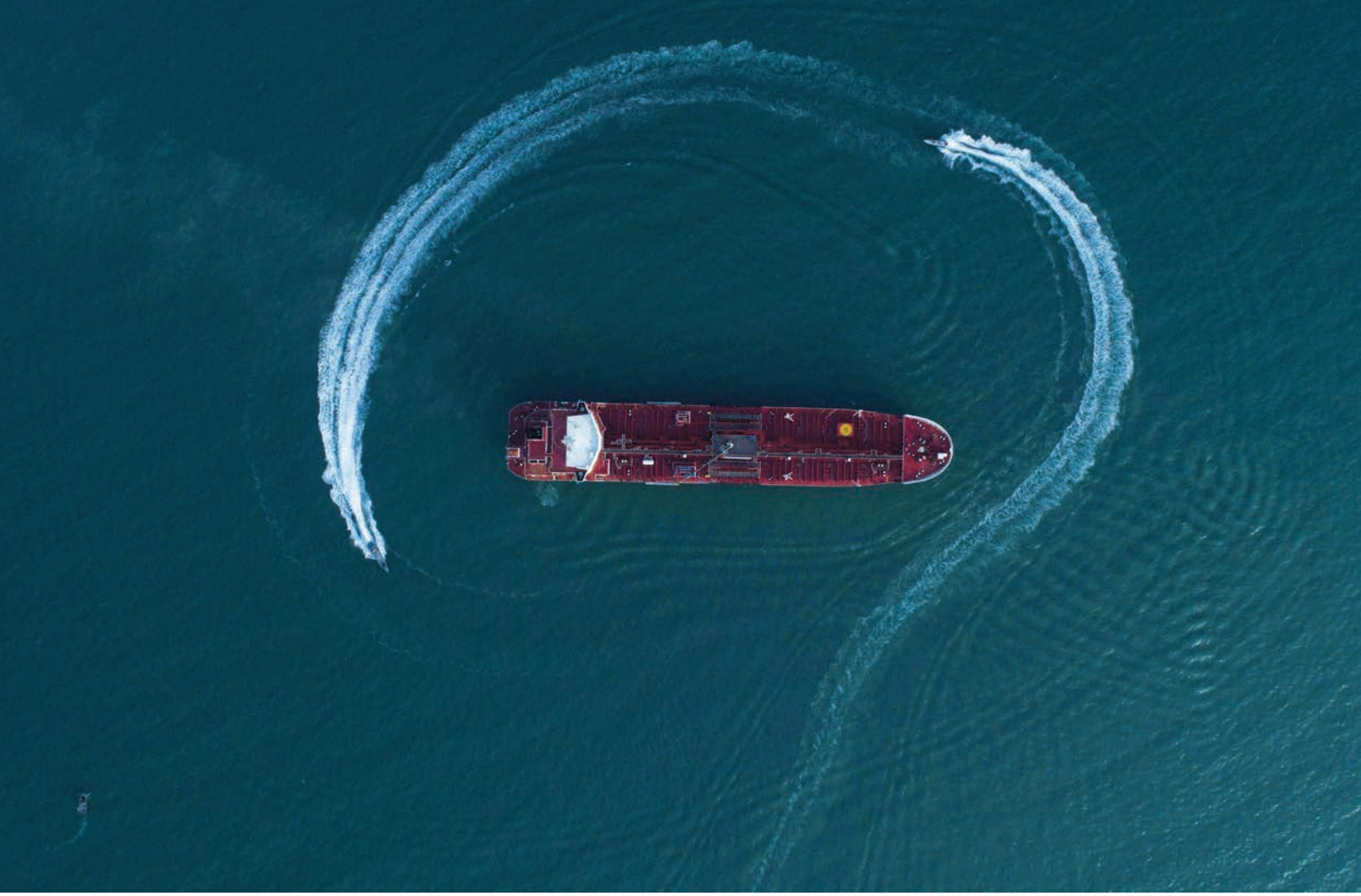


Speedboats of Iran's Islamic Revolutionary Guard Corps surround British oil tanker *Stena Impero*, in Strait of Hormuz, July 19, 2019 (Imago/Alamy)

Position, Navigation, and Timing Weaponization in the Maritime Domain

Orientation in the Era of Great Systems Conflict

By Diane M. Zorri and Gary C. Kessler

Diane M. Zorri is an Assistant Professor of Security Studies at Embry-Riddle Aeronautical University and serves as a Nonresident Fellow in the Modern War Institute at West Point and Joint Special Operations University. Gary C. Kessler, CISSP, is a Nonresident Senior Fellow in the Cyber Statecraft Initiative at the Atlantic Council. He is President of Gary Kessler Associates, a consulting, research, and training company located in Ormond Beach, Florida, and a Principal Consultant at Fathom5, a maritime digital services company headquartered in Austin, Texas.

