Chapter 16: Chinese Drones in Spratly Islands, and Chinese Threats to USA forces in Pacific

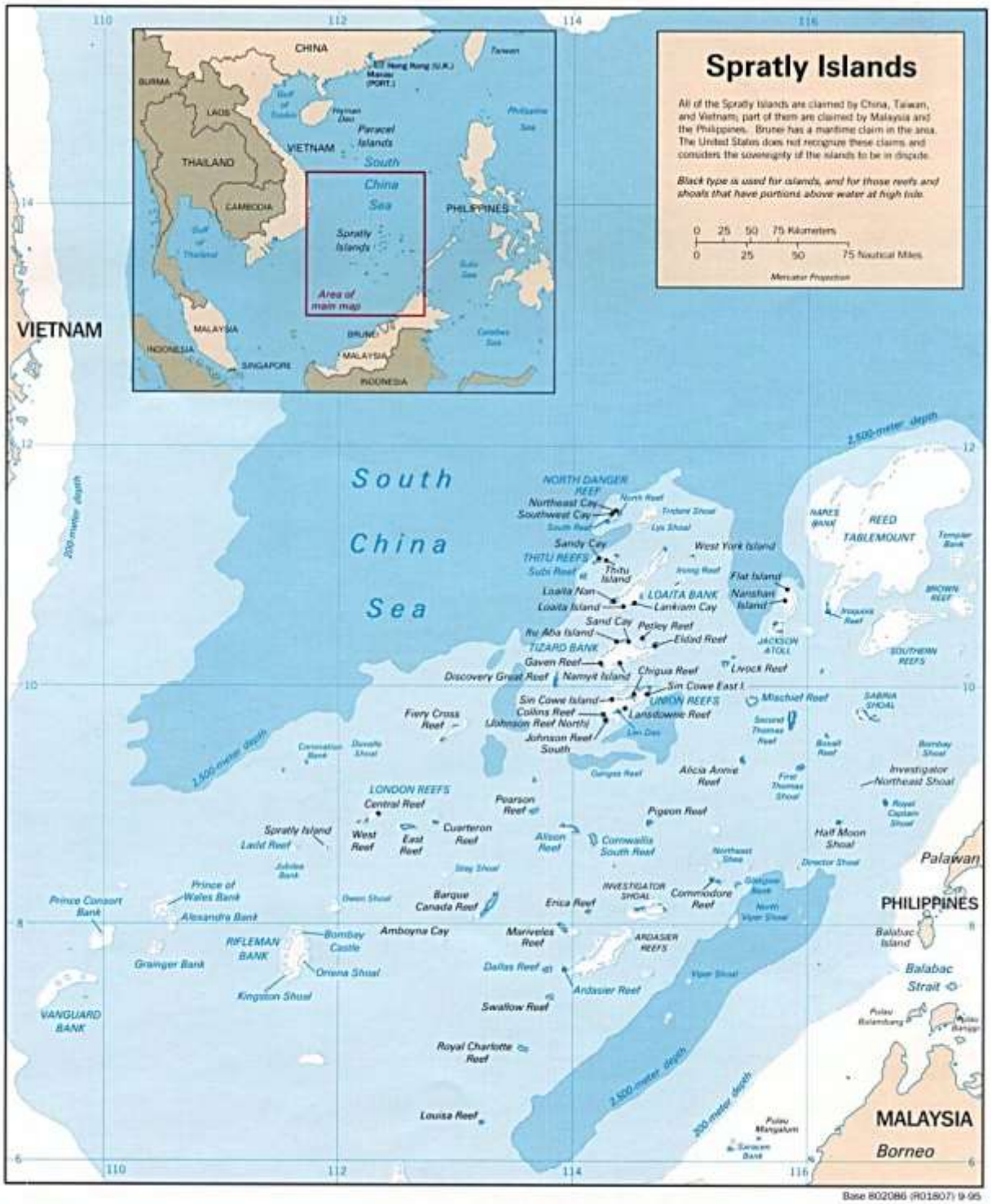
Student Learning Objectives – The student will be re-introduced to the *problem* of countering hostile use of UAS, UV / Unmanned boats / UUV against U.S. national defense interests. This chapter focuses on the Spratlys; a tiny set of islands in the South China Seas. The Spratlys are the forefront of China's military expansion and control program (Corr, 2018). From this tiny island sanctuary drones and unmanned boats are the intelligence weapons of choice. Intrusions on US capital ships has already begun and could escalate to become the flash point for WW III.[90] Deployment of Chinese GPS spoofing cyberweapons via UAS against US Naval capital ships in the Spratly Area of Operations (AO) are author-theorized.

Location of the Spratly Islands and Their Strategic Importance

The Spratly Islands are a disputed group of islands, islets, cays, and more than one hundred reefs in the South China Sea. Named after British Whaling captain Richard Spratly in 1843, they represent only 490 acres spread over 164,000 square miles. The archipelago lies off the coasts the Philippines, Malaysia and China (Wikipedia Spratly Islands, 2018).

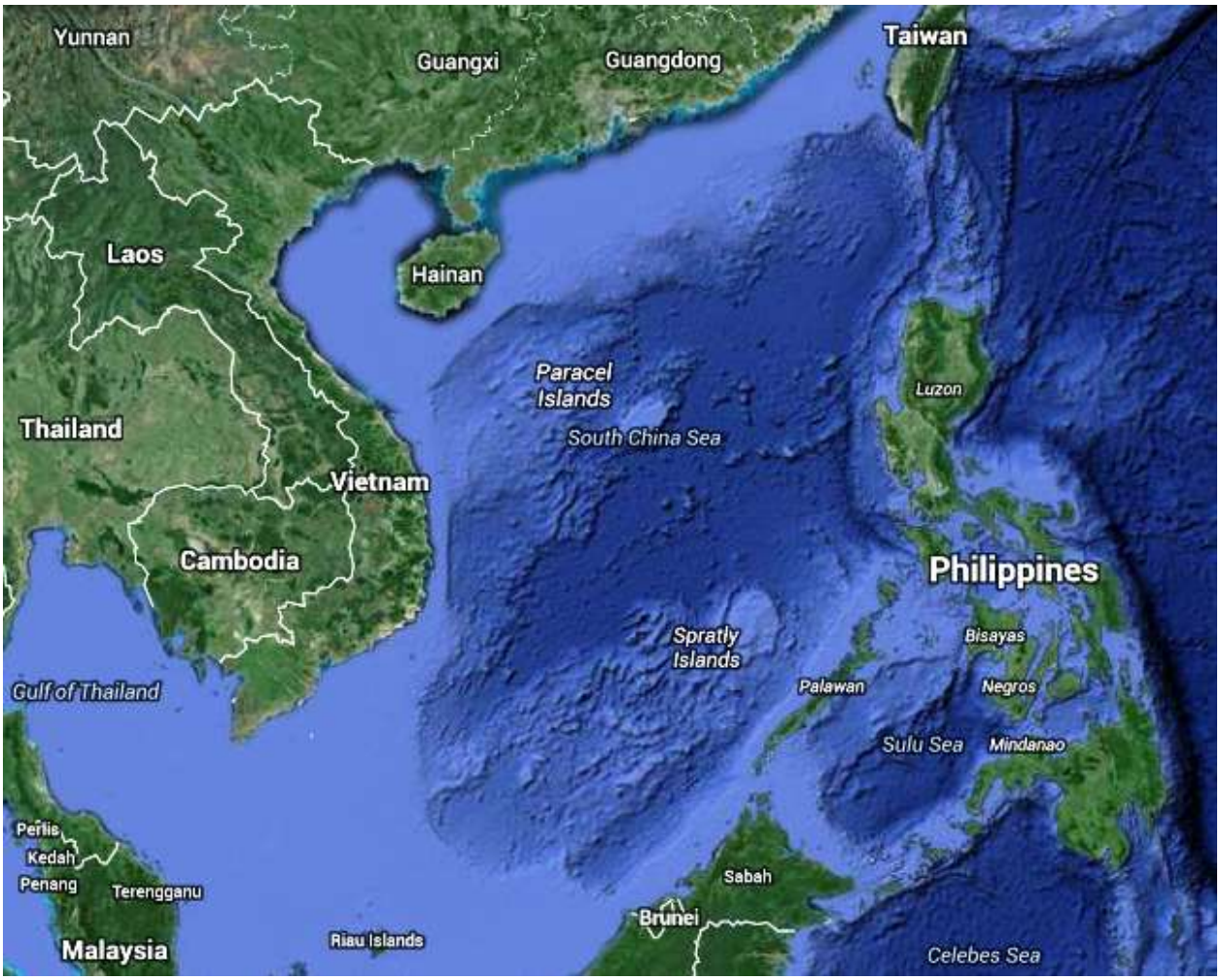
[90] Strictly authors speculation. Not supported by US official reports. Not the opinions of KSU or NPP press or co-authors. (See Discussion Question 3 in Chapter 3 Understanding Hostile Use and Cyber-Vulnerabilities of UAS: Components, Autonomy v Automation, Sensors, SAA, SCADA and Cyber Attack Taxonomy

