NMIO Technical Bulletin

National Maritime Intelligence-Integration Office

MARCH 2019 - VOL 13

Director NMIO View:
Rear Admiral Gene Price, USNR

It's a proud moment for me to present this year's NMIO Technical Bulletin, Volume XIII. The National Maritime Intelligence-Integration Office (NMIO) holds a vital role in ensuring U.S. organizations and international entities are safe and secure in the maritime environment. That obligation plays out in a variety of ways, none more important than in this communication.

I am honored to begin my service as the Director of the National Maritime Intelligence-Integration Office (NMIO) in time to present this year's NIMO Technical Bulletin, Volume XIII.

At the enterprise level, NMIO supports information-sharing across the Global Maritime Community of Interest (GMCOI). Specifically, through our Science and Technology effort, NMIO helps to identify new solutions and accelerate technology development to advance strategic, operational, and tactical decision making. The information found in this edition—certainly in the articles that focus on machine learning—is transforming business operations and government processes by using innovation to counter threats in maritime settings. The relevance of this information will continue to grow as a resource for achieving U.S. and international security objectives.

Before urging you to start turning the pages of this edition,; thanks to the authors and their sponsors for their work on futuristic themes that serve maritime security interests. Each article in this edition shows how solutions can be found to today's toughest maritime security challenges. The articles in this issue are already adding to the momentum associated with emerging scientific and technical capabilities in the maritime environment. Another source of momentum for scientific and technical ideas can be found each year when NMIO welcomes scholars and professionals from around the world to share their research and development ideas. This year the 2019 Global Maritime Forum will be held at the University of Liverpool, hosted by NMIO and our primary United Kingdom government partner, UK National Maritime Information Centre (UK-NMIC).

Given the complexity of the challenges facing the maritime intelligence community, please note not only these articles, but also a range of problem-solving activities associated with Global Maritime Forums. Whether by reading about the ground-breaking research highlighted in this volume, or by attending NMIO's annual GMF, your involvement is part of the growing field of maritime intelligence and security innovators.

As a student, policy-maker, researcher, or entrepreneur, what will your contribution be? Perhaps your role will be working with others to leverage advances in science and technology to solve emerging problems and safeguard the maritime environment.

With this lofty goal in mind, I know you will find Volume XIII of the NMIO Technical Bulletin as valuable as we at the National Maritime Intelligence-Integration Office do!

NMIO Technical Bulletin **Volume 13, April 2019**

Chief Science and Technology Advisor, NMIO: Mekisha Marshall

Editorial Support: Faith MacDonald

Email: nmios&t.fct@navy.mil

Production: ONI Media Services

Address: 4251 Suitland Road, Washington DC 20395

Correspondence: Science and Technology Team

Correspondence welcome: We welcome contributions from all Global Maritime Community of Interest stakeholders, both domestic and international. In submitting your article, please highlight who you are, what you are doing, why you are doing it, and the potential impacts of your work. Please limit your article to approximately three to five pages including graphics. Articles may be edited for space or clarity.

Cover Image: USS Abraham Lincoln in the Gulf of Alaska. (U.S. Navy photo)

Table of Contents

A SHORT HISTORY OF MARITIME INTELLIGENCE-INTEGRATION

Dr. Brian Holmes, Dean, Anthony G. Oettinger School of Science and Technology Intelligence, National Intelligence University

Introduction

Maritime Domain Awareness (MDA) and intelligence integration play an influential role at the National Intelligence University (NIU) through the historical composition of our faculty, academic leaders, and student research initiatives. The distinguished ADM Arleigh A. Burke served as the Chair of our first Board of Visitors from 1969-1971. At the time, the institution was called the Defense Intelligence School. Since 1963, eight active or retired navy officers have served as either Commandant or President of NIU and its predecessors. Mike McConnell (Vice Adm., USN Ret.), the second director of national intelligence (DNI), was a graduate of the National Defense Intelligence College, the immediate forerunner of NIU. More recently, the second Dean of the Anthony G Oettinger School of Science and Technology Intelligence with the NIU, began my career as a direct commission intelligence officer in the U.S. Navy reserves.

Figure 1. Admiral Arleigh A. Burke, USN

The Anthony G. Oettinger School of Science and Technology Intelligence

The first Master of Science and Technology Intelligence (MSTI) degree was awarded at NIU in 2012 at the July graduation, two years after the Anthony G. Oettinger School of Science and Technology Intelligence was chartered to address compelling technological issues facing the intelligence community. Several instructors hired into the School held experience or were eagerly engaged in maritime activities. This new faculty included a former navy cryptologist, a navy intelligence officer who also spent two years as a scientist at the Naval Research Laboratory (NRL) in Washington, DC, and a former researcher from the Space and Naval Warfare Systems Command (SPAWAR) in San Diego, CA. In 2013, a faculty member traveled to the Arctic as a member of a science team led by the U.S. Coast Guard Research and Development Center. Additional partners included the U.S. National Oceanic and Atmospheric Administration (NOAA), the U.S. Air Force, the Woods Hole Oceanographic Institution and the University of Alaska. The professor spent several weeks testing the national security implications of unmanned systems operating in extreme climates.

Just as importantly, the School gained graduate students from across the intelligence community, military services, and national security enterprise. These include several from the Office of Naval Intelligence (ONI), U.S. Navy, U.S. Marine Corps, and the U.S. Coast Guard. Many, based on the School's new mission, aggressively pursued unique research centered on the maritime-intelligence domain.

For example, in 2016, an intrepid student from the National Geospatial-Intelligence Agency (NGA) decided to work closely with her NIU thesis committee and engage scientists at the U.S. Naval Research Laboratory to conduct an experiment. She decided to study the environmental impact on the long wave infrared spectral signatures of automotive paints and coatings. Aspects of her work resulted not only in a published abstract submission, but her thesis won the prestigious Scientific and Technical Intelligence Committee award in recognition of a thesis that most significantly contributes to the advancement of science. The Scientific and Technical Intelligence Committee is a technical committee under the auspices of the National Intelligence Council (NIC). More recently, the School leveraged its faculty and student body to pursue unique technical research opportunities in the underwater domain. To effectively blend scientific and technical expertise with strategic relevance, outreach was required. On June 11, 2018, the National Intelligence University signed its first ever Education Partnership Agreement with Naval Surface Warfare Center Carderock Division. The intent was to stimulate student and faculty educational exchanges in the areas including, but not limited to, vessel technology, dynamics, detection, and experimentation. The immediate result was a student driven thesis focused on new detection techniques of under the waterline towable devices. The student, and a team of Carderock engineers, embarked on an experimental proof of concept using their David Taylor Model Basin. This impactful research served as a valuable precedent for cooperation between the two organizations and as a blueprint for how to integrate each other's missions in a synergistic manner.

Closing Thoughts

A few years ago, a junior officer in the Navy, and part-time student in the Oettinger School, completed his thesis research while serving aboard an assault ship as an intelligence officer. He realized during his off-hours that there was information he had ready access to from the campus consoles in Bethesda, MD, that he could not obtain, but needed while on his ship. The officer worked diligently with the Navy, and U.S. intelligence systems integrators, to solve an inherent information sharing issue effecting a significant portion of the fleet. This singular action had wide ranging, and incredibly positive implications for the maritime domain, and improving U.S. capabilities.

This is only a snapshot of how leaders and students at the National Intelligence University realized the incredible impact maritime awareness and intelligence integration has had in their evolutionary history, and continue to seek new models of curriculum and research integration to not only improve NIU's standing, but serve greater national security requirements.

About the Author

Dr. Brian Holmes is the Dean of the Anthony G. Oettinger School of Science and Technology Intelligence at the National Intelligence University in Bethesda, MD. The views expressed in this article are his alone and do not imply endorsement by the Defense Intelligence Agency, the Department of Defense, or the U.S. government. Dr. Holmes is an academic, a scientist, and a former intelligence officer in the U.S. Navy Reserve.

Figure 2. NIU Campus and seal

COMBATING ILLEGAL FISHING TO STRENGTHEN MARITIME SECURITY AND ENVIRONMENTAL SUSTAINABILITY

Robert S. Pomeroy, Professor, Department of Agricultural and Resource Economics, University of Connecticut, **John E. Parks,** Chief of Party, USAID Oceans and Fisheries Partnership, Thailand, **Gina Green**, Senior Associate, Tetra Tech

Increasing Fisheries Scarcity, Competition, and Conflict

Fishing is the largest extractive use of wildlife in the world. Fisheries products are the world's most widely traded foods, with commerce dominated by the developing countries. Fishing and fisheries-based commerce provide invaluable employment and cash income, create and grow local economies, and generate foreign exchange.

In Southeast Asia alone, over 250 million people rely on fish for at least 20% of their average per capita intake of animal protein. In some nations (e.g., Cambodia and Indonesia), fish comprises more than 50% of dietary animal protein intake (HLPE 2014). More than 200 million people in Southeast Asia rely on fisheries for their livelihood and income (Pomeroy 2013).

Despite the important role that fisheries play in maintaining the economies, livelihoods, and food security of many countries, increasing scientific evidence indicates that marine and coastal ecosystems around the world have been drastically altered during the past 50 years. These changes reduce their productivity, resilience, and potential to continue providing societal benefits in the future. Overfishing and declining fish populations in Southeast Asia are leading to increased levels of competition and conflict among fishers over remaining stocks, leading to decreased economic and food security, reduced environmental sustainability, and threats to peace and order (Pomeroy et al. 2016).

Evidence from foundational assessments (Pauly et al. 1998; Pauly et al. 2002; Myers and Worm 2003) indicate broad reductions in the size and value of fish caught, and the decimation of key, high-value fish species, particularly large predatory fish such as sharks and tuna. As larger, predatory fishery catches have declined, this has resulted in subsequent shifts to fishing for smaller and less-valuable species—a trend known as "fishing down the food web." In Southeast Asia, many fisheries have been fished down to only 5 to 15% of their original natural population levels.

Illegal, Unreported, and Unregulated Fishing in Southeast Asia

Illegal, unreported, and unregulated (IUU) fishing is one of the largest contributors to overfishing in Southeast Asia (Pomeroy et al. 2016; Pomeroy and Parks 2017). IUU fishing occurs when national or foreign fishers and vessels operate in violation of fishery laws relating to waters under jurisdiction of relevant State or international treaty obligations (FAO 2001). Types of IUU fishing include the use of unauthorized fishing methods and gears, fishing within prohibited areas or during restricted time periods, conducting unauthorized catch transshipment, and altering catch reporting and/or falsifying information.

A common example of IUU fishing occurs when overfishing and fisheries scarcity requires fishers to venture farther out beyond their traditional fishing grounds to meet catch requirements, including in

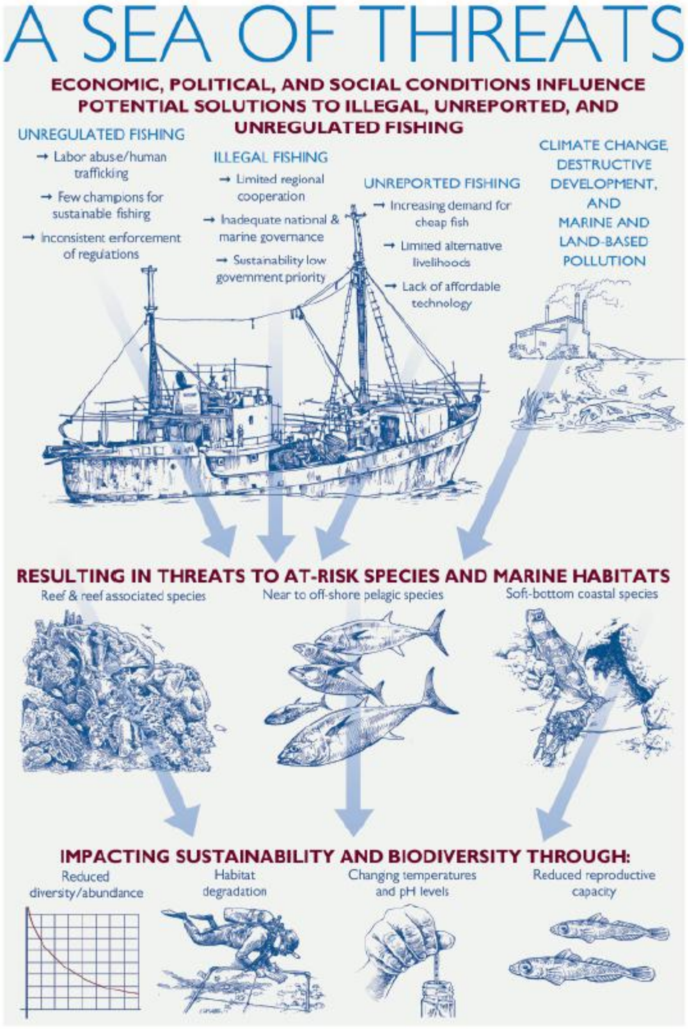

A SEA OF THREATS
ECONOMIC, POLITICAL, AND SOCIAL CONDITIONS INFLUENCE POTENTIAL SOLUTIONS TO ILLEGAL, UNREPORTED, AND UNREGULATED FISHING
UNREGULATED FISHING
→ Labor abuse/human trafficking
→ Few champions for sustainable fishing
→ Inconsistent enforcement of regulations
ILLEGAL FISHING
→ Limited regional cooperation
→ Inadequate national & marine governance
→ Sustainability low government priority
UNREPORTED FISHING
→ Increasing demand for cheap fish
→ Limited alternative livelihoods
→ Lack of affordable technology
CLIMATE CHANGE, DESTRUCTIVE DEVELOPMENT, AND MARINE AND LAND-BASED POLLUTION
RESULTING IN THREATS TO AT-RISK SPECIES AND MARINE HABITATS
Reef & reef associated species
Near to off-shore pelagic species
Soft-bottom coastal species
IMPACTING SUSTAINABILITY AND BIODIVERSITY THROUGH:
Reduced diversity/abundance
Habitat degradation
Changing temperatures and pH levels
Reduced reproductive capacity

Figure 1: A Sea of Threats

the waters of neighboring countries where they are not licensed to fish. Coupled with other negative effects from climate change, marine pollution, and coastal habitat destruction, IUU fishing can result in the decline of a country's marine populations and biological diversity, including various fish stocks and the marine habitats that they rely upon (see Figure 1). Recent studies suggest that a significant proportion of seafood products being imported into the U.S. are being illegally caught and/or mislabeled (Agnew et al. 2009).

In addition to its environmental effects, IUU fishing is also commonly linked to serious human welfare abuses, including slave labor, and represents a 'non-traditional' threat facing maritime security across Southeast Asia (Butcher 2004; Liss 2011; Williams 2013; Liss 2013). IUU fishing operations are known by law enforcement officials and fisheries managers in Southeast Asia to be associated with supporting insurgency, terrorism, and organized maritime crime, particularly piracy, kidnapping, and the illicit trafficking of narcotics, humans, and small arms. Maritime security threats are complex and interconnected, and although they may occur at sea, they are known to have extensive on-shore impact. In regions where there is ineffective governance at sea and insufficient capacity for monitoring, control, and surveillance (MCS), these threats can proliferate and lead to maritime insecurity (Pomeroy et al. 2016).

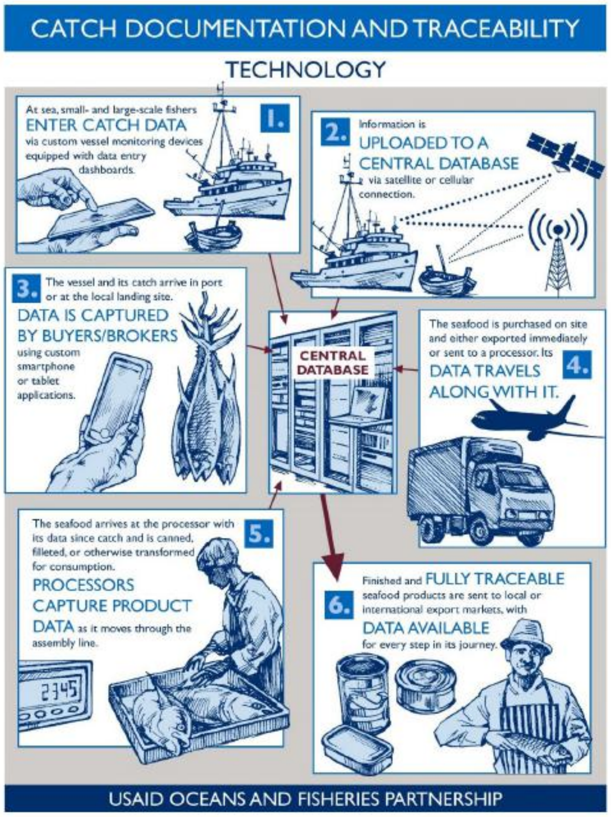
Electronic Catch Documentation and Traceability Systems

Recognizing that IUU fishing is a complex challenge facing the international community, governments and non-governmental organizations are increasingly looking to multi-national initiatives and regional policies. These approaches are designed to increase information exchange and promote collaborative efforts to combating IUU fishing within a specified area of waters (FAO 2001). Also, large seafood consuming nations, including the United States and European Union member countries, have developed new seafood import regulations that require the governments and/or private companies of exporting countries to provide verifiable documentation that their seafood products being imported are IUU-free, accurately labeled, and involve no forced labor (slavery) within their supply chain (Hosch and Blala 2017; Lewis and Boyle 2017).

