



WHITE PAPER

AUGMENTING PORT PROTECTION & SECURITY IN TERRITORIAL WATERS USING RF TECHNOLOGY

Written by **Jaimie Brzezinski**

 **CRFS**

EXTRAORDINARY
RF TECHNOLOGY



TABLE OF CONTENTS

| | |
|---|----|
| Introduction | 3 |
| Threat: disrupted communications & interference | 4 |
| Threat: remote controlled IEDs | 6 |
| Threat: vehicle trafficking | 6 |
| Threat: unmanned aerial vehicles (UAVs) | 8 |
| Threat: unmanned underwater vehicles (UUVs) | 11 |
| Threat: illegal ship-to-ship transfers | 12 |
| Threat: attacking submarine cables | 14 |
| Conclusion | 15 |



**IN 2024 80%
OF ALL GLOBAL
MERCHANDISE
WAS TRANSPORTED
BY SEA**

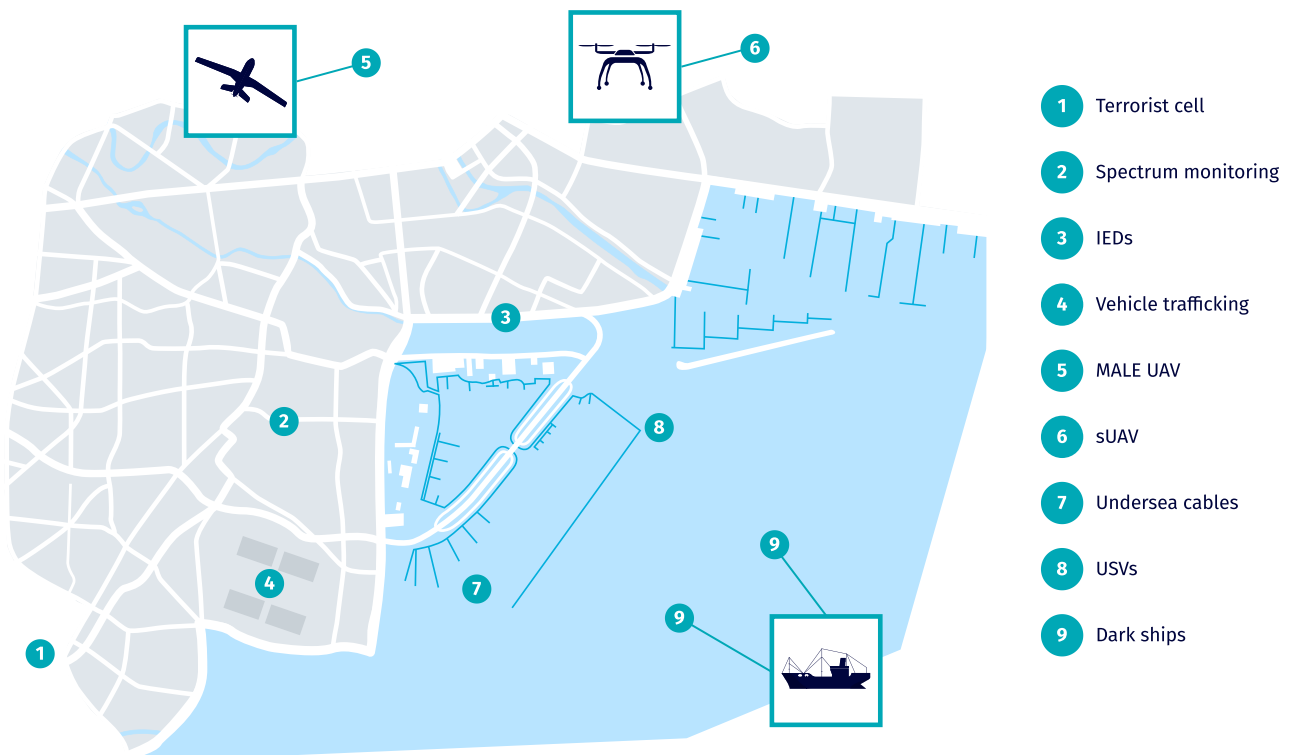
INTRODUCTION

Since the first age of globalization, maritime trade has played a central role in a nation's economic and social development. In 2024, as 80% of all global merchandise was transported by sea, commercial seaports provided access to international markets and global supply chains.

