

Drone Attacks on Industrial Wireless A New Front in Cyber Security

Jeff Melrose CISSP-ISSEP, CEH, GICSP
Sr Principal Tech Specialist
Yokogawa USA



About Jeff Melrose



Photo by Jeff Melrose

YOKOGAWA 

Co-innovating the future of
Industrial Controls, Sensors
and Networks

- ▶ Jeff is the Principal Technology Strategist for Cybersecurity at Yokogawa a leading Industrial Control Vendor. Before Yokogawa, Jeff was a Principal Security Engineer at both Lockheed and Raytheon designing secure unmanned systems for the US Military and US Intelligence Community.
- ▶ Mr. Melrose has over 20 years of experience in Computer Security. He has an MS in Mathematics and holds the Certified Ethical Hacker (CEH), Certified Information Systems Security Professional (CISSP), Information Systems Security Engineering Professional (ISSEP) and Global Industrial Control Security Professional (GICSP) certifications.
- ▶ Jeff is also a member of AFPM, ISA99, IEC Cyber Security Task Force and ISC(2).

Agenda

- Motivational Video
- Introduction to Cyber Physical Electronic Threats
- Electronic Warfare Overview
- Recent Electronic Jamming incidents
- Distance as a Weapon for Drones
- Drone Threat Scenarios
- Practical Drone EW-Cyber Defensive Strategies

No one expects: the e-chainsaw



Source: excerpt from
<https://www.youtube.com/watch?v=6Viwwetf0gU>

Introduction to Cyber Physical Electronic Threats

Illustration by Jeff Melrose

Cyber Physical defined

- ▶ *U.S. NIST Defines* - Cyber Physical systems are “smart” systems that are co-engineered interacting networks of physical and computer components.
- ▶ Example: Industrial Control Systems and Networks



Graphic by NIST

Electronic Cyber Physical Reality vs Assumptions



You don't worry
about a chainsaw
100 ft away
But 1 foot away?

<u>Security Assumption</u>	<u>Drone Reality</u>
An Adversary needs to be within physical proximity to do major harm	Drones can allow an adversary to manipulate at long distance – <i>now a hobby drone can travel <u>3 miles</u></i>
Physical security can be minimized inside the plant boundary	Drones can tailgate workers as easy as people now – <i>many drones can now <u>navigate easily inside buildings</u></i>

What about moving an Electronic Chainsaw close to Systems?



Electronic Warfare overview

Illustration by Jeff Melrose

Electronic Warfare the new Cyber Frontier

- ▶ Electronic warfare (EW) is any action involving the use of the electromagnetic (EM) spectrum or directed energy to control the spectrum, attack an enemy, or impede adversary operations.
- ▶ Uses either
 - Electromagnetic Spectrum
 - Directed Energy

EW Chainsaw

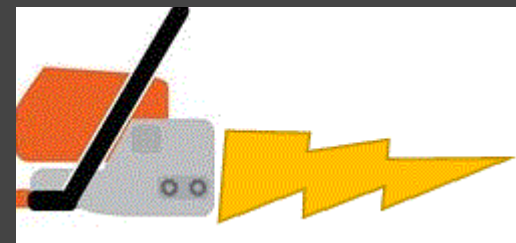


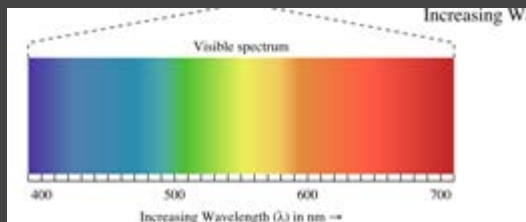
Illustration by Jeff Melrose

The Electromagnetic (EM) Spectrum

- ▶ The electromagnetic (EM) spectrum is the range of all possible frequencies of electromagnetic radiation.
- ▶ The electromagnetic spectrum extends from modern radio communication to gamma radiation.
 - *So it includes radio, microwave and visible light -*