Deception, confusion, and targeting of weak points in modern warfare is as ubiquitous now as it was in the wars of antiquity.[1] Likewise, the incongruity between perception and reality has been explored for cen-

turies. Understanding what is real is still a challenge for humankind. How does the human learn to "see" through the fog of deception? With the mind's ability to emphatically alter perceptions, modern society has become increasingly reliant on technology. Yet even technology can be deceptive, and, as Sun Tzu observed, "all warfare is based on deception."[2]

Strategists have long recognized that naval superiority and control of maritime assets are paramount in establishing global influence.[3] Alfred Thayer Mahan noted that although navies have an essential utility in safeguarding global trade and communications, a small naval force could overwhelm a much larger one by concentrating efforts on its adversary's key vulnerabilities. Consequently, when a country's maritime assets come under attack, it may have far-reaching geopolitical, military, and economic implications. The sinking of the USS *Maine* (1898) and RMS *Lusitania* (1915), as well as the attacks on the USS *Maddox* and USS *Turner Joy* (1964), precipitated major conflicts and sustained military campaigns. While the U.S. Navy remains the largest and most expeditionary force in the world, smaller forces, malign powers, and irregular adversaries are disrupting maritime transit and naval assets using new and innovative techniques. These techniques often involve a "system of systems" approach, where malign actors confront adversaries through critical components of operational systems.[4] Two of the most persistent threats to maritime security and superiority in the great systems conflicts of the 21st century stem from vulnerabilities in two of the technologies that enable position information, navigation, timing, and situational awareness: the Global Positioning System (GPS) and the Automatic Identification System (AIS).[5]

The maritime domain is often overlooked in its criticality to U.S. national security. Ninety percent of U.S. import and export trade is via ship, and the Maritime Transportation System (MTS) contributes $5.4 trillion to the national economy, representing about 25 percent of the U.S. national gross domestic product (GDP). The MTS is an expansive network of navigable channels, ports, locks, marine terminals, marinas, and seaways that facilitates this trade. Like the MTS but on a global scale, the global maritime transportation network (GMTN)—an arrangement of seaports, waterways, ports, and terminals that accounts for over 70 percent of the value of global trade and nearly 90 percent of its volume—facilitates the global economy. These systems are complex and interdependent, and much like other facets of critical infrastructure, their constituent parts are often undervalued in terms of being integral components of the global economy and strategic security.[6] It is no exaggeration to suggest that the MTS is integral to our food, energy, financial, and national security, as well as our projection of military power around the globe.[7]

GPS

The world's MTS relies on the four major global navigation satellite systems (GNSS)—BeiDou (China), Galileo (European Union), GLONASS (Russia), and GPS (United States)—for navigation, routing, and situational awareness at sea. A GNSS provides position, navigation, and timing (PNT) services that are used not only for land-, sea-, and air-based navigation but also for the precision timing necessary for critical infrastructures. The importance of timing cannot be overemphasized; if GPS timing signals fail or are severely impaired, there will be widespread failure of telecommunications, financial services, transportation, and power distribution networks, to name just a few.

GPS can offer positioning information accurate to within 3 feet of a receiver's actual location.[8] While such precision might not be necessary on the high seas (so-called blue water), accurate PNT is essential in littoral zones (brown water) and while traversing narrow chokepoints and critical nodes such as the Strait of Hormuz, Strait of Malacca, Panama Canal, Bosporus Strait, and Suez Canal.[9] GPS is widely recognized as the best GNSS in the world in terms of accuracy, precision, and reliability and, for this reason, is the most widely used system in the world.[10] GPS, however, suffers from three vulnerabilities: jamming, spoofing, and total system failure.

Jamming refers to a receiver being unable to detect a legitimate GPS signal due to interference from nearby radio transmissions. A GPS signal is transmitted from a satellite—at an altitude of 12,550 miles—at approximately 50 watts of power. The signal arrives at the Earth's surface, however, at a fraction of a milliwatt. Thus, a malign actor may broadcast signals on the GPS frequencies at even a few watts of power and overwhelm the ability of a receiver to acquire necessary PNT information from the GPS signal.[11]

GPS jamming is not a new phenomenon. While initially developed for the military, inexpensive GPS jammers have been available to the public—albeit illegal to use—for well over a decade. One of the earliest widely publicized examples of this activity involved a person fined in 2013 for using a GPS jammer in the proximity of Newark Liberty International Airport and interfering with flight operations. Rampant GPS jamming activities are taking place around the world, most notably at airports, with Norway being particularly affected. Moreover, China, North Korea, and Russia each have long histories of efforts to jam or otherwise neutralize the GNSS of other countries.[12]

GPS *spoofing* causes a receiver to report its location at one place when it is in another place. In 2012, a team from the University of Texas at Austin first demonstrated spoofing to the Department of Homeland Security by spoofing GPS signals to a drone, causing it to lose awareness of its proper altitude. In June 2013, the same team was able to spoof the location of the *White Rose of Drachs*, an $80 million, 213-foot superyacht, causing it to change course in the middle of the Mediterranean Sea.[13] GPS spoofing is not limited to laboratory conditions. The first large-scale public case of GPS spoofing in the MTS was in June 2017. M/V *Atria* was anchored in the Black Sea off the Russian port of Novorossiysk, but its GPS reported its location as Gelendzhik Airport, 20 nautical miles away. The 37.5-ton tanker was not alone; the receivers on at least two

dozen other vessels placed them in the same location.[14]

The *Atria* incident was neither an isolated event nor even the first such spoofing incident.[15] In 2019, the Center for Advanced Defense Studies released a report describing nearly 9,900 incidents of GPS spoofing incidents in the Black Sea, Crimea, the Russian Federation, Syria, and other locations as far back as 2016, all linked to the Russian military.[16] In 2020, investigative journalists reported that a German research vessel detected GPS spoofing and jamming events in many sites on its worldwide voyage in 2017 and 2018.[17]

Destruction of the entire GPS system is, of course, the ultimate vulnerability. GPS employs a constellation of more than 32 satellites, 29 of which are in use at any one time—a minimum of 24 are required for the system to operate. By design, GPS is resilient to "natural" failures; if one satellite suffers a failure, it is moved out of position and a replacement takes over. Yet Russia and China have both demonstrated "satellite killer" capability, and, since the spring of 2021, Russian President Vladimir Putin has repeatedly threatened to shoot down many, or all, GPS satellites.[18] GPS has no resiliency against such a systemic failure.