Most recently, in 2018 the United States launched the Seafood Import Monitoring Program, joining the EU in requiring robust import documentation to verify product legality. To meet these requirements, exporting countries are increasingly using electronic catch documentation and traceability (eCDT) systems to collect real-time, accurate, and verifiable information at all points along the seafood supply chain, from point-of-catch through to landing, processing, transport, and export (USAID Oceans 2017a) (see Figure 2).

The data provided along the supply chain by eCDT systems can be used by the importing country to 'trace,' or follow, the verifiable information regarding seafood products "from bait to plate," all in an effort to detect and deter IUU products (USAID Oceans 2017b). Such eCDT systems are typically a combination of hardware and software installed and used onboard fishing vessels and on land, at port, in processing facilities, and within transportation systems. Using an eCDT system, relevant information about a seafood product can be documented digitally and transmitted in real time to online data exchange services via satellite, cellular, or radio frequency information communication technologies. When combined with strong port-state control measures to prevent the importation and sale of undocumented fish, the big data that are generated through eCDT systems can significantly limit the entry of IUU fish into the fishery supply chain, thereby reducing revenues to illegal operators while strengthening market access for those producers who are operating legally and 'traceably.'

The United States Agency for International Development (USAID) Oceans and Fisheries Partnership (USAID Oceans) is currently working to combat IUU fishing and seafood fraud throughout Southeast Asia by partnering with national and local governments, the fishing industry, and other private sector actors, regional organizations, and fishery


CATCH DOCUMENTATION AND TRACEABILITY

TECHNOLOGY

1. At sea, small- and large-scale fishers ENTER CATCH DATA via custom vessel monitoring devices equipped with data entry dashboards.

2. Information is UPLOADED TO A CENTRAL DATABASE via satellite or cellular connection.

3. The vessel and its catch arrive in port or at the local landing site. DATA IS CAPTURED BY BUYERS/BROKERS using custom smartphone or tablet applications.

4. The seafood is purchased on site and either exported immediately or sent to a processor. Its DATA TRAVELS ALONG WITH IT.

5. The seafood arrives at the processor with its data since catch and is canned, filleted, or otherwise transformed for consumption. PROCESSORS CAPTURE PRODUCT DATA as it moves through the assembly line.

6. Finished and FULLY TRACEABLE seafood products are sent to local or international export markets, with DATA AVAILABLE for every step in its journey.

USAID OCEANS AND FISHERIES PARTNERSHIP

Figure 2: Catch Documentation and Traceability

stakeholders to encourage their adoption and use of eCDT systems (USAID Oceans 2018). As of late 2018, project partners have deployed and are testing eCDT systems—including policies, hardware, and software—onboard both small and large-scale tuna fishing vessels, as well as at landing sites, tuna processing facilities, and throughout transportation systems. During 2019, USAID Oceans will support the analysis and decision-making use of eCDT data to help fishery managers in regional fisheries management organizations and in national and local government agencies to manage sustainable fish catch levels, improve their understanding of fish stock status, and strengthen real-time monitoring, control and surveillance (MCS) of fishing operations at sea. Furthermore, data captured will include insight into issues associated with human welfare (e.g., forced labor) and transnational crime.

Using eCDT Systems to Enhance Maritime Domain Awareness

Maritime Domain Awareness (MDA) is the effective understanding of events, behaviors, and dynamics within the maritime domain that do or could have security, safety, economic, and/or environmental impact on the associated domain area of responsibility (Department of Homeland Security 2005; IMO 2010; Sharda 2016). To be effective, a robust MDA capability requires real- or near-real time actionable intelligence triangulated from across inter-agency, regional governments, and private sector sources. The objective of MDA is to detect, prevent, and mitigate a range of threats in real- and near-real time, such as piracy, trafficking, and other forms of transnational criminal activity, based heavily on collecting, triangulating, fusing, analyzing, and acting on information from a wide variety of sources and systems.

Used effectively, a robust MDA capability can promote economic, social, and political security and stability across Southeast Asia and other regions around the world. At recent global conferences, including the 2018 Our Ocean Conference, maritime security has increasingly attracted private and public sector interest, as evidenced by large investments backing joint initiatives. Maritime security was one of the areas of action discussed at the conference, with its potential effect on national economic growth acknowledged and the requirement for sophisticated technological innovation (Our Ocean 2018).

Under the USAID Oceans project, eCDT systems being tested in Southeast Asia to combat IUU fishing could also be used to enhance broader MDA issues and strengthen national and regional maritime security. Big data generated in real time along all points of supply chain—from both large- and small-scale operations—could be used by national and regional security partners to enhance existing MDA initiatives, including through the collection and analysis of information relating to at-sea position, fishing activities, and vessel behavior, as well as legally documented and validated fishing crews (Figure 3). These capabilities also empower responsible large- and small-scale supply chain actors to verify their commitment to responsible, legal fishing practices.

For eCDT data to be used most effectively for MDA purposes, it must be interoperable and be able to be easily exchanged across various governmental information systems, including those that house port in/out documentation, catch certificates, fishing licenses and vessel registrations, crew manifests, and various law enforcement databases. Thus, an eCDT system extends into a wide range of mission critical sectors related to maritime security to address drivers of instability, extremism, crime, and violence. During 2018, USAID Oceans engaged with the Pacific Environmental Security Forum of the United States Indo-Pacific Command (INDOPACOM) and began preliminary discussions relating to how such eCDT data could be demonstrated with national-level security and defense partners to enhance regional MDA.

Conclusion

eCDT systems in Southeast Asia can generate accurate and verifiable data relating to fishing vessel behavior, operations, and position at sea in real time to combat IUU fishing, thereby strengthening existing methods of MCS while enhancing MDA. Looking ahead, when such systems become increasingly

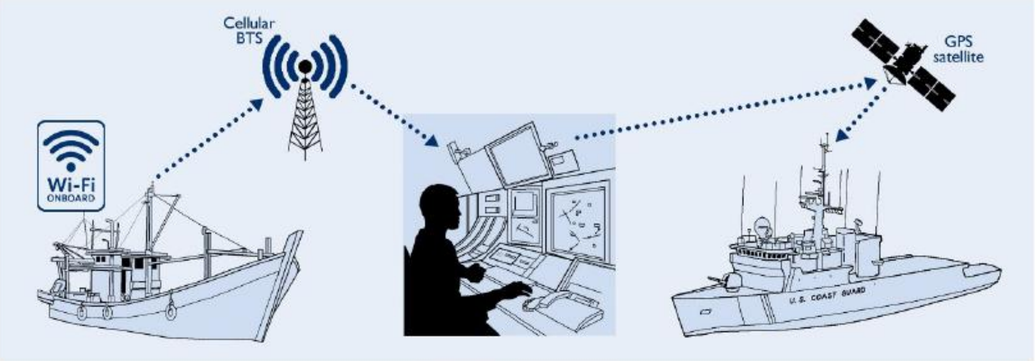


Figure 3: Wi-Fi

accepted and used, the capture of multiple types of real-time eCDT data across thousands of operators (e.g., licensed fishing companies) will generate sufficiently large data sets. Only through active machine learning with real-time, geospatial visualization tools can such data be effectively integrated, analyzed, and updated so as to provide accurate, real-time risk analysis to enhance MDA and enable defense and security priorities. With this in mind, machine learning and risk analysis of big eCDT data will become an invaluable tool used by security analysts and fisheries managers alike, in an adaptive and applied manner, at relevant scales of operations.

Not only can eCDT systems provide information on the position and behavior of fishing vessels at-sea and their crews, they also inform the status of threatened or endangered marine species and valuable fish stocks. Analysis of these big data will allow fishery managers to adaptively limit fisheries effort, restrict by-catch, and enforce the use of prohibited gear types within specified waters. Big data generated by these eCDT systems will be used not only to enhance MDA across and within ASEAN member countries, but also for the benefit of ASEAN defense allies such as the United States, through relevant regional interagency coordination and collaborative partnerships consistent with the aims of the U.S. National Strategy for Maritime Security.

Acknowledgements

This article received support from the United States Agency for International Development Regional Development Mission for Asia (USAID/RDMA) through Contract No. AID-486-C-15-00001. This publication does not necessarily represent the views of USAID or the United States Government.

References

HLPE. 2014. Sustainable fisheries and aquaculture for food security and nutrition. A report by the High-Level Panel of Experts on Food Security and Nutrition of the Committee on World Food Security, Rome

Pomeroy, R.S. 2013. Marine Fisheries in Crisis: Improving Fisheries Management in Southeast Asia. Chapter 5 in R. Hathaway and M. Mills (Eds) New Security Challenges in Asia. Woodrow Wilson Center Press, Washington, DC.

Pauly, D., V. Christensen, J. Dalsgaard, R. Froese, and F. Torres. 1998. Fishing down marine food webs. Science, 279:860–63.

Pauly, D., V. Christensen, S. Guanette, T.J. Pitcher, U. R. Sumaila, C.J. Walters, R. Watson, and D. Zeller. 2002. Towards sustainability in World Fisheries. Nature, 418:689–95.

Myers, R. A., and B. Worm. 2003. Rapid worldwide depletion of predatory fish communities. Nature 423:280–3.

Stobutzki, I., Silvestre, G. and Garces, L. Key issues in coastal fisheries in South and Southeast Asia, outcomes of a regional initiative. Fisheries Research 78, 109–118. 2006.

Robert Pomeroy, John Parks, Karina Lorenz Mrakovcich and Christopher LaMonica. 2016. Drivers and Impacts of Fisheries Scarcity, Competition, and Conflict on Maritime Security. Marine Policy. 67(May): 94-104.

Pomeroy, Robert and John Parks. 2017. Marine resource scarcity, fisheries conflict and maritime insecurity. Sustainable Security. Oxford Research Group, 25 September 2017.

FAO. 2001. International Plan of Action to prevent, deter and eliminate illegal, unreported and unregulated fishing. Rome, FAO. 24p.

Agnew, D. J., J. Pearce, G. Pramod, T. Peatman, R. Watson, J. R. Beddington, and T. J. Pitcher. 2009. Estimating the Worldwide Extent of Illegal Fishing. PLoS ONE 4(2):e4570.doi:10.1371/journal.pone.0004570.

Butcher, J.G. 2004. The Closing of the Frontier: A History of the Marine Fisheries of Southeast Asia c.1850–2000. Singapore: Institute of Southeast Asian Studies.

Liss, C. 2011. Oceans of crime: maritime piracy and transnational security in Southeast Asia and Bangladesh. Institute of Southeast Asian Studies, Singapore.

Williams, M. 2013. Will new multilateral arrangements help Southeast Asian states solve illegal fishing. Contemporary Southeast Asia. Vol. 35(2):258-83.

Liss, C. 2013. New actors and the state: addressing maritime security threats in Southeast Asia. Contemporary Southeast Asia. 35(2): 141-162.

Hosch, G. & Blaha, F. 2017. Seafood traceability for fisheries compliance – Country-level support for catch documentation schemes. FAO Fisheries and Aquaculture Technical Paper No. 619. Rome, Italy.

Lewis, S.G. and M. Boyle, 2017. The expanding role of traceability in seafood: tools and key initiatives. Journal of Food Science. 82:1. p. A13-A21.

USAID Oceans. 2017a. Fish Catch Documentation and Traceability in Southeast Asia: A Conceptual Overview. The USAID Oceans and Fisheries Partnership. United States Agency for International Development and Southeast Asian Fisheries Development Center. Bangkok, Thailand.

USAID Oceans. 2017b. Fish Catch Documentation and Traceability in Southeast Asia: Technical Concept and Specifications. The USAID Oceans and Fisheries Partnership. United States Agency for International Development and Southeast Asian Fisheries Development Center. Bangkok, Thailand.

USAID Oceans. 2018. https://www.seafdec-oceanspartnership.org/ Accessed on 31 October 2018.

Department of Homeland Security. 2005. National Plan to Achieve Maritime Domain Awareness for the National Plan for Maritime Security. Washington, DC.

International Maritime Organization. 2010. Amendments to the International Aeronautical and Maritime Search and Rescue (IAMSAR) Manual. Ref. T2-OSS/1.4. London, United Kingdom.

Sharda. 2016. A general overview of maritime domain awareness. https://www.marineinsight.com/maritime-law/a-general-overview-of-maritime-domain-awareness-mda/
Accessed on 31 October 2018.

Our Ocean. 2018. Press Release, Maritime Security: An Important Indicator for National Economic Growth. https://ourocean2018.org/assets/media/Maritime_Security_An_Important_Indicator_for_National_Economic_Growth.pdf Accessed on 9 November 2018.

MARCOS RESEARCH: MARITIME CUEING OF OPTICAL SATELLITES

Steven Pokotylo, Analyst/Project Manager, Project MarCOS, Royal Canadian Mounted Police
Marine Security Operations Centre (MSOC) West

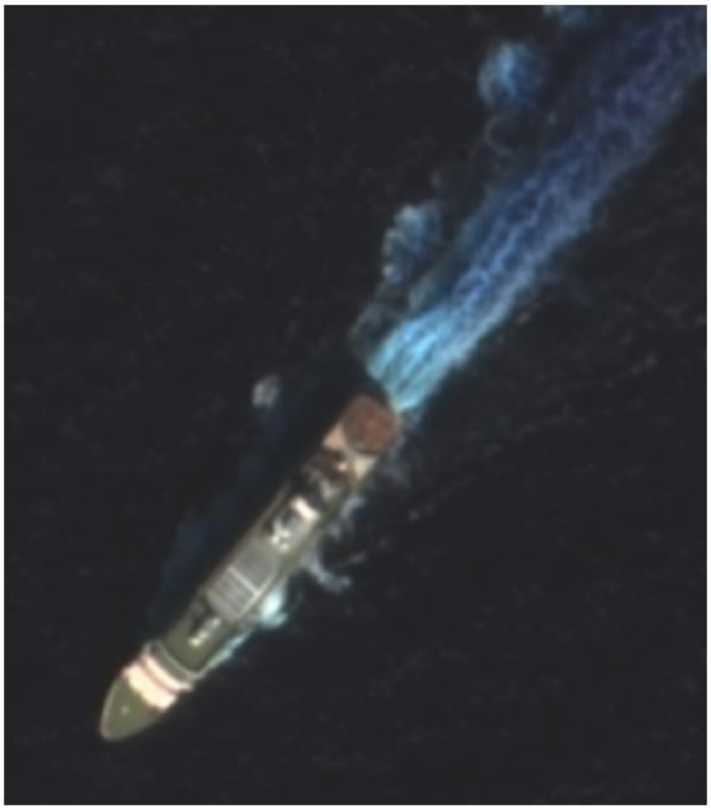


Figure 1: MS Rotterdam, North Atlantic, Aug 2018

Maritime Cueing of Optical Satellites (MarCOS) is a series of trials to rapidly cue commercial optical satellites to gather high-resolution images of vessels of interest (VOIs) underway at sea, as shown for example in Figure 1. This capability addresses an important gap in current space surveillance solutions — the need to identify "dark" contacts — and provides a foundation for future generations of maritime awareness assets.

MarCOS is funded by Defence Research and Development Canada's (DRDC) Canadian Safety and Security Program (CSSP). UrtheCast Vancouver is the prime contractor, developing tools, managing the trials, and interpreting the trial results. UrtheCast Spain provides satellite imaging through their Deimos-2 satellite. Royal Canadian Mounted Police (RCMP) 'E' Division at the Marine Security Operations Centre in Esquimalt British Columbia (BC) is the lead government agency, provides subject-matter expertise, and determines the satellite tasking in a non-operational context. All images in this article were collected by Deimos-2 under MarCOS.

