The Defense Science Board Task Force on the Role of Autonomy in DoD [U.S. Department of Defense] Systems defines autonomy as “a capability (or a set of capabilities) that enables a particular action of a system to be automatic or, within programmed boundaries, ‘self-governing.’” Autonomy is rarely absolute. Rather, it is on a spectrum extending from no autonomy (in which a system’s decisions and actions are completely controlled by humans) to full autonomy (which requires no human involvement). Most autonomous systems lie somewhere in between.

At the outset, we need to distinguish between autonomous systems and unmanned vehicles. The two sometimes overlap but are not synonymous. Most civilian unmanned vehicles currently in use are remotely controlled by humans and have little or no autonomy, while the degree of autonomy for military
A human might perceive a system’s autonomous capabilities as greater than they are or might become passive through boredom. Alternatively, a human might attempt to interfere in a system’s decisionmaking, hindering its effectiveness and potentially overwhelming it with inputs.

Exerts no control—it can be also be a fixed system that makes decisions with little or no human input (e.g., autonomous systems that immediately respond to cyberintrusions or deconflict vessel traffic).

Gradations of autonomy have been established for different applications; for example, the ability of civilian cars to drive themselves is delineated on a 0–5 scale. For some autonomous systems, the roles of humans have also been characterized (e.g., “in the loop” and “on the loop”). Managing a system with a moderate degree of autonomy is often particularly challenging. A human might perceive a system’s autonomous capabilities as greater than they are or might become passive through boredom—factors that have contributed to autonomous-vehicle fatalities. Alternatively, a human might attempt to interfere in a system’s decisionmaking, hindering its effectiveness and potentially overwhelming it with inputs.

The level of trust that humans grant an autonomous system will increase as autonomous capabilities grow, leveraging other parts of emerging information technology, such as improved sensors, machine learning, “big data,” and artificial intelligence. Future autonomous capabilities, leveraging that trust, will likely change many aspects of the Marine Transportation System (MTS) while presenting new workforce, regulatory, legal, and operational challenges for the U.S. Coast Guard.

Background: Evergreen Workshop Recurring Themes

This Perspective builds partly on the Evergreen Pinecone workshop on future threats to the MTS, which was held in November 2019, in conjunction with the annual Maritime
Risk Symposium. The workshop involved about 70 participants from the Coast Guard, academia, government agencies, and the maritime industry and was conducted over two half-day sessions at Maritime College, State University of New York. Participants were split into four groups, each of which was given a plausible state of the world in 2030. Members of the group then noted key opportunities and challenges for the Coast Guard stemming from that state of the world, as well as implications with an ambiguous potential impact on the Coast Guard. They then grouped these items into a series of clusters, each of which related to an overall risk. The risks were assigned relative values in terms of their importance for the MTS and the level of difficulty associated with addressing them. Each group then focused on a particular risk that was both important and difficult, describing its potential evolution and key implications, and shared these insights with the other groups.

Several recurring themes throughout the workshop have implications for the future of the MTS, some of which relate to autonomous systems:

- **differential paces of technological adoption**, given that private-sector companies and illicit actors might adopt novel technologies more rapidly than government agencies do because they have greater funding and organizational agility. These technologies include advances in autonomous systems that operate in the maritime domain, which could put response and regulatory agencies at a disadvantage in the timely completion of appropriate planning, regulatory, legal, and operational responses to developments.

- **workforce competence** because personnel must be capable of handling both advanced and legacy technologies, as well as partially autonomous systems. This affects the ability to recruit and retain personnel with those technological skill sets that are in increasingly high demand.

- **uncertainty about capacity demands throughout the MTS** as sources, destinations, quantities, and types of goods evolve. It is unknown how the industry will adapt and whether government agencies will be able to keep pace with the speed of technology as cargo ships, work boats, and port facilities become more automated.

- **climate change** altering the physical environment, potentially making obsolete some aspects of systems' and humans’ environmental knowledge over time. Climate change can also damage infrastructure. In some cases, the response to climate change might also entail the use of physical barriers to protect shorelines, but these barriers can themselves impede navigation.

- **governance challenges** as nations aim to address technological, economic, and environmental changes without imposing conflicting policies that hinder activities in the MTS or pose new unintended, unanticipated risks.

- **increased disease risks** due to denser populations of people and livestock, greater mobility, overuse of antibiotics, climate change, and diminished international cooperation.