Figure 16-1 Spratly Islands



Source: A Geographic Map of Spratlys, By Yuje at English Wikipedia - CIA, Public Domain, https://commons.wikimedia.org/w/index.php?curid=38157110 viewed September 12, 2018

Figure 16-2 Spratly Islands



Source: Google Earth. (2007). Spratly Islands. https://earth.google.com/web/@10.7232818,115.8264655,-0.80691633a,5610.99608667d,35y,0h,45t,0r/data=ClQaUhJKCiUweDMxODBkNjkxZmNkZjViNjk6MHg2NjM0YTQxNDY0MTIwY2UwGSmSrwRSciVAIW1xjc_k9FxAKg9TcHJhdGx5IElzbGFuZHMYAiABKAIoAg

Although, there are some civilian settlements in the approximate 45 islands, all contain structures occupied by military forces from Malaysia, Taiwan (ROC), China (PRC), the Philippines, and Vietnam. Brunei has claimed an exclusive economic zone around the Louisa Reef (Wikipedia, 2018). Figures 16-1 and Figure 16-2 show the Spratly Islands. Officially they are in the South China Sea at 10 degrees N, 114 degrees E.

Target Drones

The Spratlys may be disputed in theory, but the undeniable winner in any real this AO would be China. China has made huge investments in defensive infrastructure, military, and unmanned aircraft, and boats to solidify its position in the Spratlys. China has one of the largest UAS intelligence operations in place in the Spratlys and regularly conducts drills (Staff, 6 Jul 2018). These drills simulate fending off an aerial attack. The drills, which involve three target drones making flyovers of a ship formation at varying heights and

directions, are part of the on-going efforts to improve its real-life combat ability(Staff, 6 Jul 2018). The drones have been sent out several hundred times during more than thirty drills (Staff, 6 Jul 2018).

Shark Swarm and Wanshan Marine Test Field

China has tested an army of tiny drone ships that can "shark swarm" enemies during sea battles. It has a fleet of fifty-six unmanned craft sent out on maneuvers off the Wanshan Archipelago in the South China Sea (Barnes, 7 June 2018). The Chinese firm Oceanalpha confirmed the drones were designed to overwhelm enemies in sea battles. A mothership controls the armed swarm (Barnes, 7 June 2018).[91] Oceanalpha confirmed that the Wanshan Marine Test Field, was constructed sole purpose of conducting drone craft drills (Barnes, 7 June 2018).

Fast Drone Ship

In December of 2017, HiSIBI, a Chinese nautical firm, announced the development of the world's fastest drone ship, which can travel at 50 knots (58 mph).[92] The new speed drone is being tested in the Wanshan Marine Test field. The test field is still under construction and is believed to be the world's largest test field, covering over 297.9 square miles. Military observers have indicated that the test site for unmanned vessels was part of China's overall plans to develop autonomous systems for both civilian and military applications. The new test site dovetails with China's push to use technology to safeguard China's maritime interests (Staff writer, 6 July 2018).

Long-Range UUV

Tianjin University researchers completed a sea test of the Haiyan autonomous Unmanned Underwater Vehicle (UUV). It can endure for 30 days and has a 621.37miles range Lin, J & Singer, P.W., 4 June 2014). Just as the US Navy is conducting UUV research for facing off against China's growing Anti-Access Area Denial capabilities, the Chinese are building up these capabilities (Lin, J & Singer, P.W., 4 June 2014). UUVs cover a larger area, can operated more efficiency, use multiple sensors to monitor water temperature, conductivity, optical backscatter, and acoustics. In battle mode for detection of a stealthy submarine, using multiple sensor types increases the probability of finding the prey(Lin, J & Singer, P.W., 4 June 2014). Unlike fixed underwater sonar stations, UUVs can be rapidly deployed via ships or airdrops to new uncovered areas (such as Taiwan Straits or South China Sea), where mobility complicates enemy efforts to disrupt and destroy them (Lin, J & Singer, P.W., 4 June 2014).

The Haiyan UUV is part of the deployed assets for an Underwater Great Wall, which would be a network of sensors on the seabed, coupled with long endurance UUVs to identify and destroy enemy submarines and mines. The sister fish-like Qianlong autonomous underwater vehicle (AUV) can dive to 14,800 feet indicates Chinese interests in deep-sea robotic ships

[91] IBID Author note -this is more of a TEAM formation as discussed in chapter 3. Swarms do not have a team leader or Mother ship.

[92] The author is Captain of /owns a recreational yacht, 36-foot CRYPTOWIZ, that can do supposedly 32-35 knots at peak performance top speed on dual Volvo-Penta GXI 315 Hp in-board engines. Above 23 knots is nuts for control (unless you have a death wish and / or married with wife and children on-board). Just imagine being in the rough South China Seas.

(Katoch, 4 July 2018). These UUVs can also be used to attack targets anywhere in the Indian Ocean, in addition to collecting enemy submarine acoustics and oceanographic conditions for improving stealth and anti-stealth measures (Katoch, 4 July 2018).

Crisis Watch

The US and China are in a power struggle in the South China Sea centered around US countering Chinese military operations in the Spratlys. Defense Secretary General Mattis addressed some of the disputed issues at the Shangri-La Dialogue Asia security summit in Singapore 2 June 2018:

> U.S. Sec Defense Mattis outlined U.S. "Free and Open Indo-Pacific Strategy", consisting of expanded maritime security support for U.S. partners; helping regional navies become more interoperable with U.S. Navy; strengthening governance through defense engagements; and private sector-led development. Mattis said U.S. wants to work with regional multilateral institutions, particularly ASEAN; that new U.S. national security and defense strategies emphasize Indo-Pacific; said cooperation with China is "welcome wherever possible". Mattis criticized China's militarization of features in disputed Spratly archipelago. Also addressing Shangri-La Dialogue, China for first time publicly acknowledged that it was basing weapons and military personnel on disputed features it controls in Paracel and Spratly Islands, which it said are Chinese territory. Chinese military representative said Mattis's comments were "irresponsible" and that U.S. was the one militarizing, citing U.S. air and naval passages within twelve nautical miles of Chinese-controlled territory. U.S. 5 June flew two B-52 bombers over disputed Scarborough Shoal near Philippines; China sent ships and aircraft, said U.S. "stirring up trouble". Reuters 3 June reported U.S. considering stepping up its naval operations near disputed features. U.S. held annual Malabar naval exercise with India and Japan 7-16 June off coast of Guam and in Philippine Sea. Biennial U.S. Rim of the Pacific (RIMPAC) naval exercises began 27 June without China after U.S. late May rescinded China's invitation to participate. Citing satellite imagery dated 8 June, ImageSat International reported that China had redeployed surface-to-air missile systems to Woody (Yongxing) Island in Paracels. PLA navy 15 June carried out missile drills in South China Sea (SCS). UK and French defense ministers 3 June said they would send more naval ships through SCS to assert right to freedom of navigation. Meeting with Sec Defense Mattis in Beijing 27 June, President Xi Jinping reasserted that China would not give up any of its territorial claims in SCS; also called for deepening military-to-military ties (Staff, June 2018, Crisis Watch).

