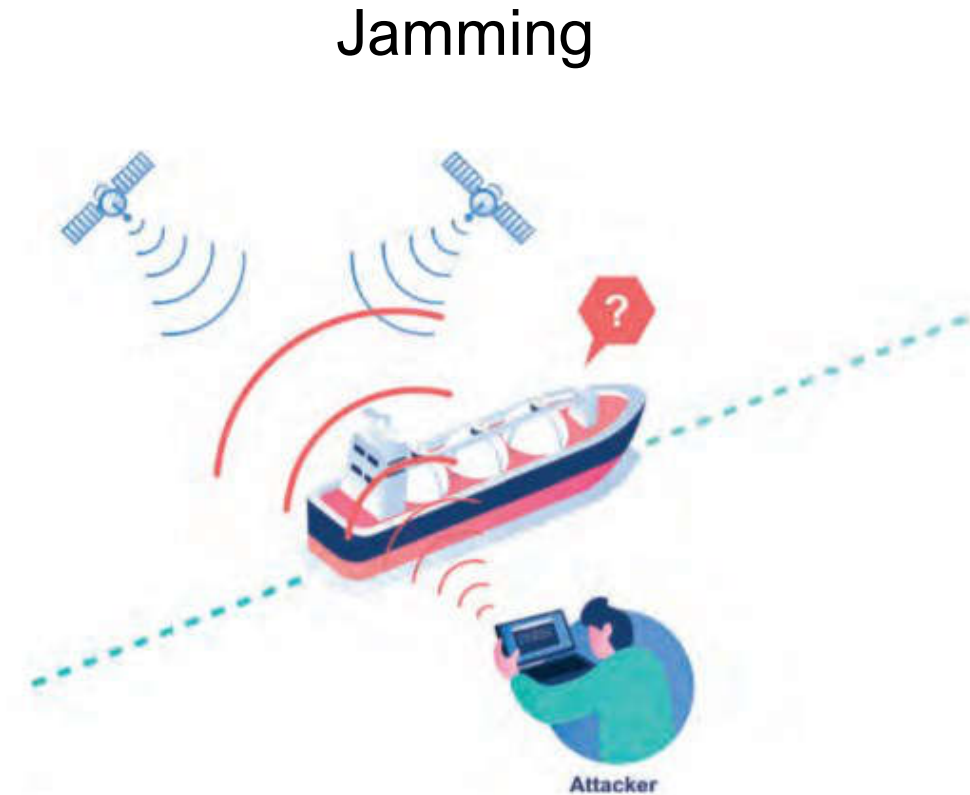
To simplify, jamming causes the receiver to **die**, spoofing causes the receiver to **lie**

Attacker

Attacker

GPS Jamming and Spoofing

- Global Navigation Satellite System (GNSS)
 - constellation of satellites transmit position and timing data to receivers
- Jamming
 - GNSS signals have low power
 - Jammed by masking the satellite signal with noise on GNSS Frequencies
 - Readily available and inexpensive




GPS Jamming and Spoofing

- Global Navigation Satellite System (GNSS)
 - constellation of satellites transmit position and timing data to receivers


- Jamming

- GNSS signals have low power
- Jammed by masking on GNSS Frequencies
- Readily available and cheap




Portable GPS Jammer
Rs 6,500/Piece [Get Latest Price](#)
Usage/Application
Type
Radius Range
Power Supply
Built-in Battery
Total Output Power
[View Complete Details](#)

Cheap GPS Signal Blocker Vehicle Global GPS Positioning For Sale



Handheld WiFi Bluetooth 3G 4G Mobile Phone Blocker GPS Jammers
8341HA-4 Handheld High power output 3G/4G/Wifi cell phone jammer must be an attractive unit for anyone who are looking out for flexible jamming solution to the various signals. The newly released jammer introducing must be the right unit for many of you: portable Wifi Bluetooth 3G 4G cell phone blocker.
\$143.78 **\$125.36**
★★★★★
[ADD TO CART](#)