The vulnerabilities of and threats to GPS are not merely issues for the maritime community but affect all aspects of modern society. There is not a concentrated effort to supplement or augment GPS in the near term. While GPS is managed by the U.S. Space Force, it is both a military and a civilian asset, so something bigger than a military solution is required.[19] The Russian invasion of Ukraine in February 2022 highlighted both the necessity of an assured PNT system and the requirement for augmentation.[20]

AIS

GPS and other GNSS facilitate the Automatic Identification System, the global system used by ships and maritime authorities to maintain situational awareness of local vessel traffic. AIS data, as aggregated by several sites worldwide, has evolved to provide a historical log of a ship's movement over time. AIS is important for tracking shipping routes, basic industry intelligence, and awareness about shipping in general. AIS was designed in the 1990s, primarily in response to the oil spill that followed the grounding of *Exxon Valdez* in 1989. Required in the 2002 Safety of Life at Sea (SOLAS) Convention, AIS has several well-known security vulnerabilities, including the lack of sender authentication, message timestamps, data validity verification, and data content integrity. Although all large U.S. military vessels have AIS transceivers, most transceivers are not broadcasting most of the time because of the warship exemption in the SOLAS requirements.[21]

One early example of a combination of GPS and AIS spoofing is the Iranian seizure of the United Kingdom (UK)–flagged tanker *Stena Impero*. Steaming through the Strait of Hormuz in international waters in July 2019, *Stena Impero* suddenly turned north and entered Iranian territorial waters, where it was promptly seized by patrol boats of the Iranian navy. This incident was likely in retaliation for the British seizure of an Iranian vessel earlier in the year due to suspected violations of European Union sanctions.[22]

The episodes of spoofing continued and morphed into more powerful displays of disruption. In July 2019, the U.S.-flagged M/V *Manukai* reported a series of false GPS and AIS readings at the Port of Shanghai.[23] Unlike previous spoofing events that made a vessel believe that it was in the wrong place, the *Manukai* saw target vessels that appeared to be jumping around. Further analysis of many events that occurred in the area made it appear that the spoofed locations appeared in circles.[24] Dubbed "crop circles," similar spoofing was found in other locations, including Tehran. In all these cases, the vessels were in the proximity of the spoofing. Later analysis showed circle spoofing occurring around Point Reyes (just north of San Francisco), where the spoofed vessels were as far as 10,000 miles away from the area.[25]

The Port of Shanghai and subsequent circle spoofing incidents have escalated from spoofing vessels within the proximity of the spoofer to where ships can be anywhere on the globe relative to the spoofed location. China is one of the chief suspects in these circle spoofing events. They have long been suspected of AIS spoofing to hide their fishing fleets that are involved in illegal, unreported, or unregulated (IUU) fishing by showing them to be hundreds or thousands of miles away from their actual locations.

These episodes of AIS spoofing have been perpetrated for many purposes, including demonstrations of capability; masking IUU fishing, smuggling, and other illegal activities; and identity laundering to avoid detection, sanctions, or inspections.[26] Widespread spoofing of warships, however, represents an even more dangerous level of escalation, exacerbated by the fact that warships do not always routinely broadcast AIS information. As an example, AIS data showed the HMS *Queen Elizabeth* and five escort vessels steaming toward the Irish Sea in September 2020, while contemporaneous satellite imagery showed an empty ocean in their supposed location. In fact, not only were the six vessels not where their AIS track put them, but they were not even together at the time—and likely not even actually broadcasting AIS messages.[27]

In this context—and that of subsequent events in the area—the AIS spoofing of North Atlantic Treaty Organization (NATO) vessels in the Black Sea in June 2021 takes on an entirely different significance. Prior to a scheduled exercise late that month, two NATO warships, HMS *Defender* (UK) and HNLMS *Evertsen* (the Netherlands), arrived in Odesa (Ukraine) on the afternoon of June 18. AIS tracking data showed both ships traveling directly to Sevastopol (Crimea) later that night, positioned within 2 nautical miles of the port housing the Russian Black Sea fleet command. YouTube video, live webcam, and other evidence, however, showed that neither vessel left its dock. Because of the contested sovereignty of Crimea and the presence of the headquarters of the Russian Black Sea Fleet in Sevastopol, the unannounced approach of NATO vessels into what Russia claims are its territorial waters could well be described as an act of provocation.[28] Indeed, AIS tracks showed

the USS *Ross* near Crimea about 10 days later, although live webcams showed it at dock in Odesa.[29]

The 2021 Black Sea incident was part of a much larger pattern of the spoofing of AIS tracks of warships from many nations over the last several years.[30] (As a demonstration of the ease with which AIS spoofing can be accomplished, one of the authors of this article showed the spoofed track of Russian guided-missile cruiser *Moskva* entering Port Canaveral on the east coast of Florida [see figure 1] at DEFCON's Hack the Ship Village in August 2021.[31])