However, ports are not only economic assets; they are also essential for ensuring food and energy security. Seaports are a critical component of a country's infrastructure and convergence points where ships and crews from across the globe meet national customs services, law enforcement, port authorities, and private shipping companies. This combination results in a level of complexity that increases vulnerability.

The continued expansion of seaports and growing management challenges mean there is an increasing need for enhanced port protection. Multi-sensor surveillance and security systems, including RF sensors, can monitor the electromagnetic spectrum for security threats that use wireless technologies.

This guide discusses critical threats (from inside port facilities to the periphery of the nation's EEZ). It demonstrates how adding RF technology to existing port security measures can help augment port protection and security in territorial waters.



THREAT

DISRUPTED COMMUNICATIONS & INTERFERENCE

Smooth port operations depend on RF systems, which play a critical role in logistics and operations. These systems are the foundations upon which the port’s wireless networks, emergency communication, perimeter monitoring, IoT devices, access control, RFID technology, and automated systems operate.

As ports and ships become smarter, more appliances and communication networks are contributing to spectrum congestion. This means there is always a high chance

of unintentional interference (co-channel interference, adjacent channel interference, intermodulation interference), which could cause problems ranging from unclear radio communications to collisions resulting from severe navigation errors.

In addition to unintentional issues, these critical systems are also vulnerable to deliberate, targeted interference by criminal or terrorist actors looking to inflict human, infrastructural, or economic damage.

| RF SYSTEM | FUNCTION | FREQUENCY RANGE |
|---------------------------------------|--|---|
| Automated cranes and vehicles | Control of automated cargo handling equipment | 2.4 GHz and 5.8 GHz |
| RFID technology | Tracking and monitoring assets | 860–960 MHz (UHF) |
| IoT devices | Monitoring and controlling port equipment | 4.33GHz, 915MHz, 2.4GHz to 5GHz (ISM bands) |
| RF surveillance systems | Perimeter monitoring and security | 30 MHz–300 MHz and 300 MHz–3 GHz) (VHF and UHF bands) |
| GPS systems | Navigation and positioning | 1575.42 MHz (L1 band), and 1227.6 MHz (L2 band) |
| Wireless networks (Wi-Fi) | Data communication and operational control | 2.4 GHz and 5 GHz |
| Microwave links | High-speed data transmission | 2.4GHz to 42GHz |
| Two-way radios | Communication among port personnel | 30 MHz–1 GHz (VHF / UHF) |
| AIS (automatic identification system) | Tracking ship movements | 161.975 MHz (AIS 1) and 162.025 MHz (AIS 2) |
| Bluetooth devices | Short-range communication | 2.4 GHz |
| VHF marine radio | Communication between ships and port authorities | 156–174 MHz |

SOLUTION

PROACTIVE SPECTRUM MONITORING


Proactively monitoring the electromagnetic spectrum using superheterodyne RF sensors can help formulate a robust spectrum management plan.

First, establishing a baseline will provide security with an overview of who and what is using the spectrum. Then, using [spectrum monitoring software](#) to coordinate frequency usage, managers can assign different frequencies (complying with regulator-assigned frequency bands) and implement systems such as dynamic frequency allocation, which can help prevent issues from becoming conflicts. Last, with complete spectrum visibility, the cause of any interference can be identified and geolocated in real-time.

Additionally, security personnel monitoring the spectrum can identify any anomalies that may need further investigation. For example, they can detect RF signals emitted from a handheld radio being used by someone walking along the port perimeter potentially coordinating criminal activities.