===== and LASERS

Visible light ➡



Source Wikipedia
https://en.wikipedia.org/wiki/Light#/media/File:EM_spectrum.svg

Source Wikipedia
https://en.wikipedia.org/wiki/File:Light_spectrum.svg

Basic Electronic Warfare Terms

Electronic Attack

Electronic Protection

Electronic Support

Source Wikipedia
<https://en.wikipedia.org/wiki/Laser#/media/File:LASER.jpg>

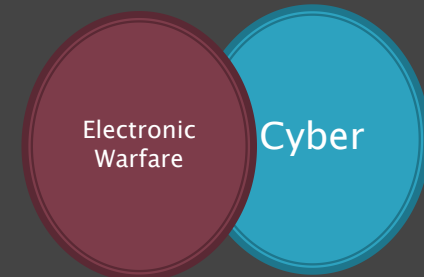
Source Wikipedia
https://en.wikipedia.org/wiki/Faraday_cage#/media/File:Heimbach_-_power_plant_07_ies.jpg

Source Wikipedia
https://en.wikipedia.org/wiki/Scanner_%28radio%29#/media/File:Uniden_BCT-15_deck_in_bracket-left.jpeg

And The other EW Vulnerable System- GPS

- satellites use frequencies, 1.57542 GHz (L1 signal) and 1.2276 GHz (L2 signal).

Source Wikipedia
https://en.wikipedia.org/wiki/Global_Positioning_System#/media/File:GPS_Satellite_NASA_art-iif.jpg



*Some would
Say Cyber and EW
Are merging*

Recent Electronic Jamming incidents

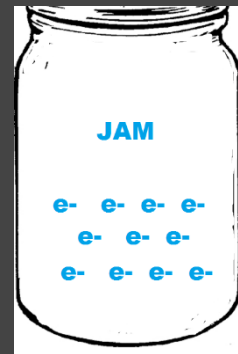


Illustration by Jeff Melrose

Recent Electronic jamming incidents

- ▶ **San Diego Harbor 1999** —A U.S. Navy radar test created EMI which affected 928.5 MHz wireless communication from SCADA systems and connected valves controlling San Diego Water Authority and San Diego Gas and Electric.
A similar incident in 2007 led to GPS and other wireless services were significantly disrupted throughout San Diego, Emergency pagers stopped working, Harbor traffic-management system guiding ships failed, Cell phones failed, ATMs failed. Found to be two Navy ships in the harbor doing a jamming training exercise
- ▶ **Newark Airport 2013** —The FCC fined a Readington, NJ, man nearly \$32,000 after it traced a problem with Newark Liberty International Airport's satellite-based tracking system to his truck. The man had purchased an illegal GPS jamming device for about \$100 and installed it in his company-owned pickup truck so his boss could not monitor his movements. Disrupted ground-based augmentation system (GBAS) which uses GPS (1.2276 / 1.57542 GHz).
- ▶ **Den Helder, Netherlands, late 1980s** —A gas pipeline control system located near a naval base found a 36 inch valve was opening and closing with the same frequency as the scanning of an D/L-band radar (1.215-1.4 GHz) system in the harbor. Shock waves induced by the rapid valve movements caused a pipeline rupture.

Distance as a Weapon for Drones

EW, Hacking and Distance

- ▶ Physics students should be familiar with this equation
 - Radio propagation and signal strength:
 - distance is a factor.
 - The closer a “Transmitter” can be to the target network, the more effective it is
 - *Hence the possible use of a **DRONE** to move the Transmitter/Disrupter close to the target.*

$$S = P_t \frac{1}{4\pi d^2}$$

Illustration by Jeff Melrose



Drones a new EW threat

► Drone Logistics

- Typically flight time is 25 min
- Camera default payload
- But can carry small computers like RasberyPI / cell phones ~1.5 lb
- Range is around 1.5 miles
- Speed is around 30 mph

• But could be faster

• But

Table 1. Select list of commercially available UAVs

Model	Weight	Payload	Flight time	Range	Max speed	Camera
Parrot BeeBop	0.4 kg	0 kg	12 mins	250 m (extendable)	29 mph	Yes (14MP)
Blade 350 QX2	1 kg	0.2 kg	10 mins	1,000 m	32 mph	Yes
		0.2 kg	16 mins	800-1,000 m	40 mph	Yes
					33 mph	Yes (14MP)
						Yes (12MP)
						Yes (12MP)
					26 mph	Yes

In just 3 MONTHS this data became obsolete !!!

