SUAS/UAS CYBER TERROR IMPLICATIONS & CYBER-NAVIGATION THREATS & CHINESE UAS INTELLIGENCE CAPABILITIES & IMPENDING INVASION OF TAIWAN

Presented By:

PROFESSOR RANDALL K. NICHOLS, DTM

Kansas State University

Salina Aerospace and Technology Campus

Director GC Aerospace Cyber Operations

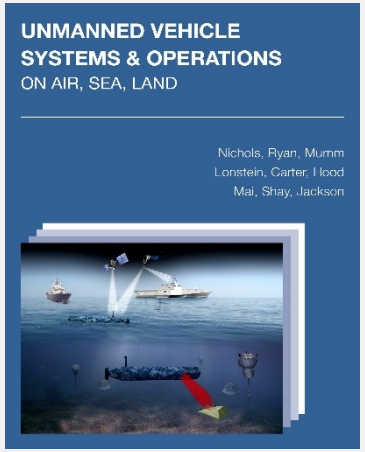
C2SR Symposium Keynote UND

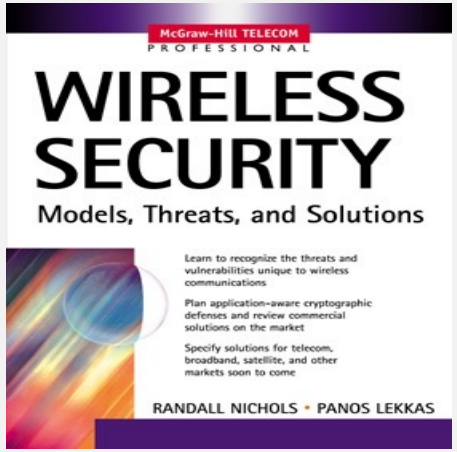
28 October 2022 1445-1530 CST

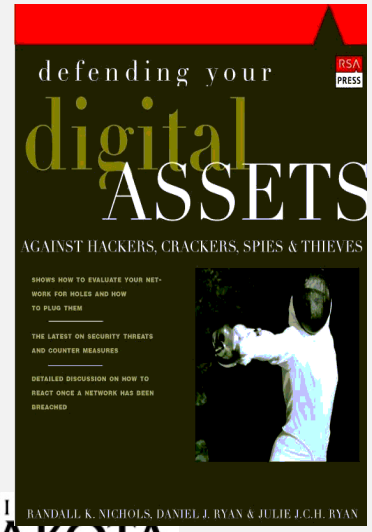
UND UNIVERSITY OF NORTH DAKOTA
COLLEGE OF ENGINEERING & MINES

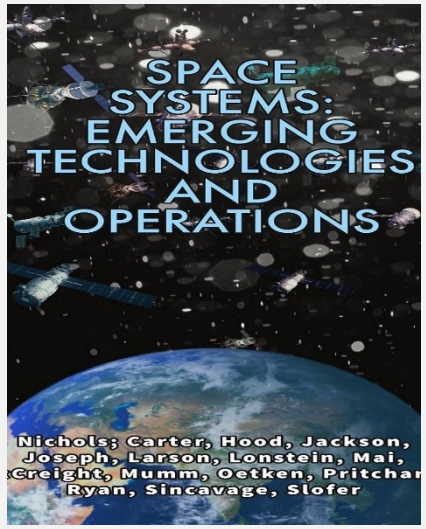
C2SR CENTER FOR CYBER SECURITY RESEARCH
CARS

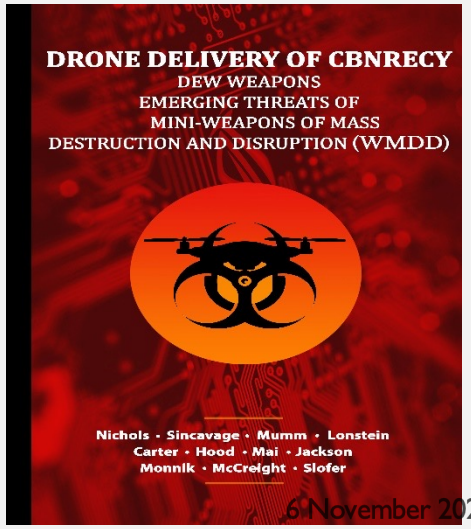
BOOKS BY PROFESSOR R.K. NICHOLS











AGENDA

- Why is there a sUAS/UAS Cyber Terror Problem?
- Ryan – Nichols Qualitative INFOSEC Risk Assessment Metric
- Terrorist Threats using UAS & Dirty Bombs
- Communication / Separation / Navigation Threats (SCADA)
- Active Countermeasures
- Spoof Proof Protection – Eichelberger Collective Detection (ECD)
- Chinese Intelligence: UAS Threats & Impending Invasion of Taiwan
- Chinese Intelligence: Submarine Sea Cables
- Chinese Intelligence: UAS / UUV Arsenal

WHY IS THERE A UAS TERROR PROBLEM?

THREAT:

The <u>RISK</u> of *SUCCESS OF TERRORIST ATTACKS* on Air Defense Systems (ADS) via UASs / sUAS is Higher

~ rapidly improving commercial capabilities & accessibility & low cost & low training requirement & easy to weaponize

HOW:

Advanced small / medium drones (air& sea) capable of carrying sophisticated imaging equipment, significant (WMDD deadly) payloads are readily available to civilian market.

