Global Maritime Forum

REPORT ON THE WORKSHOP

Challenges and Opportunities of Current & Emergent Maritime Capabilities: Exploring the Intersection of Technology and Policy

University of Washington
Seattle, Washington
15-16 November 2016

Global Maritime Forum Workshop

Challenges and Opportunities of Current & Emergent Maritime Capabilities: Exploring the Intersection of Technology and Policy

Report on the workshop jointly sponsored by
The National Maritime Intelligence-Integration Office (NMIO),
Applied Physics Laboratory and
the Center for Collaborative Systems for Security, Safety and Regional Resilience (CoSSaR) at the University of Washington

This report summarizes the presentations of the 2016 GMF workshop as interpreted by Ms. Mekisha Marshall, Chief Science & Technology Advisor, NMIO, and Dr. Mark Haselkorn, Dr. Sonia Savelli, and Ms. Sarah Yancey, CoSSaR at the University of Washington.

The conference adheres to a variation of the Chatham House Rule. Accordingly, beyond the points expressed in the presentations, no attributions have been included in this conference report.

15-16 November 2016
Seattle, Washington

Contents

I. Executive Summary

The National Maritime Intelligence-Integrations Office (NMIO) held its annual Global Maritime Forum (GMF) for 2016, with support by the Applied Physics Lab (APL) at the University of Washington (UW), bringing together a diverse group of experts and senior practitioners. The 2016 theme was *"Challenges and Opportunities of Current & Emergent Maritime Capabilities: Exploring the Intersection of Technology and Policy."* Led by Rear Admiral (RADM) Robert Sharp, Director, NMIO, the forum explored opportunities and strategies for enhancing the security, safety, and protection of the maritime domain. Discussion focused on the intersection of technology and policy in the context of emergent technologies, enhanced satellite capabilities, and enterprise systems for information sharing and safeguarding. The result of the GMF was a compelling call to move forward with a strategic approach that puts mission at the center of technology innovation, while integrating policy and other non-technical issues throughout the design, development, and use phases. Six interconnected themes or "tensions" emerged from the GMF presentations and discussions. These are:

(1) Balancing the risk of sharing information (cybersecurity) with the risk of not sharing information (operational effectiveness)
(2) Reliance on formal information security mechanisms versus common use of informal trust relationships and shared experiences
(3) Aligning commercial innovation interests with government and public innovation interests
(4) Integrating bottom up (local) perspectives with top down (Federal) perspectives
(5) Transitioning from technology-centric innovation to mission and policy-centric innovation
(6) Balancing big data aggregate analytics with contextual, specific ground truth approaches

Participant breakout groups met daily to evolve these themes into proposals for moving forward that were presented in the final forum session. Twelve plans were presented (see Section IV below) and were grouped into six "action plans." These action plans can provide roadmaps for moving forward, providing opportunities for future projects for the Global Maritime Community of Interest (GMCOI).

Action Plan #1: Bring together cybersecurity experts and operational mission experts to design information systems that support multi-agency security and safety operations, balancing the risk of sharing data and information with the risk of not sharing.

Action Plan #2: Avoid technology outpacing policy by exploring the effect of private unmanned underwater vehicles (UUVs) on maritime security operations.

Action Plan #3: Select a region and work with stakeholders to enhance the security of the information-sharing environment (ISE) through policy sensitive, mission-based technology innovation.

Action Plan #4: Foster trust-based security networks and information sharing environments by capturing existing information sharing relationships and using them to create a user-defined, trust-based entitlement security layer that supports how the community of security operational professionals actually works.

Action Plan #5: Leverage increased commercial satellite capabilities to help meet national security needs by defining policy and incentive structures that would provide benefit to commercial partners as well as government agencies, military commands and intelligence analysts.

Action Plan #6: Develop a highly reliable crowd-sourced alert system by leveraging the potential role of local, highly reliable domain expert public sources.

II. Introduction & Background

Theme & Goals

The overarching theme of the 2016 GMF was "Challenges and Opportunities of Current and Emergent Maritime Capabilities: Exploring the Intersection of Technology and Policy." With this theme in mind, the forum brought together experts and dedicated allied professionals to forge a greater understanding of how continued advancements of emergent technologies can best be integrated into mission accomplishment within the maritime domain. This goal was supported by focusing on legal, policy, and mission implications of technology innovation that both pose challenges to effective impact of innovation and create opportunities for enhanced collaborative partnerships.

Participant Information

Forum participants represented a wide array of backgrounds, including government (57%), industry (23%), academia (16%) and other (4%). Further, participation included international attendees from Canada, Czech Republic, Italy, Japan, Norway, and the United Kingdom (see Appendix A for a list of attendees).

Photo 1: Global Maritime Forum Workshop 2016.

The next section presents the central findings generated by keynote and introductory speaker presentations, panel sessions and discussions, and collaborative breakout working group discussions and presentations.

Forum Approach

During the two-day forum, each day began with keynote speakers and panel presentations, which were then followed by collaborative breakout sessions (see Appendix B for Agenda). During Day One of the forum, panel presentations highlighted available and emergent maritime capabilities and cyber innovations that create opportunities, but also posed policy and other non-technical challenges. Day One concluded with a reception at the Burke Museum on the UW campus, which stimulated numerous informal discussions and participant interactions. Day Two presentations focused on legal and policy implications of technology innovations for improved information sharing and safeguarding for enhanced maritime security and domain awareness.

The collaborative breakout sessions provided a structure for analyzing and addressing the challenges identified during the forum, such as enhanced mission accomplishment, the future role of unmanned underwater vehicles (UUV), integrated

space-based capabilities, achieving cybersecurity, promoting technological innovation for maritime domain awareness (MDA), and improved information sharing environments (e.g., for Arctic Domain Awareness).

Workshop Welcome Address

RADM Robert Sharp, Director, NMIO, hosted the 2016 GMF with support from the UW Applied Physics Lab (APL) and the Center for Collaborative Systems for Security, Safety and Regional Resilience (CoSSaR). RADM Sharp opened the forum by detailing NMIO's strategic objectives. He emphasized the importance of engaging academia, think tanks, industry, and international partners to understand the implications of emergent technology, whether innovation introduces new threats or offers new opportunities to improve security. Further, RADM Sharp addressed the ongoing need for collective and collaborative security approaches, and highlighted the fact that threats are not just "local," but are also cross-regional, national, and global. RADM Sharp pointed out that the 2016 GMF is built upon strong forums in years past, and that this year's forum is composed of a passionate group of representatives from diverse fields and backgrounds (industry, academia, government, and international partners), forming a collective group that is optimal for addressing maritime domain awareness (MDA) issues. He further echoed the importance of continually developing and maintaining a cohesive security-focused network, limited only by our imagination and our willingness to create connections and partnerships, to effectively defeat threat networks. RADM Sharp hoped that this year's forum would promote the optimal use of emergent technologies to solve common concerns and challenges. The Admiral recognized the 2016 forum as a platform to support the ongoing construction of such a security-focused collaborative network, and as an opportunity to strategize and commit to people-based partnerships for combatting threats.

Photo 2: RADM Robert Sharp.

The remainder of this report details the central findings that emerged during the keynote and panel presentations/discussions; the proposals for addressing critical and emergent maritime security issues identified as most compelling by the collaborative breakout session working groups; and plans for a path forward in response to RADM Sharp's charge to forum participants.

III. Central Findings

Given this year's GMF theme of integrating technology and policy innovation, it is not surprising that central findings emerged that involved competing perspectives and tensions in addressing critical and evolving security issues. In his keynote address, ***Professor Lewis Shepherd*** of *George Mason University* discussed the early and ongoing role of high-tech industry and academia in the evolving effort, led and funded by the Federal government, to employ innovative research and development to enhance national security. Professor Shepherd identified a number of benefits and tensions that stemmed from this partnership, and he highlighted the role of technology policy in this evolution.

As GMF presentations and discussions progressed over two days, there was general agreement that appropriately balancing competing perspectives and tensions would have a major positive effect on the design, development, and implementation of current and future capabilities for enhancing maritime security and domain awareness. The tensions highlighted included:

(1) Balancing the risk of sharing information (cybersecurity) versus the risk of not sharing information (operational effectiveness);
(2) Reliance on formal information security mechanisms versus the common use of informal trust relationships and experiences;
(3) Aligning commercial innovation interests with government and public innovation interests;
(4) Integrating bottom up (local) perspectives with top down (Federal) perspectives;
(5) Transitioning from technology-centric innovation towards mission- and policy-centric innovation; and
(6) Balancing big data aggregate analytics with contextual, specific ground truth approaches.

These tensions, and GMF activities that explored them, are described below.

(1) Balancing the risk of sharing information (cybersecurity) versus the risk of not sharing information (operational effectiveness)

An inherent tension exists between the dual goals of sharing critical information and simultaneously safeguarding it. While increased transparency and coordination that result from information sharing provides critical mission benefits, cybersecurity concerns are often seen as outweighing these benefits. One of the tensions discussed throughout the two days of the GMF was balancing between sharing information with those who have a need to know, while safeguarding it from those who could use it with the intent to do harm.

Presentations and discussion on regional and national security and safety operations, led by field professionals from operational agencies such as the Royal Canadian Mounted Police (RCMP), United States Coast Guard (USCG), and United States Custom and Border Protection (CBP), emphasized the need to enhance the sharing of data and information with the right people in a timely manner to support collaboration during complex field missions. During Panel Session IV, for example, ***Mr. Shawn McDonald****, Program Manager, Borders & Maritime Security Division, Department of Homeland Security (DHS) Science & Technology (S&T),* spoke of (DHS) efforts to enable decision makers by providing them with the mechanisms to share information "at the speed of thought." He introduced the Border & Coastal Information System (BACIS) platform that provides wide access to existing Federal, state, local, tribal, international, public, and private (FSLTIPP) data sources and allows decision makers to translate the data into actionable intelligence. The maritime component of BACIS is the Coastal Surveillance System (CSS). CSS resides on the Integrated Maritime Domain Enterprise (IMDE) architecture that enables unclassified multi-agency information sharing. CSS is a user-defined operational workspace with six operational capabilities (see Figure 1). DHS S&T is currently piloting IMDE/CSS with operators in the Puget Sound, as well as at CBP's Air & Marine Operation Center (AMOC) in Riverside, California.