WITH COMPLETE SPECTRUM VISIBILITY, THE CAUSE OF ANY INTERFERENCE CAN BE IDENTIFIED AND GEOLOCATED IN REAL-TIME

 *RFeye Site, a real-time spectrum monitoring and geolocation toolkit*

THREAT

REMOTE CONTROLLED IEDs



Remote-controlled improvised explosive devices (RCIED) can be initiated wirelessly using a transmitter and receiver (for example, with a two-way radio, simple wireless device, or remote control unit). As they can be detonated from a distance, the weapons are favored by terrorists, who consider [critical infrastructure to be an attractive target](#).

Risk assessments such as the [Common Integrated Risk Analysis Model \(CIRAM\)](#) are designed to analyze the risk level for threats to critical infrastructure. Terrorist attacks on a nation's port facilities would cause economic devastation; therefore, risk management approaches promote the use of real-time data and intelligence sharing and the implementation of technological measures to identify and respond to emerging threats.

While it is not possible to stop RCIEDs, understanding the RF environment and searching for these signals during rehearsals could provide an extra layer of port security. Moreover, in the unfortunate event that an RCIED was detonated, post-processing analysis could help identify the detonating signal—providing law enforcement with intelligence.

THREAT

VEHICLE TRAFFICKING



Port protection not only involves threats coming in from the outside; it also involves ensuring cargo leaving a country is legitimate. A 2024 [BBC report](#) stated that the global shortage of used cars and the growing international market for specific car models has made vehicle theft a top revenue generator for organized crime groups.

Cars stolen in Europe often pass through ports to be shipped to Africa and, according to INTERPOL, have even been found as far afield as [South America and Australia](#). Meanwhile, Canada is currently rated in the top ten worst countries for car thefts, with one being stolen every five minutes—many ending up abroad. Reducing vehicle trafficking is a critical consideration for law enforcement.



SOLUTION

RF SENSORS TO HELP IDENTIFY STOLEN VEHICLES

Criminals have long been wise to use GNSS-enabled vehicle trackers, so it is unlikely that port authorities will be able to detect RF signals from them.

However, RF sensors can detect jammers placed inside the cars. Jammers are intended to prevent detection by transmitting more powerful RF signals on the same frequency as the GNSS tracker, creating interference that prevents it from working. Detecting jammers inside ports could lead port security to stolen cars.

New tracker technologies are also available, which work differently from traditional trackers. According to [Sigfox](#), a company that creates one such technology: “Instead of depending on the strength of GSM signals, next-gen tracking devices send very short, low power radio signals on random frequencies over Sigfox’s global IoT network. Thieves can’t use jamming devices to disable the signal, and they won’t be able to find a device using an RF detector.”

While millions of IoT devices emit RF signals at a port, if port security maintained a database of commonly used anti-theft transmitters in vehicles, this database could be compared to signals sent from cars for shipping inside the port. Signals would need to be decoded using decoding software (such as Procitec or Decodio), but any matches could indicate a stolen car.

Additionally, vehicle-to-vehicle (V2V) communication systems continuously broadcast information about a vehicle on an assigned frequency (5.9 GHz in the US and Europe), such as its vehicle identification number (VIN). Using passive RF sensors to detect V2V signals transmitted by cars at a port and then cross-referencing the signals received with a national database of stolen vehicles could help to identify stolen vehicles entering the port.

THREAT

UNMANNED AERIAL VEHICLES (UAVs)



Adversarial drones pose significant risks to port protection due to their ability to bypass traditional maritime security measures, which are focused primarily on waterborne or land-based threats. In a 2023 study titled [Drones and Port Security in Brownsville: A Case Study on the Gulf](#), “the drone risk assessment determined that stakeholders at the port rated Uncrewed Aerial Drones (UAS) as the highest perceived threat at 7.0 high (on a 10-point scale with ten the highest).”