CYBER ATTACKS ON UAS & GPS / ADS-B REPRESENT A MUCH GREATER TERRORIST THREAT & SAFETY ISSUE THAN CURRENT FAA UNDERSTANDING

ASSESSING QUALITATIVE INFOSEC RISKS: RYAN-NICHOLS EQUATIONS

We NEED A RISK METRIC … The RYAN-NICHOLS Equations

Ryan – Nichols Equations:

Risk = {Threats x Vulnerabilities x Impact / Countermeasures }

Risk ~ f (Threats / Countermeasures)

at time state =0,

where Vulnerabilities & Impact are constants and drop out

Normal Case, Best Case, Worst - Case Analysis

RYAN-NICHOLS RISK LETHALITY LEGEND

Qualitative Measure	Quantitative Value
High	81-100%
Medium-High	56-80%
Medium	31-55%
Low-Medium	14-30%
Low	7-13%
Very Low	0-6%

TERRORIST THREATS USING UAS

RECOGNIZE THAT GPS & ADS-B LOCALIZATION SYSTEMS ARE FUNDAMENTAL TO TERRORIST OPERATIONS USING UNMANNED AIRCRAFT SYSTEMS (UAS) FOR:

Weapons Platform

- **Assassination using Drone**
- **IED Delivery**
- **Aircraft Attack**

Martyr Drone Unit

GPS / GNSS Denial / Spoofing

Drone Attack Squadron

Drone Swarm

Attacks on Vessels on open water

Attacks using UUV on vessels or submarines or rescue vehicles

TERRORIST THREATS USING UAS

Attractiveness of sUAS/UASs and Cruise Missiles to an Adversary

- **Attack over perimeter defenses**
- **Attack over national borders**
- **Carry out multiple simultaneous attacks**
- **Conduct an attack campaign**
- **Attack area targets with unconventional weapons**
- **SWARMING Attacks to overwhelm Air / Sea Defenses**

Now contemplate the Risk of the Terrorist Spoofing Signals of Friendly Forces Intelligence & Counter Weapons Assets.

TERRORIST THREATS USING UAS & DIRTY BOMBS

- **Radiological dispersal devices (RDD) = Weapon of Mass Disruption (WMD) !**
- ***Greatest effect from a nuclear incident is fear-Radiation cannot be detected by human senses***
- **Combine conventional explosives with radioactive material**
- **Would not release enough radiation to kill people or cause severe illness**
- **Conventional explosive more harmful than radioactive material**
- **RDD explosion effects**
- **Fear and panic**
- **Contaminates property**
- **Requires potentially costly cleanup**
- **Lack of prompt, accurate information available to the public may feed the panic**

Source: http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/fs-dirty-bombs.pdf

COMMUNICATION THREATS
"UAS ARE JUST FLYING SCADA MACHINES!"*

Supervisory Control & Data Acquisition (SCADA) systems facilitate management with remote access to real-time data

- **Channel to issue automated or operator-driven supervisory commands to remote station control devices**
- **A human–machine interface (HMI) is responsible for data presentation to human operator**
- **Composed by a console that makes it possible to monitor & control process**

* Quote: Prof R.K. Nichols

COMMUNICATION THREATS
"UAS ARE JUST FLYING SCADA MACHINES!"*

Inherent Vulnerabilities:

- Ease of operation outweighs security
- Commonly set up on operating systems with known vulnerabilities
- Poor authentication systems in place
- Remote access allowed for maintenance &/or IT support
- Interconnectivity to vulnerable corporate networks
- Weak access control lists on firewalls
- Proper Network Access Control (NAC) is most crucial to prevent unauthorized connection within network
- First target of compromise for an attacker

Other Vulnerabilities:

- No use of standard IT defense software
- Wireless technology common
- System connect to unsecured remote processors
- SCADA software not designed with robust security features
- Public information often available on specific systems
- Poor physical security on remote access points

COMMUNICATION THREATS
"UAS ARE JUST FLYING SCADA MACHINES!"*

Attacks on Software: Common Attack Vectors

- **Manipulated & misleading output data to actuators/reactors from controller due to tempered actors/reactors or compromised network link between controller & actuators**
- **Controller historian changes – messes up feed forward control**

HIJACKING A UAS BY HACKING INTERNAL ASIC CHIP COMMUNICATION

CORRUPTING AUTHENTICATION OF GROUND STATION COMMUNICATION SIGNALS

SEPARATION THREATS

CONVENTIONAL VULNERABILITIES OF AIR DEFENSE SYSTEMS (ADS)

Issues - ADS Optimized for Missiles & AC at High Altitude & Speeds

- Data fusion works better with larger targets.
- Reactive for longer ranges.
- Close reactive requirements sub optimal.

ADS Vulnerabilities to sUAS

- sUAS launched into action close to target(s) - ~ 1 mile. Small Radar signature.
- Reactive dictates quick response near target. Slow flight. LOW flying avoiding Radar identification.
- Electric motors are both quiet & limited thermal signature.
- Make difficult detection in noise. Urban sphere presents additional problems & potential collateral damage.

NAVIGATION THREATS

CYBER VULNERABILITIES

OBSERVED IN ATTACKS ON MILITARY DEFENSE SYSTEMS & APPLICATIONS

Backdoors & Hardcoded Passwords

- **GPS Satellite Communication (SATCOM) systems vulnerable & exploited**
- **SCADA systems vulnerable & exploited**

Insecure Authentication and File Uploading

- **GPS SATCOM systems vulnerable & exploited**

Gain Scheduling (Control during Take-Off, Landing, Cruising: Mass, Altitude, Speed, Flaps)

NAVIGATION THREATS

CYBER VULNERABILITIES

OBSERVED IN ATTACKS ON MILITARY DEFENSE SYSTEMS & APPLICATIONS

Fuzzing (Consequences: Aircraft instability ,Process lock-up ,Invalid outputs to next process)