In May 2018, the US disinvited China from the 27 nation International Naval Exercises (RIMPAC) in response to South China Sea aggression. The Pentagon claims evidence that the Chinese have deployed anti-ship missiles, surface-to-air missiles (SAM) systems, and electronic jammers to the Spratly Islands. The Chinese have landed bomber aircraft at Woody Island (Huang, 23 May 2018). This is along with the new drone systems and intelligence UAS assets discussed supra.

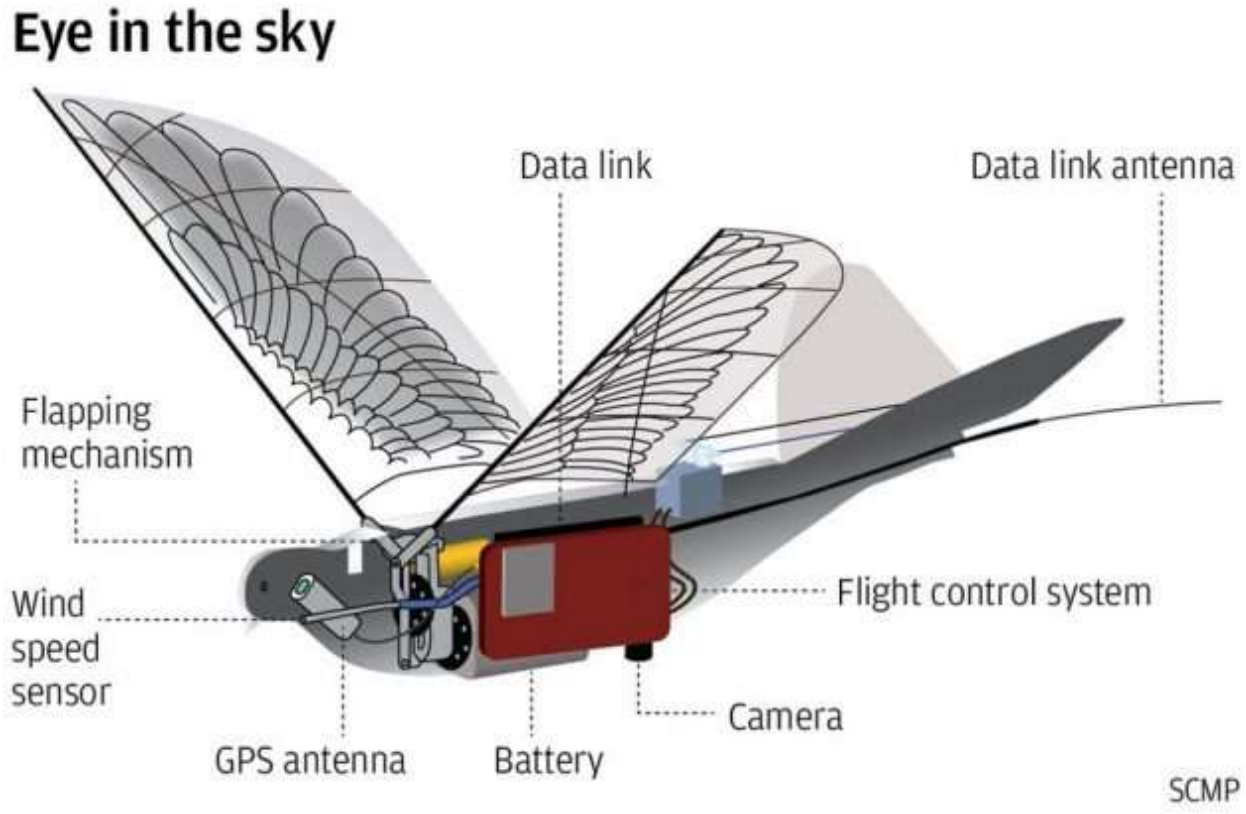
A Birds' Eye View

China has developed and deployed hi-tech drones for surveillance of population. These spy birds, code-named Dove, have completed more than 2000 test flights before deployment in real-life situations. Early versions of the bird robots had fixed wings and rotor blades. The Dove drones actual mimic the flapping action of birds, replicating about 90% of the real doves' movements and producing very little noise signature. Doves weigh only 0.441 pounds and have a wing-span of 19.685 inches. They can fly up to 24.855 mph for 30 minutes (Katoch, 4 July 2018). China is testing the Doves with facial recognition, stabilizing software, arming with explosives and increasing endurance for targeted Assassinations. The drones are being tested in Swarm formations (Katoch, 4 July 2018). Because of Chinese aggressiveness and its policy of ambiguity and deceit, the danger is clear and present (Katoch, 4 July 2018). See Figure 16-3 Chinese Dove Drone.

Red Drones over Disputed Seas

One of the best reports on how Chinese military uses unmanned drones as a means of power projection and surveillance in the contested South and East China Seas was written by (McCaslin, August 2017). China is currently undergoing a "drone" driven by heavy investment in the Chinese drone industry and by illegal acquisition of foreign drone technology (Katoch, 4 July 2018).

Figure 16-3 Chinese Dove Drone



Source: Chua, M. (3 July 2018). In China, Dove Surveillance Drone Is Watching From The Sky Above. https://mikeshouts.com/chinas-dove-surveillance-drone/