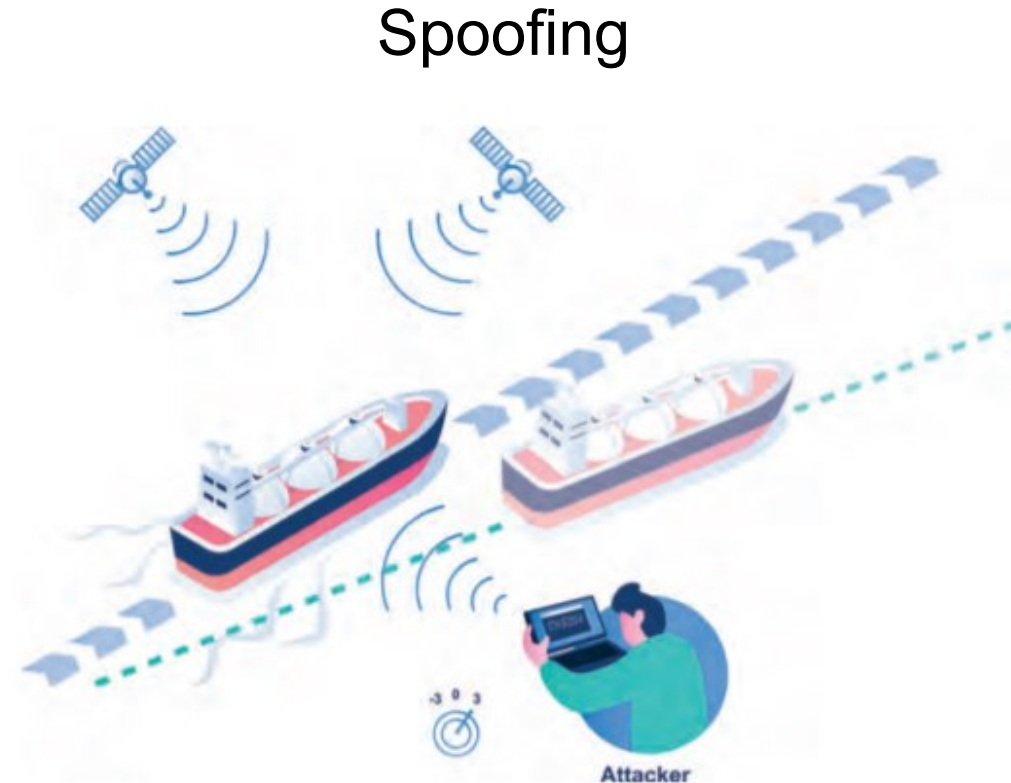
8 Antennas Handheld Cell Phone GPS Jammers,Block 2g/3G/4G and LOJACK WIFI Signals
8 Antennas Portable Cell Phone gps signal blocker,jamming all types of Android phones, Tablets, Smart Phones, iPhones, Windows phones etc. that use 2G, 3G, 4G, GPS L1-L5, LOJACK, or Remote Control 315MHz 433MHz and Bluetooth WIFI wireless signals
\$678.99 **\$387.99**
★★★★★
[ADD TO CART](#)

Jamming



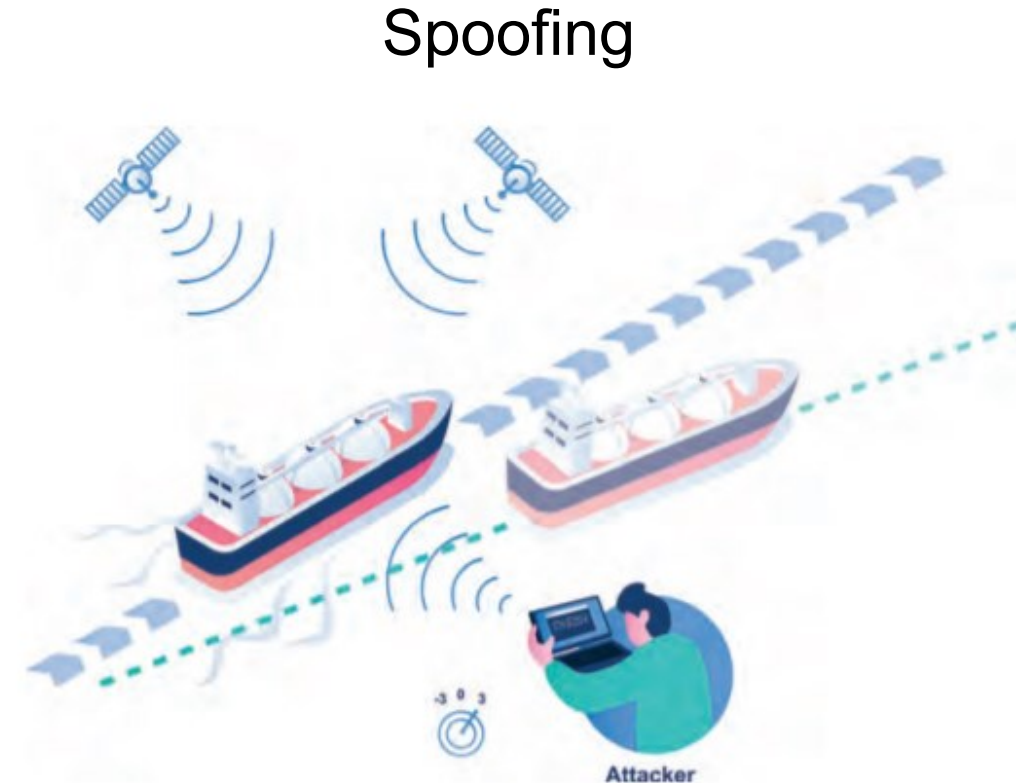
GPS Jamming and Spoofing

- Global Navigation Satellite System (GNSS)
 - constellation of satellites transmit position and timing data to receivers
- Spoofing
 - Provision of GNSS-like signals, transmitted locally and coded to fool the receiver to think it is somewhere it is not.
 - Begins by broadcasting signals synchronised with the genuine signals. The power of the counterfeit signals is then gradually increased so that the victim's GNSS receiver tracks the false signals which can then be manipulated to report a different location to the genuine signals