Digital Update Rate

Control Acquisition

SCADA Buffer Overflow

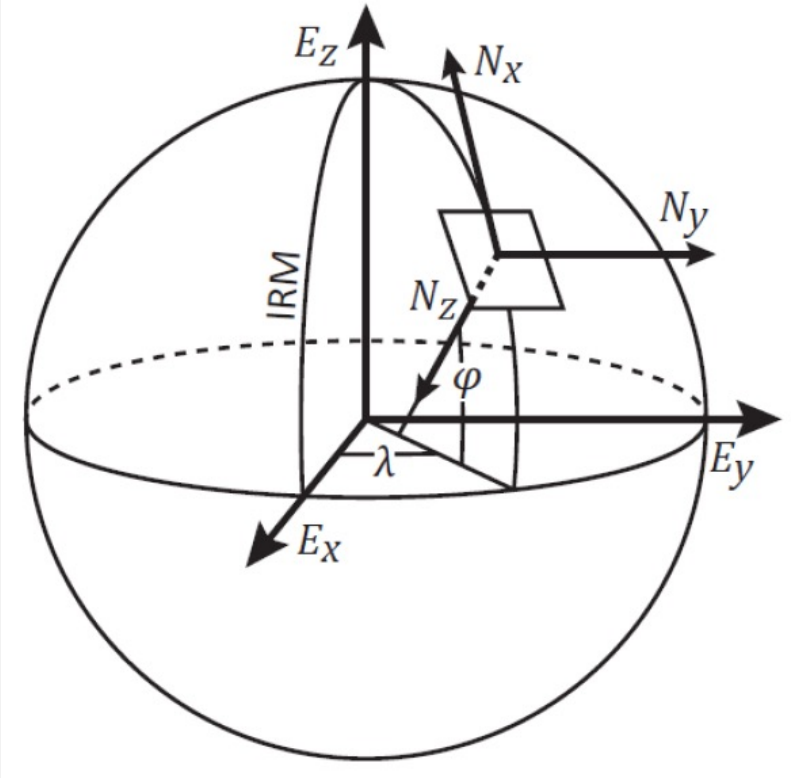
Hardware Direct (directly to UAS autopilot to give control over UAS and/or tactical data collected by:

- **Wireless**
- **Application Logic Security**

NAVIGATION THREATS

Navigation in 3D space difficult

- **Made even more difficult with additional aircraft**
- **Sense and Avoid require sophisticated sensors, algorithms, and data fusion**
- **System architecture is important for handling of data**
- **Diagram is Earth Centered Earth Fixed (ECEF)**
- **Single source vs. Multiple source attacks / countermeasures**



NAVIGATION THREATS

GPS Spoofing: Deliberate transmission of forged GPS signals resulting in the GPS receiver computing its location wrongly or fail to estimate any location at all. Spoofing threats range from simple to complex.

- **Worst Risk case: COMPLETE FAILURE OF MISSION**
- **Simulator signals not synchronized with available GPS signal and detection is easy**
- ***ECD includes the fake signal on a minimum of four satellites, and then progressively / selectively eliminates their effect until the real weaker GPS signals become apparent.***

NAVIGATION THREATS

AIS Receiver GPS Spoofing consists of *three* cyber-attack and *two* analysis activities:

1) **Breaking the existing AIS GPS receiver signal locks,**
2) **Locking the AIS GPS tracking device onto the GPS Simulator counterfeit signal,**
3) **Maintaining access by continued broadcasting of the fake GPS signal.**
4) **Collection / and Analysis of Data,**
5) **Report / Recommendations / Directions for further research**

A GPS/ SBAS GSS4100 signal generator/ simulator will serve as the spoofing device in the above attack plan

ACTIVE COUNTERMEASURES

Countermeasures:

- **Increase ability of GTA to react & improve saturation limit. Team formation allows decoys & shields. Swarm formation is easier to detect. Arrival of a cloud of robot drones hard to mask but tough to neutralize.**
- **AUDS by Liteye –Detect, Track, Disrupt sUAS operation by pulsed, brief focused broadcast of direction frequency jamming**
- **Laser –Chinese 5 sec weapon to shoot down sUAS at low altitude (500 m) with 10KW high energy laser. Range 1.2 mi, speeds up to 112 mph**
- **Sound – UAS rotors have low threshold for intense harsh acoustical noise. Result: MEMS Gyroscope degraded and rotrs spin at different speeds /malfunction**

ACTIVE COUNTERMEASURES

Passive Goals:

- **Protect Indirectly: physical protections around target, decoys, shields, organized roadblocks, nets, jamming of sensors of the aggressor, GPS total or Partial Spoof**

Countermeasures:

- **Decoys can be effective if we know the sensors employed for sUAS Kamikaze attack & how it is used in SAA.**
- **Communication Jamming effective against Level 1 & 2 drones which require pilot interaction. It can perturb inter –drone communications required for either Team or Swarm formations.**
- **Sensor Jamming – especially GPS signals – false GPS information, camera / gimbal dislocation, heading sensor demagnetization effective regardless of automation.**

SPOOF-PROOF PROTECTION
EICHELBERGER COLLECTIVE DETECTION (ECD)

- **Recognize that ADS-B is a subset of the larger receiver localization problem**
- **Solutions that apply to the larger vector space, GNSS / GPS also are valid for the subset, ADS-B, if computational hardware is available**
- **GPS is a reasonably researched topic. Many methods proposed to detect and mitigate spoofing.**
- **Lions share of the research focusses on detection of spoofing attacks**
- **Civilian COTS anti-spoofing countermeasures are rare**
- **Let's enter the brilliant mind of Dr. Manual Eichelberger, a Swiss scientist from ETZ Zurich, who invented a method for detection, mitigation and recovery of spoofed GPS Signals.**

SPOOF-PROOF PROTECTION
EICHELBERGER COLLECTIVE DETECTION (ECD)

- **ECD is my given name Honoring Dr. Manual Eichelberger's work**

- **ECD is a critical algorithm invention to detect, mitigate and recover spoofing or jamming attacks on GPS or ADS-B**
  - **ECD is a maximum likelihood snapshot receiver localization method (CD),**
  - **Does not determine the arrival time for each satellite,**
  - **Combines all the available satellite / receiver information and decides only at the end of the computation.**
- **Exploits robustness of Collective Detection (CD) with modifications to mitigate spoofing attacks**
  - **ECD shows multiple locations, including the actual one, can be recovered from scenarios in which several signals are present (including false ones)**

SPOOF-PROOF PROTECTION
EICHELBERGER COLLECTIVE DETECTION (ECD)

- **Two most powerful GPS signals spoofing attacks are Seamless satellite-lock takeover (SSLT) and Navigation Data Modification (NDM)**