Low-cost commercial off-the-shelf (COTS) drones can easily be modified to threaten port and national security in three key ways.

1. Equipped with surveillance systems such as optical, infrared, and thermal cameras and signals intercepting equipment, drones can covertly monitor security operations and logistics, capturing surveillance data and gathering intelligence that could be used to plan illicit activities.
2. Smaller COTS drones can fly into a port carrying approximately 15 kg (35lb) of narcotics. Using a radio controller, this smuggled load can be dropped in a precise location—and hidden by corrupt port workers.
3. To disrupt critical supply chains and economic development, drones equipped with small explosive payloads can wreak havoc with port operations or damage specific cargo on target ships, posing risks to safety and security. For context, the drone incident at Gatwick Airport in 2018 was reported to [cost airlines over £50m](#).

Although COTS drones (EASA class C0–C2) are the most likely to be used in criminal port operations, larger commercial drones (EASA class C3–C4) and military-grade drones could also be used to compromise port security.

In 2021 and 2022, respectively, the MV Mercer Street¹ and the Pacific Zircon vessels were attacked using military drones. Although these attacks occurred while the ships were sailing in international waters, the UK government’s guidance paper on [Countering drone threats to shipping](#) warns that “drones with improvised explosive payloads... could also be used at shorter ranges, for example, to attack a docked vessel in port.”

HOW DO OPERATORS CONTROL UAVS?

Commercial drones are usually controlled by RF systems through which the operator sends command signals to the drone using a specific frequency. The operator also receives data from the drone (from video downlinks, for example) thanks to onboard data link transmitters (typically operating in the 2.4 GHz ISM band) for real-time data download.

The 4G and 5G frequency bands are also commonly used to control drones, as these networks increase the connectivity between the drone and the operator. In the UK, 4G signals operate between 800MHz and 2.6GHz, and 5G operates at 700MHz and from 3.4GHz to 3.6GHz.

National regulators (such as the FCC in the US, OFCOM in the UK, ANFR in France, and TDRA in the UAE) determine the exact frequencies upon which commercial drones can operate. However, (as in recent conflicts) criminal actors can also change the drone C2 frequency by replacing the transmitter and receiver (as well as further calibrations).

Although military drones controlled by wireless RF systems use their own assigned frequencies, some military drones do not use terrestrial RF; they are guided by advanced systems such as satellite communications, autonomous guidance systems, or optical communications.

While different UAVs have varying levels of autonomy, even fully autonomous systems that fly with minimal human intervention generally depend on command and control (C2) sensors, which monitor mission progress and ensure the vehicle dynamically adapts to conditions or as the mission changes. These sensors rely on RF communication to transmit data between the UAV and the operator’s ground control station.



Learn more about drone detection solutions:
www.crfs.com/solutions/drone-detection

SOLUTION

USING PASSIVE RF SENSORS TO DETECT UAVs

Detecting COTS drones that operate on conventional frequencies is a straightforward task. At least four **RF sensors** positioned around a port facility create a sensor network to detect a drone thanks to the time, frequency, and power characteristics of its signals.

RFeye Site, CRFS' spectrum monitoring and geolocation software, uses **detector-based models** to detect RF signals emitted by each transmitter on the drone and the RF-emitting device used by the drone's operator. This is a fast and automated method of drone detection: 70 geolocations a second are carried out, and the data is output. When the signal has been detected, the software carries out a **3D TDoA geolocation** of the signal so port security can take countermeasures.

Image 1 shows multiple 3D TDoA geolocations in **RFeye Site's** of a DJI drone flying inside a port's facilities; however, security teams will ideally want to geolocate a target before it enters their secure space.

Image 2 shows a line of bearing for a drone transmitting at 2.4 GHz. CRFS' video link detector is identifying a target drone approximately eight kilometers outside the RF sensor network (indicated in pink). Passive RF sensors can provide an early warning of an intrusive UAV despite it flying outside the network's ideal geolocation zone for 3D TDoA (shown in Image 3).