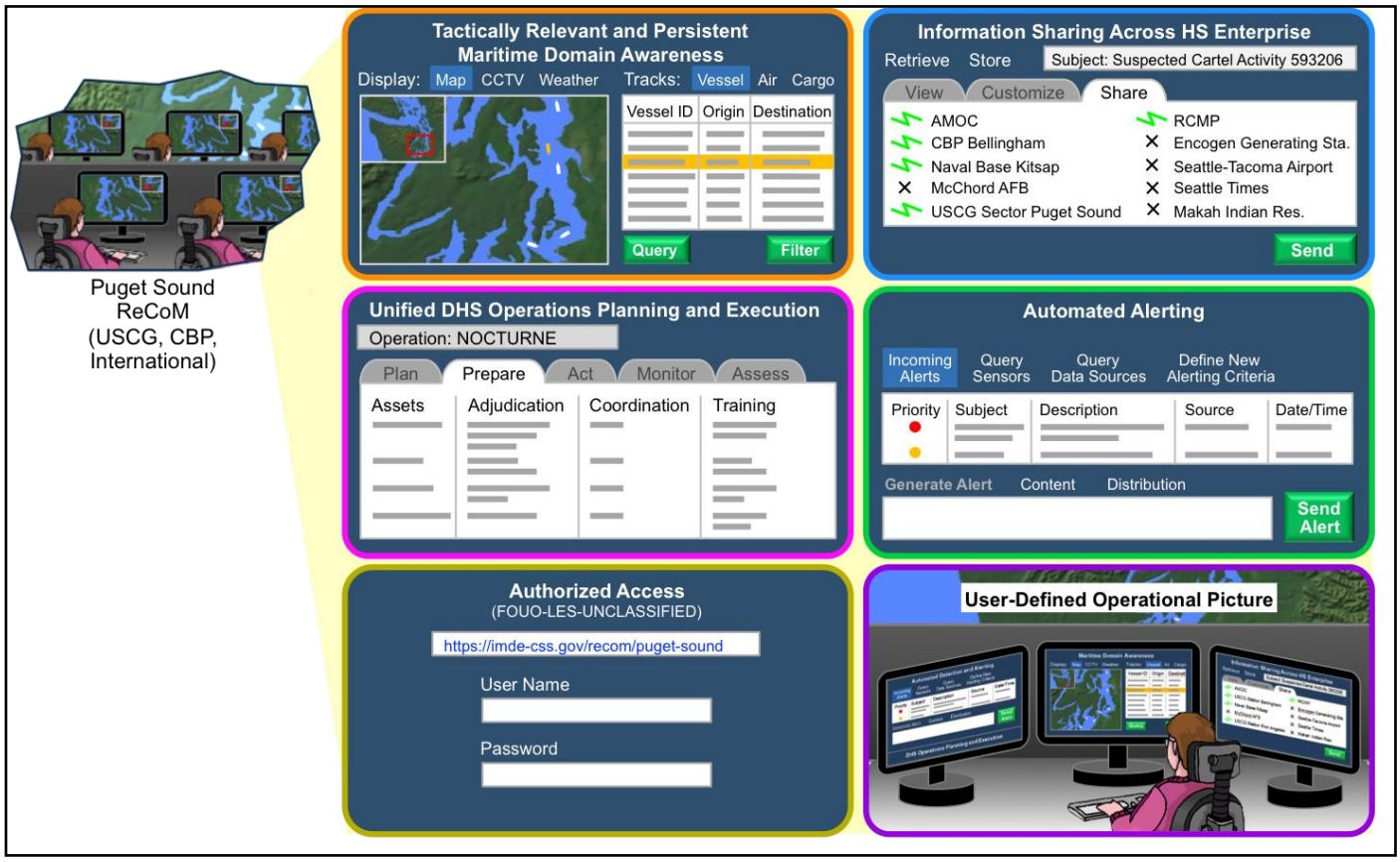

Figure 1: Six Desired Operational Capabilities of IMDE/CSS.

Mr. McDonald also highlighted the sharing/safeguarding tension that exists due to the current DHS policy requirement of a Federal background investigation (BI), even though local agencies have their own background checks and IMDE/CSS is intended to carry unclassified information. He acknowledged that if organizations have to pay for an additional Federal BI, at a cost of $1,500 per individual, then participation in IMDE/CSS would be significantly reduced.

Mr. McDonald also introduced several alternatives to BI, but all had disadvantages. For example, initializing DHS policy change to provide a path to equivalency for state/local BIs would be very helpful; however, the process to determine equivalency for each state/local entity would be time consuming. The time required to change the policy is unknown, and the staffing and justification required would be extensive. S&T proposes using the DHS Homeland Security Information Network (HSIN) to provide user identification and attribute management services. An HSIN community of interest (COI) manager is responsible for vetting the user, ensuring that the user has a demonstrated need, and has the correct attributes assigned for specific COI. This process, together with additional HSIN attributes (e.g., role, sub role, employment organization, assignment organization, protected critical infrastructure information, etc.), will be used to implement the information sharing policies throughout the enterprise and allow users to access specific datasets as defined by the data source owner. However, before the technological aspects of this requirement can be addressed, a policy that defines a common or standard set of attributes must be established that determines user roles and access to data across the FSLTIPP. Mr. McDonald concluded by reminding the audience that policy, not technology, is the major challenge that must be addressed, and that as the technology matures, so too should our policies.

Photo 3: From left to Right- Ms. Braxton, Mr. McDonald and Mr. Wheeler.

Also speaking during Panel Session IV, ***Mr. Sean Wheeler****, Operations Coordinator, Marine Security Operations, Center, Royal Canadian Mounted Police (RCMP),* provided an example of international information sharing of radar data between the United States and Canada. The Canadian province of British Columbia shares over 1,300 miles of international land and maritime border with the States of Washington, Montana, Idaho, and Alaska. To identify, locate, and track maritime threats common to the interests of Canada and the U.S., the RCMP purchased a commercial technology that provides a sensor infrastructure, allowing the Canadians to see small dark vessels in those shared waters. Mr. Wheeler described how the system synthesizes various raw radar tracks and adds map layers that include speed and direction to give a complete overview of the area of interest (AOI). The RCMP shares the synthesized radar data with the CBP and Coast Guard. A new project funded by NMIO is underway to install additional radar feeds, as well as more servers and workstations on the U.S. side to facilitate international information sharing and coordination. Mr. Wheeler discussed how the sharing of this new technology gives rise to the need for new policy, including a Memorandum of Understanding (MOU) that allows law enforcement agencies to share the location of small dark vessels along the joint international AOI.

During his welcome address, ***Captain*** (***CAPT) Joe Raymond****, U.S. Sector Commander, Coast Guard Sector Puget Sound,* emphasized the importance of policy and relationships in tackling maritime security challenges, and referred to joint activities at the U.S. and Canadian border as an example. CAPT Raymond pointed to the Shiprider program as an example of international partners with trusted relationships sharing resources to secure borders from threats to national security. The Shiprider initiative involves vessels, jointly crewed by specially trained and designated U.S and Canadian law enforcement officers that are able to enforce laws on both sides of the international boundary line of U.S. and Canadian shared waterways.

Photo 4: Mr. Johnson and CAPT M. W. (Joe) Raymond. **Photo 5: CAPT Raymond.**

CAPT Raymond cited several other non-technical examples of information sharing, such as the Puget Sound Area Maritime Security Committee (AMSC) that brings government, tribes, academia, and industry together and provides them with a collaborative environment necessary to build these relationships. He ended by emphasizing it is the relationships that develop between people over time that is the necessary ingredient for successful information sharing, not technology alone.

Mr. Nicholas Andersen*, Chief Information Officer, U.S. Naval Intelligence Activity (NIA),* also referred to these themes of sharing and safeguarding information in his introductory presentation on Day Two of the workshop. Mr. Andersen focused on the legal and policy implications of technology innovations to improve sharing and safeguarding of information for enhanced maritime domain awareness. He spoke of the need to strike a balance between sharing information with those who have a need to know while safeguarding it from those who would use it with the intent to do harm. Mr. Andersen stressed that information must be shared in a meaningful way if we are to keep our country safe. However, due to the stringent controls placed on information, sharing cannot be carried out as it is in a commercial environment, and he encouraged that we design our policies to allow the flexibility needed to achieve our information-sharing goal.

Mr. Andersen had several suggestions for creating the balance between sharing and safeguarding, which he described as more of a cultural challenge than a technological challenge. First, he suggested that at the Federal level, we must move away from closed, proprietary systems for sharing information and that we should not allow industry to develop proprietary systems for Federal agencies. Instead we must develop and encourage the development of open systems that take advantage of open architecture standards. Second, he proposed that in order to encourage information exchange, we must find ways and means to reward participation in such sharing. Finally, he said we must find alternatives to quantitative measures of operational success, as this drives people to keep information close, rather than sharing it.

Mr. Andersen also addressed issues of securing our information technology (IT) systems. He introduced a concept called "defense in depth." This is an information assurance (IA) concept in which multiple layers of security controls are placed throughout an IT system. These multiple layers provide redundancy in the event that a particular security control fails or its vulnerability is exploited. Defense in depth is divided into three areas: physical, technical, and administrative. Physical controls are anything that physically limits or prevents access to IT systems, such as placing hardware behind locked or guarded doors. Technical controls are hardware (e.g., fingerprint readers) or software (e.g., encryption) that protects

systems and resources. Administrative controls consist of policies and procedures, and include things such as data handling procedures and data security requirements.

Photo 6: From left to right- Dr. Shapiro, Dr. Koscher, Mr. Greenstein and Mr. Aucsmith.

Panel Session III focused on the other side of the sharing-safeguarding equation -- cybersecurity. Chaired by ***Dr. Paul Shapiro,*** *Professor, National Defense University*, the panel emphasized the need to design systems for the protection of potentially sensitive information, and discussed the challenges to doing this efficiently. Dr. Shapiro spoke of the strategic assessment of cyberspace as involving the three Ps: 1) Possible - from a technological perspective, anything is possible and we are only constrained by the laws of physics; 2) Permissible - what are the constraints we face? (e.g., national or international law); and 3) Preferred - what do we want to achieve? Dr. Shapiro then introduced the three speakers from Panel Session III who shared their insights into what was required to ensure a safe and trustworthy cyberspace.

Dr. Karl Koscher*, Research Scientist, UW*, shared eye-opening research on controlling an automobile, not by gaining physical access, but by gaining entry via wireless interfaces such as Bluetooth, the CD Player, and OnStar. Using these means, researchers were able to exploit vulnerabilities in the vehicle's computer system allowing them to gain control. This demonstration of how easily one could create a cyber weapon from an everyday item without any physical access has drawn the attention of government regulators and Congress. Dr. Koscher pointed out that this was another example of technology innovation outrunning policy and security issues, and that there are currently four bills in Congress to address the automotive threat and patching of vulnerabilities of the Internet of Things (IoT).

Photo 7: Mr. Matijevich.

Photo 8: Dr. Koscher.