GPS Jamming and Spoofing

- Global Navigation Satellite System (GNSS)
 - constellation of satellites transmit position and timing data to receivers
- Meaconing
 - Type of spoofing where GNSS signals are re-transmitted
 - Requires simpler equipment than that required for a spoofing attack



GPS Jamming and Spoofing

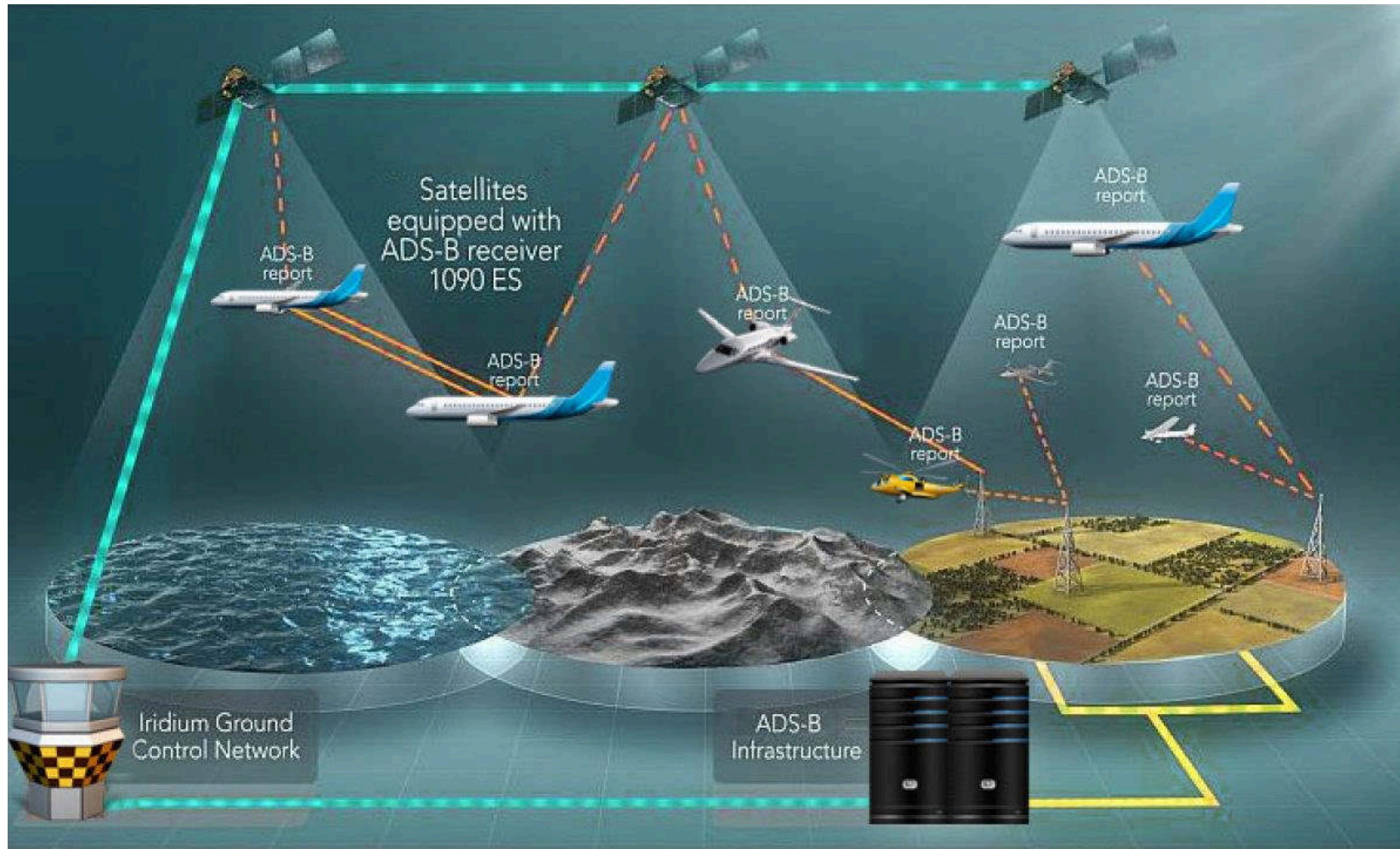
- Global Navigation Satellite System (GNSS)
 - constellation of satellites transmit position and timing
- Meaconing
 - Type of spoofing where GNSS signals are re-transmitted
 - Requires simpler equipment than that required for a spoofing attack