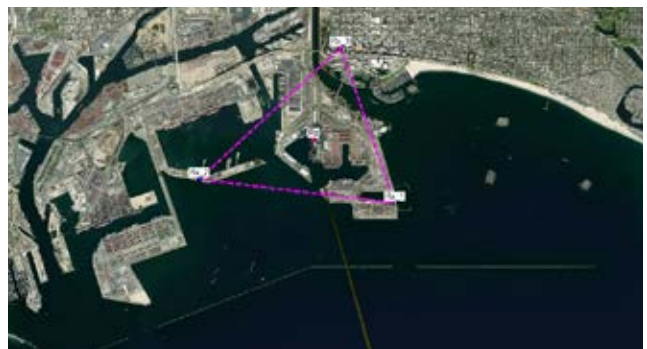
DRONES OPERATING ON UNCONVENTIONAL FREQUENCIES

Detecting COTS drones modified to operate on unconventional frequencies is more challenging; however, wideband RF sensors can scan broad swaths of spectrum and detect transitions outside the conventional frequency bands typically used by COTS drones.

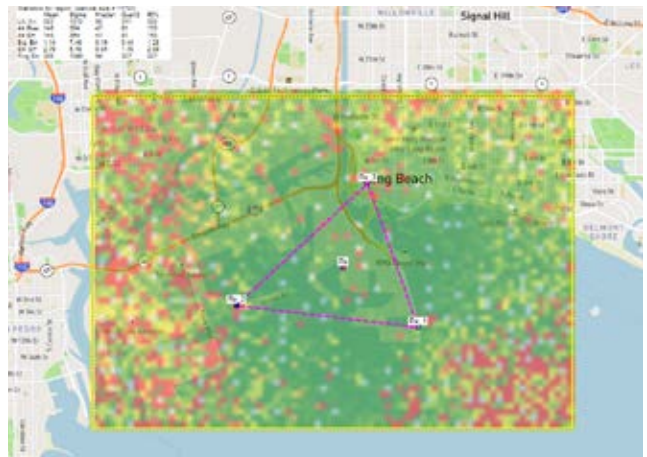
The sensors can capture and record RF data, including signal characteristics such as frequency, modulation, bandwidth, and transmission patterns. RF analysts can then use signals intelligence techniques to analyze these characteristics against known signatures of drone communications—identifying drones using unconventional frequencies. The analyst can then build a detector against the signal, automatically running a geolocation workflow anytime the software recognizes it.




^^ **Image 1:** 3D TDoA geolocations of a COTS DJI drone at one of the **world's 15 largest ports**. Red shows the most recent pattern of geolocations, while blue shows the oldest.



^^ **Image 2:** Line of bearing to a DJI drone located approximately eight kilometers outside the Port of Los Angeles' RF sensor network.



^^ **Image 3:** Geolocation area around the Port of Los Angeles. (Green depicts best-case accuracy, while red indicates worst-case accuracy.)

A flock of several drones is flying in a sky filled with soft, orange-hued clouds at sunset or sunrise. The sun is a bright, glowing orb in the center-right of the frame. Below the drones, a dark, silhouetted mountain range stretches across the horizon. The overall scene is atmospheric and high-tech.

BENEFITS OF USING PASSIVE RF TECHNOLOGY TO DETECT UAVS

Passive RF technology is a valuable tool to help port protection authorities detect a variety of drones operating on a range of frequencies. It can:

- Provide a line of bearing to drones as they approach critical airspace
- Geolocate the drone's operator if they are using an RF-emitting device
- Provide accurate 3D geolocations as the drone gets closer to critical airspace
- Identify and geolocate multiple drones or drone swarms
- Distinguish drones from birds and identify low-flying drones (difficult with radar)
- Gather significant information about the detected drone
- Eliminates the need for telecommunication licenses as it does not emit RF signals

THREAT

UNMANNED SURFACE VESSELS (USVs)



Although not currently as prevalent as UAVs, USVs are likely to present similar challenges for port security. Sensors, cameras, and surveillance equipment can gather intelligence on port operations, infrastructure, and security measures. While remaining undetected, USVs may transmit the data they collect back to their operator with telemetry transmitters that use RF-emitting components. They may also transmit VHF and UHF signals to communicate with a mothership (which could also be a dark ship).