Mr. David Aucsmith*, Chief Scientist, root9B and Senior Research Scientist, University of Washington, APL,* spoke about using physical security technologies to secure artifacts. For example, traffic lights have a malfunction management unit (MMU) that sits between the controller and the lights so as not to allow an unsafe configuration. The MMU is a hardware-level safety mechanism with valid configurations stored on a circuit board rather than in software. If an unsafe configuration (e.g., conflicting green lights) is detected, the MMU overrides the controller and forces the lights into a known-safe configuration. Similar physical security approaches can be used to protect the data on UUVs; if an unauthorized party lifted a UUV from the water, the data could either be immediately erased or require the input of a security code to prevent that data from being accessed without authorization. Mr. Aucsmith emphasized the need to take a different approach to cybersecurity by leveraging the physicality of the artifact in order to protect it.

Mr. Egan Greenstein*, Senior Director, Autonomous Maritime Systems, The Boeing Company,* described how Boeing leverages their unique aircraft building capabilities with UUV technologies to gather and share information. He spoke of the Wave Glider, a persistent mobile data-gathering platform that can be used to gather and share a wide variety of maritime-related data. By equipping Wave Gliders with on board sensors, they are able to gather information, as well as detect vessels entering or operating in an AOI. The Wave Glider could thus support immediate alerts of illegal activities to enforcement agencies.

Overall, GMF speakers and audience members identified the critical tension between information sharing and safeguarding, and agreed that finding a balance between these two activities was a central challenge facing the GMCOI. Members of the maritime community from both cybersecurity and operations backgrounds must work together to resolve this tension to ensure a secure yet operationally effective environment.

The next section presents a second related finding from the two-day forum -- the tension in the maritime domain between formal information security mechanisms and information sharing based on informal trust and experience-based relationships.

(2) Reliance on formal information security mechanisms versus common use of informal trust relationships and experiences

During panel discussions, ***Dr. Mark Haselkorn***, *UW Professor and Director of CoSSaR*, shared research conducted by CoSSaR on regional security-related information sharing environments. The research found that less formal, trust-based information sharing is more prevalent than formal systems that are based on the latest information and communication technologies.[1] Dr. Haselkorn highlighted this difference as a key consideration in future strategies for comprehensive MDA. As described above, the United States and its partners are addressing challenges faced in the maritime domain through enhanced information sharing capabilities, but with these enhancements come significant policy, legal, and operational issues, including the effective use of these capabilities in support of collaborative mission activities.

GMF presentations introduced technology advances with the potential to greatly facilitate and improve outcomes in relation to safety and security, particularly in the maritime sector; however, participants cautioned against becoming too dependent on technology, or introducing it in a way that undercuts existing effective mechanisms. GMF participants often pointed out that information sharing systems would benefit from focusing on humans first, rather than machines. For instance, ***Dr. Lilian Alessa***, *Director of the University of Idaho's Center for Resilient Communities (CRC),* presented on Community Based Observing Networks and Systems (CBONS), which leverage trusted humans as high fidelity observers capable of placing observations in context. "CBONS consist of distributed networks of skilled residents in communities throughout a region who systematically observe and document their environment on a regular basis in the context of hunting, fishing, or other livelihood activities. A key feature of CBONS is that data collection protocols and the resulting observing data are quality assured and quality controlled (QA-QC)."[2] Essentially, designated observers serve as information gatherers in real time, using Field Information Support Tools (FIST). FIST applications for smart devices have tabs that allow for reporting predetermined ecological, environmental, infrastructural or event-based indicators, such as marine debris, suspicious vessels, injured animals, communication towers, etc.

Dr. Alessa noted that designating domain experts as observers is crucial, as the wrong observer (i.e., untrained, unmotivated, ill-intentioned) could report unreliable information, just as a faulty sensor or other related technology could report inaccurate information. The type of community observers leveraged via CBONS are unique in that they are domain experts, who have specific training and use predetermined variables in context based application. As bad information can lead to bad decisions and end with unfavorable or undesirable outcomes, CBONS highlights the necessity of leveraging domain experts based on social trust and functional trust.

[1] Haselkorn M. et al., *Maritime Operational Information Sharing Analysis, Year 1 Final Report*, University of Washington, National Maritime Intelligence-Integration Office, Program Manager for the Information Sharing Environment, Department of Homeland Security Interagency Operations Center, 2014. http://www.hcde.washington.edu/files/news/MOISA1-Final-Report.pdf?pdf=MOISA-Year-1

[2] Alessa, L., A. Kliskey, P. Williams and G. Beaujean (2016). Incorporating Community Based Observing Networks and Systems: Toward a Regional Early Warning System For Enhanced Responses to Marine Arctic Critical Events. *Washington J. Environmental Law and Policy*, 6, 1-27.

Photo 9: Mr. Greenstein. **Photo 10: From left to right- Dr. Haselkorn, Mr. Sanford and Dr. Alessa.**

Along the same vein, ***Mr. John Sanford*** *of Nimitz Operational Intelligence Center, Office of Naval Intelligence* discussed the ongoing need for facilitating information sharing among allies, while actively safeguarding the information from potential threats. Currently, new technologies have made it easier than ever to obtain vast amounts of data and to analyze that data efficiently to accurately evaluate situations. However, the more data we collect, the more we may seek to share information with our partners; this comes with great responsibility to protect the integrity and security of such information, while at the same time facilitating a culture of information sharing. Mr. Sanford echoed that for many, the hesitance to share data is based on financial barriers. However, discussion supported that financial challenges could be overcome by changing the culture around information sharing by implementing more effective policy, by increasing mindfulness of cyber warfare and associated threats and, most importantly, by fostering effective relationships of trust.

Dr. Mark Haselkorn focused on the need for human centered design and engineering (HCDE) of future technology innovations for maritime security and domain awareness. He presented a brief history of HCDE and an overview of stakeholder driven, iterative design methodologies. Most importantly, however, he pointed out how these methods address policy- and mission-centric issues as well as issues of stakeholder adoption throughout the design, development, and implementation phases of technology innovation.

(3) Aligning commercial innovation interests versus government and public innovation interests

One of the most fruitful exchanges during GMF 2016 was the ongoing interaction in panels and breakout groups attended by commercial, academic, government and military experts. While the motivations driving innovation in these sectors often differed, all participants saw the possibility of increased capabilities for security, safety, and domain awareness if those differences were addressed. This was especially true of recent advances in the commercial sector, where growing capabilities presented opportunities, but also challenges to existing policies (or lack thereof).

Three commercial areas where participants brought considerable insight were unmanned aerial vehicles (UAVs), UUVs, and space-based capabilities.

Unmanned Aerial Systems (UAS) and Unmanned Aerial Vehicles (UAV)

GMF invited the Federal Aviation Administration (FAA) to speak about drone policy, with an eye towards lessons learned for the future of UUV policy. In his keynote presentation, ***Mr. Joshua Holtzman****, Director, FAA, Office of National*

Security Programs and Incident Response, stated that the United States is home to the most complex airspace in the world. The FAA has a primary duty to protect this airspace in the name of national and homeland security. In regards to UAVs, the FAA is actively attempting to balance safety with commercial growth. The FAA is working to build a full regulatory framework to accommodate current UAS/UAV operations by 2020. This framework includes plans to implement a cascading series of rules, whereby each rule informs the next, in order to meet operational needs while ensuring appropriate safeguards from risks to people and property in the use of manned and unmanned vehicles.

Photo 11: 2016 Global Maritime Forum Audience.

Mr. Holtzman pointed out that there are many different types of UAS/UAV, used for a multitude of purposes, from personal entertainment, to commercial applications, to government use. For example, UAVs are improving the safety of infrastructure, such as railway and agriculture-based operations. UAVs are also used for jobs that are physically dangerous for humans, such as surveying smoke stacks. The product life cycle of a UAV is between four and six months, compared with regular aircraft, which is about 20 years. Due to this short life span, the FAA needs to continually evolve to keep up with the technology, to take advantage of opportunities and mitigate risks in order to effectively ensure safety and security.

While the FAA is working on the overall regulatory framework for 2020, the agency is also actively working to integrate private UAV operation into the aviation system. For instance, in 2015, a new law (known as "Part 107") was established to allow the use of certain aerial "drones" (UAV) in specific conditions. Essentially, a privately owned drone is permitted for use if it is less than or equal to 55 pounds in weight and maintains a line of site of up to 400 feet in daylight. This policy greatly simplifies the remote pilot certificate application process, and allows citizens to request waivers for further specific use cases. This new rule serves as a flexible approach to integration that can be amended over time, and will serve the expected 60,000 instances of use within roughly the first year of implementation

The FAA is also collecting information (usage data, misusage data, etc.) and using it to support future regulations and registration. The UAV registration process has been running for about one year, based on a registration framework that was implemented very quickly compared to usual U.S. Government regulatory processes (in response to the rapid rate of UAV development and production). Registration provides a direct connection to operators, initially and on a continuing basis. Most private users do not understand the "rules of the road," so the registration process allows them to become educated on basic UAV usage regulations and requirements. Registration also helps with the enforcement of rules--

connecting the vehicle to the operator through the serial number. There are currently several initiatives that provide UAV owners and operators with a full range of operation information, rules, and enforcement policy. One such initiative is the smartphone app "B4UFLY" which was developed by the FAA for aerial drone users to educate them and to inculcate them into the culture of safety.

In the area of enforcement, there is an increasing trend of users violating airport airspace--more than 1600 reports in 2016 alone, at a rate of about 150 per month. There have also been disturbing reports of UAV interference in wildfire-fighting operation, particularly on the West Coast. In response to this, Congress has introduced civil penalties of up to $20,000 for disrupting firefighting and law enforcement efforts. Mr. Holtzman emphasized the need to send a clear message that this kind of behavior is dangerous and illegal. Finally, there have been several high profile security risks, including an incident involving a drone on the White House lawn in 2015. These incidents drive home the need for careful and safe integration of UAV usage into the current framework; the same will hold true with UUVs as well.

In order to analyze related emerging threats, the FAA has created an unmanned aircraft safety team. More advanced UAV research is being done at ASHORE, an FAA Center of Excellence. Current research is examining how best to use existing technology to support the increasing use of UAVs, and how to include auto-detection in UAV development. Some current tools and outfitting include dynamic geofencing, terrain avoidance, sequencing and spacing, and specifications for contingency management. Such data can be collected and synthesized by the UAV, which can provide data to human operators who in turn provide that information to leaders, enabling them to make strategic decisions.

Moving forward, Mr. Holtzman pointed out that DHS is the lead agency for working through UAS security issues, and that they are working to develop technology to track and mitigate evolving UAS threats. DHS still must develop policy for law enforcement agencies to apply regarding the use of force and common operating procedures regarding UAS.