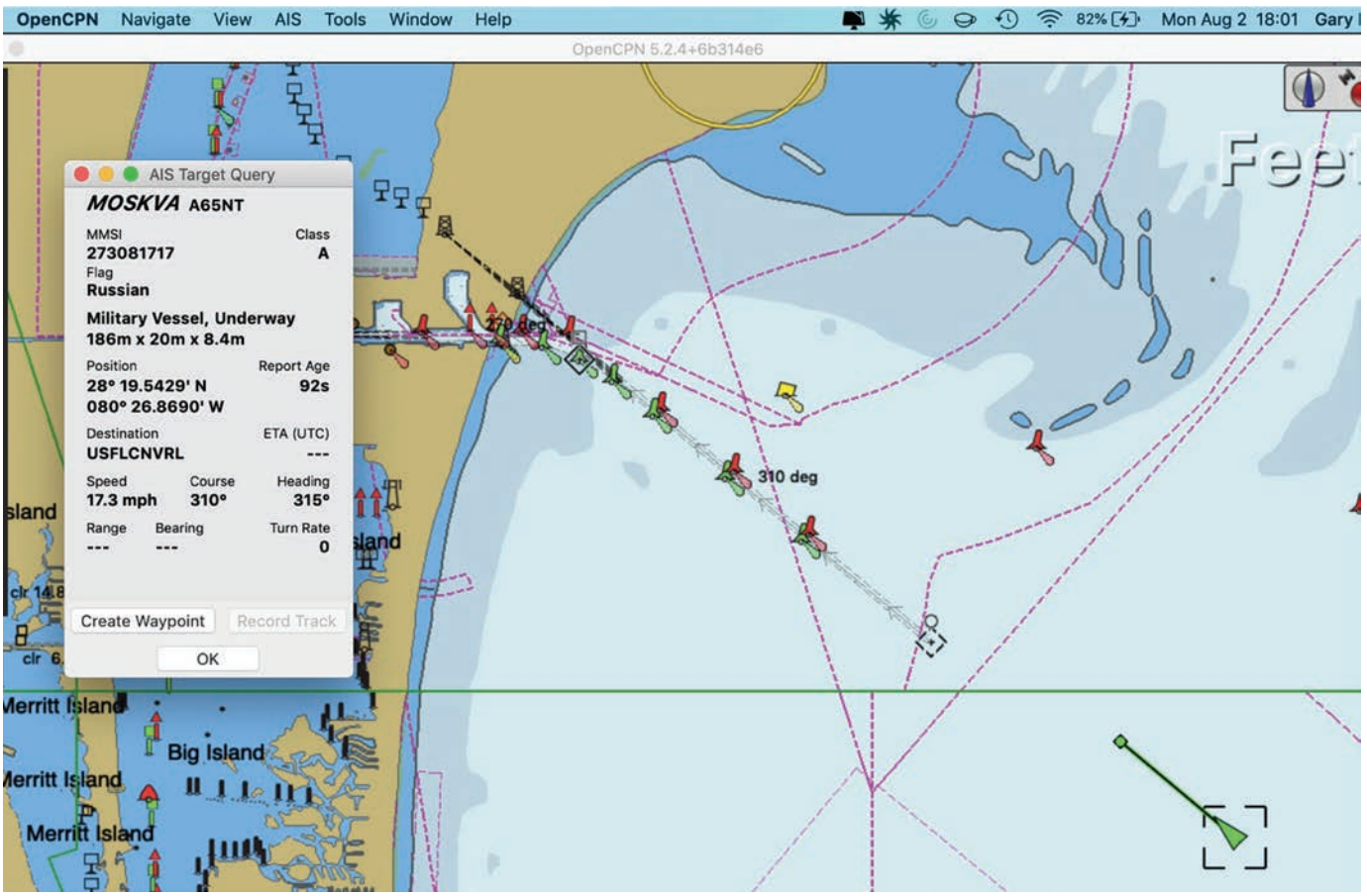
Geopolitical Risks and Implications

Historical Parallels. The 2021 Black Sea incident appears to be the pre-staging of history. The most likely source of the spoofing of NATO vessels is Russia, which was able to engage in saber-rattling rhetoric in the aftermath of the events. Although most of the world understood that the tracks were bogus, the Russian people likely believed the evidence of NATO aggression. From Putin's standpoint, his domestic audience—not the rest of the world—is the only audience that needs to be convinced of anything.

It is uncertain whether the spoof of the NATO vessels was a test of capability or if it was intended as a pretext to war. If it was the latter, it would not be the first time that false electronic signals at sea have provided a rationale for armed conflict. Consider the object lesson of the Gulf of Tonkin incidents. On August 2, 1964, the USS *Maddox* came under attack by three North Vietnamese patrol boats. At the end of the skirmish, all the attacking patrol boats had been damaged, 10 North Vietnamese sailors were killed or wounded, and one bullet hole was found in the *Maddox*. This was the first Gulf of Tonkin incident. Two days later, the *Maddox* and USS *Turner Joy* detected approaching North Vietnamese patrol boats on radar. Seeing what they thought were torpedo tracks on radar and sonar, the vessels fired on the patrol boats, even though neither ship nor any U.S. naval aircraft made visual contact with the attackers.[32] This was the second Gulf of Tonkin incident, and the precipitating rationale for Congress to pass the Gulf of Tonkin Resolution, escalating the mission of U.S. forces in Vietnam.[33]

The second Gulf of Tonkin incident, however, never occurred. While there might well have been vessels around the radar's report, there were no attacking patrol boats, and there were no torpedoes. Misinterpreted and conflicting signals intelligence from both radar and sonar caused a response when there was, in fact, no stimulus. Yet in a rush to judgment—one that was politically popular and seemed to be consistent with enemy actions of just 2 days earlier—the signals intelligence (SIGINT) was not scrutinized, and contradictions

Figure. Spoofed AIS Track of *Moskva* Near Port Canaveral, Florida, August 2021



Ships from Standing NATO Maritime Group 2, including Italian Navy ITS *Alpino*, USS *Harry S. Truman*, and USS *Cole*, sail in formation in Mediterranean Sea, July 24, 2022 (U.S. Navy/Crayton Agnew)

that were known at the time were not investigated.[34] An attack—whether real or imagined—was consistent with the narrative and political winds of the day.