- **ECD defeats the powerful and subtle attack on top of a jammed signal. Spoofer sends a set of satellite signals with adjusted power levels and synchronized to the authenticates signals to spoof receiver.**

- **ECD avoids all spoofing and jamming pitfalls and signal selection problems by joining and transforming all signals into a location likelihood distribution.**

- **Finding ECD consistent signals in 4 dimensions, space and time is computationally expensive.**

- **ECD reduces computational load by leveraging a fast branch and bound algorithm with SIC dampening**

SPOOF-PROOF PROTECTION
EICHELBERGER COLLECTIVE DETECTION (ECD)

- **Successive Signal Interference Cancellation (SIC) : ECD uses SIC - an iterative signal damping technique.**

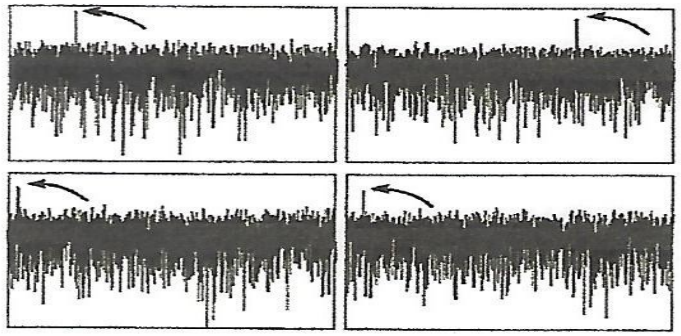
- **SIC removes the strongest received signals one by one in order to find the weaker signals.**

- ***It is impossible to differentiate between authentic and spoofed signal, a priori, ECD does not remove any signals from the sample data.***

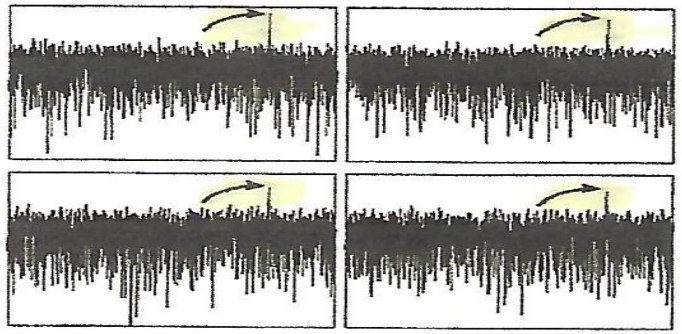
- **ECD dampens strong signals by 60% in order to reveal weaker signals. This can reveal localization solutions with lower CD likelihood. (Eichelberger, 2019)**

- See next figure

ACTIVE COUNTERMEASURES
EICHELBERGER COLLECTIVE DETECTION (ECD)



(a) Original (not shifted).

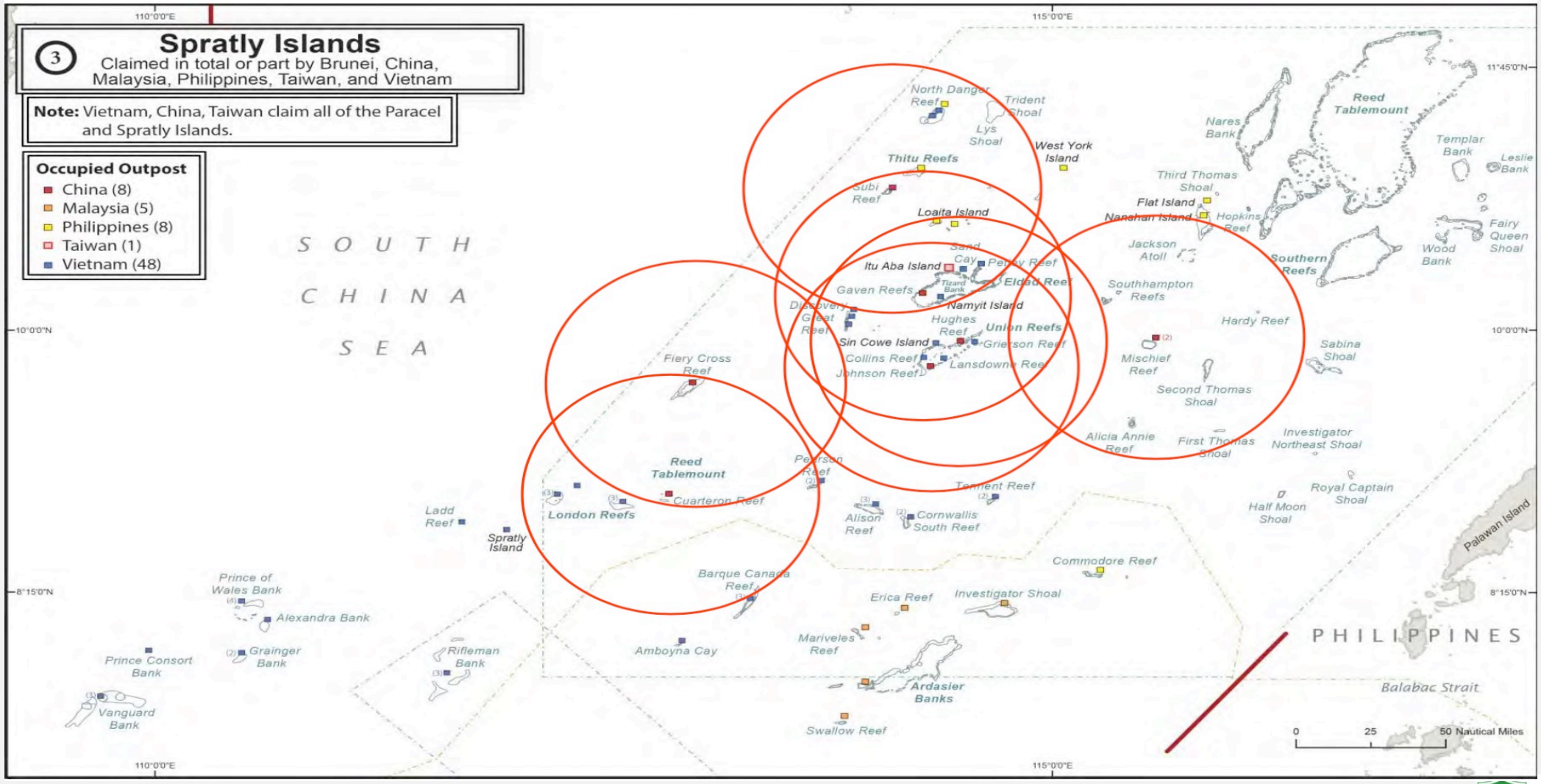


(b) Shifted (circularly) according to the distance from the receiver to the corresponding satellite.