Unmanned Underwater Systems (UUS) and Unmanned Underwater Vehicles (UUVs)

Like aerial vehicles, UUVs come in many types, and their use spans many applications and sectors, including commercial, exploration, scientific research, and government purposes. Of particular interest for GMF is the use of UUVs in providing the GMCOI with persistent maritime surveillance across a variety of missions. Autonomous capabilities have the potential to advance rapidly and the evolution of remotely operated vehicles (ROVs) and autonomous underwater vehicles (AUVs), which can operate independently of direct human input, have become an important capability in the maritime security domain.

***Mr. David Jones**, Director for Environmental and Information Systems, UW APL,* distinguished between air-based and water-based unmanned vehicles. In the aviation domain, UAVs have the potential to move at a much faster rate than UUVs, and can more easily make use of Global Positioning System (GPS) and other positioning tools. Several participants discussed limitations on UUV communication, pointing out that UUVs must breach the water's surface in order to send/receive data, making the process of data transmission significantly slower and more constrained than aviation-based vehicle communication.

Panelist ***Dr. Robert Touchton**, Chief Autonomy Scientist, Leidos,* discussed the mapping architectures for UUV autonomy and human factors for mission planning. While many autonomous behaviors are scripted and limited, there is a distributed hierarchical autonomy, meaning certain tasks are supervisory. For instance, automated vehicles can be programmed to use sensors to avoid bumping into physical objects or to maintain a prescribed perimeter. These systems, however, require a human element in order to actively evaluate higher-level situations and to evaluate whether the systems are working properly. Dr. Touchton suggested that the next five-plus years in UUV research and development (R&D) would need to focus on how to transform UUVs to work like an unmanned service vessel, with pre-designed problem solving skills/programming. Furthermore, regarding UUV movement and data collection, compared to UAVs, UUVs will need to advance navigational algorithms combined with remote operation (RO) capabilities (tethered or untethered). Today, UUVs are considerably less maneuverable than UAVs, and vary in communication rates (exfiltration challenges). While UUVs can silently go places of interest, they do so relatively slowly and require periodical surfacing and docking for exfiltration. Due to the lack of GPS underwater, UUVs require sea gliders with acoustical navigation sources to send data.

However, sea gliders pose challenges of their own, as they lack in standardization, and vehicles are limited in collaboration and advancement.

Photo 12: From left to right- Dr. Webster, Mr. Jones, Dr. Touchton, and Dr. Marburg.

According to ***Dr. Sarah Webster***, *Senior Engineer, University of Washington APL*, UUVs are limited further by their battery life; traditional UUVs are operational for about 12-72 hours before needing to be recharged. She suggested that when deploying UUVs for active missions, it is best to send multiple smaller vehicles (smaller vehicles are lower dollar assets) to collaborate as a critical network for communication. Ideally, each vehicle should be outfitted with different kinds of sensors and abilities, and together work as a system to complete a mission. This is more valuable and cost-efficient than deploying one high dollar asset UUV. Upon a single point of failure this would be a major loss in the form of both a physical asset and in the form of data exfiltration.

Along the same lines, ***Dr. Aaron Marburg***, *Senior Engineer, University of Washington APL*, urged caution when drawing strong analogies between autonomous surface and air vehicles, due to technical problems, radio frequency interface (RFI), and the immense market and R&D forces behind them. He suggested that we are currently at the end of the age of the autopilot; automated systems will get better and smarter, but only incrementally. For UAVs, there is immense potential (and market forces) to make the vehicles smarter. In contrast, UUVs face a value debt where there is no incentive to improve. For instance, UUVs have limited battery life and are restricted to react to state stages and mission stages. Underwater vehicles also face the issue of interaction and intervention—not just to move, but to touch, sense and react to things. This is particularly important to UUV implementation for scientific sampling and inspection of physical aspects of the environment.

Amid the excitement of emergent autonomous systems, GMF discussion on UUVs also focused on the role of humans. For instance, participants wondered what the implications would be for human-based skills such as flying or navigating marine vessels if autonomous systems are developed to such a degree that human interplay is unnecessary. Additionally, participants pointed out that we are not seeking autonomy for autonomy's sake. The human component is on the "team"—heterogeneous vehicles will be essential, but humans must be on the "team" as well. These "teams" represent collaborative autonomy that combines the human element with computer autonomy.

A few participants introduced the role of robots within the scheme of ocean navigation. One participant, a retired submarine officer, asserted that in the scope of oceans there will be 1000 remotely operated vehicles (ROVs) to every one Alvin (sub). Submarines move slowly for various factors, including that the UUV integration community took the approach that they are not trying to replace humans, but rather to enhance humans. Innovation could eventually lead to fully autonomous vehicles, but it would actually be more useful in the immediate future to improve standards to support existing systems. One participant pointed out that the Joint Architecture for Unmanned Systems (JAUS) worked with SAE International to standardize component pieces, and that it is important to work to avoid vendor lock by pushing for open system architectures. Discussion also touched on the need to create standard interfaces that still support flexibility in operations.

Photo 13: 2016 Global Maritime Audience Participation.

Further dialogue indicated that UUV advancement might face challenges due to the lack of commercial application. For instance, much vehicle development is in R&D labs and represents a "one off" similar to a New England farmhouse, where a room is added, then another room is added and everything is building upon old code. One solution would be to find practical commercial applications for UUVs, which would reduce the cost of developing the vehicles, which in turn would enable more rapid innovation. Discussion around ideal autonomous vehicles indicated that a "world model" for systems is much needed-- to include nautical charts, bathometry—essentially all the tools that make up the foundational capacity. Furthermore, many participants noted that this new model needs to be distributed globally in an economical and efficient fashion, which would catalyze a worldwide collaboration over the next five-plus years. Regarding global positioning devices, one participant pointed out that this would require acoustics to be more effective over long distances—having acoustic beacons along bases of interest—and pushing people to agree on transmission and encoding standards.

Space-Based Capabilities for Maritime Domain Awareness (MDA)

In addition to aerial and underwater capabilities, there were panels and discussions on the increasing role of space in the maritime domain and the latest technological advancements in space-based capabilities to enhance MDA. Space and air-based technology offer opportunities to provide constant surveillance and evaluation of maritime assets.

Dr. Jana Robinson*, Director of the Space Security Program (Czech Republic),* spoke about space-based assets, vulnerabilities and current threats to the United States. She stated that in the face of evolving vulnerabilities relevant to

Russia and China, the United States employs a crisis management methodology focusing on: (a) early threat detection, (b) deterrence and prevention strategies and (c) readiness for counteraction and response. She believes that current threats have reached new levels, which are actively affecting the current levels of tolerable actions by adversaries and allies alike. For instance, she asserted that Russia has been reported to have intentions in the Baltic Sea (attempting to capture gas and oil reserves, which are equipped with military radar equipment), as well as documented instances of Ukrainian signal jamming. In addition, China has expanded into the South China Sea, increasing the possibility of kinetic attacks on U.S. space assets. In the geopolitical setting, the risk of space systems and assets being destroyed by enemies means the potential denial or disruption of a range of national dependencies. She sees enemies mobilizing in this arena, and they are equipped to maneuver mounting attacks on our space assets and systems. She also questioned if our allies are willing and ready to use space assets for defense. Currently, there is little tangible progress on developing norms of acceptable behavior (code of conduct) for this domain, and many aggressive states are pushing the boundaries of what is acceptable via micro-maneuvers (Russia, China, etc.). In the current situation, Dr. Robinson sees limited fear of repercussions for aggressions, which means there will be more attacks and disruptions to come.

Photo 14: From left to right- Mr. Bauna, Dr. Robinson and Dr. Mittleman.

Moving forward, Dr. Robinson sees the biggest need in the area of policy to address mitigation for such attacks, as well as increasing the political willingness of allies to intervene. The development of a more formal governance architecture would catalyze a united global front among our allies, and could greatly reduce the impact of potential threats. Dr. Robinson believes that we need to send a clear and unambiguous message of what will not be tolerated, and outwardly name repercussions for aggressive behaviors (e.g., economic repercussions, to demonstrate a united global front). She feels that a stronger governance architecture will facilitate communication for a more secure space environment.

Along similar lines, ***Dr. John Hornsby****, VP Sales and Business Development, Blacksky,* introduced "Spaceflight Industries," which aims to fundamentally transform the industry by promoting innovative solutions in space. There are two parts to the organization, (1) "Spaceflight," which provides access to space to fuel global growth and (2) "Blacksky," which operates to unify data to understand the planet in real time. Blacksky is catalyzing a geospatial revolution by implementing a multi-sensor global data platform for anticipatory tasking and collection. By providing on-demand data, such as imaging and persistent surveillance, the ability to understand the global population in real time is generated.

Using a constellation deployment plan, satellites will be deployed in the future to generate imagery at a more affordable rate for consumers. This capability is not completely new; for instance, it has been used for a number of years to combat illegal fishing, using analytics and sensor data. Dr. Hornsby stated that the current initiative is particularly attractive because data measurements can be collected and relayed in minutes rather than days. This capability can be used for a multitude of purposes, such as monitoring humanitarian events, conflict events, supply chain systems etc. There were questions raised by GMF participants about the greater policy implications of such technology. For instance, while this technology is more effective, reliable, and accurate than current AIS applications, many questioned the consumer target for the collected data. From a policy perspective, regulation currently implies that recovering content is unlawful, yet the independent feed of data is to be considered legal.

Finally, ***Dr. John Mittleman,*** *U.S. Naval Research Laboratory,* brought great expertise to the discussion of the development and use of space in MDA. Dr. Mittleman stated that MDA serves two main functions: 1) to assure and support allies and 2) to provide a foundation of capability for threat deterrence. For deterrence, elements include denying any benefits to potential adversary actions and concurrently imposing costs on adversaries that would be greater than the goal that the adversary was trying to achieve. Dr. Mittleman further encouraged the importance of representatives from the Japanese government present at the 2016 GMF, as we have been working with Japan since 2010 to develop a more robust cooperation for the use of space capabilities in the maritime domain.

Photo 15: From left to right- CAPT Kimball, COL Okamoto, CDR Tachibana, RADM Sharp and Mr. Kinoshita.

(4) Integrating bottom-up (local) perspectives with top-down (Federal) perspectives

Several speakers discussed a tension that exists between the benefits and limitations of systems that are designed, developed, and/or implemented from the top down (i.e., from a Federal perspective) as opposed to those that are designed from the bottom up (i.e., from a local perspective). In her presentation during Panel Session IV, ***Ms. Melissa Braxton****, Innovation Specialist and User Experience Designer, 18F,* presented on the need to use a human-centered design (HCD) approach when developing complex interactive systems. HCD is set of methodologies that support a bottom up approach based on a commitment throughout the entire design process to involve the people who actually use the product,

technology, or service to co-create a solution. She stressed that this commitment to the people on the front lines of service delivery is particularly important in areas like maritime safety and security.