Satellite-based synthetic aperture radar (SAR) systems such as Polar Epsilon (operating on RADARSAT-2) are the primary source of active wide-area ship detection for maritime regions beyond the range of shore-based radars. SAR delivers lists of detected "white dots" which, when fused with satellite-based Automatic Identification System (AIS), Long Range Identification and Tracking (LRIT), or Vessel Monitoring System (VMS), confirm the position, identification, and destination of almost all vessels in a surveillance zone. White dots that don't match AIS, LRIT, or VMS are "dark targets" until more information can be gleaned about them.

Maritime security operations centres have few good options for following up on dark targets. Government aircraft or vessels could be sent to get "eyes on," but for many countries and regional authorities the expense may be hard to justify until more is known about the contact.

Value of Optical Imagery

Optical satellites, at first glance, seem like an obvious dark-target solution: there are many optical satellites, they are typically not busy over the oceans, and they can provide classifying information such as size, shape, heading, and activity, as illustrated for example in Figure 2. In some cases, they provide the final piece of evidence to precisely identify a vessel.

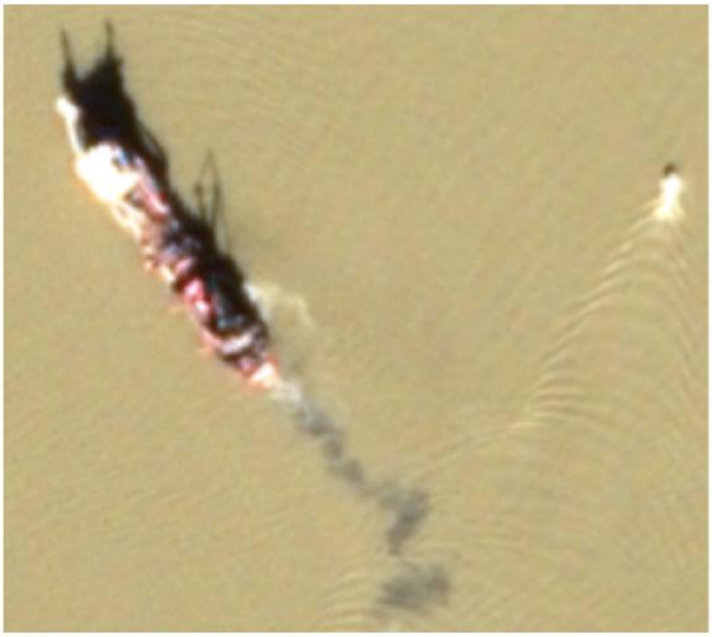


Figure 2: Dredge FRPD 309, Fraser River, Nov 2017 Rapid Tasking

There are avoidable and unavoidable limitations to using optical satellites against dark targets, however. The main unavoidable limitations are clouds and darkness – the satellite must be able to see the ship, and its vision is limited by available light. The primary avoidable limitation is the slowness of tasking cycles, and MarCOS has tackled this head-on.

Rapid Tasking has been one of the most important initiatives of the project. The Earth Observation industry primarily images landscapes, and commonly plans and tasks each satellite days ahead of time. Any time-pressure exerted on planning and tasking is perceived to introduce an element of risk for satellite safety and operations. However, unlike landscapes, ships are constantly moving, so day-long planning cycles do not work. MarCOS relies on a very rapid planning cycle. UrtheCast Spain achieved this on Deimos-2 using the "pinpointing" workflow shown in Figure 3 and summarized as follows:

- **Reserve the Satellite:** As soon as an acquisition seems probable, the client sends Deimos an approximate Area of Interest (AOI). Deimos identifies and reserves the available satellite and provides a timetable for pinpointing and imaging.
- **Pinpoint the Satellite:** About two hours before the last available uplink to the satellite, the client sends the exact scene center location (latitude/longitude) to Deimos.
- **Collect the Image:** Deimos collects the image, often less than one orbit after pinpointing.

This reduces the last-observation-to-imaging time delay, if satellite ground stations are accessible near the AOI, to as little as two hours.

Position Prediction

A dark target might travel more than 60 km in two hours, so MarCOS needs to predict where it will be at time of imaging. The prediction uncertainty must be better than the Deimos-2 image width of 12.5km.

Dark target position prediction works best when a track is available, for example from shore-based radar or other situational intelligence sources. Early MarCOS trials cued on non-dark targets, using AIS. The track speed and heading provided a solid foundation for estimating where the ship would be when the satellite arrived, but ships can (and did) change speed or heading unexpectedly. To mitigate this risk, MarCOS trials can request an acquisition that covers a longer swath, for example up to 4 scenes long (48 km x12 km). Using a tessellation mode can also mitigate the position prediction uncertainty, with some reduction in image resolution.

In seventeen trials over three seasons and three oceans, position prediction was successful 76% of the time.

Future Enhancements

The success of each MarCOS collection remains tightly dependent on the ability to reduce the time between the detection of a dark target and the collection of a high-resolution image. Time can be reduced in various ways, such as:

- **Engage more high-resolution assets:** Extend rapid tasking assets to include other optical satellites, for example through UrtheCast's membership in the Power Broker alliance of imaging satellites.
- **Expand the wide-area search:** Increase the number and variety of cueing sources. We are looking, for example, at cueing with wide-area medium-resolution optical missions such as UrtheDaily and we are already experimenting with data from the VIIRS satellite. Canada's new RADARSAT Constellation Mission is also expected to be an important asset.
- **Improve communications:** Extend the network of satellite ground stations able to uplink to the high-resolution satellites on short notice.
- **Do it all in space:** UrtheCast is developing

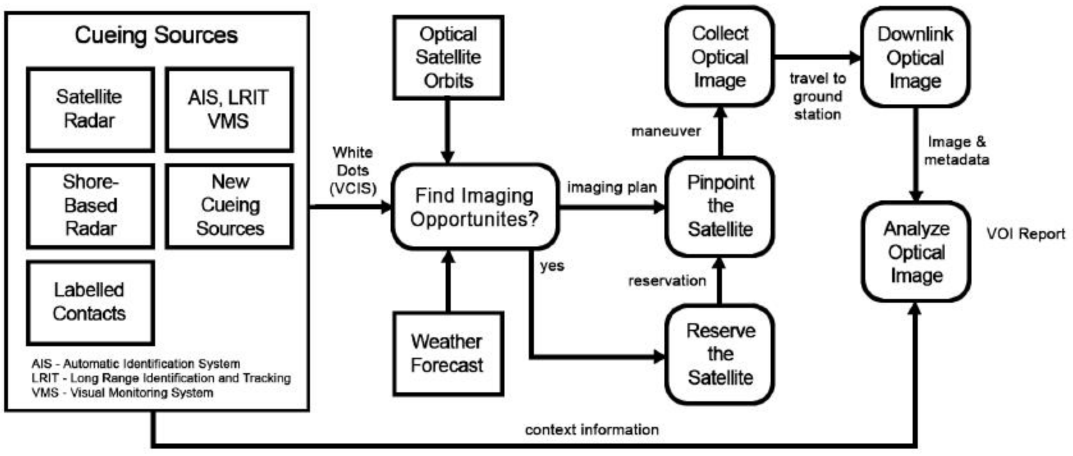


Figure 3: Workflow for MarCOS Cueing

the "OptiSAR" constellation, featuring tandem pairs of SAR and optical satellites with on-board target detection and inter-satellite cueing. This should reduce the cross-cueing delay to as close to zero as possible.

Broader MarCOS Missions

Although MarCOS was motivated by maritime security "dark target" scenarios, it offers a rapid-response capability that is expected to have wider applicability.

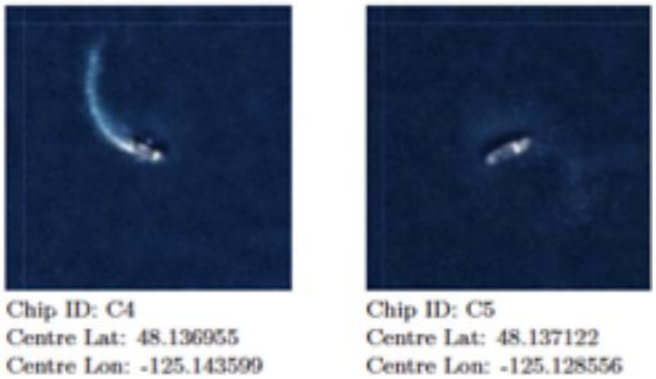
Illegal, unreported, and unregulated (IUU) fishing is expected to be an important application. Fishing regulators have already expressed an interest in the capability, and some early experiments were conducted to see how well MarCOS can characterize fishing activities. For example, optical images can identify whether a net has been deployed or whether trawling poles are extended. They can also clarify whether a dark target is a single ship, or a pair of ships transferring cargo.

Figure 4 shows fishing activity imaged by MarCOS and exemplifies how optical imagery can provide information not visible in SAR. Contact C5 was not moving, there was discoloration in the water near it, and there were white flecks indicating a flock of seagulls. These suggest that C5 was cleaning a catch. Contact C4 was 1.1 km west of C5 and was turning toward it.

Experiments are also planned to investigate and demonstrate in what ways rapidly-tasked optical assets can react to security, sovereignty, environmental concerns, or anomalies detected over remote locations. Figure 5, for example, shows part of a scene collected in the Beaufort Sea, which revealed that an icebreaker had changed course.

Conclusion

MarCOS partners believe that this developing capability offers maritime authorities a potential increase in threat detection capabilities. As noted above, the range of threats that can be identified and located by MarCOS is broader than traditional military threat detection, or can possibly enable maritime decision makers the ability to identify and respond to a range of illicit activity in their territorial waters.



Chip ID: C4
Centre Lat: 48.136955
Centre Lon: -125.143599

Chip ID: C5
Centre Lat: 48.137122
Centre Lon: -125.128556

Figure 4: Fishers Off Cape Flattery, Oct 2018

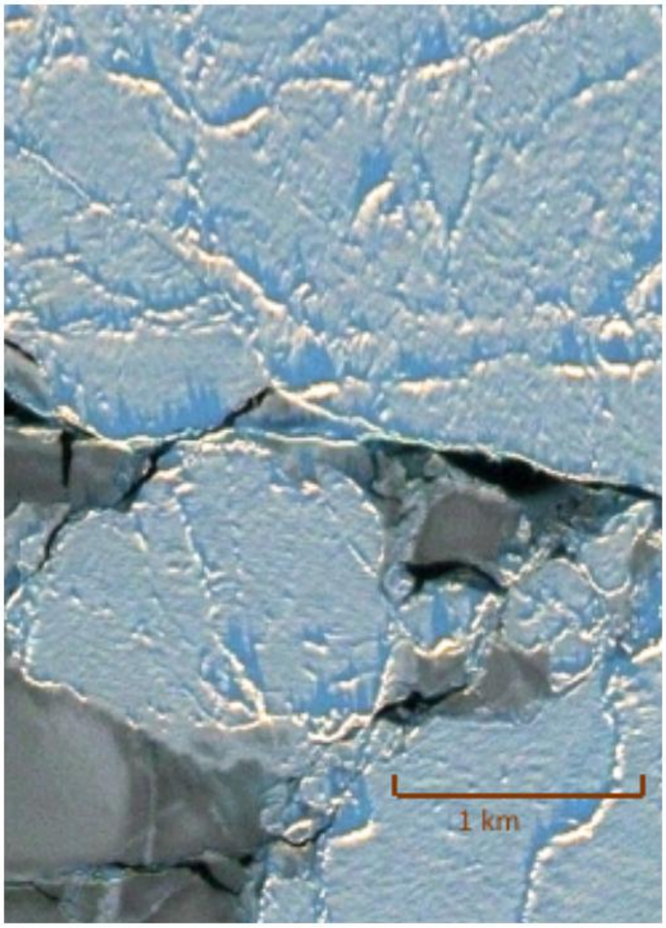


Figure 5: Ice in the Beaufort Sea, Oct 2018

AI MODELING PROVIDES INCREASED UNDERSTANDING OF THE ARCTIC REGION

Lauren Decker, PolArctic LLC

The remote and inhospitable characteristics of the Arctic historically made development of industries within the region difficult and unprofitable. This region, with its millions of miles of dynamic coastline, is of critical importance to U.S. strategic economic and defense policies. New technologies in icebreakers and deeper ports for ship access are engineering solutions to support development in the Arctic, but understanding and studying the environment will help build better strategies to enable safe passage for shipping, fishing, tourism, offshore development, and defense policies.

Sailors, crews, and marines alike require constantly-evolving bathymetric models for navigation through changing coastal hazards that traditional mapping is not capable of updating quickly and accurately enough to suit the needs of its users. New Arctic research supported by artificial intelligence is critical to satisfying this requirement, and will drive the U.S. towards a better understanding and use of a region where great uncertainty persists.

Climate change, for all of its causes, is a very real and dynamic variable within the Arctic. Sea ice levels are at some of the lowest ever measured. Rising temperatures have caused a cascade effect on the melting of permafrost, releasing previously trapped gasses back into the environment, accelerating an already fragile situation. Coastal erosion throughout the Arctic region, stretching from Alaska, Canada, Northern Europe, and Russia, has been identified as a long-term hazard. Yet, the word ‘erosion’ perhaps does not sufficiently portray the seriousness of the issues. Throughout the Arctic, erosion rates and lost coastline can be measured at feet per year, adding enormous complexity for operations within the maritime domain. Continually shifting coastlines prove challenging to most modeling and prediction methods.

Sea ice melting has opened up previously nonexistent shipping lanes for navigation. Two requirements are driving the need for innovation: are safe navigation for civilian ships not rated for ice operations and dynamic geographical needs for military exercises, operations, and transportation.

The advent of new technologies and the shifting climate creates an Arctic fresh with new risks and opportunities. From new transportation and shipping routes reducing travel time by as much as eight days from the Atlantic to the Pacific oceans, to development of untapped natural resources and precious metals, and adventure tourism to see one of the most exotic places on earth, the industrial and commercial potential of this region is immense.

Strategic Context for the Arctic

On June 19, 2018, President Trump issued Executive Order 13840, Ocean Policy to Advance the Economic, Security, and Environmental Interests of the United States. This executive order redirects Federal ocean policy towards a focus on economic growth and national security. Specifically, in the itemized goals, it states “facilitate the economic growth of coastal communities and promote ocean industries, which employ millions of Americans, advance ocean science and technology, feed the American people, transport American goods, expand recreational opportunities, and enhance America’s energy security.” The strategic nature of the Arctic, with its natural resources and potential navigation lanes, supports each of these goals necessary for furtherance of U.S. economic growth and enhanced national security.

New resource opportunities stem from increasing interest in mineral, natural gas, and oil development within the Arctic. According to the U.S. Geological Survey (USGS) 2008 assessment, the Arctic holds an estimated 13% (90 billion barrels) of the world’s undiscovered conventional oil resources and 30% of its undiscovered conventional natural gas resources. Coastal communities and port cities along the extensive Arctic coastline already engage in the economic advantages of tourism and fishing. Whale watching and fishing are major industries, both poised to grow as access to the Arctic increases.

Sustainable development is critical to maintaining the balance between economic necessity and conservation of the ocean: green development for a blue economy. In order to address the growing international environmental concerns in the Arctic waters while leveraging the economic potential, a concerted effort must be put into place. Key to such an effort is understanding the dynamic, multi-faceted scientific, ecological, and political environment of the Arctic using a combination of human expertise, high quality data, and AI.

With increased temperatures in the Arctic, rising sea levels, and changing patterns of Arctic ice flows, as well as the impact of deglaciation and permafrost changes, current modeling methods used to estimate coastal erosion and nearshore bathymetry can no longer meet the needs of coastal engineers and managers.

Within the Arctic, nearshore bathymetry is extremely shallow, unpredictable, and hazardous for ships attempting to navigate the coastal areas. Militaries require accurate understanding of the nearshore bathymetry to successfully execute aquatic landings and littoral operations. Coast Guard operations require the most up-to-date navigation tools to reduce risk associated with the conduct of rescue operations and homeland security patrols.