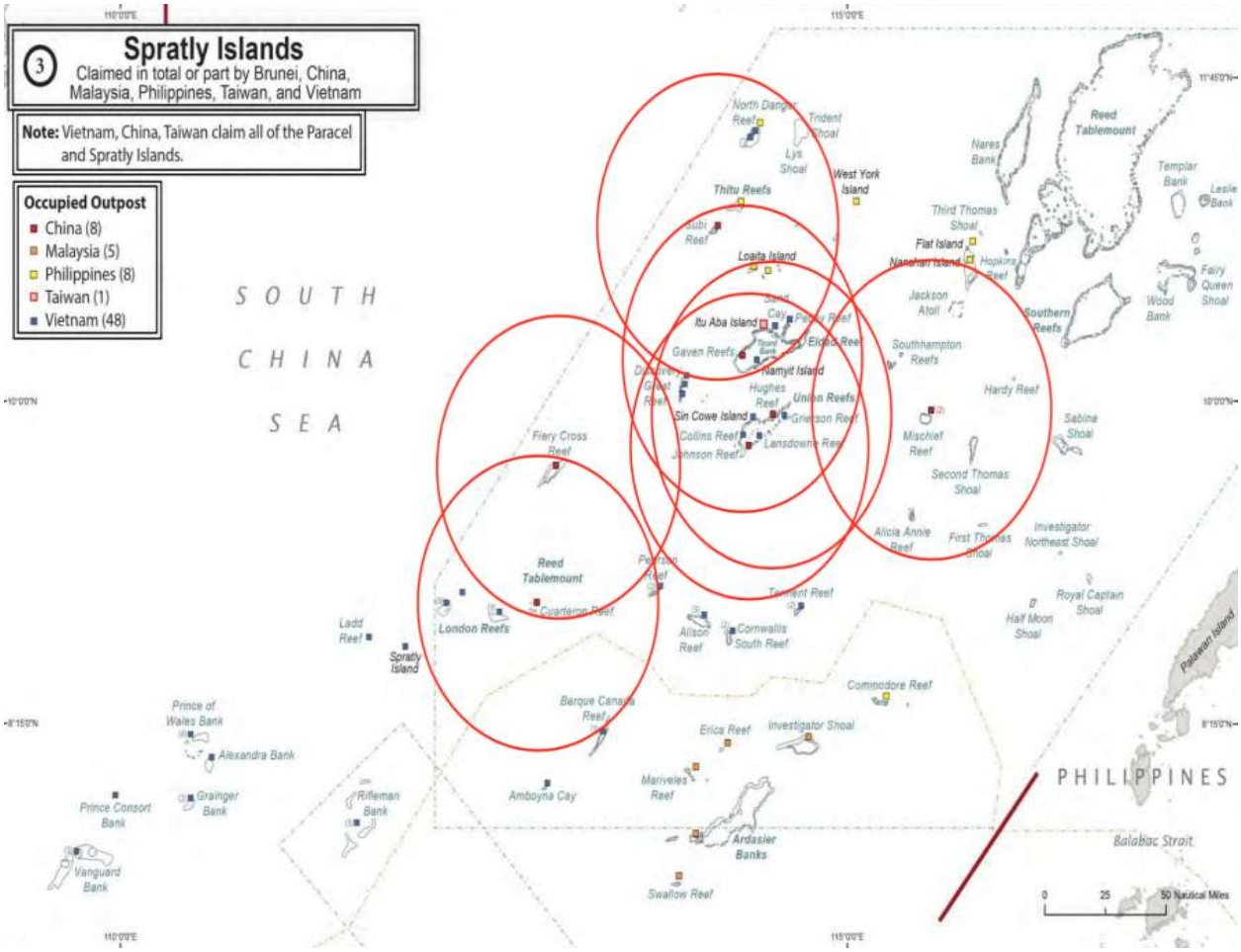
US DOD predicts China will produce tens of thousands of drones by 2023 (DoD Report, 2015). Drone sightings and proper identification is important because of lack of international rules governing treatment of drones, including in areas where sovereignty is contested (Lehman, 29 August 2017).

The report documents four drones known to be used by PLAN: The S-100, ASN-209, BZK-005, and the GJ-1. All but the S-100 are Chinese-produced. The S-100 is made by Scheibel, in Austria (Lehman,29 August 2017). The drones discussed fill a variety of roles, from surveillance (S-100) to military / weaponized (GJ-1, aka Wing Loong I model) (Lehman, 29 August 2017).
One limiting factor facing Chinese power projection is the inability of their current inventory to runway launch from aboard the Chinese Navy's sole aircraft carrier. This limits the BZK-005 (primary mission surveillance) to be launched from land (McCaslin, 2017). The S-100 uses vertical take-off and landing (VTOL) system and does not have this problem. Additionally, drones can be launched from Chinese-controlled artificial islands in the contested areas [i.e. the Spratly Group.] (Lehman, 29 August 2017).
The author contends that the BKZ-005 is suspected of being outfitted with cyber weapons to harass the US Naval forces in the Spratly AO causing chaos with the commercial and potentially US navy GPS systems.[93]

[93] This speculation is covered later in this Chapter.

S-100 by Scheibel

Figure 16- 4 S-100 Drone Trajectories in Spratly Islands



Source: McCaslin, I.B. (2017). Red Drones over Disputed Seas: A Field Guide to Chinese UAVs/ UCAVs Operating in the Disputed East and South China Seas. Released by Project 2049 Institute at: http://project2049.net/documents/Red%20Drones%20over%20disputed%20seas_PLA_project2049.pdf

Figure 16 -5 S-100 Chinese Drone

Source: Schiebel Camcopter S-100 at ILA 2010 (12 June 2010). By MatthiasKabel. CC BY-SA 3.0, https://commons.wikimedia.org/wiki/File:Schiebel_Camcopter_S-100_at_ILA_2010.jpg from Wikimedia Commons

The S-100 has an 18,000-foot ceiling, weighs 75 pounds armed with Thales Lightweight Multi-role Missiles (LMM), with a range 60 to 125 miles and can be operational for 10 hours. They are generally launched from a PLAN Type 054 /054A frigate (McCaslin, 2017).
China uses the S-100 for intelligence, surveillance, and reconnaissance (ISR). They are equipped with Synthetic Aperture Radar (SAR), Maritime Radar, Signal Intelligence (SIGINT) and Communications Intelligence (COMINT) payloads. See Figures 16-4 and 16-5 for S-100 views and ranges.

ASN-209

The ASN -209 is a medium altitude, medium endurance (MAME) UAV. It has an operational ceiling of 16,404 ft, an operational range of 124.3 miles, and an endurance of 10 hours. The ASN-209 is deployed with a rocket booster on the back of a truck and lands via parachute (Wikipedia, ASN-209, 2018) The ASN-209 is equipped with Tian Long -2 (TL-2) missile. The TL-2 has heat and fragmentation warheads. The ASN-209 is used for border surveillance, counter-terrorism, maintaining stability to target light armored vehicle, skiff or armed personnel (Wikipedia, ASN-209, 2018) See Figure 16-6.

Figure 16-6 ASN-209 Chinese Drone

Source: Chinese ASN-209 Unmanned Aerial Vehicle (UAV). http://chinesemilitaryreview.blogspot.com/2011/10/chinese-asn-209-tactical-unmanned_20.html Viewed on September 12, 2018.

Figure 16 -7 BZK -005 Chinese Drone

Source: The Cyber Shafarat – Treadstone 71. (4 October 2017). Drone Wars! Threats, Vulnerabilities and Hostile Use. https://cybershafarat.com/2017/10/07/dronewars/

BZK -005

The BZK-005 is also a MAME drone specialized surveillance missions. It has an operational ceiling of 26,247 feet, with a maximum range 1491 miles and endurance of 40 hours. The range is limited by ground-based runways, i.e. Spratly Island group (McCaslin, 2017).

It is equipped with electro-optical, infrared, SAR, SIGINT and satellite communications systems, allowing real-time data transmission capability (McCaslin, 2017). See Figure 16-7 for BZK-005 view.

The BZK-005 range permits surveillance over the entire South China Seas if launched from Chinese – controlled islands (artificial and natural): Woody Island, Subi Reef, Mischief Reef, and Fiery Cross Reef (McCaslin, 2017).

GJ- 1 Chinese UCAV

The GJ-1 is also a MAME UAV converted to unmanned combat aerial vehicle (UCAV).
The GJ-1 can carry 441 pounds. It has SAR and electro-optical loadouts. It has been equipped with 8 different weapons systems, primarily, air-to-surface missiles and small diameter bombs (McCaslin, 2017). See Figures 16-8 and 16 -9 for GJ-1 identification views.

This model has an operational capability of 2,485 miles and can fly higher than any other military drone in the Spratly AO (McCaslin, 2017). Its endurance capability is classified.