Ms. Braxton described technology innovation as an intervention into a complex system. She described this system as being far more than technology; it also involves people, organizational structures, policies, and cultures, all of which are integral to the delivery of the public service. To design for this level of complexity, Ms. Braxton stated that the action must be viewed from the bottom up, yet governmental systems are often designed and implemented using a top down approach at the Federal level, and then mandated to be used at the local level. She stressed that a transformation to a bottom up, HCD approach reduces anxiety regarding an organization's adopting a new, unknown system, and builds trust and confidence among users in the system and the development process.

Two systems that utilize a bottom up approach were discussed during the two days of Panel Session presentations. First, CBONS,[3] introduced in Panel Session V by **Dr. Lilian Alessa**, is an example of a bottom up approach to protecting the Arctic environment and conserving its resources. As described above in Finding 2, the high fidelity, boots on the ground, observations collected by indigenous people are integrated with data from other observing systems to meet the needs relevant to specific Federal, state, local, and private-sector entities. It is this local perspective that will improve our ability to ensure a secure and sustainable Arctic. The second example of a bottom up approach is the IMDE/CSS development efforts described by Mr. Shawn McDonald in Panel Session IV. DHS S&T is using a human-centered design approach that engages the operators at the local level to ensure that the system meets their requirements, in addition to providing state and Federal agencies with information to meet their needs. According to Mr. McDonald, "70 - 80 percent of our success depends on local information." While there are some issues still to be resolved (see Finding 1), it is hoped that these issues will be resolved in technical and operational demonstrations scheduled for later in 2017.

Photo 16: Dr. Lil Alessa Leads a Collaborative Breakout Session.

[3] "Community Based Observing Networks and Systems" (CBONS); see p. 3, above.

There was general agreement among participants in this year's GMF that integrating a bottom up perspective with a top down perspective to enhance system adoption was critical for achieving maritime domain awareness. Equally important was the need to move away from technology-centric innovation towards mission and policy-centric innovation. The next section briefly discusses this finding.

(5) Transitioning from technology-centric innovation toward mission- and policy-centric innovation

The tension between technology-centric innovation versus mission and policy-centric innovation was a central theme of GMF 2016, and participant after participant came down on the side of giving policy issues and mission effectiveness far more weight than they currently receive in the course of technology innovation efforts. Some examples of this tension include:

- Mr. Shepherd's keynote review of policy issues that affected research and development carried out by government, military, academia and the high technology industry;
- Mr. Holtzman's vivid examples of policy issues that the FAA must now deal with because drone technology has so rapidly outstripped our abilities to monitor it for public safety and security;
- CAPT Raymond's reminder that relationships and trust are far more important operationally than information technology;
- Ms. Braxton's reminder that technology not only affords capabilities, but also constrains the ways we can work and accomplish our missions; and,
- Mr. McDonald and Mr. Wheeler both providing first-hand knowledge of current information sharing projects where policy, not technology, was the most difficult hurdle to overcome.

The central message of the GMF involved the need to rethink how emergent technology is acquired, designed, developed, deployed, used, and maintained, in order to keep our countries secure, safe, and resilient.

Photo 17: Ms. LeVitre and Mr. Shepherd.

Photo 18: Ms. Marshall and Dr. Savelli.

GMF emphasized that emergent technologies are not in and of themselves solutions. Rather, they are opportunities for enhancements of existing capabilities and complex systems of operation. To achieve these enhancements, it is necessary not only to advance the technical features, but even more importantly to situate those features within a system of people,

policies, and organizational cultures that is already delivering services. Emergent technologies are best applied when they are viewed as opportunities to create a positive intervention within an existing socio-technical system. To achieve the benefits of this intervention, the technology features cannot be at the center of the design; rather, the center of an effective design is the mission and work that are being enhanced, and the people doing that work who are being empowered and must adopt the solution. Therefore, the mission, the people, and the policies that guide them must be at the center of technology innovation.

A final theme that emerged from this year's GMF contrasted the growing use of big data aggregate analytics for intelligence discovery with the need to balance a more human, contextual, specific ground truth approach to domain awareness.

(6) Balancing big data analytics with contextual, specific, ground truth approaches

Much of the scientific world is currently grappling with the tension between big data analytic approaches to truth and more human, contextual approaches. In medicine, for example, research used to focus on clinical observations that led to studies of what was going on with patients in the clinic. Now, we focus on big data projects (e.g., genome) and the construction of huge datasets that move us towards an "evidence-based" approach to medicine. Similarly, intelligence and security work traditionally focused on human observations of ground realities, but now are moving more and more towards the gathering of big data and the analytical methods for making sense of those big datasets.

A number of the GMF panels emphasized the importance of maintaining the role of contextual, specific ground truth approaches and integrating them with larger analytic approaches. CBONS, discussed above, is an example of a people-based, ground truth approach to data collection. As presented by Dr. Alessa, CBONS consists of distributed networks of skilled residents in communities throughout a region who systematically observe and document their environment on a regular basis. These operators are able to put data into a situational context and when combined with data from other observing systems, enrich the situation awareness of areas where information is difficult to obtain, such as the Arctic.

Mr. Sanford added another aspect to this tension, acknowledging the vast amounts of data available and the importance of our ability to synthesize this data to improve maritime domain awareness. However, Mr. Sanford also pointed out that while more data can lead to better accuracy, it is not helpful if we do not share this data with our allies. To do so, however, requires more than just technology. We must change our culture, implement policy, and build the relationships needed to facilitate and encourage responsible information sharing. Reiterating the concerns from Panel Session III on cybersecurity, Mr. Sanford cautioned that while we need to adapt our culture and environment to share data, we must also be mindful of cyber warfare and move to secure this very valuable data.

The information sharing project between the United States and Canada that was introduced by *Mr. Wheeler* is another example of how contextual, specific ground truth efforts can be combined with big data analytics for optimal maritime domain awareness. The system used by the RCMP synthesizes radar data, adds map layers that include speed, direction, etc. to give an overview of an AOI that includes small dark vessels. These vessels are not currently visible to U.S. partners other than by "eyes on the water" – patrols that monitor selected areas on a schedule. However, as Mr. Wheeler pointed out, this data system does not replace the need to send patrols and engage on the water. Rather, it makes those patrols more effective by guiding them to selected targets and supporting collaborative efforts. The best results are achieved when big data analytical efforts are designed and used to empower and make more effective the precious human resources that must ultimately come into play.

Photo 19: John Sanford Leads Discussion During the Collaborative Breakout Session.

Inspired and informed by keynote speakers, panel presentations, and group discussions, the breakout groups worked to develop their plans for the future and "pitch" these plans to the entire forum.

IV. Plans for the Future

The afternoons of both days of GMF 2016 were dedicated to collaborative breakout sessions. Each collaborative breakout group was responsible for preparing a roadmap for addressing a critical and evolving maritime security issue identified in the panel sessions and discussions. These plans were presented at the last session in a "Shark Tank" format.[4] Each collaborative breakout group identified their assigned security issue and "pitched" their roadmap, before the entire forum, to a panel of three "sharks," each representing different sectors: Dr. Lilian Alessa (academia), Mr. John Sanford (government), and Mr. Russ Matijevich (commercial). Below are the roadmaps as presented by each of the collaborative breakout teams. For the "Shark Tank" presentation, some groups (specifically groups #2 and #12 / #3 and #7) combined their presentations.

[4] "Shark Tank" is a television reality show on the American Broadcasting Corporation network, in which tough, self-made business tycoons hear business idea presentations from entrepreneurs seeking to secure funding for their proposed business ventures.


Photo 20: RADM Sharp and the Group Breakout Session. Photo 21: Mr. King Leads Group Discussion.

Group 1 focused on improving maritime domain awareness, especially related to the identification and awareness of "dark" targets. They proposed integrating current and future commercial space-based investment and technological innovation with information sharing techniques to help identify suspicious moving targets at sea. The group suggested that one government maritime surveillance system alone is not sensitive and agile enough to capture a complete resolution of desired oceanography. Ideally, we need a way to scan the entire Pacific Ocean in one sweep, and quickly filter down to scan for targets or an area of specific interest. However, as too much information can be just as problematic as not enough, they proposed that a solution to these issues will leverage and synthesize all available existing collection platforms to collect both a larger picture as well as to provide the agility needed to refine the scope of the maritime tracking data. They call their solution "MDA-On-Demand."

Group 1 identified several barriers to the development of MDA-On-Demand. First, the issue of understanding the current policies that govern information sharing in this domain. As each country has differing policies on sharing information, developing standard practices for information sharing may be difficult to develop and difficult to follow. Second, the issue of denying the information to actors who would use it to do harm. Not only must we be concerned with securing our own information, but we must also ensure that our partners are adequately securing the information we share with them. Third, it is not always in the government's interest to become too deeply committed (financially) to a system. Engaging partners early in the design process may facilitate the adoption of the system and encourage their commitment to it; a human centered design (HCD) approach will be employed.

Prior to beginning development of MDA-On-Demand, Group 1 reported that work should be done to understand the security needs being met. Commercial partners could begin by surveying areas of high maritime traffic that are likely to be of interest. Future areas of interest can be determined over time and the partners can branch out and away from the high traffic areas to other AOIs. In addition, engagement with other agencies and countries should take place to discover if similar issues are of concern or if similar development efforts are underway. This engagement would also build trust among the partners. According to Group 1, MDA-On-Demand could provide what you need, when you need it, but not need to be available all the time.

The Sharks pointed out that the effectiveness of MDA-On-Demand relies on leveraging commercial capabilities for intelligence collection. While the group emphasized the benefits to national security efforts, the commercial "Shark" was less clear on what the benefits would be to the participating commercial entities. For example, would "MDA-On-Demand" be framed as a subscription service?

Groups 2 & 12 proposed moving forward based upon a gap analysis conducted at Johns Hopkins Applied Physics Laboratory. The gap analysis used scenarios involving a red team that represented the bad actor in the scenario and a blue team that represented the response actor. The goal of the scenarios was to identify the processes that enable the actions that are beyond the "system." The group identified this approach as a way to facilitate information sharing.

Groups 3 & 7 presented a plan to identify the information sharing weaknesses and blockages that exist within the international maritime domain. The plan included creating and conducting a simulated response to a maritime incident in order to identify the information flows necessary for a successful response. The scenarios could be as simple as surveillance in a particular AOI or as complex as military crisis management. The goal of the simulations would be to highlight information sharing successes, failures, and gaps. While these types of exercises exist within an organization, few cut across organizational boundaries, and even fewer cut across international boundaries.