If USVs transmit RF signals, an RF sensor network installed at a port can detect and geolocate the signals.

THREAT

UNMANNED UNDERWATER VEHICLES (UUVs)



UUVs can be used for surveillance purposes or to smuggle narcotics into a port. Although they do not primarily use RF signals for communication due to rapid absorption and attenuation in water, UUVs may surface to transmit data, receive Positioning, Navigation, and Timing (PNT) information, or communicate with surface vessels, such as their recovery vessel.

If a UUV surfaces near port facilities, security personnel using wideband RF sensors can potentially detect it by continuously scanning the spectrum to identify unusual or unauthorized signals. They can detect anomalies by comparing these signals against known, authorized patterns. Security personnel can analyze the signal characteristics to determine its likely origin upon detecting an anomaly.

THREAT

ILLEGAL SHIP-TO-SHIP TRANSFERS



Illegal ship-to-ship transfers involve cargo, such as weapons, drugs, fish, or sanctioned oil, being moved from one tanker to another. To safeguard themselves from criminal activity, many ports have measures in place preventing vessels involved in these activities from accessing their facilities.

Currently, the focus is on illegal ship-to-ship transfers of sanctioned oil, which is reported to occur in Southeast Asia (Malaysia, the Philippines, and Indonesia) and off the coast of Africa. Aging tankers transport crude oil from US-sanctioned countries to an area close to a port. They transfer the load to a legitimate tanker to obfuscate the origin of the oil.

To carry out a [legal ship-to-ship transfer](#) of oil within 12 nautical miles of a country's coast, a vessel must notify the country 48 hours in advance of the transfer. However, illegal ship-to-ship transfers are unlikely to adhere to MARPOL standards, potentially leading to environmental damage and illicit oil entering international markets.

If oil is being transferred legally, both ships' Automatic Identification Systems (AIS) will be turned on and the vessels trackable and identifiable—a measure mandated by the [International Convention on the Safety of Life at Sea](#). However, vessels engaged in illegal activity will disable their AIS to avoid detection, converting into what is known as a “dark ship” and becoming invisible to traditional monitoring systems.

Figure 4 (available from <https://www.marinetraffic.com>) identifies ships off the coast of Jakarta, Indonesia, through their AIS. This open-source software helps port authorities manage maritime traffic and visualize ships approaching, leaving, and moving inside the port based on their AIS. However, suppose a ship turns off its AIS. In that case, it will be invisible using this software and any other technology that uses AIS to establish a ship's position and identity.

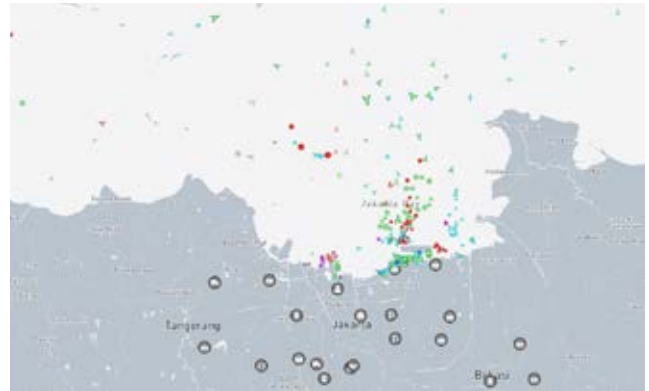


Figure 4: The location of ships around the Port of Jakarta, based on their AIS.