Implications and Countermeasures. There is great danger when the warships of rival nations come into proximity to one another. When operators can deliberately alter SIGINT and navigation signals to skew the truth—or the perception of the truth—the space is even more dangerous; intentional disruptions to these systems are provocative and have far-reaching consequences. Disrupting GPS and other GNSS creates navigational uncertainty, delays, and inefficiency in the supply chain. The disruptions can also cause accidents in littoral and near-coastal waters, narrow straits, and international chokepoints where ships operate with a small margin for error. False AIS tracks can support virulent narratives, countering the interests of U.S. allies and partners. Moreover, adversaries can spoof AIS to masquerade as a much larger force or change a ship's navigation history. While cyber attacks have not yet invoked a collective defense response or triggered Article

5 of the NATO treaty, the second- and third-order effects of these disturbances are incalculable.[35] Moreover, during each incident the U.S. Navy must quickly recognize the threats, orient its decisionmaking, and decide a response.

Given the ease of spoofing GPS and AIS signals, we are in a particularly dangerous environment. Any adversary government—whether China, Iran, North Korea, Russia, or others—could easily enter entirely fake tracks of vessel movements into the historical record, in real time. Although some might debate whether attacks on GPS and AIS are *cyber* in their nature, those arguments miss the point. The term *cybersecurity* is a misnomer; what we must focus on is protecting the confidentiality, integrity, availability, authenticity, utility, and possession of information and other necessary data.[36] From that perspective, attacks on GPS and AIS clearly affect multiple characteristics of navigational and situational awareness information.

Maritime cybersecurity is particularly pertinent today given Russia's invasion

Sailors assigned to USS *Zumwalt* participate in simulated ship transit while attending Bridge Resource Management course at Navigation, Seamanship, and Shiphandling Trainer on Naval Base San Diego, March 10, 2023 (U.S. Navy/Kevin C. Leitner)

of Ukraine. Ostensibly, one of Russia's pretexts for the war is the encroachment of NATO on Russia's borders.[37] Part of the demonstration of Alliance aggression could well be the spoofing of NATO vessels in June 2021. There is also significant evidence that Russia is using attacks on GPS in the war against Ukraine, targeting aerial, artillery, and other military systems, as well as communications systems (many of which rely on GNSS for timing).[38] Reportedly, Russian jamming has at times been so intense that it has interfered with Russia's own systems. When it comes to navigation, Russia has access to the Chayka terrestrial electronic navigation system as a backup to GLONASS and other GNSS.[39]

Now, most of the GPS jamming/spoofing mitigation strategies are short-term improvisations. Many commercial GNSS receivers, for example, can detect when an incoming signal on the primary constellation appears to be bogus. In some cases, the receiver can switch to an alternate GNSS constellation. There is, however, no backup available or augmentation capability in place for GPS. Prior to the widespread availability and use of GPS, the United States and international maritime community relied on the Long-Range Navigation (LORAN) terrestrial-based navigation system. The Department of Homeland Security decommissioned LORAN in 2010, leaving no maritime backup to GPS.[40] Indeed, today many mariners do not know how to use LORAN devices or understand LORAN markings on a chart. In 2018, the Trump administration mandated that the Secretary of Transportation establish a backup to GPS via a terrestrial-based timing system,[41] yet no work has commenced on the proposed replacement system, enhanced LORAN (known as eLORAN).[42] Another potential alternative to satellite-based position, navigation, and timing is the use of quantum sensors for positioning, yet researchers have not fully realized this capability. Likewise, while there have been several proposals to secure AIS, the international standards bodies have not been consistent in their planning or execution.[43]

Conclusion

The jamming and spoofing of GPS and AIS information has escalated in the last half-dozen years from simple demonstrations of capability to truly dangerous situations where misperceptions could ignite a major conflict. The attack surface is becoming increasingly ubiquitous and strikes on military assets can be staged via nonmilitary vectors.[44] The U.S. defense community can mitigate the vulnerabilities in its

systems in several ways. First, training and awareness can make both military and commercial mariners aware of the frailties of the systems. Maritime operators and bridge officers should have knowledge of the information and operational technology systems aboard their ships and the myriad ways in which they are interconnected and how they interact. Information security–aware officers as well as shipboard detection systems should be integrated into maritime personnel and management systems. Navigation and bridge personnel must be able to determine when the information displayed by the automated systems is suspect and must have independent means of validating those systems. In addition, celestial navigation techniques and the science of inertial and hyperbolic systems need to be integrated into the curricula of maritime practitioners. Furthermore, maritime naval exercises need to include scenarios where GNSS and AIS have been disrupted by enemy forces and test how practitioners would respond without current technology. Exercises should also integrate opportunities that test the innovative capacity of cyber defenders as well as their ability to proactively target the enemy.