- **increased Arctic activity** due to greater accessibility to and maritime activity in that region, even as land infrastructure becomes harder to build and maintain because of climate effects, such as thawing permafrost and coastal erosion. Indigenous
communities might be affected by rapid changes to habitats and resulting sources of food. The commercial and tourist use of Arctic shipping routes could increase the need for rescue capabilities.

Key Trends in Automation

Several important trends in autonomous systems could have meaningful effects on the future MTS and the Coast Guard’s role in it:

- **increased numbers and capabilities:** Advances in autonomy will likely continue, and capabilities will become available to more actors. Autonomous systems will increasingly be used by those the Coast Guard assists, regulates, counters, and encounters, as well as by partner agencies and the Coast Guard itself.

- **multisystem autonomous operations:** Technologies that help multiple autonomous systems coordinate their behaviors are emerging. Autonomous systems need to be able to coordinate not only with each other but also with manned or remotely controlled systems; they also need to interact with their physical environments (e.g., animals, winds or currents, and obstacles).

- **multidomain autonomous operations:** For the past couple of decades, unmanned-vehicle advances have been most concentrated in the air domain. However, unmanned and increasingly autonomous vehicles are emerging on the water’s surface, under the water, and on land. Autonomous vehicles will increasingly interact across domains, and some individual vehicles will be able to operate in more than one of them.

- **human–machine interfaces:** There is a critical need to ensure that humans and autonomous systems understand each other’s behavior and decisions in ways that reduce risk. Although the algorithms underlying autonomous systems are known, the interactions between machine and environment can lead to unexpected results. Although there are rapid advances in human–machine interfaces and efforts to better convey to humans what is happening, the growing complexity of machines (including autonomous ones) makes this a continuing challenge.

- **increased miniaturization:** Capacities for energy harvesting and storage will grow, even as the corresponding devices shrink. Sensors, information technology hardware, and other systems are also shrinking, increasing payload ratios for unmanned vehicles, including those operating autonomously.

- **increased importance of data sciences:** Because of increasing numbers of sensors and growing volumes of traffic, the amount of information associated with the MTS is also growing. At the same time, the ability of data sciences—such as big data, machine learning, and artificial intelligence—to analyze and act on these data sets is also increasing. This requires a critical evaluation of the viability of complex multimission autonomous platforms versus that of simpler platforms that cooperate with one another, given the challenges of communicating and interpreting large amounts of data. As data sciences advance over time, they will shape choices about
the right mix of autonomous capabilities within the Coast Guard.

In addressing how autonomous systems affect the MTS, the Coast Guard will most likely confront the following issues over various timelines:

- In the **near term (zero to five years)**, the Coast Guard can work to develop policies and limited technological changes to address current and emerging developments. It can also lay the groundwork for the introduction of more-advanced technologies and for policies to address the use of those technologies by others.
- In the **medium term (five to ten years)**, the Coast Guard can work on selecting technologies to incorporate into its capabilities, developing appropriate policies and plans, and finding both technological and nontechnological solutions to challenges posed by autonomous systems.
- For the **long term (ten to twenty years)**, the Coast Guard can be thinking creatively about emerging opportunities and threats involving autonomous systems, taking into account not only technological advances but also changes in the operational environment and other contextual factors. For example, it can seek to improve recruitment, training, and retention of people with particular skills relating to the operation and maintenance of autonomous systems.

**The Impact of Autonomous Systems on Coast Guard Roles, Statutory Missions, and Mission Enablers**

In this section, we review ways in which the Coast Guard will likely be dealing with autonomous systems in the MTS in the context of its operational roles and statutory missions. In addition, we address the broader category of mission enablers, as well as opportunities and challenges in the near term and further into the future. As autonomous systems become more capable and cost-effective, the Coast Guard could use them in a variety of contexts.

**Maritime Safety**

The maritime domain is particularly challenging for autonomous vehicles. Autonomous USVs operating on a moving surface, subject to forces from above and below, must be able to adhere to the Convention on the International Regulations for Preventing Collisions at Sea, 1972, and to avoid collisions with vessels that might not be obeying those regulations.3 These vehicles also need to avoid capsizing or having accidental collisions with fixed infrastructure.4 Autonomous UUVs need to operate without access to electromagnetic information (e.g., the Global Positioning System) because of the attenuation of electromagnetic energy underwater, while navigating in a complex, dynamic, three-dimensional environment. Autonomous systems have not yet caused a major accident in the MTS, although the Coast Guard needs to anticipate and address the potential. For example, if two large USVs collide in a major shipping channel, the Coast Guard will have to work...
to prevent obstruction of the channel, even in the absence of personnel aboard either vessel with whom to coordinate.