In March 2016 DJI released the Phantom 4 Drone

- ~3 mile control limit
- 24-28 minute flying time
- 45 mile per hour top speed
- TARGET TRACKING CAPABILITY

Drone capabilities evolving rapidly

The Remote Control project is a part of the Network for Change hosted by Oxford Research Group.

So a Funny thing happened in our Net Lab one day

It's a
Disrupter

A disrupter
helps us test
failure modes
at closer
distances



Drone Threat Scenarios

Photo by Jeff Melrose

Drones carrying Disrupters to Industrial Wireless Antennas?

- ▶ Hmm... It's lame but...



*And – It was pretty **EASY** to hover the drone and drop on a disrupter
Hobby Drones are able to hover and
do Fine Control movements in moderate wind conditions!*


Can a Drone keep in Physical Proximity Autonomously?

- ▶ Yes they can follow autonomously...
 - ▶ And now can Image Target Track MOVING TARGETS



Can a Drone Carry a "Transmitter" Physically Close Enough to Replicate the Radar Valve Incident?

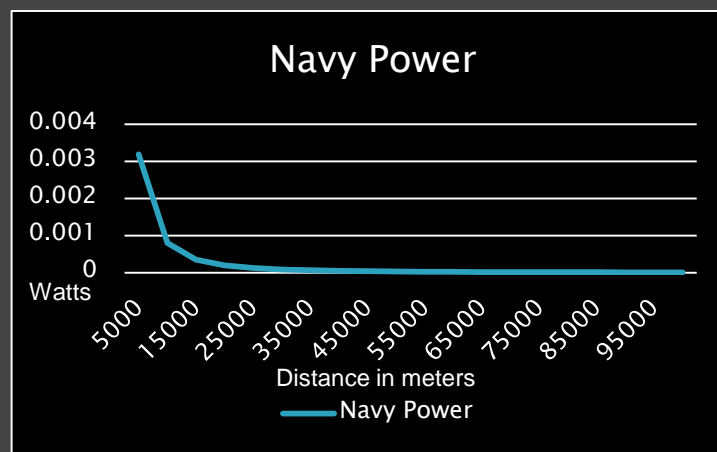
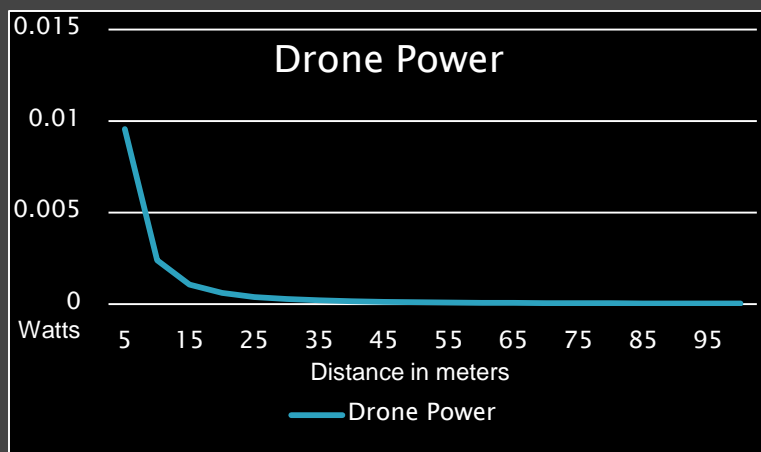
- ▶ Given the EW Incidents mentioned previously (San Diego and Den Helder).
- ▶ Equivalent ASR/EW System Power of approximately 1 gW (I so want to say 1.21 Jigga Watt here)
- ▶ Range Effect - San Diego Harbor was impacted at a defined distance (Assuming Naval Base San Diego was origin)
- ▶ An example "Yammers from Dhina" unit states that their Effective Radiated Power is 3 Watts with a range of 50 feet



It rhymes with
"Yammers from
Dhina" folks!