Next, lawmakers and funding agencies must be convinced that if the vulnerabilities in GPS and AIS are not addressed in the near term, the threat to national security is plausible and potentially cataclysmic. This onus lies on all PNT stakeholders, whether they are in the military, government, or commercial sector. Both the Chinese and the Russians use a terrestrial-based PNT system to augment their GNSS systems, giving them a significant strategic advantage over the United States.[45] Instead of recommending the short-term revival of LORAN as reserve capability, the National Space–based PNT Advisory Board has developed a strategy of toughening and modernizing the current GPS systems until non–GNSS PNT systems, like those that use quantum sensing, are widely available.[46] Another solution would be to integrate the National Aeronautics and Space Administration's Jet Propulsion Laboratory's Global Differential GPS (GDGPS) across the national security entities and critical infrastructure of the United States. GDGPS tracks data from all GNSS constellations and offers corrections and real-time accuracy for positioning applications.[47] Yet no single entity within the U.S. Government has been given the authority to fully implement a PNT augmentation capability or

U.S. Navy Quartermaster 3rd Class Hailey Pardo shoots sunlines with sextant aboard USS *Chung-Hoon*, Pacific Ocean, October 8, 2022 (U.S. Navy/Kenneth Lagadi)

oversee an integrated PNT strategy. The full integration of the GDGPS system across the national security architecture would require strategic guidance and funding. Moreover, to compete with China, which many experts have begun to recognize as a global leader in comprehensive PNT capability, the United States needs to adopt a long-range strategic plan for PNT at the national level.[48] This plan should recognize the criticality of PNT to national security and holistically work to improve all PNT capabilities (that is, low-orbit satellites, space-based satellites, terrestrial navigation, inertial navigation, quantum sensing, LORAN, and celestial navigation) as an integral system of systems.

Alternatively, AIS security solutions are highly likely to yield positive gains to commercial industries. Competitive bids for AIS systems should integrate security measures, such as public-key or asymmetric cryptography, digital signatures, or a combination of the identity-based authentication that is commonplace in commercial applications, computers, and on mobile phones.[49] Yet securing AIS might be an even harder problem to solve because it demands international agreement within two United Nations organizations—the International Maritime Organization is responsible for SOLAS and the International Telecommunication Union for the AIS over-the-air protocol.[50] Mitigating this challenge will require a clear vision and proactive leadership.

Because of the grave danger that GPS and AIS weaponization entails, it is essential that policymakers and maritime operators understand not only the risks and implications of these threats, but also the mitigation techniques and countermeasures that add resilience to the warfighter. Moreover, the U.S. Government needs to address the significant advantage that our adversaries have developed in PNT resilience and augmentation. The redundancies and security initiatives may be costly, yet both PNT resilience and augmentation and AIS security measures are vital for protecting our nation's critical assets and mitigating a future conflict. **JFQ**

The authors gratefully acknowledge the support of the Naval War College and feedback from our fellow participants at the War College's Cyber and Innovation Policy Institute 2022 Summer Workshop on Maritime Cybersecurity.

Notes

[1] Sun Tzu, *The Art of War* (New York: Simon & Schuster, 2004).

[2] Ibid.

[3] Alfred T. Mahan, *The Influence of Seapower Upon History, 1660–1783*, 12th ed. (Boston: Little, Brown and Company, 2004), 12–16.

[4] Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (Santa Monica, CA: RAND, 2018), https://www.rand.org/pubs/research_reports/RR1708.html.

[5] The term *great systems conflict* is attributed to Chris C. Demchak, "Achieving Systemic Resilience in a Great Systems Conflict Era: Coalescing Against Cyber, Pandemic, and Adversary Threats," *The Cyber Defense Review* 6, no. 2 (Spring 2021), https://cyberdefensereview.army.mil/Portals/6/Documents/2021_spring_cdr/05_Demchak-CDR_V6N2_Spring_2021.pdf?ver=fpA19JdBy-n6fRbxSh8paA%3D%3D.

[6] *Cyber Strategic Outlook: The United States Coast Guard's Vision to Protect and Operate in Cyberspace* (Washington, DC: U.S. Coast Guard, August 2021), https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf.

[7] David Alderson, Daniel Funk, and Ralucca Gera, "Analysis of the Global Maritime Transportation System as a Layered Network," *Journal of Transportation Security*, November 28, 2019, 1–35, https://calhoun.nps.edu/handle/10945/25530; Jason Ileto, "Cyber at Sea: Protecting Strategic Sealift in the Age of Strategic Competition," *Modern War Institute*, May 10, 2022, https://mwi.usma.edu/cyber-at-sea-protecting-strategic-sealift-in-the-age-of-strategic-competition/; Gary C. Kessler and Steven D. Shepard, *Maritime Cybersecurity: A Guide for Leaders and Managers*, 2nd ed. (Kindle Direct Publishing, September 2022), https://www.maritimecybersecuritybook.com/.

[8] Pratap Misra and Per Enge, *Global Positioning System: Signals, Measurements, and Performance*, rev. 2nd ed. (Lincoln, MA: Ganga-Jamuna Press, 2021).

[9] Gary C. Kessler and Diane M. Zorri, *Cross Domain IW Threats to SOF Maritime Missions: Implications for U.S. SOF* (MacDill Air Force Base, FL: Joint Special Operations University Press, 2021), https://commons.erau.edu/cgi/viewcontent.cgi?article=2765&context=publication.