The Coast Guard missions affected in terms of maritime safety are

- **Search and Rescue**: UASs can serve as more-numerous and cost-effective search assets than manned aircraft. Those with sufficient payloads could drop beacons to facilitate rescue and provide supplies for those in danger. In addition, USVs could enable conscious victims to be brought to shore. Some could be stationed offshore for long periods, then respond when alerted, arriving faster than a boat coming from shore and relieving the safety concerns of having manned aircraft in reduced-visibility, high-seas, and high-wind conditions.

- **Marine Safety**: UASs could help the Coast Guard observe possible safety risks: Handheld autonomous systems (e.g., small snake-like or crawling systems) could get into confined spaces to detect possible risks, greatly reducing the safety concerns about having humans enter confined spaces—concerns that have plagued the marine industry.

### Maritime Security

Remotely controlled UASs are already being used by criminals to monitor, interfere with, and bypass law-enforcement agencies. These systems are hard to counter through electronic or kinetic means; moreover, unless they are captured, it is hard to definitively attribute them to particular individuals or organizations. As technology advances, smugglers will increasingly be able to use autonomous unmanned vehicles to gain situational awareness, to reduce risks and costs, and to interfere with Coast Guard operations (e.g., by jamming key frequencies, creating distractions, or colliding with Coast Guard assets). The relevant Coast Guard missions are

- **Ports, Waterways, and Coastal Security**: UASs could monitor for possible threats, and visible UASs could deter them. USVs could physically interdict possible threat vessels and, with appropriate sensors, monitor for undersea threats. Unmanned vehicles could also cue humans and, when authorized, use force.

- **Migrant Interdiction**: Visible UASs and USVs near shorelines could deter illegal migration. They could also aid in tracking vessels, communications, and rescue operations.

- **Drug Interdiction**: UASs could provide situational awareness less expensively than manned platforms can. In large areas, UASs could be launched from and recovered by USVs that would also provide power and conduct maintenance diagnostics. (Tethered balloons or UASs could also be used by USVs to achieve altitude in a fixed location, without the complexity of launch and recovery.) Visible, audible UASs could be used to induce compliance (for example, ordering a vessel to stop). With human authorization, UASs could eventually employ warning shots and disabling fire against noncompliant vessels. USVs that linger in the environment could also be used to physically interdict drug vessels when needed and remain undetected thanks to their small size. With the right sensors, USVs could help detect semisubmersible or submersible threats.
• **Defense Readiness**: Implications here are the same as those for Ports, Waterways, and Coastal Security, although requiring more consideration of how autonomous systems could interoperate with U.S. Department of Defense systems, particularly during contingencies.

**Maritime Stewardship**

Overall, autonomous systems could potentially facilitate the efficient movement of goods and people through the MTS while also reducing resource costs and helping to ensure the continuity of the MTS. The Coast Guard missions affected are

- **Ice Operations**: There are applications for autonomous systems in support of polar and domestic icebreaking operations. UASs or light UGVs preceding icebreakers could observe ice conditions to support safe ship navigation. UASs could also be used in support of the International Ice Patrol, reducing costs in identifying and tracking icebergs in lieu of predictive methods and time-consuming, potentially hazardous manned missions.

- **Living Marine Resources**: Autonomous fishing could bring unprecedented changes to the fishing industry in the ways in which fish are caught, processed, and brought to the market, requiring some commensurate level of monitoring and regulation enforcement. It could also result in a dramatic reduction in the number of injuries and fatalities associated with manned commercial fishing, routinely regarded as one of the most-hazardous occupations. UASs and USVs could be used to monitor closed areas and to observe vessels and their behaviors.

- **Aids to Navigation (ATON)**: Through the use of UASs, the Coast Guard could monitor the physical condition of ATONs and, through exchange of information with self-diagnostic technology on the ATONs, could reduce the use of limited resource hours and potentially the future need for manned maintenance activities at sea, which is regarded as both dangerous and arduous work.

- **Marine Environmental Protection**: Spill responses are inherently dangerous missions. They often occur in remote and unforgiving terrain, where this risk is magnified. Real-time aerial views provide site evaluation, hazard identification, and responder orientation. With expanding payloads, potential mission-set opportunities increase dramatically, such as through remote air monitoring and infrared cameras. Autonomous systems could mitigate or eliminate significant hazards. UASs for spill assessment and response could provide commands with a rapid and clear operating picture while simultaneously acting as a force multiplier for responders. A UAS operating on a spill site could identify the source, determine the extent of impact, and direct response efforts, allowing the prioritization of resources and personnel. These capabilities could translate into increased recovery rates and reduced impacts to the marine environment. UASs, USVs, and UUVs could monitor spills. USVs could deploy cleanup materials into the water or recover contaminants. Handheld autonomous tools could be used in tight spaces on a ship to observe possible
violations or aid in inspection and investigation of marine casualties.