Figure 5.2: Correlation functions for four satellites. Above are the correlations of the received signal with the PRN sequences of four different satellites. The spikes indicating the beginning of the PRN codes in the received signal are marked with arrows. If we shift the correlation vectors according to the true distance to the satellites, we see below that the peaks all align. (SEE YELLOW HIGHLIGHTED PEAKS)

CHINESE TERRORIST THREATS USING UAS IMPENDING INVASION OF TAIWAN

TERRORIST THREATS USING UAS & CHINA



TERRORIST THREATS USING UAS & CHINESE BKZ-005

Using <u>BKZ-005</u> Medium Altitude drone to support NK threats

- **In 2017, Suspected Used to launch Cyber weapons to Spoof GPS Signals to Commercial Vessels, Alnic MC & ACX forcing them to collide with US Navy Destroyers USS JOHN S MCCAIN and USS FITZGERALD in Pacific. 20 Dead sailors!**
- **In 2017, Suspected in GPS positional spoofs (collision /grounding incidents) against guided-missile cruisers USS LAKE CHAMPLAIN, USS ANTIETAM, and ballistic-missile submarine USS LOUISIANA**

Source: http://www.businessinsider.com/isis-has-demonstrated-drone-capabilities-2014-8

TERRORIST THREATS USING UAS & CHINA

Asymmetric target ships: ACX, Alnic MC, Korean fishing boat, USN Navy Offshore Support Vessel Incidents 2017

[BKZ-005] Maximum Range of 1491 miles, Operational ceiling of 26,246 feet

- Long-endurance, not VTOL, launched from carriers or ground – based runways in East & South China Seas
- Electro-optical, infrared, synthetic aperture, signals intelligence sensors & satellite communications
- Like Predator drone, Used for ISR for PLA of China, Modified for weapons payloads

Source: http://www.businessinsider.com/isis-has-demonstrated-drone-capabilities-2014-8

TAIWAN: TARGET CHARACTERISTICS LSAS

Strategic Location

- **Taiwan Strait**
  - **Part of the South China Sea**
  - **Connects to the East China Sea in the North**
  - **Separates Fujian Province from Taiwan**
  - **Many Islands in the Strait**
- **PRC controlled Islands**
  - **Xiamen, Gulangyu, Pingtan**
- **ROC controlled Islands**
  - **Kinmen, Matsu**
- **The Min & Jiulong Rivers empty into the Strait**

GEOGRAPHY - LSAS

Strategic Location – China's Perspective

- **Taiwan is a critical link in the "first island chain"**
- **Includes Japan, the Ryukyus, the Philippines, Malaysia, Indonesia, and Australia**
- **China considers the area between the islands as "Navigational Choke Points"**
- **It constrains the PLA naval access to the "second island chain"**

GEOGRAPHY - LSAS

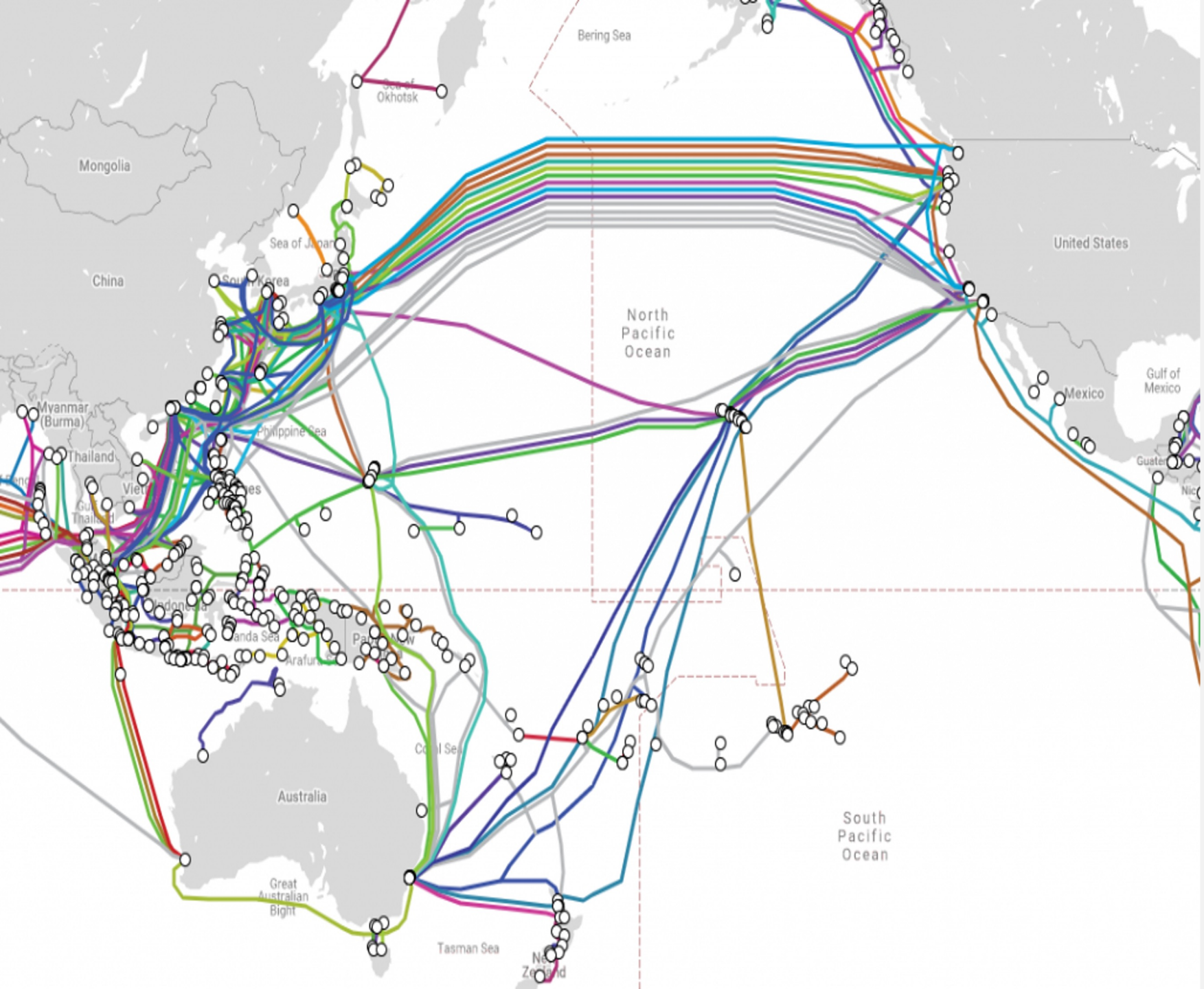
Strategic Location – China's Perspective