[10] Bill Bostock, "Downed Russian Fighter Jets Are Being Found With Basic GPS 'Taped to the Dashboards,' UK Defense Minister Says," *Business Insider*, May 10, 2022, https://www.businessinsider.com/russia-su34-jets-basic-gps-receivers-taped-to-dashboards-uk-2022-5.

[11] Tom Nardi, "Teardown: Mini GPS Jammer," *Hackaday*, September 8, 2020, https://hackaday.com /2020/09/08/teardown-mini-gps-jammer/.

[12] Tegg Westbrook, "The Global Positioning System and Military Jamming: The Geographies of Electronic Warfare," *Journal of Strategic Security* 12, no. 2 (2019), 1–16, https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1720&context=jss.

[13] Mark L. Psiaki, Todd E. Humphreys, and Brian A. Stauffer, "Attackers Can Spoof Navigation Signals Without Our Knowledge. Here's How to Fight Back GPS Lies," *IEEE Spectrum* 53, no. 8 (August 2016), 26–53.

[14] Dana Goward, "Mass GPS Spoofing Attack in Black Sea?" *The Maritime Executive*, July 11, 2017, https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea.

[15] Westbrook, "The Global Positioning System and Military Jamming."

[16] "Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria," Center for Advanced Defense Studies (C4ADS), March 26, 2019, https://c4ads.org/reports/above-us-only-stars/.

[17] Katherine Dunn, "The Long Ocean Voyage That Helped Find the Flaws in GPS," *Fortune*, January 24, 2020, https://fortune.com/2020/01/24/gps-disruption-test-voyage/.

[18] Dana A. Goward and John Garamendi, "Putin Is Holding GPS Hostage. Here's How to Get It Back," *Defense News*, April 12, 2022, https://www.defensenews.com/opinion/2022/04/12/putin-is-holding-gps-hostage-heres-how-to-get-it-back/.

[19] Dana A. Goward, "Get the Bullseye Off GPS," *Space News*, April 19, 2022, https://spacenews.com/op-ed-get-the-bullseye-off-gps/.

[20] Olivier Chapuis, "En guerre en Ukraine, la Russie brouille la navigation par satellites et utilise le système Loran" [At war in Ukraine, Russia jams satellite navigation and uses the Loran system], *Voiles et Voiliers*, March 19, 2022, https://voilesetvoiliers.ouest-france.fr/equipement-entretien/electronique-embarquee/gps/en-guerre-en-ukraine-la-russie-brouille-la-navigation-par-satellites-et-utilise-le-systeme-loran-efd085fa-a6ac-11ec-969a-2a6df02632f3; Brian G. Chow and Brandon W. Kelley, "Russian Invasion of Ukraine Reinforces the Urgency of Fixing U.S. Satellite Vulnerability by 2027," *Space News*, March 8, 2022, https://spacenews.com /op-ed-russian-invasion-of-ukraine-reinforces-the-urgency-of-fixing-u-s-satellite-vulnerability-by-2027/.

[21] Kessler and Shepard, *Maritime Cybersecurity*.

[22] Michelle W. Bockmann, "Seized UK Tanker Likely 'Spoofed' by Iran," *Lloyd's List*, August 16, 2019, https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran.

[23] Mark Harris, "Phantom Warships Are Courting Chaos in Conflict Zones," *Wired*, July 29, 2021, https://www.wired.com/story/fake-warships-ais-signals-russia-crimea/.

[24] "Shanghai GPS Spoofing," video, 0:42, C4ADS, 2019, for download, https://drive.google.com/file/d/1dTWu7H9JjRyN0uQPZ9HwiUzCFd7cd5pL/view.

[25] Bjorn Bergman, "AIS Ship Tracking Data Shows False Vessel Tracks Circling Above Point Reyes, Near San Francisco," *Sky Truth*, May 26, 2020, https://skytruth.org/2020/05/ais-ship-tracking-data-shows-false-vessel-tracks-circling-above-point-reyes-near-san-francisco/.

[26] James R. Watson and A. John Woodill, "Anticipating Illegal Maritime Activities From Anomalous Multiscale Fleet Behaviors," *Arxiv*, October 15, 2019, https://arxiv.org/pdf/1910.05424.pdf.

[27] Harris, "Phantom Warships Are Courting Chaos in Conflict Zones."

[28] H.I. Sutton, "Positions of Two NATO Ships Were Falsified Near Russian Black Sea Naval Base," *USNI News*, June 21, 2021, https://news.usni.org/2021/06/21/positions-of-two-nato-ships-were-falsified-near-russian-black-sea-naval-base.

[29] Yoruk Isik, "And . . . All Fake Like HMS Defender Incident. USS Ross Is in Odesa's Cabotage Harbor!" *Twitter*, June 29, 2021, https://twitter.com/yorukisik/status/1409992626477191175.

[30] Harris, "Phantom Warships Are Courting Chaos in Conflict Zones."

[31] Gary C. Kessler, "AIS Spoof of a Warship," video, 2:13, August 22, 2021, https://www.garykessler.net/gck/202108_MOSKVA_spoof.mp4. The *Moskva* sunk in the Black Sea during the Russian invasion of Ukraine in April 2022. The DEFCON hacker convention regularly hosts mini-conferences titled "Hack the Sea" or "Hack the Village," where participants in the information and security community are invited to partake in experiential learning on how to protect cyber assets.

[32] Robert J. Hanyok, "Skunks, Bogies, Silent Hounds, and the Flying Fish: The Gulf of Tonkin Mystery, 2–4 August 1964," *Cryptologic Quarterly* 19/20 (Winter 2000/Spring 2001), 4–10, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB132/relea00012.pdf.