Figure 16 -8 GJ-1 Chinese UCAV Drone (Armed)

Source: Mil.huanqui.com. (February 6, 2018) Jane's: China sells the most advanced drones at the Singapore Air Show, http://mil.huanqiu.com/world/2018-02/11586378.html. See also https://www.youtube.com/watch?v=0QCNQfqkgDY

Figure 16 -9 GJ-1 Chinese UCAV Drone (Armed)

Source: Mil.huanqui.com. (February 6, 2018) Jane's: China sells the most advanced drones at the Singapore Air Show, http://mil.huanqiu.com/world/2018-02/11586378.html. See also https://www.youtube.com/watch?v=0QCNQfqkgDY

Think of Chinese use of swarming drones on the seas, in the air, floating nuclear power plants, underwater mining, robot freighters and anti-submarine UUVs. In the author's view, they are leapfrogging US technology and antiquating defenses (Lehman, 29 August 2017). [94]

[94] with additional author commentary

Interference with US Ships – Exploring the Cyberweapon deployed from UAS against US Capital Ships

It should be clear that the Chinese (PLAN) are heavily invested in military operations using unmanned aircraft and naval vessels in the Spratly Islands. This researcher has been tracking Chinese UAS and Intelligence assets /facilities / naval vessels since 2014. Figure 16-3 shows a glimpse of the deployment in the Spratly Area of Operations (AO). The black pin is the Spratly Islands group. Blue pins represent US Navy capital ships involved in either collisions or groundings in the AO. Red pins represent center of known Chinese UAS Intelligence elliptical paths. Green pins represent Chinese Intelligence facilities or seaborn assets. Figure 16-3 is not comprehensive. An exploded map view would show many more Chinese assets in the AO (Nichols & Carter, 4 May 2018).

Given the capabilities that Chinese (and US) UAS systems can deploy in almost any conditions and any location, it seems reasonable to this researcher, that the Chinese military might test their cyberweapons from their UAS in the Spratly AO coverage to harass US vessels and potentially disrupt US Navy capital ships navigation systems. [This would be a natural priority for the Wanshan Marine Test Facility.] As a lesser alternative, the Chinese might take the 911 approach [i.e. turning planes into missiles loaded full of fuel and ramming them straight into fixed buildings] by disrupting (signal spoofing) the GPS /AIS unencrypted signals of huge commercial vessels and forcing them to act as Greek trireme vessels, colliding into the US Naval vessels in restricted maneuverable waters. [95]

[95] Triremes were used in the Peloponnesian Wars to ram at about 4 knots at a 60-degree angle of attack. The greater the angle of attack the lesser the speed requirement for ramming. What is interesting is that the Athenians used a multi-trireme attack, an early predecessor to Swarm tactics. They also used grappling hooks to engage the enemy ships directly up close. This was the predecessor to piracy tactics in the 1500's – 1830's. Wikipedia.

Figure 16-10 Chinese UAS Chinese Intelligence Assets Deployment in Spratlys

Source: Nichols, R.K & Carter, C. (4 May 2018). RSCAD Presentation of Research to KSUP Faculty on Deployment of Chinese Cyber-weapons and GPS spoofing of Naval Vessels

The Case for Cyber Weapon Spoofing of Legacy GPS Signals Affecting Us Navy and Commercial Vessels in Pacific

U.S Navy Vessel Collisions in the Pacific

In 2017 there was a chain of incidents/collisions involving four U.S. Navy warships and one U.S. Navy submarine.

On 17 June, the destroyer USS Fitzgerald collided with the ACX, a 30,000-ton container ship resulting in seven dead. Records show that the ACX turned sharply right at the time of collision. *The captain of the Philippine-flagged container ship accused the Navy destroyer of failing to heed warning signs before the crash***.** Those warning signs came from the commercial vessels Automated Collision Systems (AIS) on the bridge. On 9 May, the guided-missile cruiser USS Lake Champlain collided with a South Korean fishing boat off the Korean Peninsula. There were no injuries (Department of the US Navy, Office of Chief of Naval Operations: 29 November 2017). On 31 January, the guided-missile cruiser USS Antietam ran aground dumping more than 1000 gallons of oil into Tokyo Bay. On 18 August, the ballistic-missile submarine USS Louisiana collided with the Navy Offshore Support Vessel in the Strait of Juan de Fuca.

There were no injuries. "On 20 August, the guided-missile destroyer USS John S McCain collided with the 600-foot oil and chemical tanker Alnic MC at 0624 JST resulting in ten dead (Navy Office of Information, 11/1/2017)". (Weise E. , 2017)

Navy Response

In all five incidents, the U.S. Navy blames their field leadership for not responding in an appropriate manner. This response means that the Skipper / XO / COB and at least 5 watch sailors on each Naval vessel (roughly 40 - 50 personnel including bridge staff plus 130 lookouts on the USS McCain because of ordered watch conditions) have been judged incompetent (Navy Information Office, 11/2/2017). Their careers are over, and some will face courts marshal and possible brig time. This response also implies that all five Navy vessels' radar, emergency positioning alert systems, AIS, sonar, and long-range collision avoidance equipment must have been functioning perfectly, without a catastrophic failure or interference of any kind. This conclusion assumes that none of the ships were in difficult maneuverable waters or serious traffic. The Navy blames funding, readiness and training. However, their response may not fully account for the commercial vessel accident data, actions required, or GPS positional data received (Olson, August 30, 2017).

The Navy Official Reaction regarding the possibility of Cyber-Weapon or Cyber-Attack

The Navy has downplayed the possibility of a Cyber Weapon or Cyber Attack. "Chief of Naval Operations (CNO) Admiral John Richardson said in a tweet on Monday 23 August, referring to the USS McCain and USS Fitzgerald collisions, "there was no indication of the possibility of cyber intrusion or sabotage was involved or that the Navy ships were hacked, but the review will consider all possibilities." (Weise E. , 2017) The Navy investigators after inspecting the physical damage to the USS McCain and USS Fitzgerald agree with the CNO's conclusions (Olson, August 30, 2017).

"Navy experts in the technology and researchers at University of Texas at Austin say there are certainly scenarios they can imagine in which GPS hacks could have been used to foil ships' navigations systems but emphasize there's no evidence such attacks took place in the case of the Navy collisions." (Weise E. , 2017) "The technology to jam or misdirect navigational software is readily available, though the Navy uses a much more robust encrypted version of GPS that would be very difficult to disrupt." (Weise E. , 2017)

The only way to spoof such a system is a *record and replay* attack, "where a recording is made of the encrypted location data being sent from GPS satellites to the naval ship. Replaying the recording at a slightly later time could fool a ship into thinking it is someplace else. This is a very sophisticated and difficult hack that requires multiple recordings of the navigation data stream from multiple angles, and then sending the recorded signal from two or more locations." (Weise E. , 2017) "To ensure that nearby ships do not also get the false data, it would have to be transmitted from close to the Navy ship being targeted, perhaps using multiple drones." (Weise E. , 2017)

However, according to "Professor David Lust, former president of the Royal Institute for Navigation in the United Kingdom, "it takes two to Tango…. I" think you just have to attack the weakest of the pair, which

is the commercial vessel." Commandeering the GPS of the cargo ship to get it to veer off course could cause collision, and it is a much easier hack." (Humphreys, 2009)

The Case for a Cyber Weapon

There appears to be valid evidence to support the theory that at least two of the U.S. Navy Warships, USS John McCain and the USS Fitzgerald AND/OR the commercial vessels involved were the on the wrong end of a Cyber-Weapon and were receiving incorrect GPS generated positional information. In agreement with Dr. Lust's conclusions, the Cyber Weapon may have been deployed by an adversary's UAS off a small nearby vessel. The author believes that the subject Cyber-Weapon is an advanced modular entity that can spoof the GPS signals received by all vessels in its range. J.S. Warner & R.G. Johnson established in 2013 that the cyber-security of many common automated navigational systems today lacks basic cyber-attack protection; vessels using incorrect data will make wrong decisions in terms of navigation and emergency responses, leading to potential collisions and deaths (Warner &Johnson, 2013).

Surfacing Questions

*Spoofing i*s generation of false transmissions masquerading as P(Y) [the encrypted] Precise Signal that makes up the military vessel positioning basis, or unencrypted C/A [Civilian Acquisition] code from GPS satellites. In a virtual world tracking invalid data streams or non-integrity- based data is difficult, especially on three dimensional vessels moving in time. However, there may be more than one method to spoof a signal no matter how well it is encrypted. The cargo ships involved could have received unencrypted GPS ranging; a much less complex method than is required for military vessels.