- **Other Law Enforcement:** UASs and USVs could monitor key areas or particular vessels. If visible, they could also contribute to deterrence.

### Mission Enablers

Autonomous technologies could also enable missions by improving critical functions:

- **logistical support:** Having autonomous delivery vehicles could cut personnel requirements and reduce the logistical challenges of offshore supply operations by, for example, potentially increasing on-station time.

- **training:** Autonomous vehicles could reduce personnel requirements and costs for training by serving as noncompliant vessels or vessels in distress, targets for use of force, towing, underway replenishment, refueling, and other multivessel operations.

- **command, control, communications, computers, intelligence, surveillance, and reconnaissance:** Because attackers are likely to use rapid, algorithm-based capabilities for cyberattacks, the Coast Guard will likely need similarly rapid and automated capabilities to defend its networks. The Coast Guard could use autonomous fixed systems to coordinate operation of unmanned vehicles that are providing communications and intelligence, surveillance, and reconnaissance capabilities, as well as to coordinate among manned and unmanned platforms. It will also need to partner with other government entities for their unmanned assets. However, using autonomous systems also creates vulnerabilities: The “cyberattack surfaces” of systems grow with increasing autonomy and complexity. The Coast Guard should anticipate diverse types of cyberthreats, including those involving insider elements. It also needs to address electronic warfare threats, such as jamming and spoofing.

Commercially available hobby UASs can already be a menace by interfering with flight operations, monitoring law enforcement, or illicitly moving small amounts of drugs; in the future, they will become more autonomous, more numerous, and more capable.
Other Challenges and Opportunities

Regulation

As addressed in the *Maritime Commerce Strategic Outlook*, “The Coast Guard must promote a shift from a rules-based regulatory structure in the maritime environment to a risk and principles-based regulatory structure to keep pace with emerging issues and technology advancements, such as electronic and autonomous systems.” The Coast Guard already faces remotely operated UASs, primarily owned by hobbyists and regulated by the Federal Aviation Administration, operating in the MTS. Even if the Federal Aviation Administration were to retain primary regulatory oversight of UASs, the Coast Guard will be responsible for regulating commercial and recreational use of other unmanned vehicles, including USVs, UUVs, and even UGVs (the latter primarily in port environments), that could create safety hazards. As a result, the Coast Guard will need to develop policies and protocols for preventing unsafe or unlawful behaviors, including licensing, certification, and countermeasures against unauthorized usage. Commercially available hobby UASs can already be a menace by interfering with flight operations, monitoring law enforcement, or illicitly moving small amounts of drugs; in the future, they will become more autonomous, more numerous, and more capable. It is even possible that, in a few decades, autonomous USVs will be delivering goods or conducting commercial fishing, requiring further regulation. Meanwhile, the Coast Guard has the advantage of being a leader in the international maritime community to help shape standards and guidelines on autonomous systems.

Response

Autonomous systems have not yet caused a major accident or security breach in the MTS, although the Coast Guard needs to anticipate and address such threats. For example, if two large USVs collide in a major shipping channel, the Coast Guard will need to prevent obstruction of the channel, even in the absence of personnel aboard either vessel with whom to coordinate.

Law Enforcement

Remotely controlled UASs are already being used by criminals to monitor, interfere with, and bypass law-enforcement agencies. The use of these systems is hard to counter through electronic or kinetic means; moreover, unless these systems are captured, it is hard to definitively attribute them to particular individuals or organizations. As technology advances, smugglers will be increasingly able to use autonomous unmanned vehicles to gain situational awareness, to reduce risks and costs, and to interfere with Coast Guard operations (e.g., by jamming key frequencies, creating distractions, or colliding with Coast Guard assets). As autonomous USVs and UUVs become more capable, and autonomous smuggling UASs become harder to discern amid large numbers of innocuous UASs, the Coast Guard will have to find ways to address these new and increasing threats.

Partnerships

If the Coast Guard is to effectively monitor this emerging technology in the maritime environment, the importance of creating, maintaining, and improving information...
sharing and relationships with interagency partners and the maritime industry will only continue to grow. Federal, state, local, international, and private-sector partners are beginning to use autonomous systems in a variety of capacities. The extent to which such systems are used and the degree of autonomy they have will likely increase over time. For these reasons, the Coast Guard will increasingly need to interact with other entities’ autonomous systems. For example, when responding to an oil spill, the Coast Guard might interact with other agencies’ autonomous UASs that are being used to monitor the situation; in time, it might also interact with private-sector USVs that contribute directly to cleanup.