- **Second Island Chain**
  - **Guam, the Marianas, the Palau island group and other small islands in the central Pacific**
  - **From there, China would have open ocean**
- **China's coastline in the East China Sea lacks deep water ports**
- **Unable to put Naval bases there**
- **Submarines must operate on the surface until Ryukus archipelagos**

GEOGRAPHY - LSAS

Strategic Location – China's Perspective

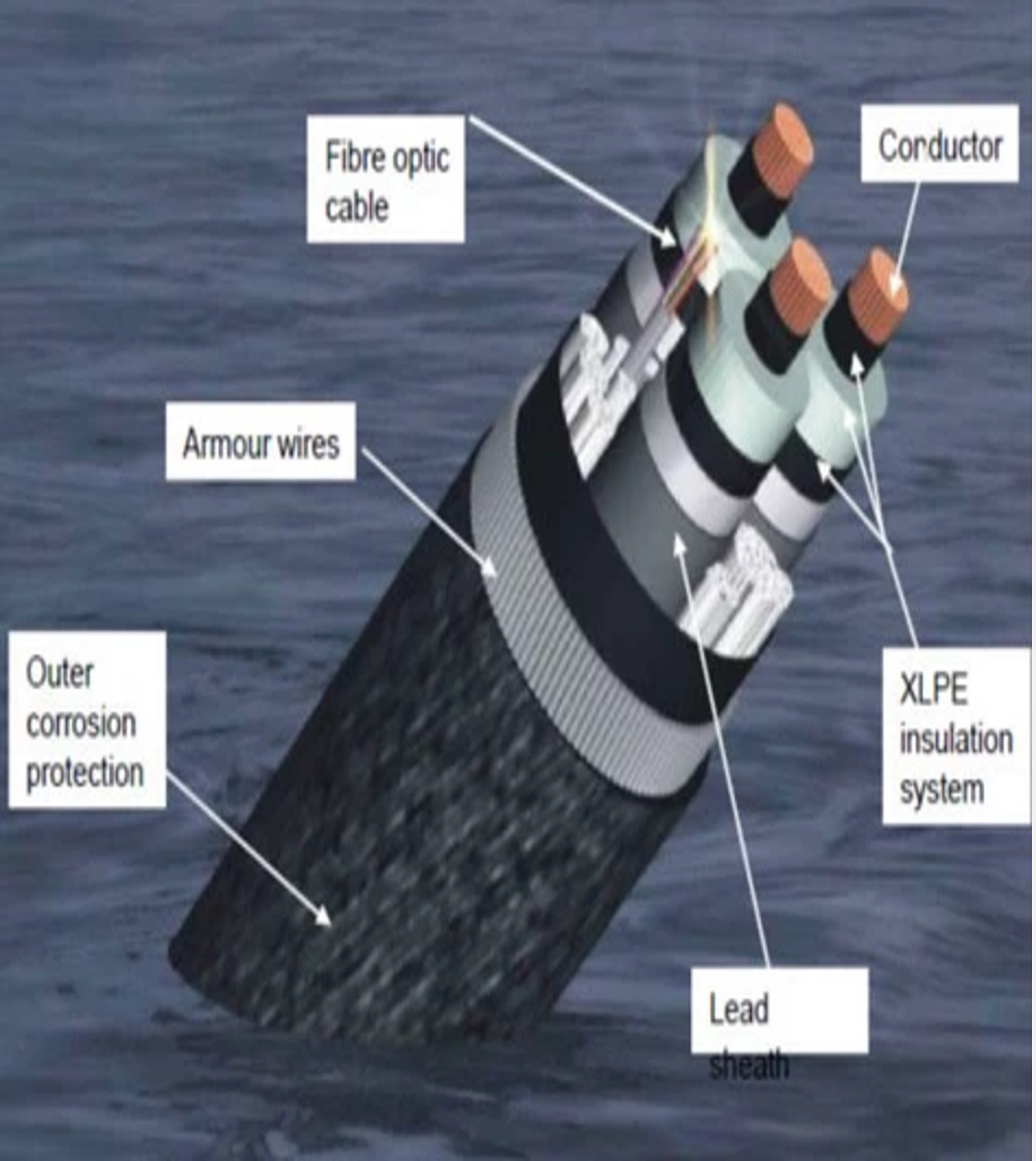
- **Chinese controlled Taiwan**
  - **Submarines have an easier exit from deep water ports into the Pacific**
  - **Increased threat for Japan by controlling the sea lanes**
  - **Increased threat to the US 7th Fleet, Guam, Hawaii, and the US West Coast**
  - **Possibly endanger South Korea as US more focused on China than North Korea**