Both ships do not need to be disabled or spoofed. All ships (military, commercial, recreational, specialized service) in international waters require detailed positional information. GPS systems accurately supply a 3-D position, velocity and time fix in all types of weather, 24 hours a day.
GPS satellite signals are ranging devices that deliver two signals made up of a civilian carrier, C/A code, NAV message, P-Code, and a military carrier. See Figure 16-11 (Balduzzi, et al 2014)

Figure 16-11 GPS Signals

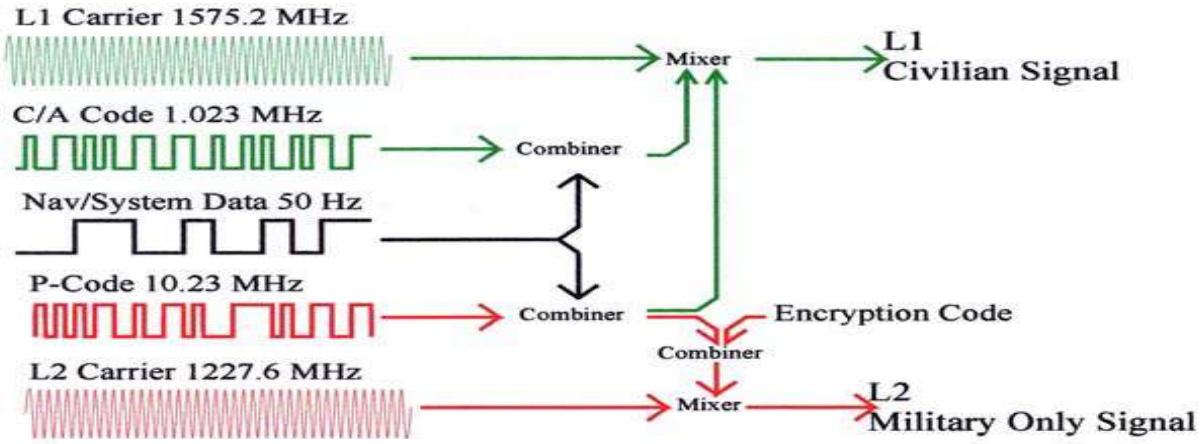


FIGURE 16-47: LEGACY GPS SIGNAL STRUCTURE

Source: Balduzzi, M. W. (2014). A Security Evaluation of AIS. Retrieved from Trend Micro. https://www.acsac.org/2014/program-final/oc_multifile/3/62.pdf

Delivered GPS signals also include a 50 Hz NAV message that is combined and ultimately mixed with the two codes to form the Civilian and Military Signals sent to the multiple radar and GPS receivers on both the Navy and Civilian vessels. Subframe 4 of the NAV message has a flag that tells the receiver that the P code is encrypted into the P(Y) code, thereby protecting the military signal. The Civilian signal has no such flag. Spoofing the civilian signal would be as simple as switching off the flag to make both the civilian and military components of the L1/L2 GPS signals unencrypted. If an adversary controls the signal the vessels are receiving, then the false position calculated by their receivers will be wrong regardless of encryption algorithms, military security enhancements or communication protocols used. Another spoofing method would overpower the real signal with a false one, then lock on and maintain access.

Because of cost, most systems on commercial vessels have legacy GPS systems. In the author's view, even if the GPS signals of the military vessels were not hacked the unencrypted C/A - L1 Civilian signal may have been. *It is also provable that this spoof is technically feasible* on the legacy systems. Experiments by Warner and Johnston out of Los Alamos, and surveys by Schmidt, et al out of Queensland University clearly support the GPS/GNSS Cyberattack threat vector. (Warner, 2013) In 2013, Humphreys and his students successfully spoofed an $80MM Yacht's GPS system. (Humphreys, 2009)

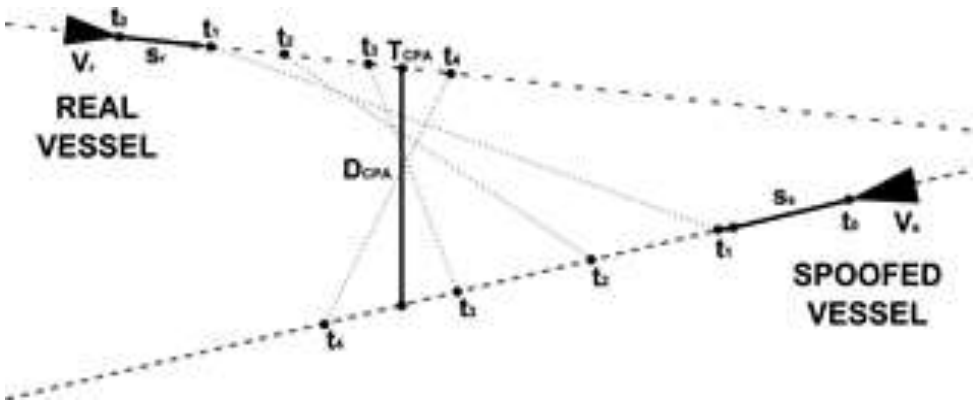
What the physical damage indicates for the USS McCain and USS Fitzgerald is that both naval vessels appear to have collided on the starboard side. This leads to the theory that the Civilian vessels involved in crossing or approaching the US Naval vessels were relying on faulty information for their position. Further, the cyber weapon may have been delivered by small UAS from a nearby fishing or recreational vessel. It would be a perfect delivery vehicle: stealth, quiet, low radar signature, requiring only 1- 25 watts signal spoofing power. Since the true GPS signal strength reaching the surface of the Earth is about -

160dBw (1x 10**-16 Watts), a 1-Watt GPS jamming spoof signal can over-ride C/A code acquisition for more than 620 miles (Line of Sight (LOS) to horizon.) (Warner, 2013)

Closest Point of Approach (CPA) Spoofing

"Collision avoidance is one of the primary objectives of using long range Automated Identification Systems (AIS), especially in open sea where port authority monitoring does not occur. CPA works by computing the minimal distance between two ships, at least one of which is in motion. CPA can be configured to trigger an alert (e.g., visually on the captain's console or acoustically via a siren) when a possible collision is detected so the ship can change course or speed or both." (Warner, 2013)

Figure 16-12 CPA Algorithm



Source: (Balduzzi, 2014) Balduzzi, M. W. (2014). A Security Evaluation of AIS. Retrieved from Trend Micro https://www.acsac.org/2014/program-final/oc_multifile/3/62.pdf

"The CPA algorithm shown in Figure 16-12 allows ship captains to compute time and distance remaining before they collide with another ship, if the vessels are traveling at fixed speeds and courses. A CPA alarm is triggered if one of the two parameters is lower than the transponder's configured thresholds. **T*CPA*** refers to the amount of time left before reaching the CPA point, **D*CPA*** refers to the distance between the vessels before they reach the CPA point, ***w(ti)*** refers to the distance between the vessels at a certain time ***(ti),* and *Sr* and *Ss*** are the vessels' vectors." (Balduzzi, 2014) "***CPA spoofing involves faking a possible collision with a target ship***. This will trigger a CPA alert, which could lead the target off course to hit another vessel." (Balduzzi, 2014)

The question arises, what if the civilian vessel was given a **false position at [X0, Y0, T0; X1, Y1, T2] distance (range)** directly below the true point of collision (offset DCPA,) that the commercial vessel would receive [Z0), Z1 assumed negligible]? According to Warner, this range difference could be 2000 ft. or approximately 1/3 of an Nm! That is an enormous potential navigation error considering that normal legacy GPS signal is off only 9-15 feet at 95% RMS. See Figure 16-13.