Technology, Data, and Information

Arctic conditions closely correlate to environmental change. It is vitally important to possess the tools necessary to observe large areas over many years in order to effectively detect change, identify causes, and forecast its impact. This poses a daunting challenge, as the isolation and extreme nature of the climate make field science difficult and expensive. To offset the cost of these methods, new inroads have been established in the areas of high-quality remote observation through the use of satellite imagery and data aggregation. In addition, new ice-sensitive technologies are allowing autonomous floats and vehicles to be actively sampling in the Arctic at all times, without putting people at risk.

The National Oceanographic and Atmospheric Administration (NOAA) has teamed up with the National Aeronautics and Space Administration (NASA) to create the Joint Polar Satellite System, which will gather global measurements of atmospheric, terrestrial and oceanic conditions, including sea and land surface temperatures, vegetation, clouds, rainfall, snow and ice cover, fire locations and smoke plumes, atmospheric temperature, water vapor, and ozone. This system will provide full global coverage twice a day. NASA also recently launched its ICESat-2 mission in September of this year. This system uses LIDAR to daily monitor and measure height of ice sheets, glaciers, sea ice and vegetation.

Satellite imagery of the Arctic has proven incredibly effective at measuring sea ice changes over decades. According to the National Snow and Ice Data Center, Arctic sea ice extent in 2018 ended tied with 2008 for the sixth lowest average September extent in the satellite record. Beyond measuring ice composition and flow, satellite imagery also provides the necessary data to map the Arctic coastline and identify coastal areas shifting due to erosion.

Satellites support broad observations of the Arctic from space. To compliment this perspective are new technologies allowing in-situ sampling in the water and under the ice. These new technologies (remote sensing, satellite imagery, and in-situ measurements) are giving scientists the necessary information and data to build new and more reliable models. Autonomous Underwater Vehicles and floats have been developed that have sensors and algorithms for ice-avoidance.

The modeling challenge in the Arctic comes down to two factors: its dynamics and its nonlinearity. The dynamics make it difficult because the Arctic models demonstrate a sensitivity to parameter choices – that is, if you pick a slightly wrong number for a model, you can reach a very wrong conclusion. The nonlinearity presents difficulties because most models are linear, meaning that when a model produces incorrect results, Arctic-focused users will not know whether the reality is too high or too low.

Artificial Intelligence (AI), beyond the buzzword, is a technology that is capable of describing very complicated systems that were never possible to describe before. At the core of what AI does is find relationships and patterns in data, and relates them to solutions. New tools give us new power, but there are three primary hurdles that must be understood for this new tool to be useful.

First: Model architects must understand the larger context of the models and the data being used. Understanding the need and policy behind the model will guide more valid structuring solutions.

Second: Garbage in, garbage out. If data is incomplete, misrepresenting the system, or otherwise weak, no model will be structured in a meaningful way that can derive answers of any value. Identifying high quality data is still in the realm of experts.

Third: AI is limited in its ability to be 'debugged' as a model, and AI systems have been referred to as 'black boxes'. Special architectures, one described briefly here, are employed to help gain insight into the 'why' of solutions that have been identified.

When these three criteria are met: an understanding of the larger system, assured high quality data, and a developed understanding the derivation of the solution, then a robust and powerful model can be constructed.

Architecture of an Artificial Intelligence Model

There are risks when working in the Arctic. Those engaged in the Arctic modeling industry must be well informed on the dynamic environment and what variables exist in order to effectively mitigate and compensate for such risks.

While the development potential of the Arctic region is immense, it can come at an environmental cost. Monitoring of resource development in national waters and on continental shelves—and ensuring protection of endangered species from the risks of pollution—are required to sustain the environment and sustain fishing and a growing tourism industry.
Traditional models are hard to maintain and incorporate new findings. This means operational models can trail the state of the art by years and decades with no easy way to leverage current scientific knowledge to bring them up to date. The Arctic environment has so many new parameters and variables that there will be gaps in current coastline and nearshore bathymetric models.

AI and Machine Learning have historically been leveraged to produce a "what" black-box answer to scientific questions in many very dynamic and complicated systems - like the Arctic. However, the "why?" of these solutions is obscured and hidden within the AI algorithms.

PolArctic is developing a tool that will leverage the power of AI in identifying patterns of nonlinear and extremely complex systems, while also building visibility and providing accessibility into the operation of the AI algorithm. Our architecture is designed to start with 'current knowledge' using human readable relationships and graphs. Then, an AI Neural Network generates a solution to the knowledge graph as a codebase. The code can be reviewed and compiled as a traditional model.

The power of this system is found with the curation of the codebase using the neural networks. Our AI-curated model architecture is capable of dynamically generating models to run complicated analyses. The goal of the system is to identify and quantify complex and subtle patterns both new and existing in a system; reorganize a structure maintaining the relationships describing the patterns; then use an AI to incorporate new connections to produce an application that implements the curated model. The end result being a model suited to the needs of the complex Arctic system—born from a dynamic nonlinear system to model a dynamic nonlinear system.

This architecture has several unusual traits that differentiates it from classical AI architectures. For example, where traditional "deep learning" methods are employed, the solutions are buried in hidden neuron layers that are non-linear by design, and the inputs and solutions are directly linked into and out of the architecture. There is little to no insight into why the AI found that answer, and you can not go one step forward or backward in the system to gain an understanding of how a solution was obtained.

In the new architecture described here, the initial and final steps are also human-readable. The relationship graph explaining the model identifies the core of how the model should operate and the output is a codebase that can be reviewed. Allowing scientist to still leverage the power of nonlinear tools and pattern recognition have made AI and deep learning fundamental in modeling the natural world.
With advances in monitoring and data collection tools integrated with advanced artificial intelligence modeling, new depths of understanding are possible regarding the dynamic variables impacting coastline and nearshore bathymetry. This includes the breakup and reformation of the ice in the Arctic region. For these reasons, PolArctic is committed to being the industry's foremost leader in oceanographic collation and modeling of the Arctic.

Conclusion

PolArctic is leading the way for Arctic oceanographic modeling through fusion of remote sensing, autonomous systems, geospatial imagery, data analytics, and artificial intelligence to provide scalable, tailored, and easy to understand products. PolArctic understands artificial intelligence is often viewed as a magical solution to big data problems, but our hybrid approach in developing self-learning and correcting algorithms provides a unique solution keeping experts informed on the inner workings of the model, which is not found within traditional artificial intelligence processes.

LEARNING BEHAVIOR OF MARITIME MESH NETWORKS FOR INTEGRATING UNDERWATER AND ORBITAL DOMAINS

Alex Bordetsky, Naval Postgraduate School; **Carsten Glose,** German Armed Forces (Bundeswehr) /Exchange Scientist; **Steven Mullins,** Naval Postgraduate School; **Eugene Bourakov**, Naval Postgraduate School

In this article we briefly describe two experimental studies on how to capture semi-autonomous intermittent maritime-land mesh network behavior, and transition the network operation process to machine learning adaptive management techniques.

1. Manned-Unmanned Littoral Mesh Network Operation Experiment

The introduction of unmanned systems into a multi-domain self-forming maritime-land mesh, presents a significant challenge to network management techniques. This highly dynamic environment calls for a new approach based on automated adaptive management and machine learning techniques. For more traditional maritime networks with a number of fixed nodes ashore and ship based nodes with known routes, complex network operations would be typically conducted by a Network Operations Center (NOC) crew.

Greater automation has been shown to be feasible in managing a decentralized network by using distributed artificial intelligence.[7] In the field of tactical networks, the idea of distributed network management was proposed by Bordetsky and Hayes-Roth over a decade ago. [2] They propose the concept of hyper-nodes for command and control networks because the early fundamental advantages could be demonstrated. [1] However, the details of network management and control systems for the hyper-nodes were not explained at that time.

Recently, Chen, et al [4] developed an algorithm for cloud radio access networks based on echo state networks that could predict several relevant parameters in a simulated environment, such as users' positions and data flow.

Although this could result in more automated network management, research regarding the automation of network management has tended to focus on standard or mobile networks, and it has generally ignored networks in contested or austere conditions such as tactical military networks. For these networks, large training datasets, which are also required for initiating machine learning based on artificial neural networks model [8], practically don't exist. The experiment described below contributes directly to this goal of providing a maritime mesh behavior training set and exploring the challenges of transitioning to machine learning of captured network behavior patterns.

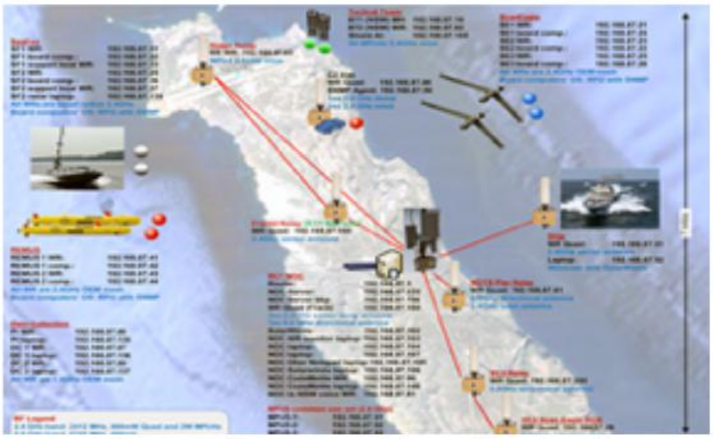


Figure 1. Experimental mesh network

2. Experiment Setup and Description

The first experiment was conducted in a littoral area around an island off southern California coast by implementing a manned-unmanned maritime mesh network setup, comprising:

- Two Scan Eagle Unmanned Aerial Vehicles
- Two Sea Fox Unmanned Surface Vehicles
- Two Remus Autonomous Underwater Vehicles
- One Shield AI Quadrotor UAV
- One large ship

Mesh network performance data, including the behavior of the unmanned nodes was captured and collected based on a Simple Network Management Protocol (SNMP) technique (see e.g. [10]).

Data was collected by novel plug-in SNMP agents specifically created for this research utilizing a Node.js framework. For this particular experiment, the SNMP Agent was running on Raspberry PI 3 and Odroid microcomputer boards (Linux OS) added to the unmanned aerial vehicle (UAV) and unmanned surface vehicle (USV) payloads. As distributed remote monitors, these plug-in agents were able to record performance and device-specific non-SNMP data autonomously when reachback to the NOC was intermittent or unavailable. The data were uploaded to a central database after the experiment. This database consists of online and offline network performance data. In addition to the automated recorded data, significant events, interesting discoveries and relevant information that could not be collected automatically were recorded in textual form, manually entered into the central database. For our analysis, we used only the automatically recorded data. The manually recorded data had no standard structure, and would have been prohibitive to incorporate into our machine learning analysis. Nevertheless, the manually recorded data was helpful meta-data for cleansing the dataset and to identify and filter out invalid values.

3. Maritime Mesh Network Operation Dataset Analysis

In total, 135,546 network operation variable instances (objects) were captured by the NPS novel control network of plug-in SNMP agents. A detailed description of this data set can be obtained upon request.

3.1. Principal Component Analysis

The Principal Component Analysis (PCA) for the attribute "reachable" and a variance of 95% covered, resulted in 12 remaining attributes. Although this result fell short of our expectations regarding the reduction of attributes, we found ourselves in the unusual situation where we were able to identify key factors and derive conclusions just by closely looking at the components.

Table 1. Excerpt of PCA result

#	Prop.	Component
1	0.217	0.56platform=AUV-0.56platform=USV+0.506depth...
2	0.157	-0.541throughputout-0.536pktloss-0.47throughputin-0.313pktsize+0.199OriginID...
3	0.138	-0.664sideslip_vel-0.638forward_vel-0.366yaw-0.057platform=AUV+0.057pla...
4	0.118	-0.663OriginID+0.606pktsize-0.264throughputin-0.23pktloss-...
5	0.077	-0.983yaw_rate-0.098rtt+0.097throughputin-...
6	0.075	0.979rtt-0.119pktsize-0.091yaw_rate-0.063throughputout+0.06 depth...
7	0.056	0.868yaw-0.383forward_vel+0.16 platform+...
8	0.047	0.791throughputin-0.359throughputout-0.328pktloss-0.288OriginID-0.203pktsize...
9	0.034	0.709pktloss-0.514throughputout-0.303OriginID-0.3pktsize 0.146depth...
10	0.029	0.609pktsize+0.557OriginID-0.482throughputout+0.205thr...

3.2. PCA Findings

Platform-specific attributes (platform type) have the greatest influence (component 1 and 3). This is unsurprising, as the platforms possessed different capabilities and fulfilled different functions.

A bigger packet size and a larger throughput make reachability more difficult (component 2). We presume that this is caused by the priority algorithms in the device's network stack. With a higher workload, packets such as the SNMP poll request could be dismissed,which is to be expected. This part of the system could offer room for improvement.

We found that it matters which entities communicate (components 2, 4). This result is expected because it directly correlates to the "platform" attribute.

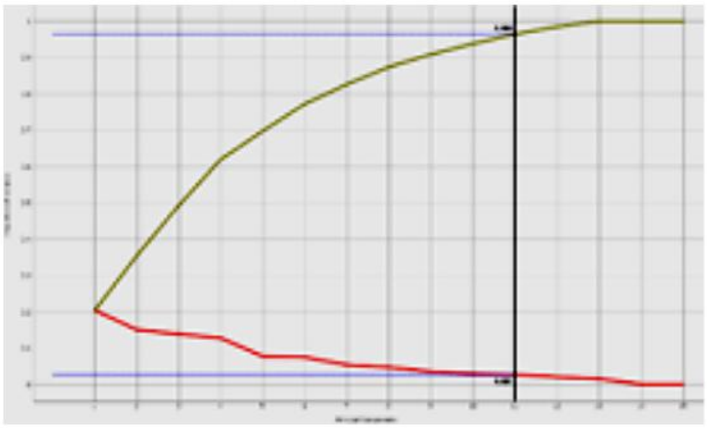


Figure 2. Number of PCA components vs. variance covered

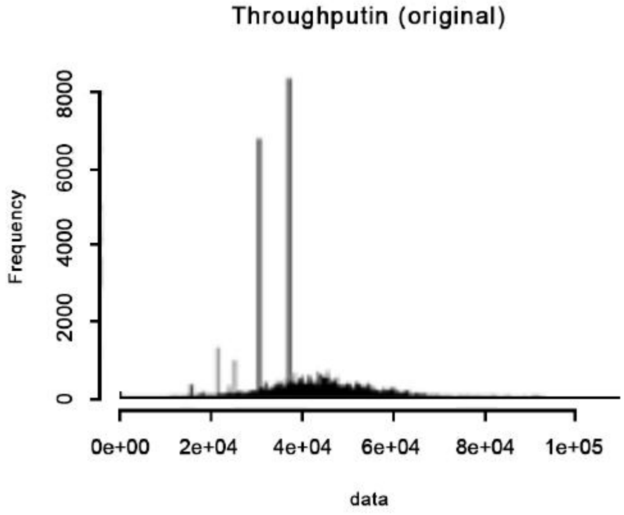


Figure 3. Histogram of "throughputin"

Velocity and yaw can have a positive or a negative impact on reachability (components 3, 5, 6, 7). This is an inconclusive result and requires further investigation.

The first four components account for approximately 60% of variance. The rest seems to be quite random and noisy, and without a direct interpretation. Figure 2 depicts this. A closer examination of the statistical properties of the original attributes revealed some interesting insights. We found that the attribute "throughputin" seems to have an underlying Gaussian distribution.

Having said that, it is notable that we found several outliers for certain frequencies (see Figure 3). Several protocols use fixed-size messages. It seems plausible that these outliers are a direct result of this. A similar situation exists for the attribute "throughputout" where an underlying superimposition of two Gaussian distributions seems to take place.

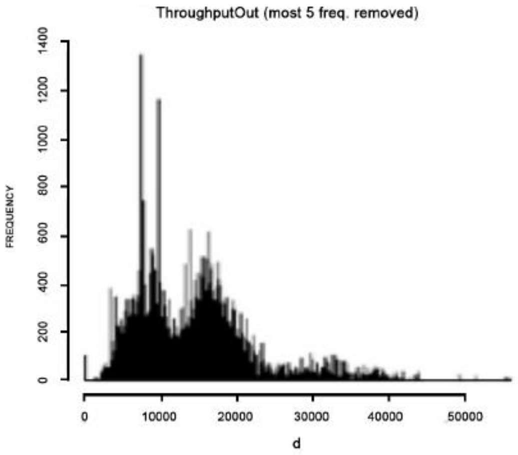


Figure 4. Distribution of "throughputout"

It our understanding that this kind of outlier and the huge variance could manifest a special feature of tactical mesh network behavior.