Photo by Jeff Melrose

Yes! a Drone can get physically close enough



- ▶ And the answer is a “transmitter” has to get with about **8.66 meters** to be able to cause an equivalent effective range of EW system
 - * *and this corroborates effects we have seen at ~10 Meters*
 - * *~100 meters+ is problematic*

Can a Drone maintain Electro-magnetic Distance Autonomously? On a fast moving target?



Ripped from the pages...

- ▶ 'MouseJack' Attacks Hack Wireless Keyboards And Mice From 100 Meters (Forbes Feb 23, 2016)
 - Researchers have exploited a range of vulnerabilities in wireless keyboards and mice, taking control of them from up to 100 meters away. The researchers, from Internet of Things security start-up Bastille, focused on a range of dangle-linked devices from Logitech, Dell , Gigabyte, HP, Lenovo , Microsoft and Amazon Basics.

*But with a **DRONE RELAY**...
this attack could be made
miles away*

Source <https://the-parallax.com/2016/02/23/mousejack-exploit-affects-billions-of-wireless-keyboards-mice/>

Can a Drone keep a Transmitter close Autonomously to a target?

- ▶ Yes!... but there is a problem -
- ▶ Observation – Modern hobby drones utilize the 2.4 Ghz spectrum as does WiFi, 802.15.4 etc. So any disruption needs to be away from the drone and controller due to possible loss of control.
 - Hack for this is to utilize a Tethered Electromagnetic Transmitter.



Can a Drone keep a Transmitter close Autonomously? On a stationary target?

- ▶ Yes! – Field Wireless Transmitter test



Can a Drone keep a Transmitter close Autonomously? On a Moving target?

- Yes! – Field Wireless Gateway test

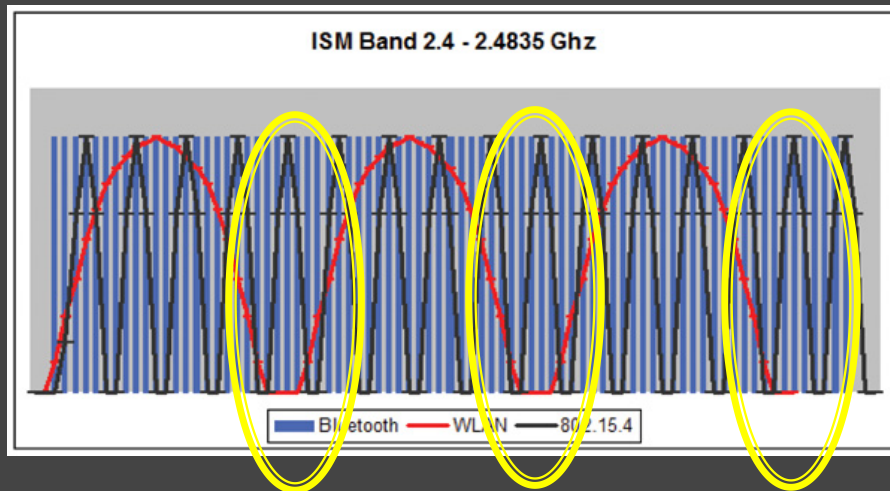


****Note – Results were 5-10% packet loss due to weak commercial transmitter, concept demonstrated*

Interesting Observation – This attack is not limited to 2.4 Ghz it could also be used in the 1.57542 GHz (L1 signal) and 1.2276 GHz (L2 signal) For GPS!!! Thus potentially impacting
Telematics and Autonomous Vehicle navigation systems !!!