The group recognized that the first step was to identify a group of international partners who were willing to scope and take part in the exercises. They stressed that a body of diverse scenarios, covering a range of AOIs, was necessary in order to get a complete understanding of the information sharing gaps as well as to identify new policies that would need to be put in place to enable information sharing. The group saw these exercises as a way to provide decision makers with tangible evidence of gaps or barriers to information sharing rather than wait for a catastrophic event to reveal these gaps. The group expressed that theirs was a bottom up approach, which would provide leadership with direct evidence of information sharing failures. The Sharks cautioned that overcoming institutional inertia from top leadership must be a top priority if this project is to get off the ground.

Group 4 pointed out that any plans for moving forward in a more mission-centric, policy-sensitive, non-technology-centric way depended on a culture change in the government and military. They asserted that policy owners are often disconnected from operational perspectives and needs, and that this can lead to lack of trust of "top" levels by "bottom" levels. In order to move towards mission-centric development efforts, the organizational cultures must give more value and power to operational elements.

Photo 22: Mr. Randy "Church" Kee.

Photo 23: Ms. LeVitre During the Group Breakout Session.

Group 5 proposed using the IoT[5] to increase maritime resilience and prevent disaster. The group proposed a system similar to the one for air travel where x-ray technology is used to screen luggage and passengers, with policies and laws enforcing this screening. This same type of system can be employed in the maritime domain using IoT technology. According to the group, due to the future reduction in the cost of sensors, they can be used to screen vessel cargo. They suggested having two screening processes: a fast lane similar to the Transportation Security Administration (TSA) pre-check, and a slow lane for rigorous screening. They emphasized that policy for enforcing the screening as well as reporting on the screenings was a critical component of their proposed plan. The group also stressed that the proposed screening system should be designed so as not to negatively affect trade and commerce.

For the screening system to succeed, the group recommended having a representative, such as RADM Sharp, to sponsor the required screening policies. They believed this representation is necessary to achieve compliance from all agencies and nations. They proposed beginning the efforts by focusing first on large vessels and then moving to smaller vessels. As

[5] "Internet of things"; see p. 9, above.

a first step, they recommended identifying key stakeholders who are willing and able to "sell" this screening system to industry. Next, data and screening standards must be created. For example, what data will be required, who will own the data, and who will be responsible for tracking the data, etc. They also discussed the need to create a repository that will house all of this data, as well as someone to act as a broker for other nations wanting this information. This could be similar to the Maritime Safety & Security Information System (MSSIS), the system that provides information to approximately 80 countries and maintained by the U.S. Department of Transportation. Finally, and perhaps most importantly, the group stressed that international policy must be in place up front and agreed to by all parties.

Group 6 presented a plan to use space-based maritime capability to prevent the intentional misuse of the maritime domain to commit hostile, harmful, or unlawful acts. The group proposed starting with a baseline inventory of the maritime domain that would include sites, sensors, analytical capabilities, resources (human and non-human), available training, etc. This inventory could then be used to identify the information gaps, as well as the barriers to information sharing. The next step would be to plan and execute exercises in a particular AOI, incorporating metrics to quantify persistence and awareness. These exercises should be conducted biannually to allow for methods and training to be refined quickly. The group would leverage the DHS sensor/analytics/capability survey that was currently underway and available in the fourth quarter of 2017.

According to the group, while there are many assets available to monitor the maritime domain, there is little to no coordination or collaboration among agencies. Data is being recorded, analyzed and stored, but not shared with the people who need it. It is easy to say that agencies should share their information, but in practice, this rarely happens without some type of quid-pro-quo situation. It is imperative that legislation, policies, and even cultures shift toward providing data fusion across all assets because until required by law, no one agency is going to expend resources on information sharing and data fusion for the benefit of other organizations.

To promote this required cultural shift, the group proposed requiring mandatory self-identification, similar to a Radio Frequency Identification (RFID) tag, by requiring vessels to carry beacons or perhaps adopting the use of a technology such as *Boat Beacon*, a cell phone application that provides bearing, range, and closest point of approach (CPA) calculations in addition to all the standard AIS information. It transmits as well as receives AIS and continuously monitors CPA (http://pocketmariner.com/mobile-apps/boatbeacon/). The group also proposed designing a crowd sourcing gaming application to encourage boat spotting that could be another source of information for vessel tracking. While the Sharks liked the idea of self-identification, they were concerned about exposing vulnerabilities that could be used by adversaries to do harm.

Group 8 proposed using UUVs to detect foreign exterior objects and parasitic devices on vessel hulls. This capability would have international application, and in the U.S. would meet mission needs of the Navy, Coast Guard, Customs and Border Protection, and local law enforcement agencies. This capability would allow unmanned scanning of vessel hulls in low visibility conditions prior to entry into a port. The group recommended developing policies regarding the role of UUVs. For example, what entities are allowed to operate such UUVs to scan ship hulls and under what circumstances; if an unauthorized item were found attached to or accompanying a vessel, how would authorities determine whether the object is benign or actionable? They also raised the issue of standardization of operations and training of personnel as things that must be considered before implementation of this plan.

The group identified the following milestones:

a) resolution of policy issues;
b) development of Concept of Operations (CONOPS);
c) procure funding;
d) design and develop the product;
e) deliver the product;
f) implement it on a Federal level; and,
g) creation of data and records management protocols to maintain chain of custody, data storage, and enforcement of standards.

The group concluded their presentation by emphasizing that using UUVs in this capacity would reduce the likelihood that parasitic devices could be used for smuggling or sabotage.

The Sharks had several questions for the group. First, they questioned who would be responsible for damages if the UUV caused harm to a vessel or the environment. They also cautioned the group that the UUVs must not impede port activities.

Group 9 chose to tackle the challenge of improving international collaboration in maritime security through increased information sharing. To do this, they proposed building trust through training and the creation of common standards for information sharing. Training is required to not only build trust, but also because the transient nature of the workforce requires team members to build deep knowledge in the shortest time possible. Common standards will also help the transient workforce learn the language, culture, and information sharing networks quickly. The group offered that scenario planning must be incorporated into the training materials and that currently scenario planning is inadequate. Finally, they suggested that financial incentives are needed to motivate partners to share information.

The group proposed cargo tracking as an area for improved international collaboration because every country wants to know what a vessel is carrying; yet many nations do not currently share this information with their international partners because there is no incentive to do so. They suggested creating a standardized format for chain of custody that would reside in the cloud so that it could be readily accessible by all who have a verified need to know the contents of a particular ship's cargo. This system could be similar to the current TSA pre-check system.

The first step is to identify key stakeholders, as well as those organizations that are attempting to solve the same problem. The information needs of each organization would then need to be determined before arriving at standardized formats and identifying a place where the information could be consolidated. A special interest group may be needed to facilitate collaboration. The team also suggested that engaging academic researchers who understand human behavior might help to realize this plan.

The Sharks were in favor of Group 9's plan and suggested that they review the U.S.'s "National Maritime Domain Awareness Plan," as there was information that could be help to inform their "Cargo Tracking Hub" application.

Like Group 9, **Group 10** was concerned about international cooperation and coordination. They presented a plan to create a *Global Fusion Center* that would leverage data from all willing international partners. The Center would include access to commercial satellite data in addition to sensor data that is already collected by the various government agencies.

Photo 24: Ms. McBryde and CAPT Schmidt. **Photo 25: Mr. Plankey.**

Group 11, like Group 4 before it, pointed out the need for fundamental changes in order to achieve the forum's vision of mission-centric, policy-sensitive technology innovation in support of critical information sharing. Whereas Group 4 focused on culture change (e.g., a culture of trust within the security community), Group 11 focused on organizational change. They called for the establishment of a senior maritime advisory board to review and provide recommendations to the U.S.'s Maritime Domain Awareness Executive Steering Committee (MDA ESC)[6] for validation and updating the 20 MDA challenges, including threats and vulnerabilities for each challenge. This would result in prioritized requirements, recognized process "owners", and investment recommendations for implementation. The group proposed that this review should include a validation of national MDA governance, and recommendations for additional member agencies for national MDA ESC.

Group 13 echoed Group 1 in calling for the leveraging of growing capabilities from commercial satellites to help achieve national and global maritime security.

Group 14 proposed a crowd-sourced "911"-style[7] mobile application for the maritime domain. The proposed application would use high-fidelity contributors to report evolving maritime incidents, similar to the way in which CBONS (discussed above) uses a network of highly reliable domain experts to observe and document the activities in the Arctic. For example, the application could be given to regular ferry operators or riders, certified as highly reliable, to use the application to report evolving onboard incidents. They also suggested that the application could include a feedback loop, whereby analysts would look at information to seek patterns and provide feedback into the application. This feature would help to devise more efficient and effective allocation of resources for maritime security.

When Group 14 presented this idea to the forum, it turned out that other regions were already working on or implementing similar plans. The Sharks recommended identifying and pulling together these regional plans, identifying the best aspects of each plan and expanding the capabilities as appropriate for the various types of regional awareness systems and incident management plans that could be enhanced through crowd-sourcing approaches. The Group 14 members agreed that this was a good approach. In addition, they stressed that initiatives like these need to be managed differently with an

[6] The MDA ESC, comprised of senior representatives from the U.S. Departments of Defense, Transportation, and Homeland Security, and chaired by RADM Sharp (in his roles as Director NMIO/National Intelligence Manager (NIM)-Maritime) representing the Intelligence Community, reports to the National Security Council's Maritime Security Interagency Policy Committee.

[7] In the United States, dialing "9-1-1" enables a caller to reach an emergency telephone operator.

eye towards fostering a positive disruption in the current system. They emphasized that the focus must be fueled by innovation that is policy and mission centric rather than technology centric.

Photo 26: CDR Imme and CAPT Schorr.

Photo 27: Ms. Green and Ms. Yancey.

V. Conclusion

GMF 2016 presented an extraordinary wealth of issues and opportunities for enhanced maritime security, stimulated by discussion of emergent technologies. The higher-level themes to emerge were relatively focused and centered on human issues (policy, organization, mission, etc.) that needed to be addressed in order to gain significant achievable enhancements from those capabilities.

The group presentations described above provided the forum's thoughts on how we can best move forward to integrate technology innovations into mission accomplishment. The central advice from those groups is captured in six strategic action plans presented below. In many cases, the group presentations suggested specific projects that, if conducted, would make progress towards the goals of these six strategic action plans.