Figure 4 shows the frequency of the values of the attribute "throughputout." The figure was restricted to values under 60,000, and the five most frequent values were removed. Values over 60,000 occurred relatively rarely in the dataset and the Gaussian distribution of the data is hard to see in the full picture (compare e.g. to Figure 3).

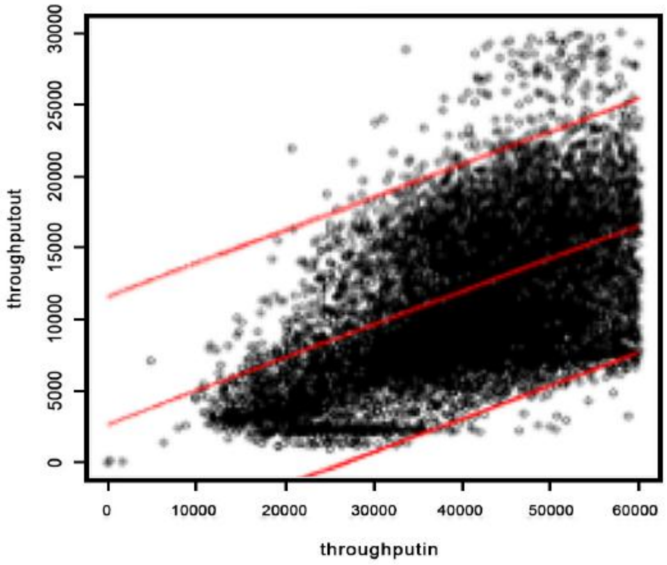


Figure 5. Linear fit for throughputin vs. thoughputout

We did find a linear correlation between the attributes "throughputin" and "throughputout."

Figure 5 shows the identified linear model for the attributes "throughputin" related to "throughputout". The plot was restricted to values under 30,000 for "throughputout" and values under 60,000 for "throughputin" to clear the clutter of a lot of outliers.

We think that this finding can explain a feature of the mesh network. Many incoming messages are forwarded to neighbor nodes and as such, output traffic correlates to input traffic. This indicates that our network design and setup for a mesh network is sound, as there appear to be no "supernodes" which receive and transmit all the data to the network. In addition, this also suggests that communication devices used in mesh networks could be designed with symmetrical up- and downlink channels.

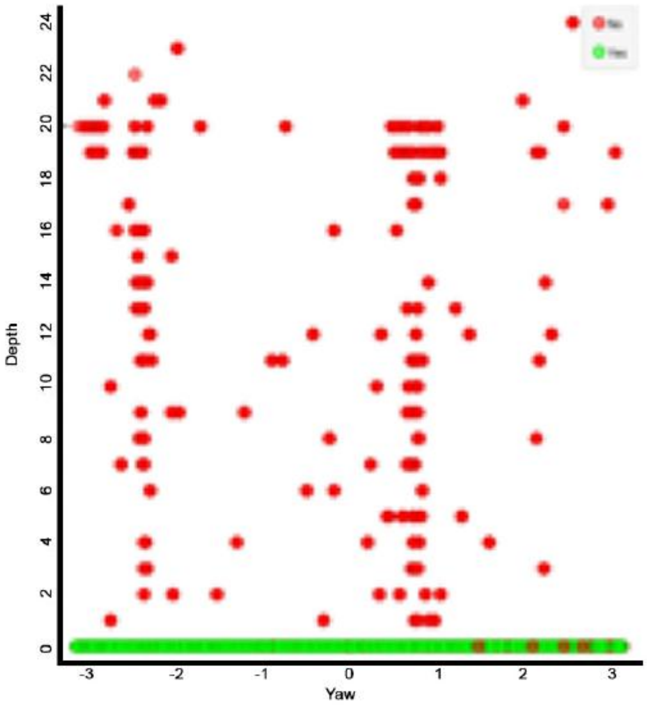


Figure 6. Yaw vs depth (altitude)

Additionally, we found that a positive "yaw" value leads to unreachability in higher altitudes (Figure 6). Our assumption is that features of the antenna characteristics and subsequently characteristics in the beam pattern lead to a link loss if the device moves or rotates.

Our analysis indicates statistical regularities applied to all attributes. Based on this assessment, we decided to use all remaining 12 PCA attributes for the machine learning step.

4. Application of Machine Learning Techniques to the Recorded Dataset

We applied several supervised machine learning methods with the target attribute “reachable” to examine whether learning could be done in this environment. The prior probability of the target attribute is 71.2%. The analysis was conducted with Weka [11] and Orange [6]. We used cross-validation with a 10-fold for each run.

Many classic machine learning algorithms master this particular learning problem (Table 2). Except for Naïve Bayes, Logistic Regression, SVM and Ripper, performance does not differ significantly between the learning algorithms. As 5% of the variance is lost via the PCA transformation, we were surprised that the best learning algorithms have a higher classification rate and were curious whether we could obtain better results by using the original dataset. As it turns out, a very similar performance result is achieved with the original dataset. Interestingly, the kNN and Naïve Bayes algorithms perform very differently between the transformed and untransformed datasets. Whereas kNN benefited enormously (performance of 57.28% correct classification on the untransformed dataset compared to 96.59% on the transformed dataset) from the transformation; Naïve Bayes suffered (from 84.76% correct classification to 56.39% on the transformed dataset) from the transformation. Closer examination of the learned models (original and transformed datasets) suggests that the models are over-fitted. One example of this overfitting is the tree built by the J48 algorithm with a size of 3175 and 1588 leaves. As we do not have a dataset from a different experiment available, we have not yet been able to investigate whether and to what extent the models generalize to different scenarios.

Algorithm	Impl.	Correct Classificat'n	F-Score	Remarks
Random Forest	Weka	97.09 %	0.97	# of trees: 10 No split subsets smaller than 5
kNN	Weka iBK	96.59 %	0.96	5-NN
C 4.5	Weka J48 (prune)	96.45 %	0.96	Size: 3175 # of Leaves: 1588
Neuronal Network	Orange	95 %	0.95	Hidden Layers: 50,150 Activation: ReLu, Solver: Adam
RIPPER	Weka JRIP	94.86 %	0.94	17 Rules
SVM	Weka (SMO)	92.52 %	0.91	Poly-kernel
Log.Reg.	Weka	91.56 %	0.90	Regular-ization Ridge (L2), C=1
Naïve Bayes	Weka	56.39 %	0.62	

Table 2. Result regarding target attribute “reachable”

5. Maritime-Land-Orbit Mesh Network Extension

Based on the encouraging results of the experiment described above and subsequent machine learning trials, our team at the NPS Center for Network Innovation and Experimentation (CENETIX) recently completed two more experimental steps.

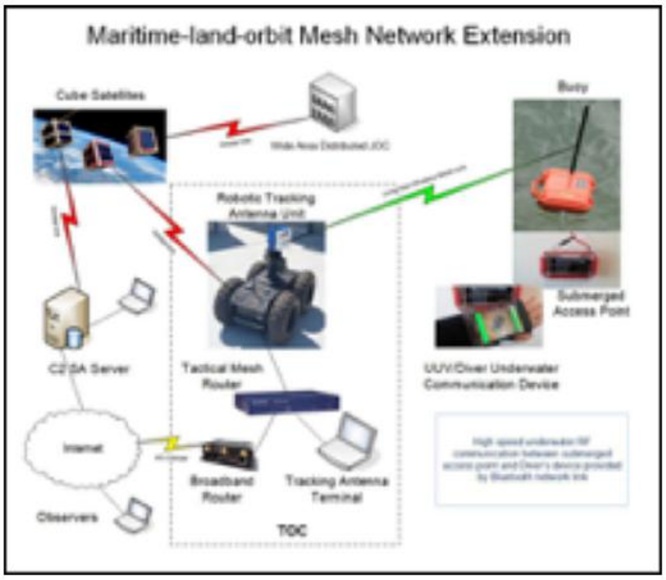

Maritime-land-orbit Mesh Network Extension
Cube Satellites
Wide Area Distributed JOC
Buoy
Robotic Tracking Antenna Unit
Submerged Access Point
C2/SA Server
Tactical Mesh Router
UUV/Diver Underwater Communication Device
Internet
Broadband Router
Tracking Antenna Terminal
Observers
TOC

Figure 7. Underwater-orbital mesh network extension testbed

The first set of trials was dedicated to monitoring and capturing vital datasets for maintaining maritime-land-orbital mesh networking extensions (Figure7).

In order to accomplish the task, a working prototype of Maritime-Land-Orbit networking was developed. The overall networking diagram is shown at Figure 1. The main objective was to capture a SAAB radar image on a distant coast and immediately transfer it to an AUV/diver underwater communication device via an orbital network cluster. The high speed RF 2.4 GHz underwater network comprised an AUV/diver underwater communication device and a submerged access point.

The tactical operations center (TOC) used a tracking antenna unit to maintain directional link to the remote buoy at a range of several miles. The tracking antenna unit prototype was developed by CENETIX based on an RMP400 Segway robotic platform (Figure 7). The TOC provided an orbital link to allow a remote operator to download images to the diver and submerged device.

In the experiment, the image taken by the SAAB coastal radar was transferred via a simulated orbital link to a command and control situational awareness (SA) server. A specially developed software listener running on the SA server captured the image and forwarded it to a tracking antenna unit in the field of operation. The tracking antenna unit routed it to the buoy via a local mesh network link. An underwater communication device also developed by CENETIX acquired the radar image.

In order to maximize the range to the surface buoy from the satellite ground station, we used a UGV-based directional steerable relay to the buoy site. It proved to be efficient, stretching the ground-to-buoy mesh link to 5-7 miles neighbor-to-neighbor distance on-the-move. Applying a steerable directional antenna to the ground node-buoy mesh networking enabled us to increase a typical 0.8-1.2 mile surface-land mesh link range to up to 7.5 miles. It is a significant improvement, which lowers network LPI/LPD characteristics and extends the individual link range 3-4 times.

In exploring the challenges of extending self-forming maritime mesh networks from underwater to orbit, we needed to address the gap in integrating short-living aerial nodes into the formation. A network of plug-in control agents allowed us to extend the application level mesh by integrating a unit of paratroopers conducting a slow descent HAHO jump, simulating a scaled manned-unmanned formation data exchange. Figure 8 illustrates the network behavior data set captured during the trial.

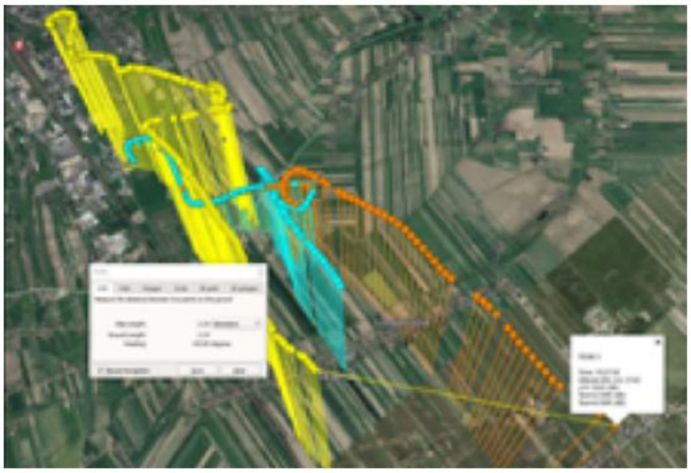


Figure 8. Visual 3D view of paratrooper dataset

This relatively stable pattern of aerial mesh enclave SA sharing communication does four things:

- Highlights the feasibility of extending a subsurface-based mesh to a high altitude aerial domain,
- Provides quantitative constraints for drafting way-point algorithms needed to control autonomous UAVs,
- Provides threshold numbers for TTPs needed to support human operators.
- Illustrates machine learning of captured constraints and transitioning the derived rules into the NOC and human operators TTPs—currently a work in progress. We hope to reflect it its results in our next publication.

6. Conclusions

Based on the first experiment, we found strong statistical regularities in the recorded network data of the observed mesh network designed to support a tactical military mission. These regular patterns are sufficient to predict relevant network management decision features related to unmanned system operation, subject to changing network performance and configuration conditions. The results of the second set of experiments strengthen the first trial-based conclusions that machine learning of distributed autonomous maritime mesh network is feasible. Establishing control network of plug-in agents-monitors is critical to the success of ongoing, frequently autonomous and intermittent, network behavior dataset generation. It is correspondingly critical to the subsequent machine learning and knowledge transfer to self-organizing nodes techniques and procedures.

Acknowledgements

We would like to thank Dr. Raymond Buettner, Dr. Douglas Horner for an opportunity to conduct the multi-domain mesh experiment. We are grateful to Ms. Mekisha Marshall and Ms. Shala Malone for sponsoring the second set of experiments described in the paper.

References

[1] Bordetsky, A. and Hayes-Roth, R., 2007. Extending the OSI model for wireless battlefield networks: a design approach to the 8th Layer for tactical hyper-nodes, In International Journal of Mobile Network Design and Innovation. Inderscience Publishers

[2] Bordetsky, A. and Hayes-Roth, R., 2006. Hyper-Nodes for Emerging Command and Control Networks: The 8th Layer, In 11th International Command and Control Research and Technology Symposium (ICCRTS)

[3] Burbank, J. L. et al., 2006. Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology, In IEEE Communications Magazine, vol. 44, no. 11, pp. 39-45, November 2006.

[4] Chen, Mingzhe, et al., 2016. Caching in the Sky: Proactive Deployment of Cache-Enabled Unmanned Aerial Vehicles for Optimized Quality-of-Experience. In IEEE Journal on Selected Areas in Communications 2016, 10.

[5] Chiang, C. y. J., et al., 2006. Towards Automation of Management and Planning for Future Military Tactical Networks. In MILCOM 2006 - 2006 IEEE Military Communications conference, Washington, DC, 2006, pp. 1-7.

[6] Demsar J., et al., 2013. Orange: Data Mining Toolbox in Python. In Journal of Machine Learning Research 14, pp. 2349-2353.

[7] Koch, F., et al., 2004, Distributed Artificial Intelligence for Network Management Systems --- New Approaches. In Service Assurance with Partial and Intermittent Resources. Springer Berlin Heidelberg.

[8] Kotsiantis, S. B., 2007. Supervised Machine Learning: A Review of Classification Techniques. In Proceedings of the 2007 Conference on Emerging Artificial Intelligence Applications in Computer Engineering: Real Word AI Systems with Applications in eHealth, HCI, Information Retrieval and Pervasive Technologies. IOS Press.

[9] Sohail, S., 2010. Automation of Network Management with Multidisciplinary Concepts. In International Journal of Computer Technology and Applications, 2010, 11.

[10] Subramanian, M., 2010. Network Management: Principles and Practice. Prentice Hall; 2nd edition.

[11] Witten, Ian H., et al, 2016. The WEKA Workbench. Online Appendix for “Data Mining: Practical Machine Learning Tools and Techniques”. Morgan Kaufmann, 4th edition, 2016.

MARITIME PORT SYSTEMS CYBER SECURITY VULNERABILITY

John Filitz, Information Security Specialist, One Earth Future

Most attention concerning maritime domain cyber security focuses on inherent vulnerabilities of the shipping sector. An oft-neglected area until recently has been the cyber vulnerability of maritime ports. Recent efforts to develop an action plan to implement and advance the National Cyber Strategy in the Maritime Transportation System (MTS) are to be commended. One such effort addressing gaps is led by the National Maritime Intelligence-Integration Office. Further effort to prioritize cyber security of critical infrastructure at the international level, however, is required. Maritime ports, as an integral part of MTS, play a vital and strategic role in global trade, with 90% of the world's trade carried by sea.[1] In the U.S., more than $1.3 trillion in cargo is handled by the nation's maritime ports each year.[2] Maritime ports also play an indispensable national security role, supporting U.S. armed forces logistics, including private military contractors, in international security efforts.

Critical Maritime Port Systems

Industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems can be found aboard vessels, as well as in terminal operating systems. For instance, in automated port cargo and terminal management, these technologies aid port operators in the management of volatile and hazardous, containers, liquid and dry-bulk cargo, navigation of vessels, among other applications.

To meet the challenges of ever-increasing competition, trade volumes and technological redundancies of legacy information systems, many maritime ports around the world are in the early stages of Internet of Things (IoT) port operational technology adoption. In 2018, IoT devices are expected to overtake the number of smartphones on the internet, and by 2022 there will be 18 billion IoT devices connected to the internet.[3] Although the mainstreaming of this technology will have positive impacts on improving overall port governance, the rapid rollout in the short-to-medium term raises the likelihood that nation-state and non-state actors will attempt to take advantage of poorly-secured IoT-enabled, maritime port infrastructure.