Air Traffic Control

- Traffic Monitoring and Collision Avoidance tools
 - ADS-B and TCAS

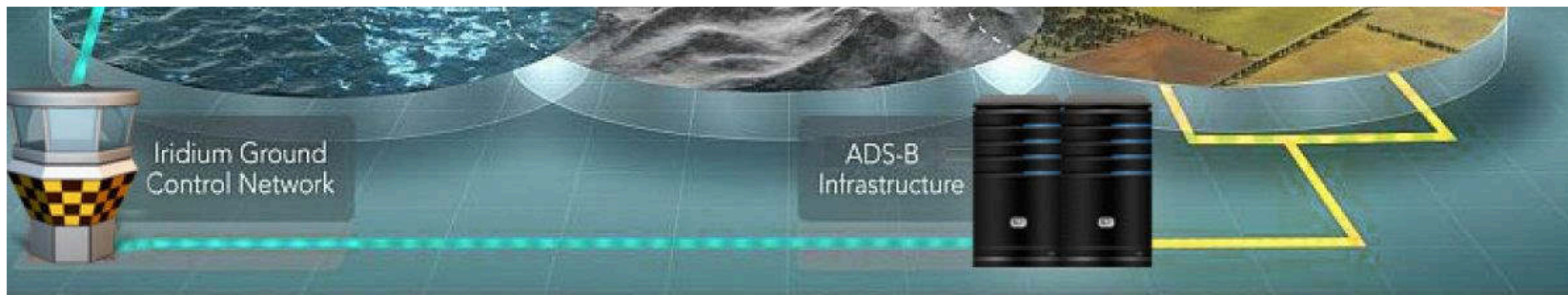
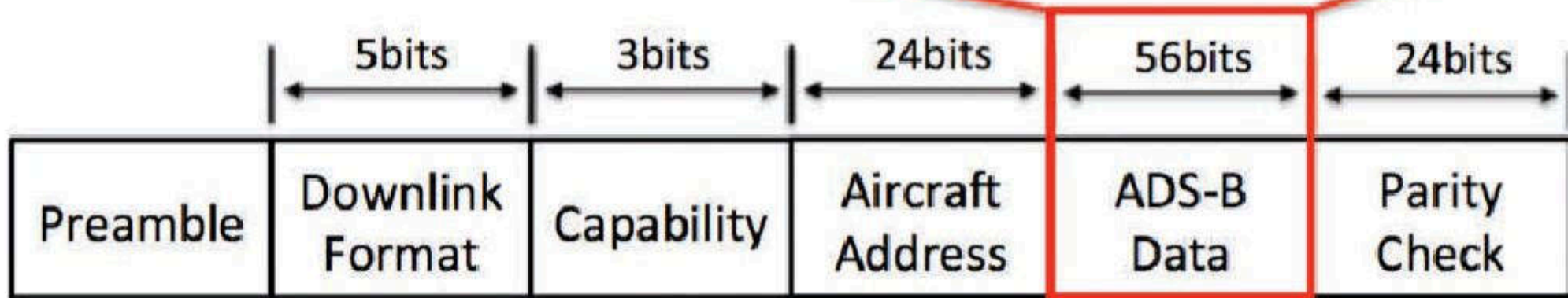




Air Traffic Control

- Traffic Monitoring and Collision Avoidance tools

[TC --]	[--- Altitude ---]	T F	[----- Latitude -----]	[----- Longitude -----]
00000 000	00000000000000	0 0	00000000000000000000	00000000000000000000



- Traffic Monitoring and Collision Avoidance tools
 - ADS-B and TCAS



AliExpress™ Radio frequency 1988 Store 98.1% Positive feedback + Follow 929 Followers

I'm shopping for... On AliExpress

Store Home Products ▾ Sale Items Top Selling Feedback

NEW 1PC FlightAware Pro Stick Plus ADS-B USB Receiver with Built-in Filter from FlightAware


★★★★★ 5.0 ▾ 9 Reviews 28 orders

US \$48.43 ~~US \$52.64~~ -8%

US \$3.00 New User Coupon [Get coupons](#)

Quantity: 1 427 pieces available

Shipping: US \$5.34
to Pakistan via AliExpress Standard Shipping ▾
Estimated Delivery: 21-39 days 🕒

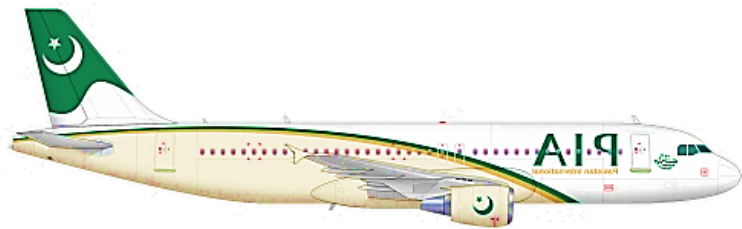


FlightAware Pro Stick Plus v1.0 ADS-B/Mode S Receiver
R820T2 + RF Amp + 1090 MHz Filter
<https://flightaware.com/adsb/prostick>