Figure 16-13 CPA Algorithm Details

$$\begin{cases} T_{CPA} = \dfrac{-W(t_i)(S_T - S_S)}{|S_T - S_S|^2} \\ D_{CPA} = |W(t_i) + T_{CPA}(S_T - S_S)| \end{cases}$$

Source: Balduzzi, M. W. (2014). A Security Evaluation of AIS. Retrieved from Trend Micro. https://www.acsac.org/2014/program-final/oc_multifile/3/62.pdf

The starboard side collisions suggest that one of the vessels may have turned port or that the commercial ship tried to avoid a fake collision target received by turning starboard at the wrong time. The USS Fitzgerald report confirms this observation. These are huge vessels. Turning, stopping or reversing course on a dime are not possible. Decisions must be made well in advance of potential collision alerts. This is also why delivery of a cyber-weapon by UAS is so attractive. It would be a small bird *in the glasses* while attention was directed to the huge targets closing in on each other. In the chaos, the adversary wins.

How could be the GPS chaos to US Vessels be achieved?

The author believes, that for the spoofing GPS signal theory [targeting a commercial vessel by cyber weapon to give it a false position and potentially cause collision to itself or another vessel], to be possible. It would require an enemy Unmanned Aircraft System (UAS) to be launched from either a sea-based vessel or land-based intelligence station in the Spratly Islands. The methodology contemplated consists of three cyber-attack activities:

1) Breaking the existing AIS GPS commercial vessel 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.

The problem is interesting because there are two three-dimensional maritime targets moving in time based on inaccurate or false ranging (GPS position) signals. The clocks used in GPS satellite systems are extremely accurate and present synchronization difficulties with the target naval / commercial vessel receivers. If it is possible to simulate and spoof the GPS signals to the commercial vessel using AIS collision avoidance systems (Cyber-weapon CONOP), then it is also possible that the US Navy may not have given proper attention to the non – personnel issues in their accident investigations.

Further, the possible delivery of such a Cyber-Weapon by close range UAS means that adversaries may have increased their knowledge management and understanding of U.S. Navy defensive systems. Using asymmetric warfare tactics and attacking the commercial traffic, which deploys legacy and cheaper GPS receivers, forces dependence on faulty information. Unfortunately, it is an effective tactic that bypasses much of the military modernization of GPS signals and satellites. This same possibility could affect military and commercial aircraft also, especially at airports where traffic speeds are reduced, and aircraft are closer to each other.

Discussion Questions

Consider the Signal Spoofing theory supra as the only Discussion Question for Chapter 16. Would the methodology work?

Bibliography

Balduzzi, M. W. (2014). *A Security Evaluation of AIS.* Retrieved from Trend Micro: https://www.acsac.org/2014/program-final/oc_multifile/3/62.pdf

Humphreys, T. e. (2009, January 1). *Assessing the Spoofing Threat: Development of a Portable Civilian GPS Spoofer.* Retrieved from Cornell University: https://gps.mae.cornell.edu/humphreys_etal_iongnss2008.pdf, Cornell University

Warner, J. &. (2013). *A Simple Demonstration That the Global Positioning System (GPS) is Vulnerable to Spoofing.* Retrieved from Journal of Security Administration: https://pdfs.semanticscholar.org/8ddb/89f56dd3e2ae265047822bc47cfb06815d9a.pdf, LAUR-03-6163

Weise, E. (2017, August 23). *could-hackers-behind-u-s-navy-collisions.* Retrieved from USATODAY: https://www.ruidosonews.com/story/tech/news/2017/08/23/could-hackers-behind-u-s-navy-collisions/594107001/

Readings

Adamy, D. (2001) *EW 101 A First Course in Electronic Warfare*, Boston: Artech House.

Adamy, D. (2004) *EW 102 A Second Course in Electronic Warfare*, Boston: Artech House.

Adamy, D. (2009) *EW 103 Tactical Battlefield Communications Electronic Warfare*, Boston: Artech House.

Adamy, D. (2015) *EW 104 EW against a New Generation of Threats*, Boston: Artech House.

Anonymous, (2017) *GPS/SBAS Signal Generator, GSS4100,* Spirent Communications Data Sheet.
Satellite AIS, Exact Earth, Ltd.

Anonymous, (8/22/2017*) Nationwide Automatic Identification System*, www.navgen.uscg.gov

Anonymous, (8/22/2017*) Long Range Identification and Tracking (LRIT) Overview*, www.navgen.uscg.gov

Anonymous, (8/22/2017*) How AIS Works*, www.navgen.uscg.gov

Anonymous, (2015) *Satellite AIS,* Exact Earth, Ltd.

Anonymous, (6/21/2015) *Cyber Threats against the Aviation Industry,* in SCADA on April8, 2014, INFOSEC Institute.

Anonymous, (2012) *A Guide for Testers of GPS Devices and Systems*, spectracom, Test & Measurement technical Note, TN15-101A – What You Want to know about GPS.

Anonymous, (5/14/2012) *what is a GPS Simulator*? spectracom, Test & Measurement White Paper, WP08-101A.

Anonymous, (1/10/2014) GPS Signal Plan, Navipedia, http://www.navipedia.net/index.php/GPS_Signal_Plan

Anonymous, (4/2017) Counter-Unmanned Aircraft System Techniques, HQ, Department of the Army, https://fas.org/irp/doddir/army/atp3-01-81.pdf

Barker, B.C Capt., et.al. (2006) *Overview of the GPS M-Code Signal*, MITRE Report.

Barnes, T (7 June 2018) China Tests army of tiny drone ships that can 'shark swarm' enemies during sea battles. Independent. Retrieved 07072018 from https://www.independent.co.uk/news/world/asia/china-drone-ships-unmanned-test-video-military-south-sea-shark-swarm-a8387626.html.

Bay-Yen, J. (2000) Chapter 5: GPS C/A Code Signal Structure, Fundamentals of Global Positioning System Receivers: A Software Approach, New York: John Wiley, http://read.pudn.com/downloads85/ebook/326017/Fundamentals%20of%20Global%20Positioning%20System%20Receivers/booktext05.pdf

Buesne, G & DeSanto, D. (2017*) GNSS Receivers and the Cyber-Threat: Lessons from the Information Security Community*, Spirent Communications, Baltimore, MD

Buesne, G & Holbrow, M. (6/29/2017*) GNSS Threats, Attacks and Simulations,* Spirent: PNT Advisory Board, Baltimore, MD

Chachak, E. (retrieved 9/1/2017) U.S. Naval Mishaps – Human Error or Cyber Malfeasance?

Corr, a. (2018) Great Powers, Grand Strategies: The New Game in the South China Sea. Naval Institute Press Annapolis.

Crosby, J. (12/16/2017) *here's What USNS Bowditch Does*, Inverse Innovation, https://www.inverse.com/article/25346-usns-bowditch-underwater-drone-stolen-china

CyberDB.https://www.cyberdb.co/u-s-naval-mishaps-human-error-or-cyber-malfeasance/

Department of the US Navy, Office of Chief of Naval Operations: (29 November 2017) Report on the USS Lake Champlain Collision (https://www.documentcloud.org/documents/4316708-171129-USS-Lake-Champlain-Collision-Report.html

DoD Report: https://www.defense.gov/portals/1/documents/pubs/2015_china_military_Power_report.pdf

Easton, R.D. & Frazier, E.F. (2013) *GPS Declassified: From Smart Bombs to Smartphones*, University of Nebraska Press.