Of concern are the vulnerabilities present in legacy industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems found in terminal automated operating systems. Vulnerable existing and new IoT-enabled port infrastructure presents multiple opportunities for cyber-attacks to successfully disrupt, inflict damage, or steal proprietary data; to be deployed in hybrid warfare campaigns; or to enable other nefarious activity such as transnational organized crime.[4]

Hybrid-War Scenario

The US needs to respond to an emerging international security crisis in Eastern Europe, requiring deployment of air and naval assets. Several NATO allies suffer a targeted and coordinated cyber-attack, compromising maritime transportation infrastructure at several strategic maritime ports, affecting GPS and port operating systems. The consequences of the attack are profound: The high-volume seaborne traffic in European territorial waters are severely impacted, with key shipping routes congested. Efforts to respond to the emerging international security crisis suffer a setback of several days, allowing the bad actor to gain a strategic upper hand. The attack results in a strategic rival capturing state territory belonging to a NATO ally. This has altered the balance of geopolitical power in the region against NATO and US interests. In the short-term, US and NATO interests remain vulnerable to hybrid offensive campaigns using the same modus operandi. The impact of the cyber-attack on the European economy has resulted in billions of dollars in damages. Six months after the attack, affected maritime ports, supply chains and the broader economy are yet to fully recover.

Maritime Port System Vulnerability

The increasing technological modernization of maritime ports through IoT however brings with it an expansion of risk, with ICS and SCADA especially vulnerable to being compromised. The inherent vulnerability in ports arises as legacy infrastructure is integrated with new infrastructure, and non-critical systems are integrated with critical systems.[7] Although situational awareness concerning the extent of maritime port cyber security vulnerabilities has improved in recent years, more attention to this issue is warranted. In a recent survey, 38% of the 126 maritime industry executives in the U.S. reported that they were targets of a cyberattack in the past year. Of these respondents 10% had suffered a successful attack, and 28% suffered an attempted breach in the past year.[5] In September 2018, the Ports of Barcelona and San Diego were the latest victims of a targeted cyber-attack.[6]

What makes the maritime ports so susceptible to the risk of cyber-attacks concerns its notorious reputation for operating and relying upon legacy operational and IT technology. This trend has, however, started to move in the opposite direction given a plethora of challenges faced by ports, including increased competition, significant growth in trade volumes, and, finally, the growing importance of information security.

A significant reason for why these systems are so vulnerable is that the vast majority of ICS and SCADA were designed without consideration of exposure to the Internet.[8] Maritime ports in the U.S. are particularly vulnerable given that over 42% of global ICS systems found in the U.S..[9] Just how vulnerable ICS are to cyber-attack was demonstrated in 2007 in the now infamous Aurora Generator Test. This test showed that changing the operating cycle of a generator remotely by a computer could set the turbines on fire and ultimately destroy the machine.[10] Further examples of ICS and SCADA vulnerability include the Stuxnet attack on the Iranian nuclear program. This attack demonstrated that even insulated critical infrastructure such as an off-grid nuclear facility can be targeted indirectly, via an infected USB.[11]

Arguably the best demonstration of ICS and SCADA systems vulnerability concerns Russian efforts to destabilize the Ukraine. On December 23, 2015, Ukraine's regional power producer, Ukraine Kyivoblenergo, was targeted, with significant parts of the power producer's system taken offline due to an external attack on its SCADA systems, affecting 225,000 customers. Malware was delivered by email to individuals in the administrative and IT network of the utility company, in this way, nefarious actors gained access to the network six months before the actual attack.[12] During this time, the attackers were able to capture login credentials giving them unprecedented access to sensitive parts of the network. The attackers were able to shut down parts of the network as well as takeover workstations, locking out individual employees. At least 27 substations were taken offline. The attackers also installed malware that even upon retrieving access to workstations would not allow employees to remotely bring substations back online. During the same period, the attackers also launched distributed denial of service (DDOS) attacks on the company's call center, flooding it with thousands of calls. This was a multipronged and sophisticated nation-state attack.[13]

The effectiveness of the Stuxnet and the Ukrainian attacks have focused attention on

Maritime Port Cyber Threats

The key cyber threats faced by maritime ports include:

- Targeted cyber-attacks: This includes nation-state attacks such as the Not-Petya attack by the Russian military, and the Advanced Persistent Threat hacking groups with links to nation-state actors. Examples include Russian hacking groups Fancy Bear (APT 28), Cozy Bear (APT 29) and China's Wekby (APT18);
- Cyber espionage by nation-state and non-state actors, including hacktivists;
- Ransomware attacks by nation-state and non-state actors. Examples include WannaCry ransomware originating from North Korea;
- Facilitation of organized criminal activity by corrupting and altering cargo manifests to intercept cargo and traffic contraband;
- Hacktivists and insider threats seeking to cause disruption or to sabotage infrastructure.

the "outdated and obsolete security of critical infrastructure," specifically concerning legacy ICS and SCADA systems.[14] Widely used maritime navigation technology integral to terminal and port management, such Automatic Identification System (AIS) and Global Positioning System (GPS), already pose significant security vulnerabilities. This was recently demonstrated in the 2018 NATO Operation Trident Juncture exercises in Norway, with suspected Russian state interference with GPS signals causing disruption to the exercises.

Organized criminals too are also increasingly exploiting the technological advances of the cyber age. No better was this demonstrated than by the infiltration of the Port of Antwerp's information system by Netherland's-based narcotics traffickers. Through the help of contracted hackers, the narcotics traffickers were able to generate fraudulent bills of lading on the ports information system. The fraudulent documentation was then used in plain sight to successfully intercept cocaine and heroin consignments at the port for a two-year period.[15] A second incident reported by Verizon concerns the compromising of a large shipping conglomerate cargo manifest by an organized criminal group for purposes of identifying high value cargo for robbery at sea.[16]

New Global Threats

It is within this context that cyber war, cyber crimes, and cyber terrorism are increasingly being seen as the leading threats to the global order.[17] This realization is premised on the increasing prevalence of the cyber domain being front-and-center of highly orchestrated cyber war, espionage, and crime campaigns. Nation-state and non-state actors can carry out sophisticated and targeted cyberattacks against opponents, with attribution in most cases difficult to prove. The most active nation-state actors waging these cyber campaigns, also referred to as Advanced Persistent Threat (APT)[18] campaigns, include Russia, China, Iran, and North Korea.

Terrorists and transnational organized criminal groups too, have for quite some time been involved in perpetrating criminal acts in the cyber domain. The fluidity with which terrorists have been able to expand their reach has been amplified by significant advancements in information and communication technologies. Terrorist groups (including Al Qaida and the Islamic State) all have used the cyber domain to advance their campaigns.[19] In the early 2000s, Al Qaida were actively doing cyber reconnaissance work, seeking among other things to target U.S. critical infrastructure, including waste water facilities and electric systems. [20]

Hacktivists and insider threats also pose challenges to the integrity of information system security. Each year we are met with alarming facts and figures of cyber-attacks on private companies and global institutions. In the first three months of 2016, the FBI reported that ransomware attacks had cost U.S. organizations $209 million, up from $24 million in 2015.[21] The 2017 NotPetya attack in 2017 is now considered the costliest global cyber-attacks to date, with damages in excess of $10 billion.[22] According to the Online Trust Alliance (2018), 2017, "marked another 'worst year ever' in personal data breaches and cyber incidents" globally. The number of cyber incidents (including ransomware attacks), email hacks doubled to 159,000 in 2017. Many attacks however go unreported with estimates closer to 350,000 for 2017. Alarmingly, over 93% of these attacks were avoidable, with poor decision-making by users attributed as the single greatest cause of the attacks."[23]

Mitigation

Given the vulnerabilities identified in ICS and SCADA, it is recommended that, at a minimum, basic security measures need to be implemented to ensure the security and integrity of critical port systems.[24] Maritime port information system security is no longer a "nice to have" or convenient "add-on." It should underpin and be integrated with any maritime port authority, private actor or regulatory authority's overall business and organizational strategy. Information system security should be viewed as the backbone of any business plan, given that a severe compromise can result in significant financial and national security implications.

On this basis, steps to safeguard information system security expenditure should include prioritizing information system security in the short-to-medium terms alongside other critical expenditures such as the acquisition of new operational technology. Further steps include enforcing cyber security governance across the respective maritime domain, including the extended shipping and port-side supply chains. As a first step for maritime ports, there is need for establishing a port information system security baseline, one that is continually updated to reflect advances in technologies. This requires developing an overarching information security policy and risk framework that should include information and data security, physical and environmental security, as well as maintenance, backup and recovery plans.[25] The National Institute of Standards and Technology (NIST) Cybersecurity Framework 1.1. and the NIST Framework for Improving Critical Infrastructure Cybersecurity offer practical recommendations to secure information systems in this regard.[26] Additionally, using machine learning and Artificial Intelligence for cyber-attack scenario development and advanced penetration testing are also increasingly seen as essential for critical infrastructure cyber security protection.[27]

.

Policy and Rule of Law

There are several existing efforts at the international level attempting to garner attention to the cyber threat that the world is facing. This includes the Paris Call of 12 November 2018 for Trust and Security in Cyberspace, Microsoft's launch of a Digital Geneva Convention, and the European Union's passage of the General Data Protection Regulation (GDPR) on May 25, 2018. In the U.S., there are several efforts at the Federal and state levels to address cyber security issues related to maritime ports,[1] among other critical infrastructure.[2] This includes talk of a Cyber Moonshot[3] approach to energize the private sector, tertiary education institutions, and the government to address cyber security threat, both at a national and international level. These effort and initiatives are to be commended.

Maritime Port Information System Security Measures

- Comprehensive information security risk appraisal;
- Port-wide cyber hygiene training. This includes cyber security contractual obligations for supply chain vendors;
- Developing an incident response and recovery plan;
- Categorizing ICS and SCADA systems;
- Network configuration and segmentation;
- Boundary protection and Intrusion Detection Systems;
- Regular vulnerability/penetration testing;

What is missing, however, is an urgency by global leaders in efforts undertaken to date. This absence in leadership urgency on this matter can best be epitomized by the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. These leaders for setting a global cyber security agenda are failing to reach consensus in the fourth and final session. While a UN resolution was passed on 8 November 2018 to establish a new open-ended working group to further the global cyber security agenda, significant work remains to be done.[28]

The current state of efforts undertaken to date on the global cyber security threat challenge highlights the fundamental need for global leadership on this matter. The MTS sector faces significant vulnerabilities given the nexus of MTS with global trade underscored by reasons outlined in this paper.[4] Evidence of the cyber fragility inherent in the MTS was recently exposed by the NotPetya attack on the container shipping company Maersk, resulting in significant disruption to its entire fleet, ports around the world, and causing in excess of $300 million in damages.[29]

Further Research and Conclusion

Securing IoT enabled maritime port infrastructure from attack is a complicated and multifaceted challenge. The threat vectors are increasing daily as more and more IoT-enabled devices and infrastructure are brought online, driven by expanding demand pressures on maritime ports to stay nationally and globally competitive. ICS and SCADA systems are particularly vulnerable, given that many of these systems were designed without consideration to internet exposure. The most effective immediate intervention to safeguard maritime ports from successful cyber-attack concerns the prioritization of information security

[1] The Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2017 was introduced and passed the House in October 2017. This Act however is yet to be voted on by the Senate.

[2] The latest in this regard concerned the release of the National Cyber Strategy (2018) and the passage of the Cybersecurity and Infrastructure Security Agency Act of 2018. Also see California's passage of SB327 Information privacy: connected devices. Other relevant policy and guidance include the NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1. (2018), and the NIST Cyber Security Framework, Version 1.1. (2018).

[3] The Cyber Moonshot refers President Kennedy's call to action to the private sector, tertiary education institutions and the government to get humans to land on the moon.

as integral to the overall operational management of the port. It is also imperative that further research efforts are undertaken to identify threat and attack scenarios, to provide mitigation strategies and to aid the establishment of best practice standards. Only through such research will stakeholders (including port authorities, law enforcement, and private sector operators) be able to take steps necessary to put in place safeguards to protect maritime port infrastructure and the MTS. There is also a fundamental need for global leadership to champion the importance and urgency of MTS cyber security, as part of a broader global effort tackling the global cyber security challenge.

About the Author

John Filitz is a Researcher with Stable Seas, a program of the One Earth Future Foundation. His experience includes policy development, institutional development, and research on varied topics and in multiple jurisdictions. John led the development of the Africa: Illicit Trade component of the Stable Seas program's Maritime Security Index. His current research centers on transnational organized crime and cyber security in the maritime sector with a focus on maritime port governance. He holds a Master's degree in Development Studies and a Bachelor's degree in Political Science and Economic History, both from the University of KwaZulu-Natal, South Africa. John is currently studying towards a Master of Science in Information Assurance at Regis University.

[4] Although efforts by the United Nations' International Maritime Organization such as its adoption of Resolution MSC.428 (98) on Maritime Cyber Risk Management in Safety Management Systems are to be commended, there is a need for a more wide-ranging effort to improve maritime cybersecurity governance.

References

[1] IMO (International Maritime Organization). Retrieved from https://business.un.org/en/entities/13

[2] Government Accountability Office. (2015). Maritime Critical Infrastructure Protection. Government Accountability Office, 16-116T. Retrieved from https://www.gao.gov/assets/680/672973.pdf

[3] Ericsson. (2018). The connected future: Internet of Things forecast. Ericsson. Retrieved from https://www.ericsson.com/en/mobility-report/internet-of-things-forecast

[4] UNCTAD. Review of Maritime Transport. United Nations Conference on Trade and Development. Retrieved fromhttps://unctad.org/en/PublicationsLibrary/rmt2017_en.pdf

[5] Jones Walker LLP (2018). Maritime Cybersecurity Survey. Jones Walker LLP. Retrieved from https://www.joneswalker.com/insights/jones-walker-llp-releases-inaugural-maritime-cybersecurity-survey.html

[6] MAREX. (2018, September 27). Port of San Diego Hit by Cyberattack. Maritime Executive. Retrieved from https://www.maritime-executive.com/article/port-of-san-diego-hit-by-cyberattack

[7] AlDairi, A., & Tawalbeh, L. (2017). Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. Procedia Computer Science, 109C, 086-1091. DOI: https://doi.org/10.1016/j.procs.2017.05.391

[8] Abu-Nimeh, S., Foo, E., Fovino, I.N., Govindarasu M. & Morris, T. Cyber security of networked critical infrastructures. IEEE Network, 27(1), 3-4. DOI: 10.1109/MNET.2013.6423184

[9] SIM-CI. (2017, December 22). 'Cyber security of critical infrastructures at risk.' SIM-CI. Retrieved from https://www.sim-ci.com/cyber/cyber-security-critical-infrastructures/

[10] Powers, S. (2013). The Threat of Cyberterrorism to Critical Infrastructure. E-International Relations Students. Retrieved from http://www.e-ir.info/2013/09/02/the-threat-of-cyberterrorism-to-critical-infrastructure/

[11] Collins, S. & McCombie, S. (2012). Stuxnet: the emergence of a new cyber weapon and its implications. Journal of Policing, Intelligence and Counter Terrorism, 7(1). DOI: 10.1080/18335330.2012.653198

[12] Defense Use Case. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. Electricity Information Sharing and Analysis Center. Retrieved from https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

[13] Defense Use Case. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. Electricity Information Sharing and Analysis Center. Retrieved from https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

[14] Abu-Nimeh, S., Foo, E., Fovino, I.N., Govindarasu M. & Morris, T. Cyber security of networked critical infrastructures. IEEE Network, 27(1), 3-4. DOI: 10.1109/MNET.2013.6423184

[15] Leyden, J. (2014). Drug gang hacks into Belgian seaport, cops seize TONNE of smack. The Register. Retrieved from https://www.theregister.co.uk/2013/06/18/drug_smugglers_using_hackers/

[16] Data breach digest: Scenarios from the field. Verizon. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf

[17] Drzik, J. (2018). Cyber risk is a growing challenge. So how can we prepare?.' World Economic Forum. Retrieved from https://www.weforum.org/agenda/2018/01/our-exposure-to-cyberattacks-is-growing-we-need-to-become-cyber-risk-ready

[18] FireEye. Advanced Persistent Threat Groups. FireEye. Retrieved from https://www.fireeye.com/current-threats/apt-groups.html