Conclusion

In this Perspective, we have briefly highlighted key aspects of autonomous systems and their potential to affect the MTS, as well as how they might shape the Coast Guard’s relevant roles, responsibilities, and capabilities. Autonomous systems will increasingly be used by legitimate actors, criminals, and attackers, as well as by the Coast Guard and many other partner agencies. In the next decade and beyond, the Coast Guard will increasingly need to incorporate issues relating to autonomous systems into its strategies, policies, concepts of operations, and tactics.

Further Reading

The literature about autonomous systems and their prospective applications is voluminous and growing. In addition to the works cited in this Perspective, the interested reader can consult the following publications.


In the next decade and beyond, the Coast Guard will increasingly need to incorporate issues relating to autonomous systems into its strategies, policies, concepts of operations, and tactics.


**Notes**


4. The U.S. Navy’s Sea Hunter USV program is working to address many of these challenges. See, for example, Joseph Trevithick, “Navy’s Sea Hunter Drone Ship Has Sailed Autonomously to Hawaii and Back Amid Talk of New Roles,” The Drive, February 4, 2019.


**References**


About This Perspective

This Perspective documents support by the Homeland Security Operational Analysis Center (HSOAC) to the U.S. Coast Guard’s Evergreen project. Founded in 1996, Evergreen is the Coast Guard’s strategic foresight initiative, which has historically run in four-year cycles and uses scenario-based planning to identify strategic needs for the incoming service chief. In 2019, Evergreen was restructured in order to best support executive leaders in their role as the Coast Guard’s decision engines. The project objective is to help posture the Coast Guard to better bridge the gap between future challenges and near-term plans, which typically focus on the urgent needs of the present. HSOAC analysts reviewed Evergreen activities, examined Coast Guard strategy-making and planning processes, adapted an approach for developing scenarios, and narrated a set of exemplar global planning scenarios. The individual Perspectives that resulted from this project reflect themes and specific subjects that have emerged from a series of workshops that were conducted with subject-matter experts and were identified as areas of particular interest for senior leadership strategic-planning activities and emerging policy development.

This research was sponsored by the U.S. Coast Guard Office of Emerging Policy and conducted within the Strategy, Policy, and Operations Program of the HSOAC federally funded research and development center (FFRDC).

The RAND Corporation operates HSOAC under contract to the U.S. Department of Homeland Security (DHS). RAND is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. For more information, visit www.rand.org/hsrd/hsoac.

About the Authors

Scott Savitz is a senior engineer at the RAND Corporation. Much of his research focuses on how to improve the effectiveness and resilience of operational forces, as well as the impact of reallocating resources among those forces. He has a PhD in chemical engineering.

Aaron C. Davenport is a senior policy researcher at the RAND Corporation. His research focuses include border and maritime security, emergency preparedness and response, occupational health and safety, and national security strategy. He is a graduate of the U.S. Coast Guard Academy and retired Coast Guard senior officer with security assistance, search-and-rescue, and law-enforcement experience. He has an MS in environmental sciences, with a certificate in industrial hygiene and a minor in hazardous materials.

Michelle D. Ziegler is a technical analyst at the RAND Corporation. Her research focuses include U.S. Army logistics, disaster recovery, U.S. Coast Guard capability and capacity analysis, and cooperation and domain awareness in the Arctic. She has an MS in astronomy.

The Homeland Security Act of 2002 (Section 305 of Public Law 107-296, as codified at 6 U.S.C. § 185) authorizes the Secretary of DHS, acting through the Under Secretary for Science and Technology, to establish one or more FFRDCs to provide independent analysis of homeland security issues. The RAND Corporation operates HSOAC as an FFRDC for DHS under contract HSHQDC-16-D-00007.

The HSOAC FFRDC provides the government with independent and objective analyses and advice in core areas important to the department in support of policy development, decisionmaking, alternative approaches, and new ideas on issues of significance. The HSOAC FFRDC also works with and supports other federal, state, local, tribal, and public- and private-sector organizations that make up the homeland security enterprise. The HSOAC FFRDC’s research is undertaken by mutual consent with DHS and is organized as a set of discrete tasks.

The information presented in this Perspective does not necessarily reflect official DHS opinion or policy.

For more information on this publication, visit www.rand.org/t/PE359.