SUBMARINE CABLE NETWORKS ACROSS - PACIFIC OCEAN

- Google and Facebook had helped pay for construction of the now completed telecommunications link - never received approval from U.S. authorities to use it
- Around 300 submarine cables carry 99 percent of the world's data traffic, with more than 20 established Trans-Pacific systems

C2SR CENTER FOR CYBER SECURITY RESEARCH
CARS



THE RESULT - SEVERING UNDERSEA CABLES

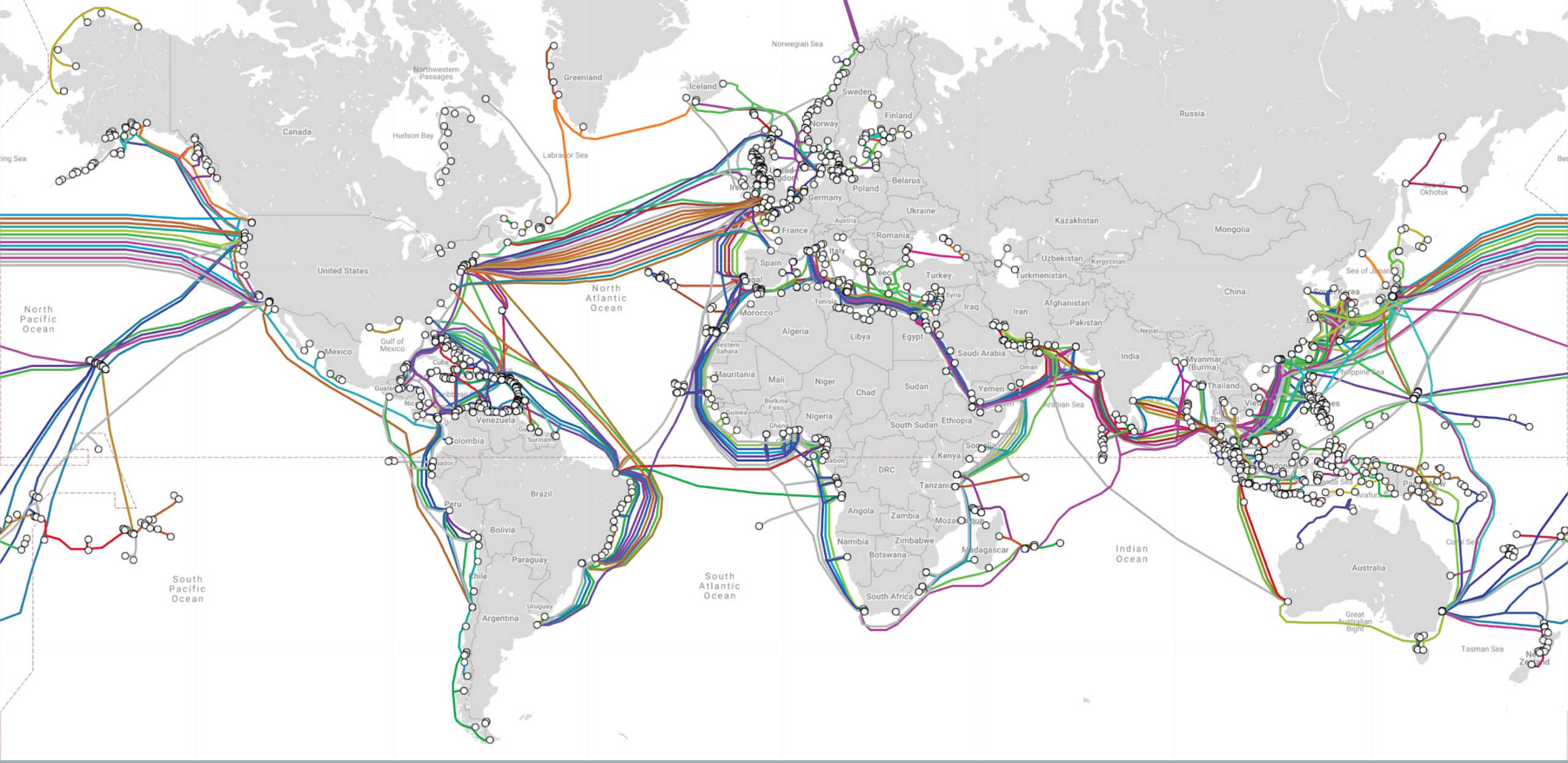
- Cutting off military communications – Early stages of Conflict
- Cutting off government communications - Early stages of a conflict
- Eliminating internet access for a targeted population
- Sabotaging an economic competitor
- Economic disruption for geopolitical purposes.
- Actors - pursue several or all of these objectives simultaneously

C2SR CENTER FOR CYBER SECURITY RESEARCH
CARS

SUBMARINE CABLES = PROFIT

- Submarine cables - subject to Chinese influence - intentional delay of repair permits within China's EEZ
- China claims 85 percent through its infamous nine-dash-line.
- The SCS is a major shipping corridor that hosts one-third of all maritime traffic - shocking $5 trillion in trade annually - yield 130 billion barrels of oil
- China aggressively defends its claim - created 3,200 acres of new or expanded islands - including those in the Spratly Group - to house military equipment and infrastructure in the SCS

C2SR CENTER FOR CYBER SECURITY RESEARCH
CARS



GLOBAL MAP OF SUBMARINE CABLES

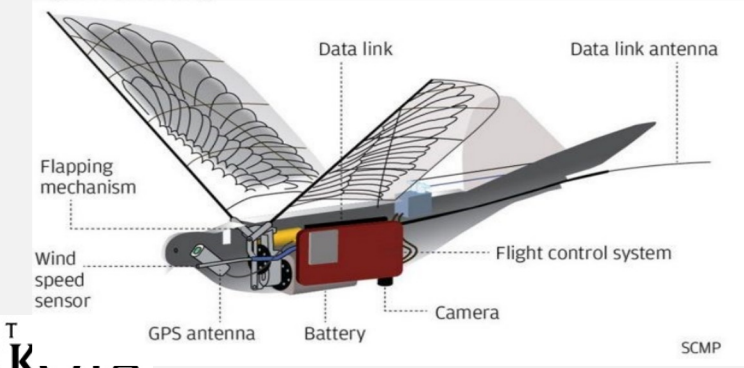
C2SR
CENTER FOR CYBER SECURITY RESEARCH
CARS

INTELLIGENCE: CHINESE UAS ARSENAL

BZK-005

GJ-11 SHARP SWORD

DOVE UAV



VTOL S-100

INTELLIGENCE: SWARM CAPABILITIES

Source: (Poliak, 2022)

INTELLIGENCE: LETHAL PAYLOAD DELIVERY

Drones are being used to drop Molotov cocktails against Russian troops in Ukraine.