[19] Powers, S. (2013). The Threat of Cyberterrorism to Critical Infrastructure. E-International Relations Students. Retrieved from http://www.e-ir.info/2013/09/02/the-threat-of-cyberterrorism-to-critical-infrastructure/

[20] Powers, S. (2013). The Threat of Cyberterrorism to Critical Infrastructure. E-International Relations Students. Retrieved from http://www.e-ir.info/2013/09/02/the-threat-of-cyberterrorism-to-critical-infrastructure/Ibid

[21] Greenberg, A. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. WIRED. Retrieved from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[22] Wilbur, J. (2018). 'The Cyber Incident Tsunami - Time to Get Ready.' Online Trust Alliance. Retrieved from https://otalliance.org/blog/cyber-incident-tsunami-time-get-ready

[23] Thakur, K. Ali, M.L., Jiang, N. & Qiu, M. (2016). Impact of Cyber-Attacks on Critical Infrastructure. 2016 IEEE 2nd International Conference on Big Data Security on Cloud, IEEE International Conference on High Performance and Smart Computing, and IEEE International Conference on Intelligent Data and Security, New York, 183-186. DOI: 10.1109/BigDataSecurity-HPSC-IDS.2016.22

[24] Ismail, S., Sitnikova, E. & Slay, J. (2015). Studying SCADA Organisations Information Security Goals: An Integrated System Theory Approach. Association for Information Systems. Retrieved from https://aisel.aisnet.org/pacis2015/77/

[25] National Institute of Standards and Technology (NIST). (2018). Cyber Security Framework version 1.1. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[26] Ahn, W., Chung, M., Min, B-G., & Seo. (2015). Development of Cyber-Attack Scenarios for Nuclear Power Plants Using Scenario Graphs. International Journal of Distributed Sensor Networks. DOI: http://dx.doi.org/10.1155/2015/836258

[27] UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. United Nations. Retrieved from https://dig.watch/processes/ungge

[28] Greenberg, A. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. WIRED. Retrieved from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

ADVERSARIAL MACHINE LEARNING AND ITS IMPLICATIONS FOR MARITIME SURVEILLANCE FROM SPACE

Christopher R. Ratto, Ph.D. and I-Jeng Wang, Ph.D., The Johns Hopkins University Applied Physics Laboratory, Laurel, MD

The practice of denial and deception (D&D) has a long history in modern warfare. D&D techniques add uncertainty to products of intelligence, surveillance, and reconnaissance (ISR) through the use of decoys, camouflage, spoofing/jamming, and overflight warnings. The particular tactics range from the very primitive (e.g. inflatable decoys) to the very sophisticated (e.g. radar signature reduction). The Navy has long practiced D&D in the design of surface ships, perhaps most famously through the development of “dazzle” paint schemes during the First World War (Figure 1). While varied in their exact approach, the myriad D&D techniques have the common goal of fooling the senses, whether they be human or artificial.

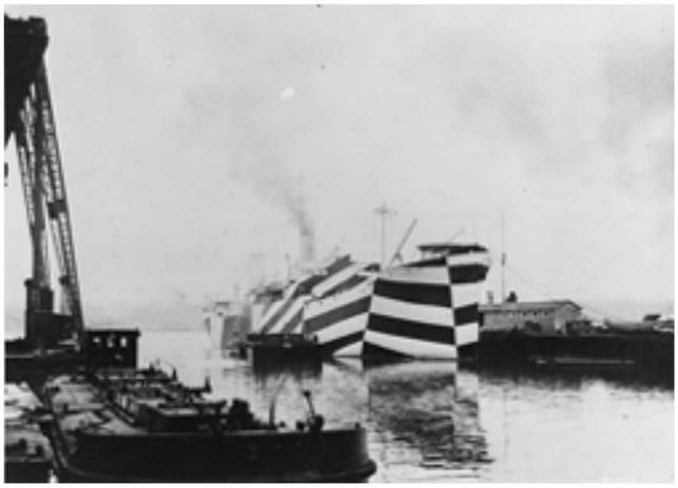


Figure 1. A 1918 photograph of the USS West Mahomet (ID-3681) in port, painted with a dazzle camouflage pattern to distort the appearance of her bow.

Currently, the world is experiencing revolutions in artificial intelligence (AI) and space-based surveillance, and D&D practices have not yet caught up to the technology landscape. The global AI revolution is being driven primarily by advances in deep learning, which itself is made possible by the combination of artificial neural networks, big data, and graphical processing units (GPUs).

While artificial neural networks were initially developed in the mid-20th century as a highly nonlinear model for statistical decision-making, it was not until the advent of convolutional neural networks (CNNs) that they became generally useful for computer vision. Unlike traditional pattern recognition, in which a regression of classification model is fit to hand-engineered features, CNNs enable algorithms to automatically learn which features are relevant to the problem at hand. In order to do so, CNNs require very large data sets to learn from (e.g. millions of labeled images). In the era of big data, such data sets are in abundance for a variety of applications. Finally, GPUs enable CNNs to extract features from images at much faster speeds than standard CPUs, which allows for quick algorithm training and decision-making at real-time speeds. The combination of neural networks, big data, and GPUs enabled AI to advance beyond human-level performance on tasks such as image classification [1] and strategy games [2].

Much of the revolution in big data has come from the proliferation of sensors, including those in space. The private sector has tapped into a burgeoning market for satellite imagery and analytics driven by industry demands (including, but not limited to, agriculture, energy, insurance, and finance, as well as government interests). Between 2006 and 2015, a total of 163 electro-optic (EO) imaging satellites have been launched by private companies from 35 countries. Over the next decade, over 400 satellites greater than 50 kg are expected to be launched, and far more small satellites (< 50 kg) could be launched as well. By 2025, the market for commercial EO data is expected to reach $3 billion, with an additional $5.3 billion for additional services such as analytics [3].

The proliferation of Earth-observing satellites coupled with deep learning AI will drive new technological development in D&D for maritime surveillance. Much of this development will emerge from the field of adversarial machine learning (AML), which is the practice of teaching AI to fool another AI. In other domains, AML is being used to develop camouflages and decoys with the purpose of spoofing a deep learning algorithm that processes visual information. Conversely, the AML field is also developing counter-countermeasures to make deep learning more robust to spoofing attacks. We encourage the Navy and Intelligence Communities to follow developments in this area very closely and recommend that programs be initiated to investigate AML specifically for maritime surveillance applications.

Adversarial Machine Learning

AML techniques exploit the notion that CNNs are sensitive to perturbations in the input space that significantly affect the performance of the feature extraction layers. Many studies have demonstrated that subtle perturbations to an image can not only fool a CNN, but the perturbation can be designed to achieve a desired effect [4, 5]. For example, an image of a school bus is perturbed in a visually-imperceptible manner that causes a state-of-the-art DNN to misclassify it as "ostrich" with high confidence (Figure 2). The perturbed image is known as an adversarial example (AE). In [4, 5], AEs were designed with little constraint – any number of pixels in an image could be modified to take on any [R, G, B] value, provided the total perturbation to the image (measured by the l∞-norm) was below a prescribed level to make the perturbation imperceptible to the human eye. In [6], AEs were constrained so that at most N pixels are perturbed. Among those

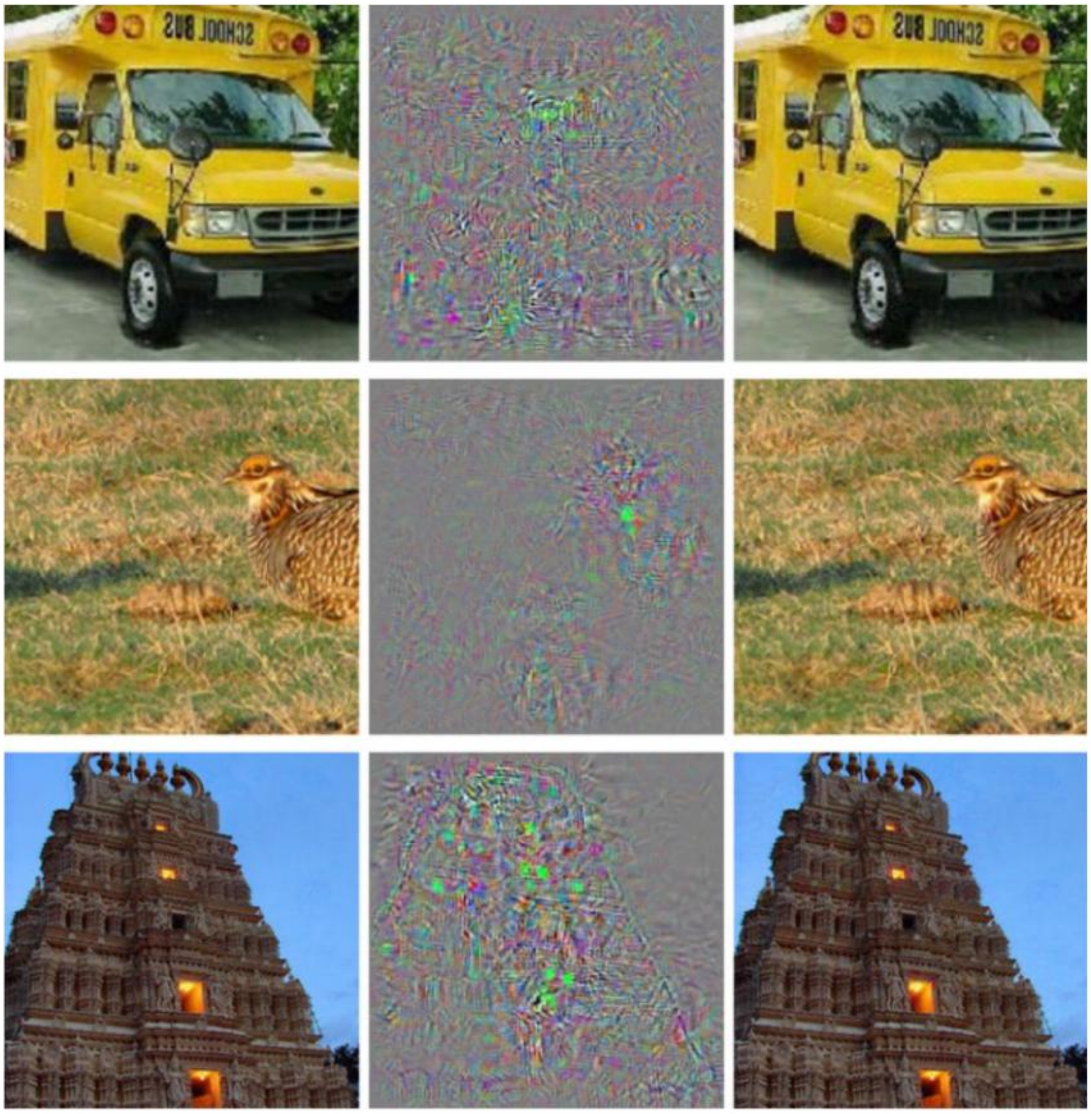


Figure 2. Original image (left column), perturbation added to image (center column), and the resultant adversarial example (right). All three adversarial examples are classified by AlexNet as "ostrich, Struthio camelus." Image originally published in [4].

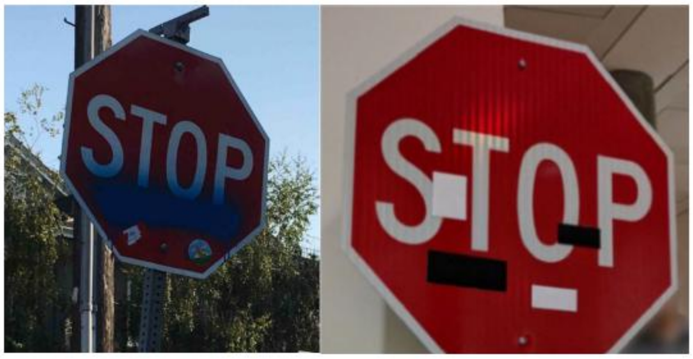


Figure 3. Stop sign with typical graffiti (left), and with AML-designed modifications to cause a CNN to misclassify it as "Speed Limit 45" sign (right). Image originally published in [8].

demonstrated were extremely subtle attacks, even as subtle as a single pixel, with the ability to fool a CNN classifier.

Most work in AML to date has focused on "digital" perturbations to the CNN input, e.g. altering [R, G, B] values of pixels in an image. Developing AML for practical sensing applications (including D&D) will require developing a better understanding of how adversarial perturbations can be manifested in the physical domain. This problem was introduced in [7], in which digital AEs were printed and tested with a camera. Unlike the "digital" domain, physical AML involves designing perturbations to the physical characteristics of an object in order to fool a CNN applied to some sensor. Physical AEs have only been explored in a few small-scale use cases. In [8], physical adversarial perturbations were learned for stop signs in the form of optimally-placed and colored stickers. The stickers were shown to cause a CNN to misclassify the stop sign as a "Speed Limit 45" sign under a variety of lighting conditions and viewing geometries (Figure 3). Similarly, in [9], an "adversarial patch" was designed that could be printed and placed on any object to fool a CNN (Figure 4). While robust to a variety of imaging conditions, the physical AEs developed in [8, 9] are overt and may cause suspicion if encountered in the real world. A more covert approach was taken in [10], where models of small objects were 3-D printed with built-in adversarial perturbations to confuse a CNN at a variety of poses.

These results are promising for the development of AML-driven D&D, and begs the question

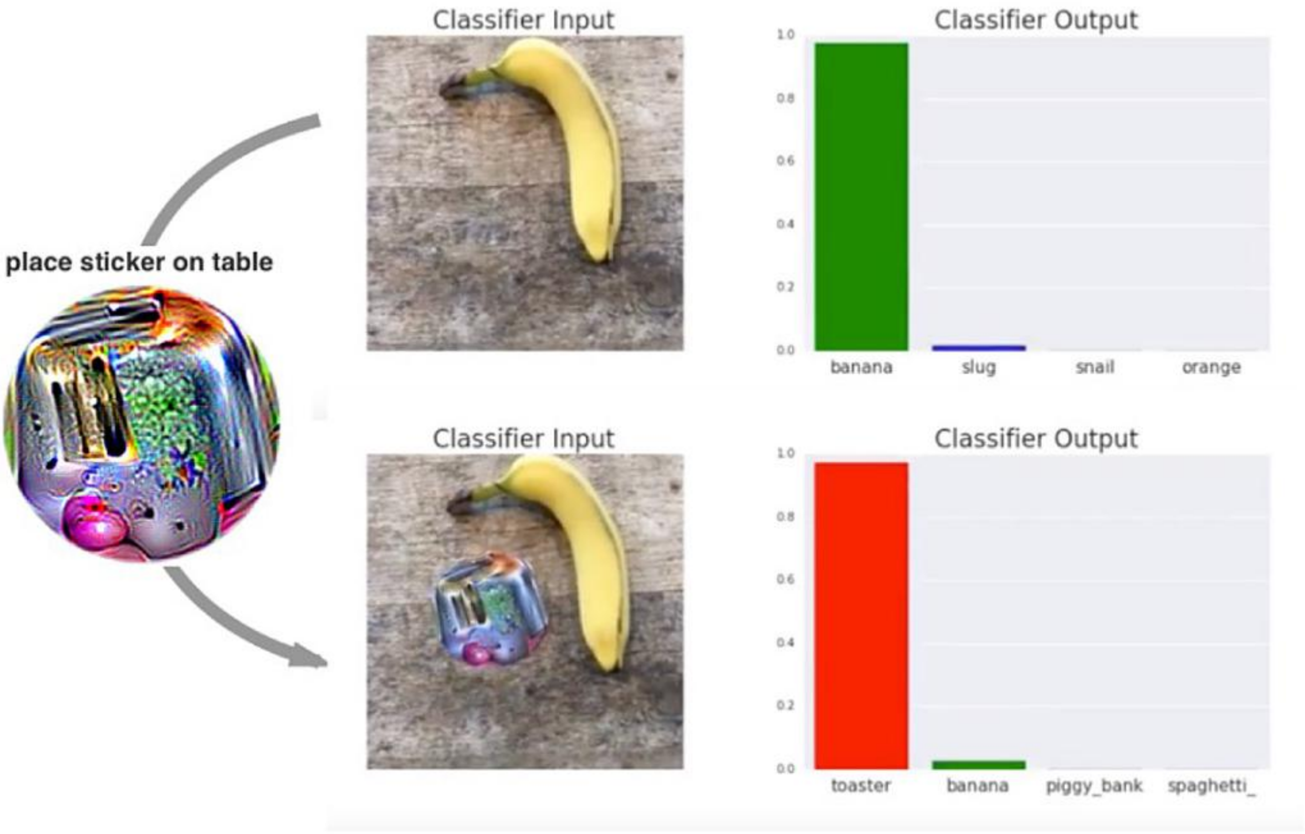


Figure 4. Image of a banana correctly being classified by a CNN (top) and misclassified as a "toaster" when an adversarial patch is placed next to it (bottom). Image originally published in [9].

of whether AEs can be designed on a larger scale and have the same effect on satellite image classifiers. In FY18, the Johns Hopkins University Applied Physics Laboratory (JHU/APL) considered the problem of whether physical AEs were achievable for large objects (e.g. buildings) observed in satellite imagery [11]. This work leveraged the Functional Map of the World (fMoW) data set, which was curated by JHU/APL in support of an IARPA challenge that was conducted in the same year [12]. The fMoW data set consisted of over 1 million commercial satellite images of 63 different land use classes (various types of buildings, facilities, roads, and other infrastructure) collected from over 200 different countries. Unlike more common datasets used in computer vision research, such as ImageNet [13], the fMoW data set includes geolocation and ephemeris metadata as well multiple views of the same target that can supplement the information contained in the images' pixels. In [11], JHU/APL demonstrated that adversarial patches can be learned from the fMoW data with physical constraints such as adhering to the size of a roof and adjusting pixel brightness based on the presence of shadows. It was successfully demonstrated that adversarial patches with realistic constraints can cause targeted misclassification of specific land use classes. Future work will more explicitly account for the three-dimensional structure of scenes and extend AML to other sensing modalities, such as synthetic aperture radar (SAR) and hyperspectral imaging.