Editor, (8/31/2017) GPS Block IIIA, Wikipedia, https://en.wikipedia.org/wiki/GPS_Block_IIIA

FCC Wireless Telecommunications Bureau, Marine VHF Radio Channels, per 47 CFR 80.371© and 80.373(f)

Fessenden, F. & Watkins, D. (6/18/2017) *the Path of the Container Ship that Struck a U.S. Destroyer*, NYT. https://www.nytimes.com/interactive/2017/06/18/world/asia/path-ship-hit-uss-fitzgerald.html?mcubz=3

Haider, Z. & Khalid, S. (8/2016) *Survey on Effective GPS Spoofing Countermeasures*, 6th International Conference on Innovative Computing Technology (INTECH 2016), https://www.researchgate.net/publication/313543601_Survey_on_effective_GPS_spoofing_countermeasures

Heath, T. (5/7/2015) How to Hack a Military Drone Parts I & II, Technology-Hackers, www.cybersecurityintelligence.com/blog/

Hodge, H. (8/23/2017) *why are Navy Ships colliding in the Pacific? Experts Weigh In*, Military.com

Huang, P. (23 May 2018) US Disinvites China from International Naval Exercise in Response to South China Sea Aggression. The Epoch Times. Retrieved from: https://www.theepochtimes.com/us-disinvites-china-from-international-naval-exercise-in-response-to-south-china-sea-aggression_2535152.html

Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing, Submitted to the Subcommittee on Oversight., Investigations, and Management of the House Committee on Homeland Security.

Kao, Lee, Chang, and Ko. (2007) A Fuzzy Logic Method for Collision Avoidance in Vessel Traffic Service, *Journal of Navigation*, 60,17-31.

Katoch, P.C, Gen (4 July 2018) New Chinese Drones – formidable challenge. SPSMAI. Retrieved from: https://spsmai.com/experts-speak/?id=556&q=new-chinese-drones-formidable-challenge

LaGrone, S. (8/21/2017*) Chain of Events Involving U.S Navy Warships in the Western Pacific Raise Readiness, Training Questions*, USNI News

LaGrone, S. (1/31/2017*) Cruiser USS Antietam Runs Aground in Tokyo Bay*, Spills Oil, USNI News.

Lehman, C.F. (29 August 2017) Report: China Increasing Drone Operations in Disputed Seas, Freebeacon. Retrieved from http://freebeacon.com/author/charles-lehman

Lin, J & Singer, P.W. (4 June 2014) Not a Shark, But a Robot: Chinese University Tests Long-Range Unmanned Sub. Popular Science. Retrieved from: https://www.popsci.com/blog-network/easter-arsenal/not-shark-robot-chinese-university-tests-long-range-unmanned-mini-sub#page-3

McCaslin, I.B. (2017) Red Drones over Disputed Seas: A Field Guide to Chinese UAVs/ UCAVs Operating in the Disputed East and South China Seas. Released by Project 2049 Institute at http://project2049.net/documents/Red%20Drones%20over%20disputed%20seas_PLA_project2049.pdf

Navy Information Office (11/1/2017) Navy Releases Collision Report for USS Fitzgerald and USS John S McCain Collisions Story Number: NNS171101-07Release Date: 11/1/2017 9:01:00 AM

Navy Information Office (11/2/2017) Navy Releases Results of the Comprehensive Review of Surface Force Incidents Story Number: NNS171102-06Release Date: 11/2/2017 12:22:00 PM

News Correspondent, (8/22/2017) *USS McCain crash is 4th Navy Accident in Pacific this Year*, The Washington Post, AP.

News Correspondent, (8/31/2017) *DDG 51 Arleigh Burke Class Destroyer*, Military.com

News Correspondent, (8/21/2017) *CNO Orders Operational Pause, Review After Latest Ship Collision*, Military.com

News Correspondent, (8/21/2017) *10 Sailors Missing, 5 injured after Destroyer Collides with Tanker*, Military.com

News Correspondent, (8/22/2017) *Remains of Navy Sailors found on USS John S McCain*, Military.com

News Correspondent, (8/17/2017) *Navy Fires Commander, XO from USS Fitzgerald for Fatal Collision*, Military.com

News Correspondent, (7/21/2017) *Investigation Faults Navy in Fitzgerald Collision Report*, Military.com

News Correspondent, (6/20/2017) *Stories of Fitzgerald Sailors Killed in Destroyer – Container Ship Crash*, Military.com

News Correspondent, (6/16/2017) US Navy Destroyer Collides with Japanese Merchant Ship, Military.com

News Correspondent, (5/09/2017) *US Navy Ship Collides with South Korean Fishing Boat*, Military.com

News Correspondent, (1/31/2017) *Oil Spill in Tokyo Bay After Navy Cruiser Runs Aground*, Military.com

Nichols, R.K & Carter, C. (4 May 2018) RSCAD Presentation of Research to KSUP Faculty on Deployment of Chinese Cyber-weapons and GPS spoofing of Naval Vessels

Nichols, R.K (8/31/2017) *Stand By for a whole slew of military short articles on the Navy Collisions (my students only),* Private memo to COT799 & CMST 455.

Nichols, R.K. & Lekkas, P.L. (2002) *Wireless Security: Threats, Models, Solutions*, New York, McGraw Hill.

Olson, W. (August 30, 2017) *Adm No Evidence of Hacking in McCain Fitzgerald Collisions* pdf. Stars and Stripes.

Ranganathan, A, et.al, *SPREE A Spoofing Resistant GPS Receiver*, Department of Computer Science, ETH Zurich, Switzerland, Zurich Information Security and Privacy Center.

Richardson, J. Adm., (8/31/2017) *No Evidence of Hacking in McCain and Fitzgerald Collisions*, Military.com

Schallhorn, K., (9/1/2017) US Military crashes, collisions in the Pacific, FoxNews. http://www.foxnews.com/us/2017/08/28/us-military-crashes-collisions-in-pacific.html

Schmidt, D. et.al., (5/2016) *A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures*, ACM Computing Surveys, Vol 48, No 4, Article 64

Shouts, M. (3 July 2018) Science blog. https://mikeshouts.com/chinas-dove-surveillance-drone/

Sickle, J.V. (8/25/2017) *GEOG 862 GPS and GNSS for Geospatial Professionals*, Lessons 1-10 complete, Penn State University, College of Earth and Mineral Sciences https://www.e-education.psu.edu/geog862/node/1407 [Superb Course on the subject]

Staff (6 Jul 2018) Chinese navy deploys drones in South China Seas missile drills. Diplomacy and Defense article. https://www.scmp.com/news/china/diplomacy-defence/article/2150957/chinese-navy-deploys-drones-south-china-sea-missile/

Staff writer. (6 July 2018), China starts work on world's biggest test site for drone ships near South China Sea. Today. Retrieved from: https://www.todayonline.com/world/china-starts-work-worlds-biggest-test-site-drone-ships-gateway-south-china-sea.

Staff (June 2018) Crisis Watch. Retrieved from map overlay, https://www.crisisgroup.org/crisiswatch

Sterling, J. 8/21/2017) *A Spate of US Navy warship accidents in Asia since January*, CNNNEWS. http://www.cnn.com/2017/08/21/politics/navy-ships-accidents/index.html

YouTube Gongji GJ-1 UAV, https://www.youtube.com/watch?v=0QCNQfqkgDY

Volpe, J.A, (8/29/2001) *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System, Final Report*, Office of Assistant Secretary for Transportation Policy, U.S. Department of Transportation, John A Volpe Transportation Systems Center.

Warner, J.S. & Johnson, R.G. (2003) *GPS Spoofing Countermeasures*, *Journal of Security Administration*, LAUR-03-2384, Los Alamos, NM: Los Alamos National Laboratory

Weise, E. (8/23/2017) *Could Hackers Be Behind the U.S. Navy Collisions*? USATODAY.

Wikipedia, S-100. Images, https://en.wikipedia.org/wiki/Schiebel_Camcopter_S-100,Retrieved 08082018.

Wikipedia, ASN-209, https://en.wikipedia.org/wiki/Aisheng_ASN-209, retrieved 08082018

Wikipedia, BZK-005, https://en.wikipedia.org/wiki/Harbin_BZK-005, retrieved 08082018

Patents

Berry, R. & Cook, C. (2016) *Detection of wireless data jamming and spoofing*, US 9466881 B1