Air Traffic Control

- Traffic Monitoring and Collision Avoidance tools
 - ADS-B and TCAS

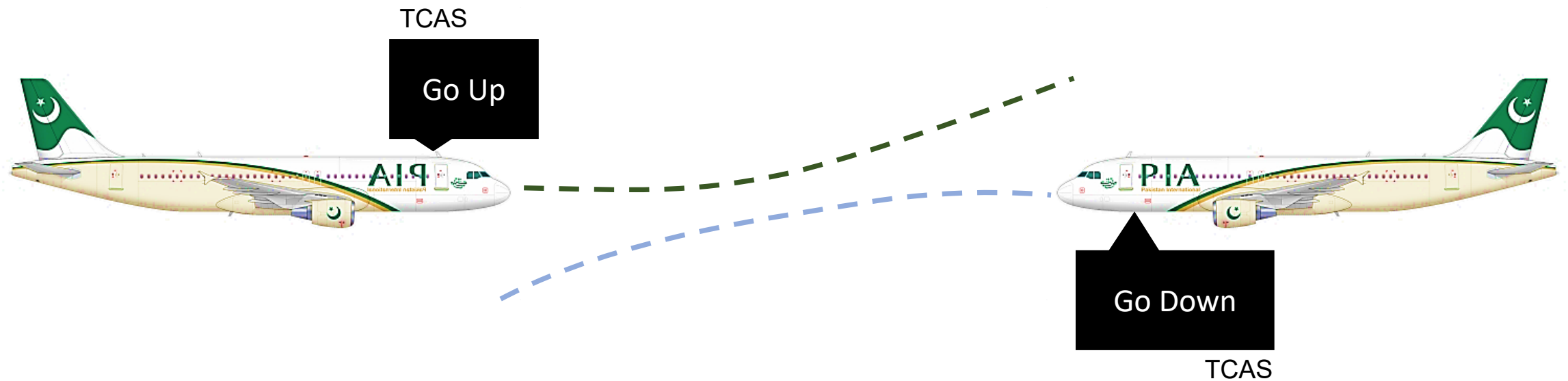




Air Traffic Control

- Traffic Monitoring and Collision Avoidance tools
 - ADS-B and TCAS

- Collision induction through collision avoidance

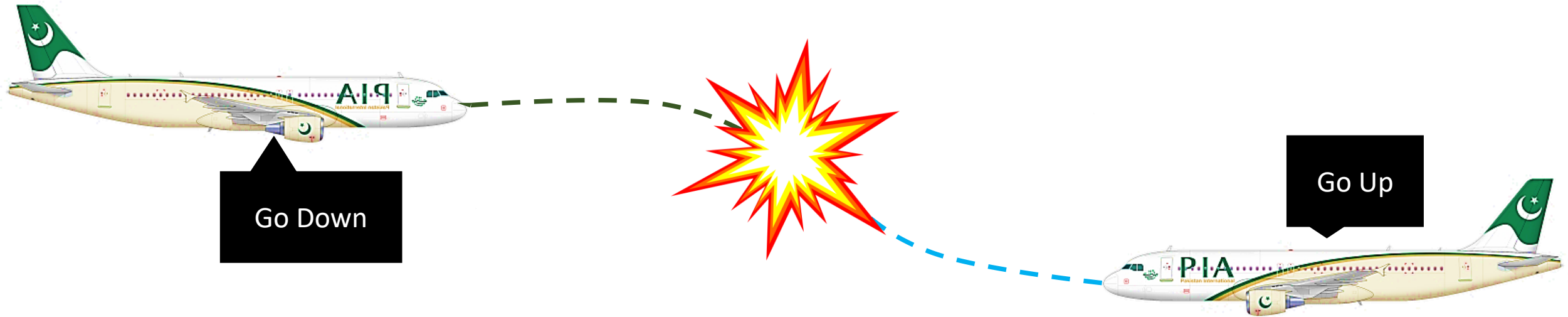




Air Traffic Control