SOLUTION

USING PASSIVE RF SENSORS TO HELP DETECT DARK SHIPS

Illegal transfers of oil require coordination through communication between the two ships, which is extremely difficult without leaving a wireless footprint. So, although it is not possible to detect a dark ship (as the AIS is turned off), it is possible to detect RF signals (such as marine VHF radio and other communications signals from the HF, MF, and LF bands).

An RF sensor network around the port—which could be complemented by [UAVs carrying an RF sensor payload](#)—would allow port security to analyze how many ships broadcasting AIS data are also producing RF emissions. This can provide insights into ships that are potentially operating “in the dark.” Image 5 shows the geolocation of a VHF signal; this type of monitoring can be paired with AIS data.

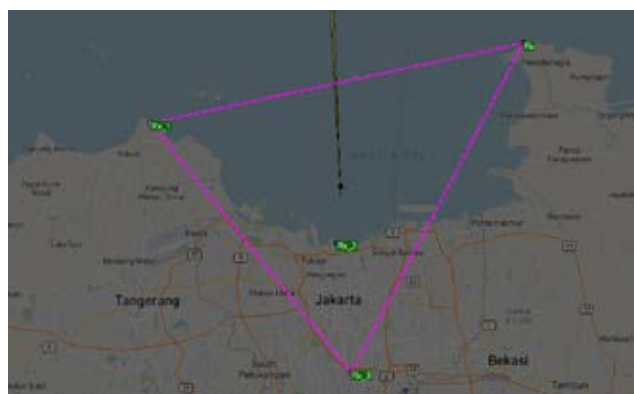


Image 5: Geolocation of a VHF signal off the Port of Jakarta.



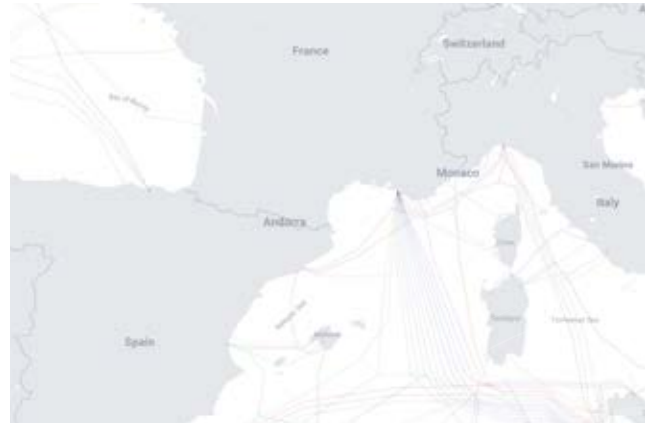
Image 6: RF sensor network around the Port of Jakarta. (Green depicts best-case accuracy, while red indicates worst-case accuracy).

THREAT

ATTACKING SUBMARINE CABLES

Submarine cables' landing infrastructure can be placed anywhere on a nation's coastline. However, given port facilities provide strategic advantages in connectivity, infrastructure, and security, some ports, including the Port of Marseille-Fos, France, the Port of Virginia, USA, and the Port of Singapore, have chosen these places as landing sites for submarine cables carrying terabytes of data internationally.

Ports, while being strategic assets, also have significant vulnerabilities due to their status as high-value targets. Multiple undersea cables converge at these locations, making them susceptible to coordinated attacks as part of sub-threshold warfare.