Action Plan #1: Design information systems that support multi-agency security and safety operations by balancing the risk of sharing data and information with the risk of not sharing

Presentations and discussion on cybersecurity, led by IT experts, emphasized the need to design systems for the protection of potentially sensitive information and discussed the challenges to doing this efficiently. In addition, presentations and discussion on regional and national security and safety operations, led by field professionals from operational agencies like RCMP, USCG, and CBP. They emphasized the need to enhance the sharing of data and information with the right people in a timely manner to support collaboration during complex field missions. These missions could involve FSLTIPP entities. The differences in IT and information sharing capabilities across these diverse partners is especially challenging due to varying controls for sharing, mission variance, and other policy-based restrictions. For example, representatives from DHS presented a S&T enterprise architecture project that was facing this sharing/safeguarding tension, working to provide enhanced methods for interagency information sharing even as it struggled with DHS requirements for background checks to gain access to the system. Projects to improve shared regional awareness (e.g., those discussed at the GMF occurring at the U.S.-Canadian Border) need to bring together, throughout the design, development, and use phases, IT-based stakeholders who understand cybersecurity with mission-based stakeholders who understand the impact of missing, late, or incorrect information on operations. The local-level was highlighted as underrepresented and especially in need of being included as trusted partners in these system architectures.

Action Plan #2: Explore the likelihood and impact of private unmanned underwater vehicles (UUVs) on maritime security

Panel presentations and breakout groups discussed the emergent presence and sophisticated capabilities of private UUVs and their current and potential future impacts on issues of interest to the GMCOI. Some technical issues such as power and communications presented limitations that were a focus of current work, but currently unaddressed policy issues were seen as even more pressing. Issues discussed included authority (e.g., whether the Coast Guard's authority to board a vessel to conduct a security sweep extends to private UUVs or not) and liability (e.g., which entity/organization would be responsible if a private UUV damages a vessel causing an oil spill). In the context of the Federal Aviation Administration (FAA) GMF presentation on emergent drone policy, there was considerable concern about the likely rise of private and commercial UUVs. A common theme was that the maritime security community is unprepared to cope with a rising number of private UUVs (e.g., how will port security managers identify the physical presence of private UUVs; and how will they manage/mitigate the potential security threat posed?). The current technology-centric development efforts (efforts that GMF participants strongly suggested be changed -- see #3 below) mean that policy usually lags behind technology. GMF participants proposed a project to get ahead of the curve on the likelihood and impact of private UUVs on cargo and port security. *(Note: this action area was identified prior to the recent incident precipitated by China's seizing of a U.S. UUV in international waters.)*

Action Plan #3: Enhance the security information sharing environments (ISEs) through stakeholder-centered, policy-sensitive, mission-based technology innovation

Participants recognized a need to move from technology-centric innovation to policy-sensitive, mission-centric innovation. In addition to the UUV example mentioned in Action Plan #2, above, participants identified a need to incorporate mission and policy in technology innovation in a number of current efforts to enhance information sharing environments. These included the international, multi-agency CANUS project to enhance information sharing on the U.S.-Canadian Pacific Northwest border; the IMDE/CSS project being conducted at various locations (including the Puget Sound) by DHS S&T, and the Community-based Observing Networks and Systems (CBONS) project being conducted by the Arctic Domain Awareness Center in support of high-fidelity human information gathering and sharing. Breakout discussions catalyzed questions about policies that affected the incentives and disincentives for sharing information. One way forward would be to select a region and work with stakeholders to articulate a complex multi-agency mission, understand the current ISE (including policy) in support of that mission (the "as-is"), articulate the desired ISE (the "to-be"), and design a technology/mission/policy enhancement that addresses identified gaps and pain points. The Arctic was identified as a region with considerable information gaps and disparate information sources, making it an ideal domain for a project to enhance ISE.

Action Plan #4: Foster trust-based security networks and information sharing environments

Trust-based and relationship-based security networks were a theme throughout GMF. RADM Sharp echoed this during the opening comments, where he emphasized "the ongoing need for collective and collaborative security approaches, and… the importance of continually developing a cohesive security-focused network, limited only by our imagination and our willingness to create connections and partnerships to effectively defeat threat networks." Participants questioned whether current policy on information security classification was supportive of the way security operations are actually conducted. UW researchers cited studies (funded by the Office of the Program Manager- Information Sharing Environment (PM-ISE), the NMIO and the DHS Interagency Operations Center (IOC) led by the USCG) which found that 80 – 90 percent of regional security information sharing was informal, based on trust and shared experiences. Arctic researchers, who emphasized the critical importance of "social trust" in the information-sharing arena, further supported this. Representatives from DHS S&T discussed the need to expand beyond formal definitions of identity and access management (e.g., required background checks, Memoranda of Understanding (MOU), etc.), especially when developing systems to increase information sharing with non-Federal partners. Many participants saw the need to design future security networks and ISEs that leverage existing trust relationships and operational practices, rather than impose formal security classification systems that further complicate collaborative security efforts. A way forward could be to capture existing information sharing relationships and use them to create a user-defined, trust-based entitlement security layer that supports how the community of security operational professionals actually works. This approach would also support

future analytics on the vast majority of security information sharing that are currently being lost because they are informally conducted via phone, e-mail, and face-to-face.

Action Plan #5: Leverage increased commercial satellite capabilities to help meet national security needs

One of the most fruitful aspects of GMF 2016 was the interaction of thought leaders from diverse backgrounds and perspectives. The participation of commercial experts was particularly revealing; on one hand, participants from commercial entities provided insights into the growing capabilities of private industry in areas like UUV and satellite deployment, data acquisition, analysis and storage. These insights stimulated group brainstorming on the integration of growing commercial capabilities into efforts to achieve superior ocean domain awareness for national security and cargo transport reliability. However, it was also evident that commercial interests and motivations were not necessarily aligned with those of government and the public. For example, one breakout group, inspired by commercial innovations in satellite sensing, proposed a "Maritime Domain Awareness On-Demand Portal." This portal would leverage growing commercial capabilities to increase the flexibility of data collection in response to dynamic and unpredictable international maritime security threats. Presented in a "Shark Tank" environment, however, this innovative proposal was met with a "What's in it for me?" concern from the commercial "Shark." A possible resolution of this tension would focus not only on exploiting technical capabilities, but also even more importantly on defining policy and incentive structures that would provide benefit to commercial partners as well as government agencies, military commands and intelligence analysts.

Action Plan #6: Develop a highly reliable crowd-sourced alert system

In his opening welcome, CAPT Joe Raymond of Coast Guard Sector Seattle emphasized the importance of a coordinated, flexible regional security community that relies on timely effective information and communication. One "nightmare scenario" that was described was an active shooter incident on a ferry, an incident that would be difficult for responders to reach and which could involve any number of agencies, depending upon where the incident occurred in the region. In such an incident, every minute of response time could mean the loss of innocent lives. One breakout group focused on this challenge, incorporating discussion of the potential role of local, highly reliable domain expert public sources. They imagined, for example, regular ferry riders who would be certified as highly reliable and given phone applications that allowed them to report evolving incidents. When this idea was presented to the forum, it turned out that other regions were already working on or implementing similar plans. A potential solution for this requirement would be to identify and pull together all such regional plans, identifying the best aspects of each plan and expanding the capabilities as appropriate for the various types of regional awareness systems and incident management plans that could be enhanced through crowd-sourcing approaches.

On the final day of GMF, RADM Sharp showed a clip from the film *The Internship* in which two applicants for an internship at Google (played by actors Vince Vaughn and Owen Wilson) are asked an interview question about what they would do if they were shrunk down and tossed in a blender. Their answer focused on the amazing possibilities that would be presented after they got out of the blender (much to the consternation of the interviewers, who wanted to focus on their being in the blender). The Admiral agreed with the applicants: it was what could happen after getting out of the blender that was most important. His message was clear. GMF is the blender, and for two days, we were whirled around by the intense, special experience of bringing together 130 experts focused on the future of technology and policy for maritime security. However, what is most important is *now*, after we are out of the blender. The above plans point a way forward to turn the intense experience of GMF 2016 into ongoing concrete benefits for both the United States and the Global Maritime Community of Interest.

Appendix A: List of Attendees

Last Name, First Name	Organization
Aardahl, Chris	Pacific Northwest National Laboratory (PNNL)
Acrey, Anthony	U.S. Customs and Border Protection (CBP)
Alessa, Lilian	University of Idaho, CRC
Allen, Craig	University of Washington, School of Law
Andersen, Nicholas	U.S. Naval Intelligence, N2/N6 CIO
Ansay, Michael	Naval Undersea Warfare Center
Aucsmith, David	University of Washington, Applied Physics Laboratory
Bauna, Tony	Kongsberg Satellite Services AS
Baxter, Brent	MSOC(W) / Department of National Defence
Belton, David	MDA Geospatial Services
Blaney, Hank	U.S. Coast Guard (CG-255)
Bragg, Michael	University of Washington, Dean of Engineering
Brandenberger, Jill	Pacific Northwest National Laboratory (PNNL)
Braxton, Melissa	GSA/18F
Brown, Malcolm	National Maritime Information Centre (UK)
Cameron, Timothy	ONI/ National Maritime Intelligence-Integration Office (NMIO)
Chavez, Ashley	GBI-GISAC
Clark, Bradford	U.S. Coast Guard / Interagency Operations Center
Cothron, Tony	General Dynamics Information Technology
Coupe, Gregory	NORAD (North American Aerospace Defense Command)
Cousino, Vicki	ODNI / PM-ISE
Diaz, Chanel	National Maritime Intelligence-Integration Office (NMIO)
Donohue, Brian	Johns Hopkins University, Applied Physics Laboratory
Doorey, Tim	Center for Civil-Military Relations, Naval Postgraduate School
Fitzpatrick, Rory	National Space Centre Ltd
Furukawa, Yoko	U.S. Office of Naval Research Global
Fusco, John	U.S. Navy / NY State Police Office of Counter Terrorism (OCT)
Grant, Jay	Inter-port Police
Green, Michelle	National Maritime Intelligence-Integration Office (NMIO)
Greenstein, Egan	The Boeing Company
Harris, Christian	SPAWAR System Center Pacific
Haselkorn, Mark	University of Washington, CoSSaR
Hernandez, David	NSWC IHEODTD
Holliday, Ken	ODNI/PM-Information Sharing Environment
Holtzman, Joshua	Federal Aviation Administration (FAA)
Hussein, Chris	University of Washington, CoSSaR
Hornsby, John	Blacksky
Imme, Salvatore	Italian Navy/ Liaison Officer
Jackson, Chrisma	Sandia National Laboratories
Johnson, Troy	Air and Marine Operations CBP/DHS
Jones, David	University of Washington, Applied Physics Laboratory