Source: (Kesslen, 2022)

DJI drone caring grenade in an improvised carrier made from a plastic jug

Source: (McCarthy, 2021)

INTELLIGENCE: LAMS AND CHINESE ADOPTION

Switchblade® 600 | Tactical Angle

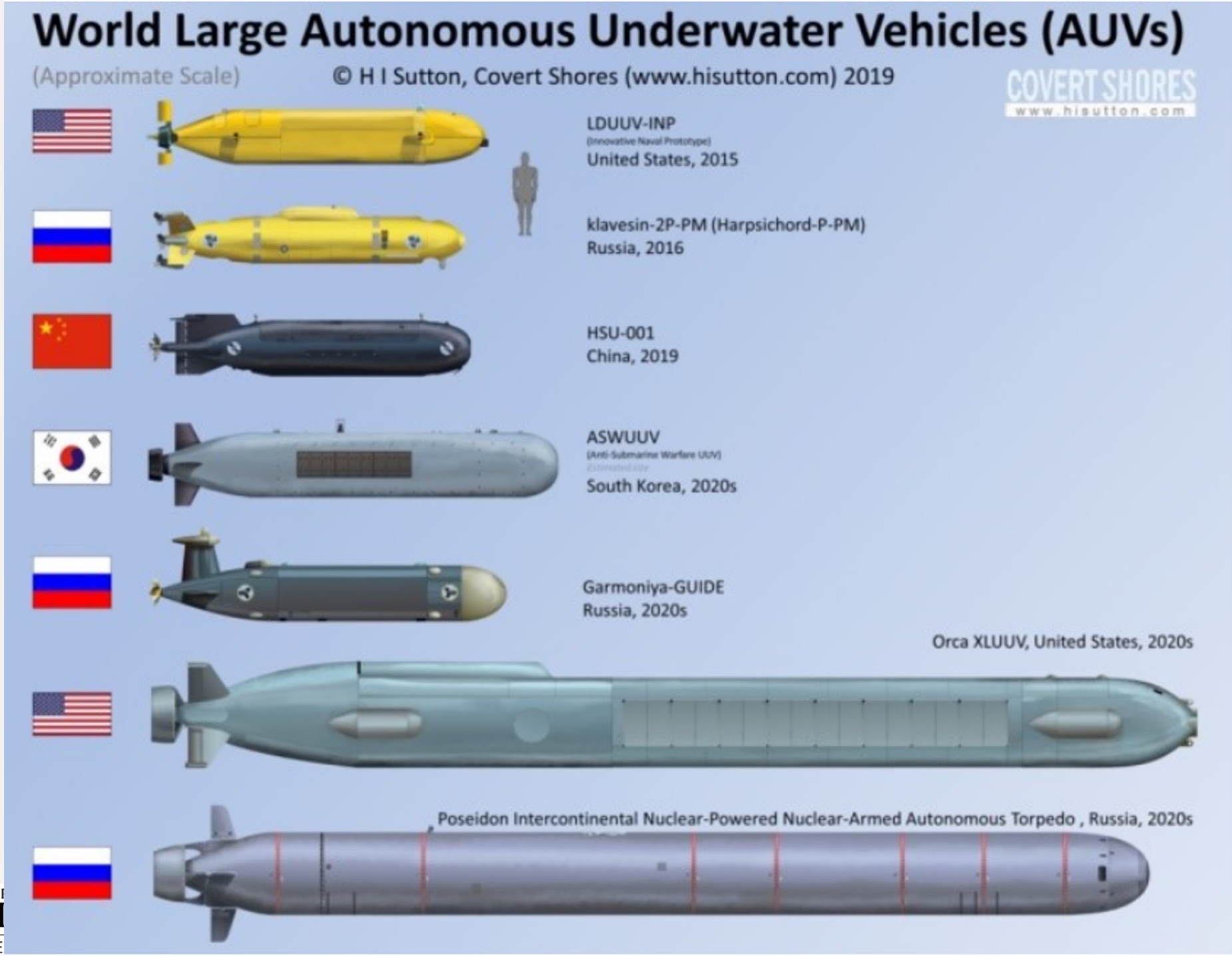
Switchblade® 300 | Sideview

INTELLIGENCE: CH-901

INTELLIGENCE: CH-901 DEPLOYMENT

CHINESE UUV (CAPTURED BY INDONESIA)

INTELLIGENCE: LARGE CHINESE UUVS


World Large Autonomous Underwater Vehicles (AUVs)
(Approximate Scale)
© H I Sutton, Covert Shores (www.hisutton.com) 2019
COVERT SHORES
www.hisutton.com
LDUUV-INP
(Innovative Naval Prototype)
United States, 2015
klavesin-2P-PM (Harpsichord-P-PM)
Russia, 2016
HSU-001
China, 2019
ASWUUV
(Anti-Submarine Warfare UUV)
South Korea, 2020s
Garmoniya-GUIDE
Russia, 2020s
Orca XLUUV, United States, 2020s
Poseidon Intercontinental Nuclear-Powered Nuclear-Armed Autonomous Torpedo , Russia, 2020s

INTELLIGENCE: CHINESE USVS

The new USV is remarkably similar to the US Navy's Sea Hunter.

RECON: CHINA'S "ARTIFICIAL ISLANDS" IN SCS