- Traffic Monitoring and Collision Avoidance tools
 - ADS-B and TCAS

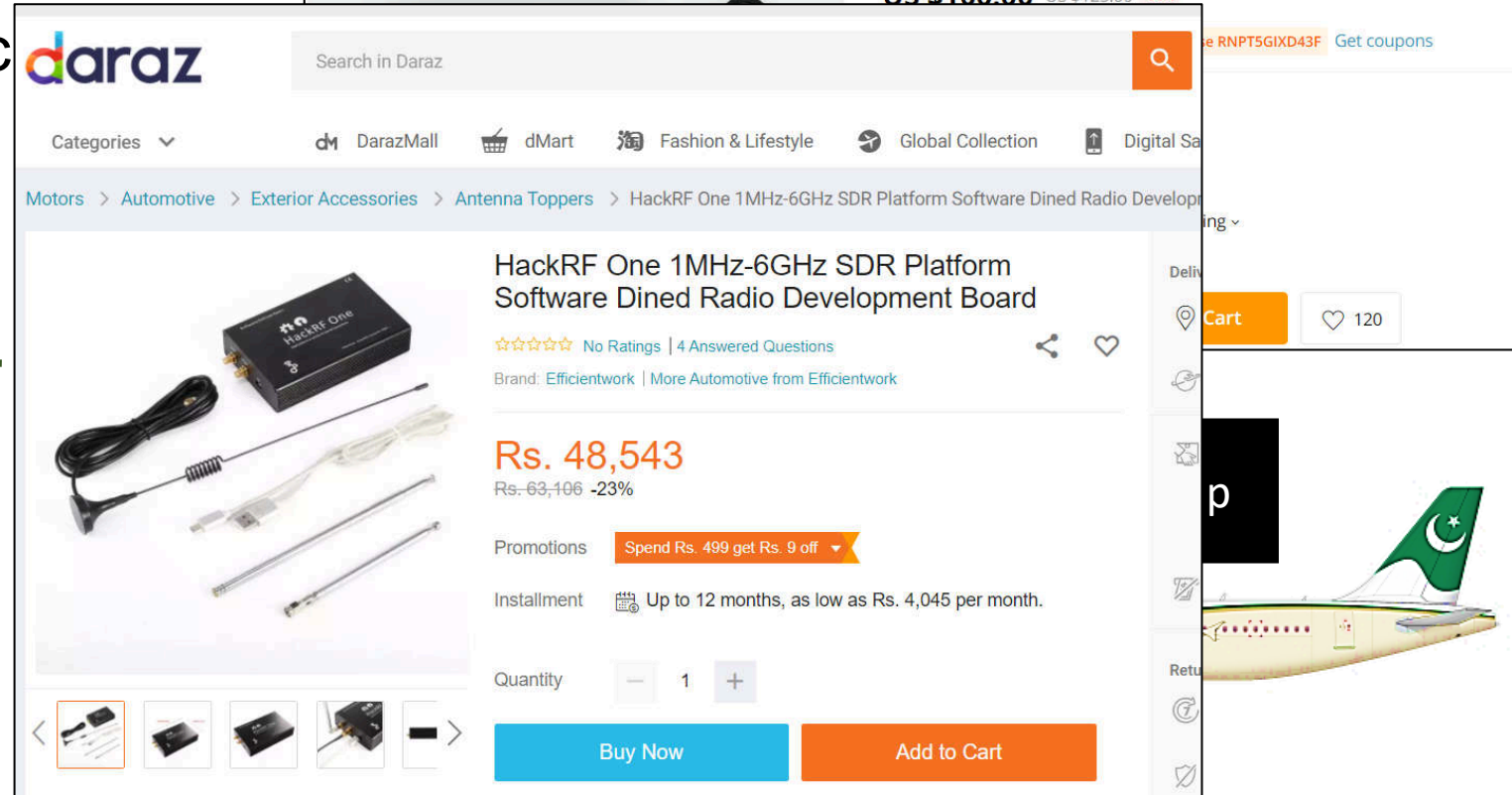
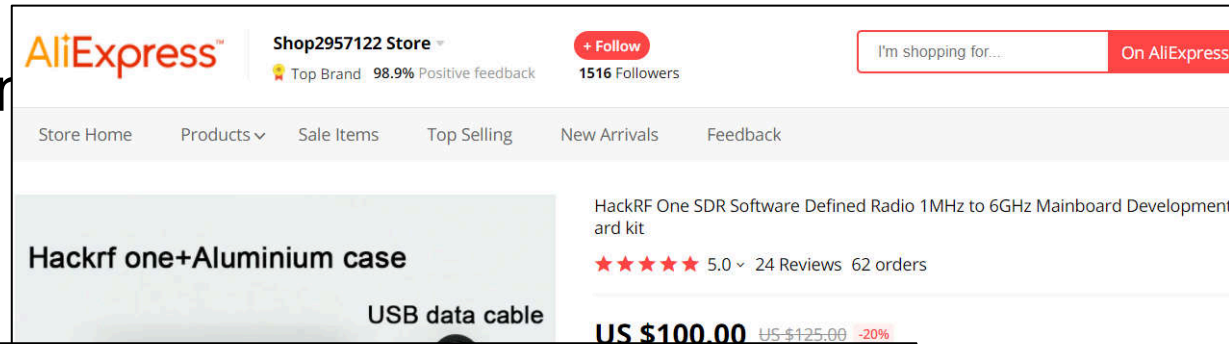
- Collision induction through collision avoidance





Air Traffic Control

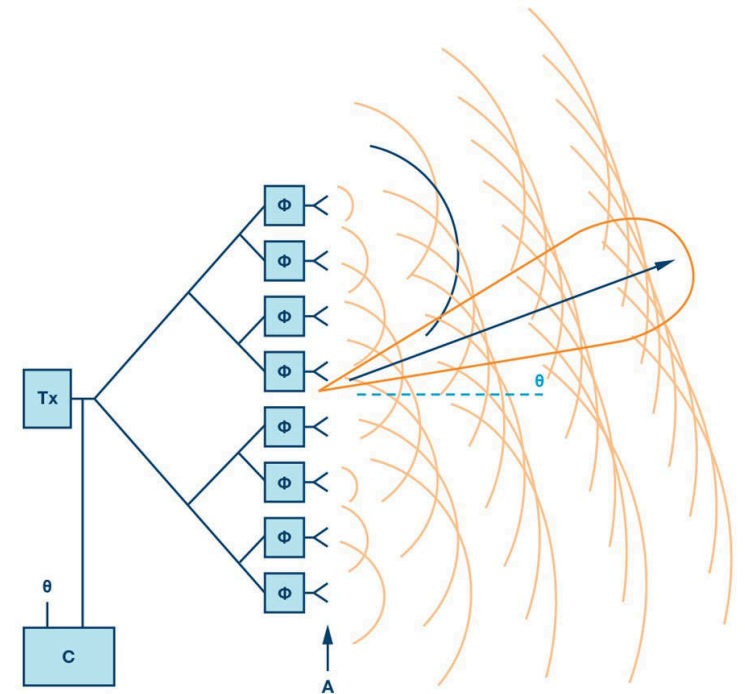
- Traffic Monitoring and Collision Avoidance
 - ADS-B and TCAS
- Collision induction through c