Jones, Dennis	unknown
Jones, Mark	Pacific Northwest National Laboratory (PNNL)
Kee, Randy	University of Alaska Anchorage/Arctic Domain Awareness Center
Kessler, Michael	U.S. Navy
Kimball, Joe	U.S. Coast Guard, CG711 Aviation Forces
King, Greg	NGA
Kinoshita, Hideki	Secretariat of the Headquarters for Ocean Policy, Government of Japan
Kloske, John	SRI International
Kob, Paul	Oaklea Simpson Security, LLC
Kocak, Donna	Harris Corporation
Koeln, Greg	MDA Information Systems, LLC
Koeln, Greg	MDA Information Systems, LLC
Koscher, Karl	University of Washington, Computer Science & Engineering
Kubik, David	Johns Hopkins University, Applied Physics Laboratory
Lau, Edward	MDA Information Systems, LLC
Lea, Lyston	National Maritime Intelligence-Integration Office (NMIO)
Lee, Cassie	Vulcan Inc.
Lehnert, Hi Dee	DHS/CBP/AMO/AMOC
LeVitre, Rosanne	U.S. Government
Limjoco, Florian	PAE
Lynn, Ian	National Maritime Information Centre (UK)
Marburg, Aaron	University of Washington, Applied Physics Laboratory
Marshall, Mekisha	National Maritime Intelligence-Integration Office (NMIO)
Matijevich, Russ	HawkEye 360
Mays, Robin	University of Washington, CoSSaR
McBryde, Doris	Department of State (Foreign Affairs Office)
McDonald, Shawn	DHS S&T
Miller, Mark	U.S. Coast Guard
Mittleman, John	U.S. Naval Research Laboratory
Mottarella, David	Harris Corporation
Newberry, Dave	U.S. Coast Guard
O'Brien, John (Jay)	U.S. Coast Guard
Okamoto, Hidefumi	National Security Secretariat, Government of Japan
Olds, Bob	U.S. Navy Marine Mammal Program
Palmer, Neil	DSTL - NMIC Science Advisor
Paskal, Cleo	Chatham House
Payne, Craig	Johns Hopkins University, Applied Physics Laboratory
Pilliod, Paul	North Florida HIDTA
Pilsl, Brad	Booz Allen Hamilton
Pinkerton, Robert	Delaware State Police
Plankey, Sean	U.S. Naval Intelligence
Porterfield, Richard	Institute for Defense Analyses
Powell, Mark	Vulcan Inc.
Ramirez, Art	ORBCOMM
Raney, Chris	SSC-Pacific

Raymond, Joe	U.S. Coast Guard, Sector Puget Sound
Reid, Justin	Hydroid, Inc
Roberts, Mark	Defence Space 101
Robinson, Jana	Prague Security Studies Institute (PSSI)
Robison, Tom	NORAD (North American Aerospace Defense Command)
Roscoe, Elizabeth	U.S. Coast Guard
Ryan, Norbert	The Spectrum Group
Sanford, John	iMDA/Nimitz Operational Intelligence Center, ONI
Sappenfield, Everett	Department of Navy
Savelli, Sonia	University of Washington, Applied Physics Laboratory
Schgallis, Richard	NRL Naval Center for Space Technology
Schmidt, Harry	National Maritime Intelligence-Integration Office (NMIO)
Schorr, Sueann	U.S. Navy Reserve
Schroeder, William	The Spectrum Group
Shaffer, Gary	OPNAV N81
Sharp, Robert	National Maritime Intelligence-Integration Office (NMIO)
Shepherd, Lewis	George Mason University, Information Sciences & Technology
Shimizu, Shuji	Japan Aerospace Exploration Agency
Sisto, Frank	DoD Exec Agent for MDA
Stastny, John	Space and Naval Warfare Systems Center Pacific
Suchodolski, Jeanne	University of Nebraska, School of Law
Tachibana, Hiroshi	National Security Secretariat, Government of Japan
Tani, Leina	Vulcan Inc.
Thew, Kent	USCG, Maritime Intelligence Fusion Center Pacific
Thomas, George Guy	C-SIGMA LLC
Touchton, Robert	Leidos
Walker, Lewis Willis	Charleston County Sheriff's Office
Webster, Sarah	University of Washington, Applied Physics Laboratory
Wheeler, Sean	Royal Canadian Mounted Police (RCMP)
Wilgenbusch, Craig	U.S. Navy/SPAWAR Systems Center Pacific
Wilson, Tom	University of Washington, CoSSaR
Yamamoto, Aya	Remote Sensing Technology Center of Japan
Yancey, Sarah	University of Washington, CoSSaR
Zachry, Mark	University of Washington, CoSSaR

Appendix B: Agenda

Date	Time	Event
Tuesday 15 November	**0730 – 0830**	**Registration & Morning Coffee/Continental Breakfast**
	0830 – 0845	**Welcome Remarks** **Ms. Mekisha Marshall** *Chief Science & Technology Advisor* *National Maritime Intelligence-Integration Office* *&* **Dr. Mark Haselkorn** *University of Washington, Center for Collaborative Systems for Safety, Security and Regional Resilience (CoSSaR)*
	0845 – 0930	**Welcome Address** **Dr. Michael Bragg, UW, Dean of College of Engineering** *University of Washington* **Captain Joe Raymond** *Sector Commander, Coast Guard Sector Puget Sound* **Rear Admiral Robert Sharp** *Director, National Maritime Intelligence-Integration Office,* *Commander, Office of Naval Intelligence*
	0930 – 1000	**Keynote** **Mr. Lewis Shepherd** *Adjunct Faculty, George Mason University; Professor of Big Data Analytics at ODNI; Former Director and CTO, Microsoft Institute for Advanced Technologies*
	1000 – 1030	**Mr. Joshua Holtzman,** *Director, Federal Aviation Administration, Office of National Security Programs and Incident Response* How the Proliferation of Unmanned Aerial Vehicles affected Airspace and FAA Policy and set the stage for New Regulation for the safety of the Aviation Transportation System – Lessons Learned for the Maritime Community
	1030 – 1045	**Break**

	1045 – 1145	**Panel Session I: Unmanned Underwater Vehicles (UUVs) –** Autonomous capabilities have the potential to advance rapidly and the evolution of remotely operated underwater vehicles (ROVs) and autonomous underwater vehicles (AUVs), which can operate independently of direct human input, has become an important capability in maritime security domain. UUVs span across many applications to include commercial, exploration, defense and scientific research and provide the Global Maritime Community of Interest (GMCOI) with the ability to provide persistent maritime surveillance across a variety of missions. **Chair:** *Mr. David Jones, Director of Center for Environmental and Information Systems, UW Applied Physics Laboratory* **Speaker 1:** *Dr. Robert Touchton, Chief Autonomy Scientist, Leidos* **Speaker 2:** *Dr. Aaron Marburg, Senior Engineer, UW APL* **Speaker 3:** *Dr. Sarah Webster, Senior Engineer, UW APL*
	1145 – 1245	**Panel Session II: The Emergence of Space-Based Capabilities for Maritime Domain Awareness (MDA) –** The increasing role of space in the maritime domain and the latest technological advancements in space-based capabilities to enhance MDA offers opportunities to provide constant surveillance of maritime assets. **Chair:** *Dr. John Mittleman – Naval Research Laboratory* **Speaker 4:** *Dr. Jana Robinson – Space Security Program Director, Prague Security Studies Institute* **Speaker 5:** *Mr. Peter J. Marquez – Vice President, Global Engagement, Planetary Resources* **Speaker 6:** *Mr. John Hornsby – Vice President Sales and Business Development, Blacksky*
	1245 – 1300	**Workshop Photo**
	1300 – 1400	**Lunch**
	1400 – 1500	**Panel Session III: Securing Unmanned Autonomous Systems from Cyber Threats -** Emerging capabilities of unmanned autonomous systems span air, ground and undersea domains, but rapid advancement can increase the difficulty of securing network communication while also increasing the GMCOI's ability to share information. **Chair:** *Dr. Paul Shapiro, Professor at National Defense University* **Speaker 7:** *Mr. Egan Greenstein, The Boeing Company* **Speaker 8:** *Mr. David Aucsmith, Chief Scientist at root9B* **Speaker 9:** *Dr. Karl Koscher, UW Department of Computer Science & Engineering*

	1500 – 1700	**Group Parallel Collaboration Sessions for Day One Topics**
	1700 – 1730	**Group Parallel Collaboration Session Report Out and Wrap up - Adjourn to Reception**
	1800 – 2200	**Please join us for a reception at the Burke Museum, University of Washington (The reception is included in the workshop fee. Appetizers and soft drinks will be served along with a no host bar).**

Date	Time	Event
Wednesday 16 November	**0730 – 0800**	**Morning Coffee/Continental Breakfast**
	0800 – 0830	**Day Two Keynote Speaker** **Mr. Nicholas Andersen** Chief Information Officer, U.S. Naval Intelligence
	0830 – 0930	**Panel Session IV: Integrated Policy & Technology Issues –** Enhancing situational awareness of vulnerabilities, threats and consequences to the maritime domain is vital, but the lack of agreed upon policies on development, deployment and use is slowing the ability to field promising emerging technologies beyond R&D. **Chair:** *Dr. Mark Haselkorn, Director, UW APL Center for Collaborative Systems for Safety, Security and Resilience (CoSSaR)* **Speaker 10:** *Mr. Sean Wheeler, Marine Security Ops Center, RCMP* **Speaker 11:** *Ms. Melissa Braxton, PhD Candidate, Human Centered Design & Engineering (HCDE) UW* **Speaker 12:** *Mr. Shawn MacDonald, Program Manager, Borders & Maritime Security Division, DHS S&T*
	0930 – 1030	**Panel Session V: Technology Innovation & Trust-based Information Sharing in support of MDA –** Exploring trust-based information sharing as a key element in future strategies for comprehensive MDA. The U.S. and its partners are addressing challenges faced in the maritime domain through enhanced information sharing capabilities, but with these enhancements come significant policy, legal and operational issues to be addressed. ***Chair:*** *Dr. Sonia Savelli, Research Scientist, UW APL* **Speaker 13:** *Dr. Lilian Alessa, President's Professor and Director, Center for Resilient Communities (CRC) University of Idaho* **Speaker 14:** *Mr. John Sanford, Director, iMDA, Nimitz Operational Intelligence Center, ONI* **Speaker 15:** *Dr. Mark Haselkorn, Director, CoSSaR*
	1030 – 1045	**Break**
	1045 – 1145	**Parallel Collaboration Sessions for Day Two Topics**

	1145 – 1230	**Lunch**
	1230 – 1330	**Parallel Collaboration Sessions**
	1330 - 1515	**Report out on Parallel Collaboration Sessions -Takeaways and the Path Forward** Present session conclusions, insights and the path forward for current and emergent technological advancements to enhance MDA
	1515 -1530	**Closing Remarks**