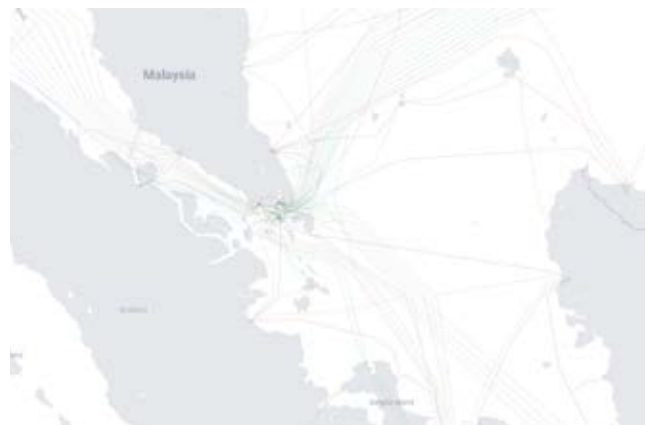


^^ **Image 7:** Fifteen undersea cables leaving the Port of Marseille-Fos, France. Source: <https://www.submarinecablemap.com/submarine-cable/iceni>

SOLUTION

MONITORING RF EMISSIONS

While it is inherently difficult to detect an act of sub-threshold warfare is taking place, a spectrum monitoring program can contribute to protecting a nation's territorial seas. By monitoring RF emissions in the areas around ports and along subsea cable routes, port authorities and coast guards may be able to detect suspicious signals potentially emanating from vessels involved in sabotage. For example, detecting VHF radio signals in an area where no AIS is detected may indicate criminal activity.



^^ **Image 8:** Large number of undersea cables leaving the Port of Singapore.

CONCLUSION

A nation's port facilities and EEZ are critical for its economic, social, and energy security. However, being large, open places where public, private, and international interests meet makes them inherently vulnerable to corruption, criminal gangs, terrorism, and espionage.

The growing number of threats to national security are the result of increasing geopolitical tensions and new uncrewed technologies that facilitate criminal activity while being difficult to detect.

One robust way to augment security around critical national infrastructure is to use multiple sources of intelligence in combination with as many sensors as possible. This approach is in line with policies such as the Australia Critical Infrastructure Protection Act, Singapore's Infrastructure Protection Act (IPA), and the US Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, which advocate for the strengthening and securing of critical infrastructure.

Integrating an RF network into existing port security is a powerful way of adding an additional layer of protection. Most threats use RF systems to operate; therefore, monitoring the invisible radio spectrum for suspicious signals can provide port security with actionable intelligence that can immediately be acted upon.

**RECEIVE A SIMULATION
FOR YOUR DESIRED SETUP**



QUICK LINKS



CRITICAL INFRASTRUCTURE PROTECTION

Passive RF solutions help protect critical infrastructure through 24/7/365 spectrum monitoring

www.crfs.com/solutions/infrastructure-protection



Subscribe to infrastructure protection content

www.crfs.com/blog-subscription



RFeye® Receiver (Node)

High-performance spectrum sensor (receive / record) to 40GHz



RFeye® Array

Direction finding from 20MHz to 40GHz



RFeye® Site

Real-time spectrum monitoring & geolocation toolkit



RFeye® Mission Manager

Automated monitoring & mission management



RFeye® DeepView

Forensic signal analysis software with 100% probability of intercept



RFeye® SenS Remote

High fidelity RF Recording (I/Q data) for enhanced intelligence



RFeye® Integrated Vehicles

Mobile spectrum monitoring, geolocation & tactical deployments



RFeye® Integrated Drones

Lightweight, rugged RF sensors fitted onto drones



EXTRAORDINARY
RF TECHNOLOGY

CRFS is an RF technology specialist for the defense industry, national security agencies, and systems integration partners. We provide advanced capabilities for real-time spectrum monitoring, situational awareness, and electronic warfare support to help our customers understand and exploit the electromagnetic environment.



CRFS Inc
Chantilly,
VA, USA
+1 571 321 5470

CRFS Ltd
Cambridge,
United Kingdom
+44 (0) 1223 859 500

CRFS and RFeye are trademarks or registered trademarks of CRFS Limited. Copyright© 2024 CRFS Limited. All rights reserved. No part of this document may be reproduced or distributed in any manner without the prior written consent of CRFS. The information and statements provided in this document are for informational purposes only and are subject to change without notice.



UK Certificate number: F5576625