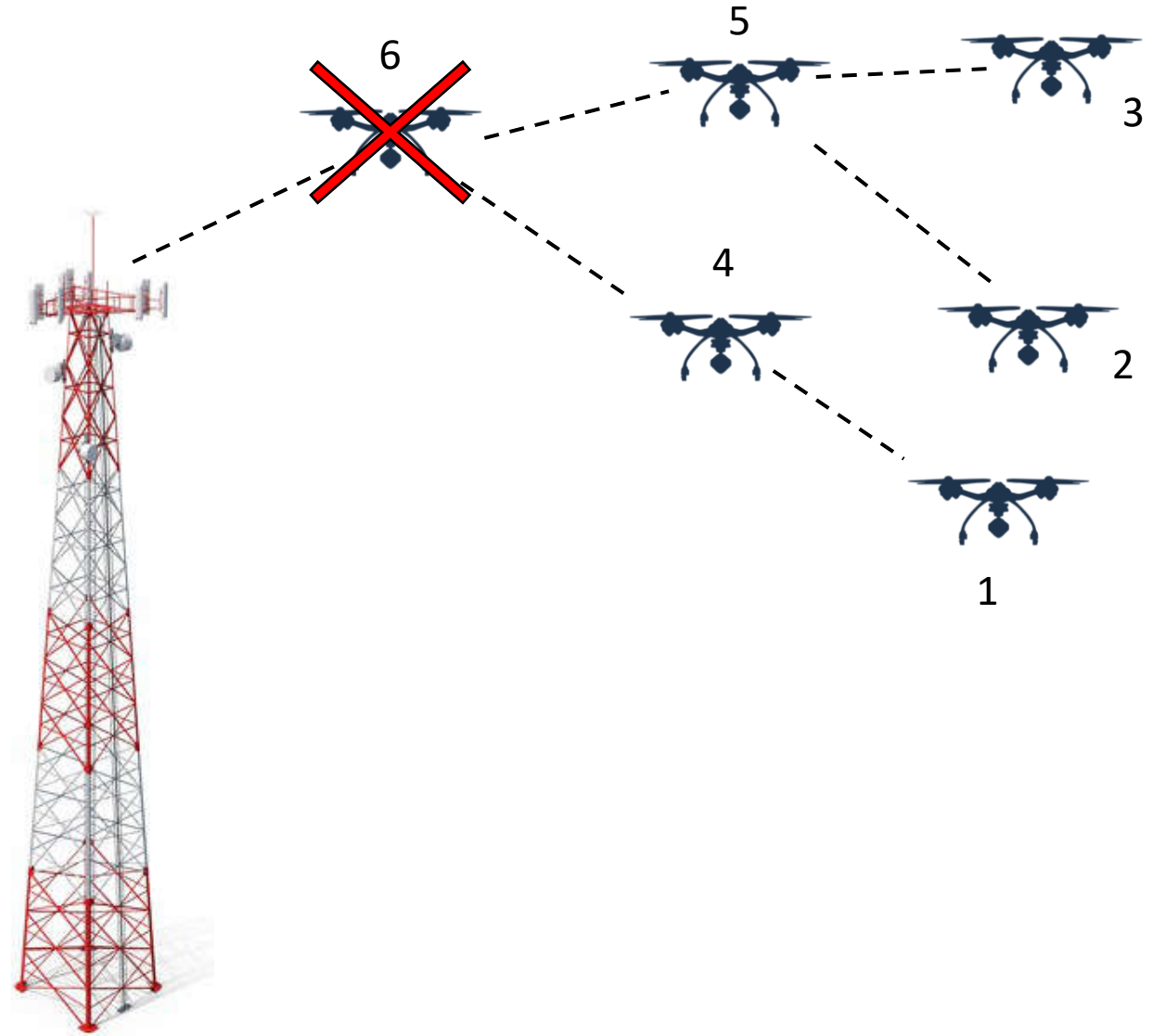
- Induction of fail-safe mechanism
 - Hover (**make kinetic attacks and capture easier**)
 - Return to base (**combined with navigation attacks may lead to capture**)
 - Land (**=capture**)
 - Self-destruct

- **Adaptive Radios:** Manipulation of environmental parameters (spectrum sensing)
- Manipulation of anti-jamming solutions such as direction of arrival estimation in **Beamnulling**
- Exploiting of antenna pattern and orientation (TCAS Attack)