Practical Drone EW-Cyber Defense Strategies

Know Your Radio Spectrums

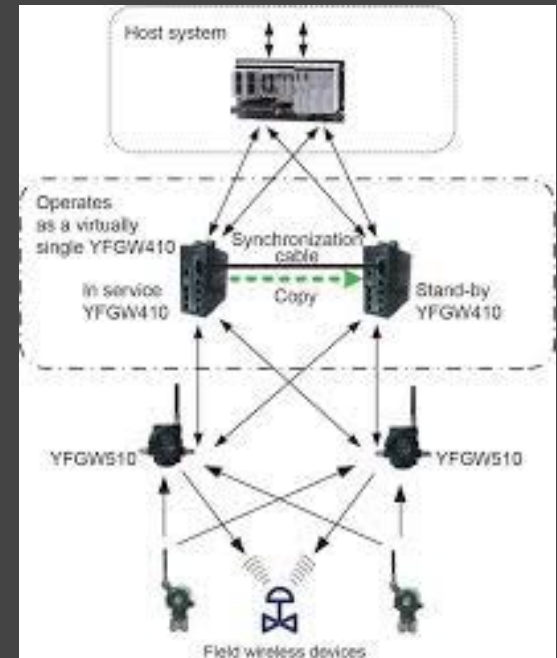


Graphic -
<http://www.qualitymag.com/articles/91465-wireless-measurement-data-acquisition>

- ▶ The 2.4-2.835 GHz Spectrum is VERY crowded. It is used by
 - WiFi/WLAN
 - Bluetooth
 - 802.15.4 (Industrial Wireless – ISA100, WirelessHART, ZigBee)
- ▶ Since WiFi 802.11 is the major wireless target jammers will leave GAPS in EMI between WiFi channels 1,6,11
- ▶ Therefore 802.15.4 users should channelize to 802.15.4 **Channels 15, 25,26 (14*, 20** - note 802.15.4 channel numbers)**
 - *But unfortunately there will be no gaps with a Bluetooth interference****

Industrial Wireless will need to go with MESH network topologies

- ▶ Multiple redundant telemetry and sensor routes need to be supported
- ▶ But this will most likely **Impact BATTERY Life** of field devices due to repeating overhead

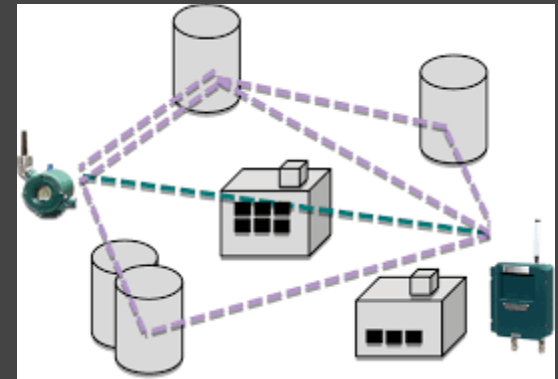


Graphic by Yokogawa

Graphic by Yokogawa

Industrial Wireless Networks vs EMI vs Distance

- ▶ EMI effects like RF reflection around metallic structures like tanks and vessel reactors should be utilized for multi-path support
- ▶ Use of Repeaters needs to be considered from high vantage points
- ▶ EM and Spectrum surveys should be incorporated into plant security procedures.
- ▶ Yokogawa has excellent guidance on this guidance is named “An Excellent Method to Lay Out ISA100.11a Field Wireless Devices” and is located at <https://www.yokogawa.com/rd/pdf/TR/rd-te-r05502-009.pdf>

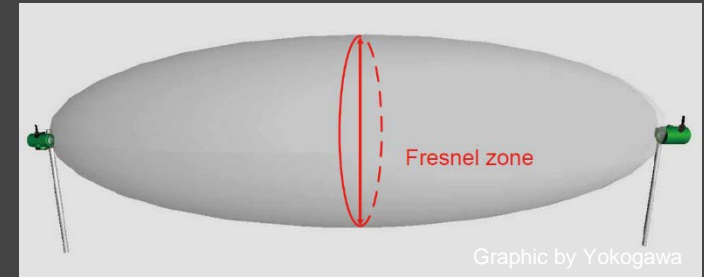


Graphic by Yokogawa

Graphic by Yokogawa

Certain overhead areas need to be secured

- ▶ Police your Fresnel Zones!
 - A Fresnel zone (fray-NEL), is a series of concentric ellipsoidal regions indicating wave strength between two antennas.
- ▶ Drones can interfere with Fresnel zones so like fences and doors physical security should note these... because could land in Fresnel Zones and perform persistent interference.



THE END