Improving Robustness To Adversarial Examples

Given the reality that AML can design patterns that can reliably fool a CNN, the research community has made significant progress towards improving the robustness of CNNs to adversarial attacks. In 2017, the Advances in Neural Information Processing Systems (NIPS) conference conducted an Adversarial Attacks and Defenses Competition in which researchers competed against one another to develop AEs (i.e. "attacks") and CNNs resistant to those patterns (i.e. "defenses") [14]. The competition was necessary towards advancing the community's understand of AML because it provided a means of analyzing an open-ended problem. A successful defense has to provide a CNN robust to AEs coming from an unknown data-generating process. Meanwhile, a successful attack would need to be developed with limited knowledge of the targeted CNN. A white-box attack can be developed with full knowledge of the CNN's architecture and feature sensitivities, but such a scenario is unlikely in real-world situations. Note that all of the AML techniques discussed in the previous section are considered white-box attacks. The black-box attack scenario is more likely, in which no prior information about the target CNN is available. The NIPS competition pitted developers of adversarial attacks against defenses in a black-box scenario to reflect conditions most likely encountered in the real world. The data set used for evaluating performance was selected to be compatible with ImageNet, but was not shared with the developers.

The results of the NIPS competition were based upon the average performance of each defense against all attacks, and vice versa. Much insight was gained regarding best practices for improving the robustness of a CNN against AEs in a black-box scenario. The first-place winning defense, developed by a team of Chinese researchers, was a neural-network based denoising autoencoder that preprocessed the imagery before passing it on to a CNN for classification [15]. It is noteworthy that the same team also developed the first-place winning attack strategy. The attack was an improvement to the fast gradient sign method (FGSM) originally developed in [4], but applied to an ensemble of CNNs rather than just attacking one. The ensemble of methods included several variations on the Inception [16] and ResNet [17] CNNs (the best performing networks on ImageNet) trained with and without adversarial examples, and their decisions were fused together to produce a final class prediction.

More insights into how to design CNNs with improved robustness to AEs can be gained from the runners-up to the defense competition. The second-place defense, developed by an international collaboration of private sector and academic researchers, used randomization in an attempt to destroy the structure of an adversarial pattern. An additional layer was added to the early stages of the CNN that randomly resized and padded the input image prior to feature extraction. The CNN was then trained using adversarial examples. The fourth-place finisher in the defense competition, a Kazakh researcher, also used preprocessing to remove the adversarial pattern;

he first used spatial smoothing followed by a fusion ensemble of different CNN architectures trained using adversarial examples.

The results of the 2017 NIPS Adversarial Attacks and Defenses Competition highlighted approaches for AML in a black-box scenario most reflective of real-world conditions. Successful attacks utilized an ensemble approach, in which adversarial examples were developed to have transferability (i.e., the ability to successfully attack) across a variety of CNN architectures. For defenses, successful approaches used a combination of denoising and adversarial training. Denoising could be accomplished through an autoencoder network, randomization, and/or filtering, and then the CNN should be learned with adversarial examples included in the training set.

Implications For Maritime Surveillance

With the progress made in AML in recent years, the Navy and Intelligence Communities stand to benefit from its advances in developing novel D&D tactics, especially with regard to remote sensing satellites flown by foreign governments or commercial entities. The widespread proliferation of sensors and deluge of imagery expected to be produced by them will necessitate AI, of which deep learning will play a significant part, to sift through the volumes of data and find the entities of interest to the consumer. The threat of automated satellite image collection and exploitation must be considered when developing the next generation of Naval countermeasures and D&D tactics. For example, combatant ships or sensitive facilities could be painted or actively illuminated with a pattern designed using AML in order to fool an ensemble of CNNs likely to be applied to satellite imagery.

The research community has made significant progress towards this envisioned future by developing physical adversarial examples. However, to date they mostly have been demonstrated in controlled conditions on a small scale. In order to be of utility for D&D, adversarial perturbations must be able to fool a CNN under a variety of environmental conditions (including weather and lighting) as well as viewing geometries (near-nadir as well as oblique angles). Continued research is needed to determine whether the physical adversarial examples proposed in the literature are indeed robust under such variations. Where the limits of performance are also a focus of continue research. Furthermore, the task of building physical adversarial examples at large scale (e.g. the size of a naval ship) will involve a multitude of design trades that the research community have not yet considered. These may include cost, covertness, degradation over time, materials, etc. Any development of large scale adversarial examples will require a trade study to determine whether the development is both feasible and economical. Such a trade study is not likely to be undertaken by the academic research community, but is well suited for government laboratories, federally-funded research and development centers (FFRDCs), university-affiliated research centers (UARCs), and not-for-profit think tanks to pursue.

Meanwhile, the Navy and Intelligence Communities should focus on developing safeguards to ensure that their own collection and exploitation capabilities employing AI are robust to adversarial attacks. While physical adversarial examples, especially ship-sized ones robust to the multitude of factors at play in remote sensing, will not be realized for several years, digital attacks may still be possible through cyber vulnerabilities. One of the key takeaways from the NIPS competition is that preprocessing followed by an adversarially-trained CNN is a promising recipe for robustness. With several Navy and intelligence community programs having already developed CNNs for classifying known patterns in satellite imagery, future acquisition programs should consider imposing a requirement that algorithms include some degree of adversarial training and be subject to robustness tests against adversarial examples.

References

[1] A. Krizhevsky, I. Sutskever and G. E. and Hinton, “ImageNet classification with deep convolutional neural networks,” in Advances in Neural Information Processing Systems, 2012.

[2] D. Silver et al.,, “Mastering the game of Go with deep neural networks and tree search,” Nature, vol. 529, p. 484, January 2016.

[3] G. Denis et al.,, “Towards disruptions in Earth observation? New Earth Observation systems and markets evolution: Possible scenarios and impacts,” Acta Astronautica, vol. 137, pp. 415-433, 2017.

[4] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow and R. Fergus, “Intriguing properties of neural networks,” arXiv:1412.6199 [cs.CV], 2014.

[5] A. Nguyen, J. Yosinski and J. Clune, “Deep neural networks are easily fooled: high confidence predictions for unrecognizable images,” in Computer Vision and Pattern Recognition, 2015.

[6] J. Su, D. V. Vargas and K. Sakurai, “One pixel attack for fooling deep networks,” arXiv:1710.0886 [cs.LG], 2018.

[7] A. Kurakin, I. Goodfellow and S. Bengio, “Adversarial examples in the physical world,” in International Conference on Learning Representations, 2017.

[8] K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, C. Xiao, A. Prakas, T. Kohno and D. Song, “Robust physical-world attacks on deep learning visual classification,” in Computer Vision and Pattern Recognition, 2018.

[9] T. B. Brown, D. Mané, A. Roy, M. Abadi and J. Gilmer, “Adversarial patch,” in Neural Information Processing Systems, 2018.

[10] A. Athalye, L. Engstrom, A. Ilyas and K. Kwok, “Synthesizing Robust Adversarial Examples,” in International Conference on Machine Learning, 2018.

[11] W. Czaja, N. Fendley, M. Pekala, C. Ratto and I.-J. Wang, “Adversarial examples in remote sensing,” in ACM SIGSPATIAL, 2018.

[12] G. Christie, N. Fendley, J. Wilson and R. Mukherjee, “Functional Map of the World,” in Computer Vision and Pattern Recognition, Salt Lake City, 2018.

[13] Jia Deng et al., “ImageNet: A large-scale hierarchical image database,” in Computer Vision and Pattern Recognition, Miami, 2009.

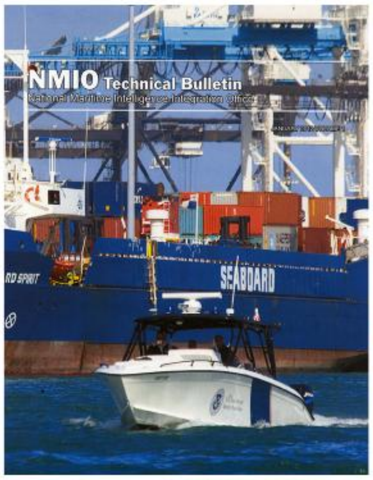
[14] A. Kurakin et al., “Adversarial Attacks and Defences Competition,” arXiv:1804.00097 [cs.CV], 31 March 2018.

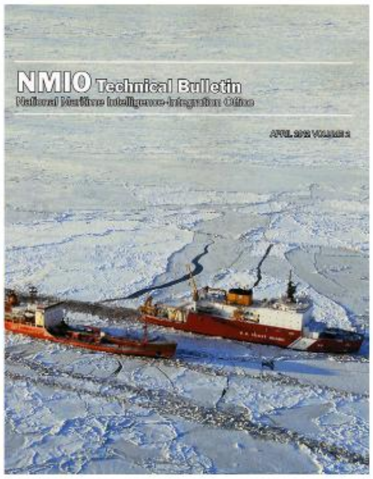
[15] Fangzhou Liao et al., “Defense against Adversarial Attacks Using High-Level Representation Guided Denoiser,” arXiv:1712.02976 [cs.CV], 8 May 2018.

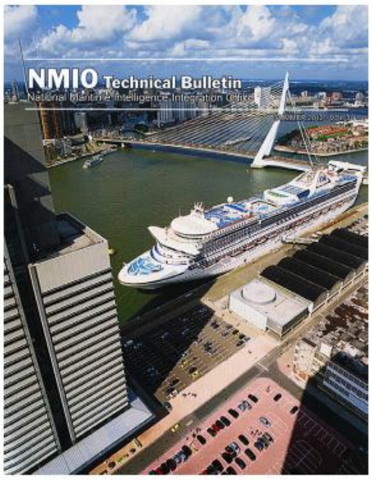
[16] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens and Z. Wojina, “Rethinking the Inception Architecture for Computer Vision,” in Computer Vision and Pattern Recognition, Las Vegas, 2016.

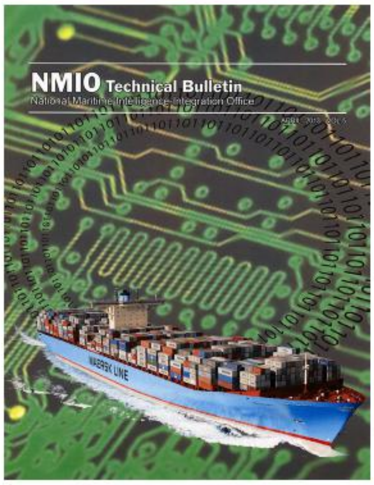
[17] K. He, X. Zhang, S. Ren and J. Sun, “Deep Residual Learning for Image Recognition,” in Computer VIsion and Pattern Recognition, Las Vegas, 2016.

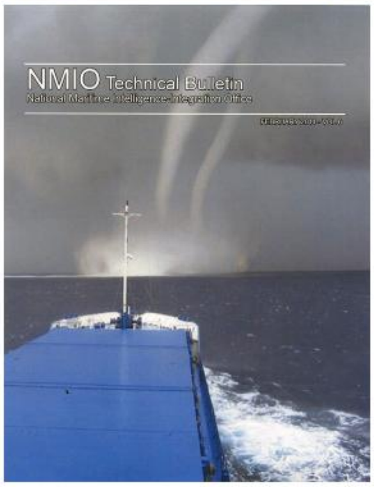
NMIO Technical Bulletin

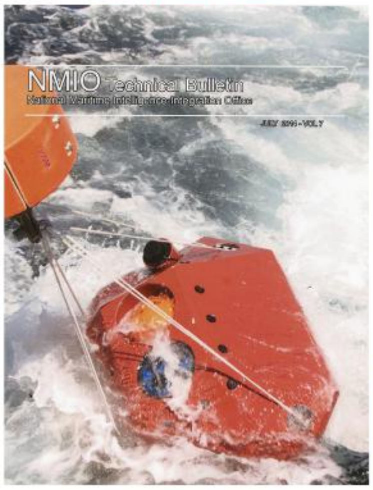


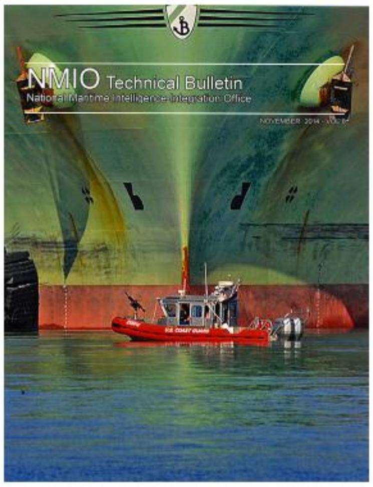


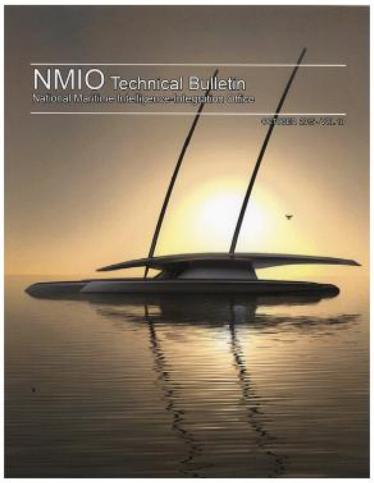


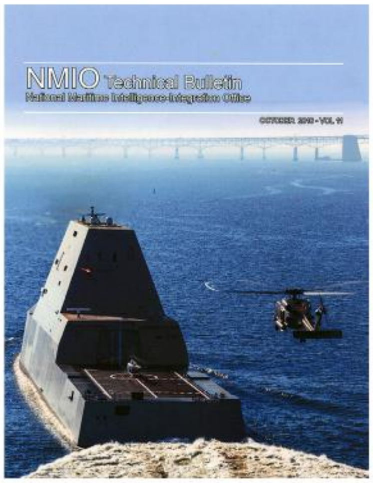


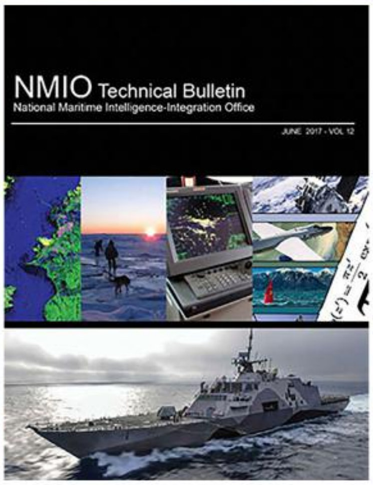












Previous editions of the NMIO Technical Bulletin can be found at:
http://nmio.ise.gov/media/techbulletin/

NATIONAL MARITIME INTELLIGENCE-INTEGRATION OFFICE
Collaboration
Unity of Effort
UNITED STATES OF AMERICA