Link Layer and Network Layer

- Traffic Analysis
- Topological Attacks on multi-UAV
- Routing Attacks (Black Holes)





Them: "AI is going to take over the world and kill us"

Meanwhile AI:



THE DIPLOMAT
READ THE DIPLOMAT. KNOW THE ASIA-PACIFIC

ALL SECTIONS SEARCH SIGN IN SUBSCRIBE

CENTRAL ASIA EAST ASIA OCEANIA SOUTH ASIA SOUTHEAST ASIA SECURITY POLITICS DIPLOMACY ECONOMY SOCIETY ENVIRONMENT DRI MAGAZINE ALL

RECENT FEATURES

COVID-19 Has Dimmed Xi's Approval Ratings Abroad - But Not in China

Why Have Singaporeans Turned Against Indian Professionals?

Suganomics: Abenomics Minus Yasukuni?

China's Disinformation Campaign in the Philippines

ASIA DEFENSE | SECURITY

AI Defeats Human Pilot in DARPA Organized Dogfight

The performance of the artificial intelligence program marks an important but modest milestone.

By [Abhijnan Rej](#)
August 22, 2020

Activate Windows

ASIA TIMES EST 1995

China NE Asia SE Asia South Asia Middle East World Opinion Newsletters Membership AT Financial ATimesCN

UNITED STATES

DARPA's AlphaDogfight sees AI defeat F-16 pilot

Banger and Heron Systems' AI fought in five different fighter maneuver scenarios using only the Fighting Falcon's guns

By [DAVE MAKICHUK](#)
AUGUST 23, 2020

Can we use the exploits in meaningful way?

ANTI-DRONE technology

Israel Way

DefenseNews Air Land Naval Space Cyber C4ISR Pentagon Congress Global

Land

Israel uses Patriot missile to shoot down drone

By: The Associated Press November 13, 2017

f t

Popular Latest

The Atlantic Sign In

GLOBAL

THE VERGE TECH REVIEWS SCIENCE CREATORS ENTERTAINMENT VIDEO MORE

Israel Shoots Down Drone with Patriot Missile

As the battle between Israel and Hamas intensifies, a drone reportedly cost Israel a million dollars when it was shot down with a Patriot missile.

ADAM CHANDLER JULY 14, 2014

This article is from the archive of our partner

As the battle between Israel and Hamas intensifies, a drone reportedly cost Israel a million dollars when it was shot down with a Patriot missile. From the Atlantic


The unmanned aerial vehicle was shot down with a Patriot missile, the Ashdod. There's no evidence of Israeli military intelligence

A US ally shot down a \$200 drone with a \$3 million Patriot missile

This will be a bigger problem as more drones show up on the battlefield

By Andrew Liptak | @AndrewLiptak | Mar 16, 2017, 10:13am EDT

f t SHARE



Apple's today's

JORDAN GOLSON

08.27.15 07:00 AM

Welcome to the World, Drone-Killing Laser Cannon

American Way



3 Billion Dollars

French Way

WorldViews

Terrorists are building drones. France is destroying them with eagles.

France trains eagles to attack and destroy drones

Like 16.5M Monday, Oct 1

MailOnline

Home News U.S. | Sport | TV&Showbiz | Australia | Femail | Health | Science | Money | Latest Headlines | Coronavirus | Royal Family | Crime | Boris Johnson | Prince Harry | Meghan Markle | World

Eagle trained to bring down terrorist drones attacks a five-year-old girl enjoying a picnic after it mistook her white T-shirt for an enemy

- Eagle trained to swat drones out of the sky mistook a girl for one of the devices
- Youngster, five, was enjoying a picnic when the huge bird swooped down on her
- It left her with 'minor injuries' and air force personnel apologised to the group
- Eagles are trained to claw drones that could be used by terrorist to carry bombs

By PETER ALLEN IN FRANCE FOR MAILONLINE
PUBLISHED: 17:24 BST, 7 June 2018 | UPDATED: 21:36 BST, 7 June 2018

Share 173 shares 107 View comments

A French airforce eagle designed to claw drones out of the sky attacked a five-year-old girl dressed in white because she looked like one of the aircraft.

The drama took place in the picturesque Col d'Aubisque - a mountain pass in the Pyrenees close to the South West town of Tarbes.

English Search Newsletters

euronews.

Europe World Business Sport Culture Living Sci-tech Travel Video Live

BREAKING NEWS Paul R Milgrom and Robert B Wilson win the 2020 Nobel Prize in Economics for improvements to auction theory and inventions of new auction formats

Home > News > World > Where Eagles Dare: France trains birds to bring down drones

FRANCE

Where Eagles Dare: France trains birds to bring down drones

COMMENTS

By Catherine Hardy • last updated: 16/02/2017

SHARE THIS ARTICLE TEXT SIZE

Pakistani Way



Bullets < 1\$

Thanks a lot



If you are taking a Nap, **wake up**.....Lecture Over