[33] Dale Andradé and Kenneth Conboy, "The Secret Side of the Tonkin Gulf Incident," *Naval History Magazine* 13, no. 4 (August 1999), https://www.usni.org/magazines/naval-history-magazine/1999/august/secret-side-tonkin-gulf-incident.

[34] Hanyok, "Skunks, Bogies, Silent Hounds, and the Flying Fish."

[35] Cassia Sari, "Cyberattacks Can Invoke NATO Defence Clause," *The Organization for World Peace*, April 25, 2022, https://theowp.org/cyberattacks-can-invoke-nato-defence-clause/.

[36] Donn B. Parker, "Toward a New Framework for Information Security?" in *Computer Security Handbook*, 6th ed., ed. Seymour Bosworth, Michel E. Kabay, and Eric Whyne (Hoboken, NJ: John Wiley & Sons, Inc., 2015).

[37] Michael Klipstein and Tinatin Japaridze, "Collective Cyber Defence and Attack: NATO's Article 5 After the Ukraine Conflict," *European Leadership Network*, May 16, 2022, https://www.europeanleadershipnetwork.org/commentary/collective-cyber-defence-and-attack-natos-article-5-after-the-ukraine-conflict/.

[38] Jake Thomas, "'They're Jamming Everything': Putin's Electronic Warfare Turns Tide of War," *Newsweek*, June 3, 2022, https://www.newsweek.com/theyre-jamming-everything-putins-electronic-warfare-turns-tide-war-1712784.

[39] Chapuis, "En guerre en Ukraine, la Russie brouille la navigation par satellites et utilise le système Loran."

[40] *Terminations, Reductions, and Savings: Budget of the U.S. Government, Fiscal Year 2010* (Washington, DC: Office of Management and Budget, 2009), https://www.govinfo.gov/content/pkg/BUDGET-2010-TRS/pdf/BUDGET-2010-TRS.pdf.

[41] *Frank Liobondo Coast Guard Authorization Act of 2018*, Public Law 115-282, 115th Cong., 2nd sess., December 4, 2018, https://www.congress.gov/115/plaws/publ282/PLAW-115publ282.pdf.

[42] Aaron Martin, "Senate Bill Would Require Establishment of Land-Based Alterative to GPS Satellite Timing Signals," *Homeland Preparedness News*, December 19, 2017, https://homelandprepnews.com/stories/25836-senate-bill-require-establishment-land-based-alternative-gps-satellite-timing-signals/; Athanasios K. Goudosis and Sokratis K. Katsikas, "Secure AIS with Identity-Based Authentication and Encryption," *TransNav* 14, no. 2 (June 2020), 287–298, http://dx.doi.org/10.12716/1001.14.02.03; Gary C. Kessler, "Protected AIS: A Demonstration of Capability Scheme to Provide Authentication and Message Integrity," *TransNav* 14, no. 2 (June 2020), 279–286, http://dx.doi.org/10.12716/1001.14.02.02; "PNT ExCom Backs eLoran as a Step to Full GPS Backup System," *Inside GNSS*, December 10, 2015, https://insidegnss.com/pnt-excom-backs-eloran-as-a-step-to-full-gps-backup-system/.

[43] Kessler and Shepard, *Maritime Cybersecurity*.

[44] Kessler and Zorri, "Cross Domain IW Threats to SOF Maritime Missions."

[45] Baorong Yan et al., "High-Accuracy Positioning Based on Pseudo-Ranges: Integrated Difference and Performance Analysis of the Loran System," *Sensors* 20, no. 16 (August 2020), 4436, https://doi.org/10.3390/s20164436; Dana Goward, "China Expanding Loran as GNSS Backup," *GPS World*, October 12, 2020, https://www.gpsworld.com/china-expanding-loran-as-gnss-backup/; Wenhe Yan et al., "An eLoran Signal Cycle Identification Method Based on Joint Time–Frequency Domain," *Remote Sensing* 14, no. 2 (January 2022), 250, https://doi.org/10.3390/rs14020250.

[46] Michael J. Biercuk and Richard Fontaine, "The Leap Into Quantum Technology: A Primer for National Security Professionals," *War on the Rocks*, November 17, 2017, https://warontherocks.com/2017/11/leap-quantum-technology-primer-national-security-professionals/.

[47] Christine Bonniksen, "Global Differential GPS (GDGPS) System Future," National Aeronautics and Space Administration, Space-Based Position Navigation and Timing National Advisory Board Meeting, July 1, 2020, https://www.gps.gov/governance/advisory/meetings/2020-07/bonniksen.pdf.

[48] Dana Goward, "China Leads World With Plan for 'Comprehensive' PNT," *GPS World*, November 14, 2019, https://www.gpsworld.com/china-leads-world-with-plan-for-comprehensive-pnt; David H. Millner, Stephen Maksim, and Marissa Huhmann, "BeiDou: China's GPS Challenger Takes Its Place on the World Stage," *Joint Force Quarterly* 105 (2nd Quarter 2022), 23–31, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2999161/beidou-chinas-gps-challenger-takes-its-place-on-the-world-stage/.

[49] Garath Wimpenny et al., "Securing the Automatic Identification System (AIS): Using Public Key Cryptography to Prevent Spoofing Whilst Retaining Backwards Compatibility," *Journal of Navigation* 75, no. 2 (2022), 333–345.

[50] Kessler and Shepard, *Maritime Cybersecurity*.