Unmanned Systems: an Emerging Threat to Waterside Security

Bad robots are coming

Mark R. Patterson
Autonomous Systems Laboratory
Virginia Institute of Marine Science
Gloucester Point, Virginia, 23062, USA
mrp@vims.edu

Susan J. Patterson
Below the Waterline Security
116 Henry Tyler Drive
Williamsburg, Virginia, 23188, USA
belowthewaterline@me.com

Abstract—**Unmanned Vehicles (UxVs) are now a key Intelligence Surveillance and Reconnaissance (ISR) resource for first-world defense organizations. But the barrier to entry for making unmanned systems has fallen, with terrorist groups and crime syndicates capable of creating sophisticated robots using Commercial Off-The-Shelf (COTS) components. With the explosive growth of unmanned systems in the air, on the water, and underwater, the threat from misuse of these technologies increases. Maritime Domain Awareness (MDA) for ports, harbors, and protection of cruise ship and military marine assets has largely focused on threats above the waterline from more conventional threats like suicide boaters, or unauthorized entry. MDA at and below the waterline presents severe but not insurmountable challenges. Effective risk mitigation from UxVs involves a probabilistic approach to disruptive scenarios that reverse-engineers the Concept of Operations (CONOPS) likely to be used, based on the capabilities of rogue UxVs, and the skill level of their operators. Consideration of oceanographic and meteorological data available to the public in real-time or near real-time from observing systems is part of the risk prediction. Technical countermeasures that exploit rogue UxV weaknesses, and training of personnel involved in MDA, are logical components to close the gap. Our group is developing approaches to reduce risks of successful UxV attack, and crafting appropriate responses to an unmanned systems disruption. We also are developing new tools and training measures that will be of use to waterside security personnel.**

Keywords-UxVs; terrorist use; Maritime Domain Awareness (MDA); Autonomous Underwater Vehicles (AUVs); Autonomous Surface Vehicles (ASVs); rogue robot

I. INTRODUCTION

"Therefore, important components of STA [Situation and Threat Assessment] are the identification of the "different", "unknown", "unconventional", or "unimaginable" and the discovery of underlying causes of observed situational items and their behavior." - [1, p. 111]

The destructive power of individuals and small groups of actors has increased exponentially within the last few decades in large part because of increased access to sophisticated technologies [2]. One set of technologies now within the reach of terrorist groups, criminal organizations, or disgruntled individuals are unmanned systems, which can be fully autonomous. For the purposes of this paper we refer to unmanned vehicles as UxVs, where x can equal U (Underwater), or S (Surface = boat). The focus of our investigation is how rogue actors could use UUVs and USVs to compromise waterside security, and how this risk might be mitigated. Our analysis does not address mines, another significant threat to waterside facilities [3], or attack by Unmanned Aerial Vehicles (UAVs), only attack by UUVs or USVs. We also do not address how to defend against a fast-moving torpedo-like UxV (or a stolen torpedo), because we believe it is beyond rogue operator capability at this time. Detection of bad robots and strategies for reducing the success of an attack is not an explicit part of current strategies for Maritime Domain Awareness (MDA) [4].

II. UNMANNED SYSTEMS THREATS TO WATERSIDE SECURITY

A. A Hole in Maritime Domain Awareness?

Maritime Domain Awareness for ports and harbors has focused on methods for detecting and thwarting suicide boaters [5], swimmers [6], larger vessels that may have been compromised below the waterline [7], and unauthorized access to waterside facilities inside the fence [8]. A related problem, security of cargo, has received great attention because of the potential for a compromised container to act as a vector of something bad into a working port [9]. Homeland security agencies in the developed world often divide intelligence and surveillance resources as a function of distance of the approaching ship from the homeland coast, using a layered approach that maximizes threat reduction per dollar spent. Unmanned system threats have rarely been considered, with a notable exception being a recent study by the RAND Corporation [10] that analyzed UAV threats to population centers, but not specifically as a threat to a port or harbor. Hezbollah has used UAVs to enter Israeli airspace [11] and to attack a warship [12]. The conclusion of [10] was that while the UAV threat is credible it is still a niche threat, because other less technical means of executing an attack are likely to be favored in the near future, as they are perceived to have a higher success probability by a terrorist group.

Threats to waterside security at or below the waterline from unmanned systems are often dismissed by security personnel

Travel support provided by J. Wells, Virginia Institute of Marine Science, College of William & Mary.

for several reasons: (a) Lack of near-term intelligence that an actor has a working unmanned asset, (b) back of the envelope calculations that the waterside asset could not be destroyed using the payload capacity possible using a Do It Yourself (DIY) UxV, and (3) the necessity for a precision hit to sink a hardened target like a modern warship. We believe this analysis ignores the significant asymmetric warfare value of disrupting a working port, including the attendant economic losses that could stretch for indefinite periods of time. Our analysis focuses on how to mitigate the threat posed by a UxV attack.

B. Few Barriers to Making and Using Sophisticated UxVs

The Internet is an expanding source of information useful in the construction of UxVs. The genie is now out of the bottle. Given the explosive growth of UxVs as multi-billion dollar industries, it is not surprising that DIY hobbyists have assembled sophisticated systems using COTS components. For example, a DIY UAV recently flew over Google headquarters and took high-resolution pictures [13]. The numbers of young persons well-versed in UxV technology is also increasing exponentially, in part inspired by the success of high-school and college-level robotics competitions [14, 15]. Resources available for inspiration and use by our next generation of tech workers unfortunately could be used for terrorist purposes. Subsystems useful in rogue UxV fabrication, e.g., smartphones with integrated GPS, attitude and rate sensors, are now common consumer items. The widespread availability of UxV components greatly increases the probability that a sophisticated UxV will be assembled inside the target country by rogue actors. There is precedent for the approach of assembling an offensive technology from components inside a defended perimeter by terrorist groups [16].

Both underwater and surface vehicles are potential instruments for use by terrorists. Underwater vehicles are more complex technically with respect to navigation and water proofing against pressure at depth, but achieve greater stealth. Surface vehicles are easier to detect during approach, but still pose significant risk if launched in large numbers during a single swarming attack. A recent exercise in Canada used a swarm of USVs, controlled by a single operator, to simulate a suicide boat attack (USS Cole-style incident) during a target training exercise [17]. Although the goal of using the USVs was training for defense against suicide boaters, it provides a sobering example of UxV potential to cause mayhem, when viewed through a different lens.

Operators of UxVs for non-terrorist purposes include hydrographic agencies, defense agencies, resource management agencies, and academic institutions. Although underwater vehicles are under export control, many of these assets are poorly protected in their home institutions, and could be easily stolen.

All UxV missions share commonalities, even those launched by terrorists. The common stages are mission planning, launch, and mission supervision. Proper mission planning includes an analysis of bathymetry, water density, and currents, which includes the state of the tide. Compared to a traditional oceanographic sampling mission, a terrorist UxV mission would be relatively short. Batteries that would otherwise be used for hotel and thrust load can be removed, and the space gained is now available for explosives or a chemical, biological, or radiological agent. Similarly, some navigational sensors may be sacrificed to increase the destructive payload at the expense of a navigational accuracy that would be irrelevant for a planned terrorist mission.

Real-time ocean observing systems are a great aid to mission planning and execution. Best practices for UxV mission planning and execution include acquiring *a priori* knowledge of the environment to be surveyed. Knowledge of water temperature and salinity can be used to compute water density, useful in properly ballasting a UxV in a variable salinity environment. Likewise, profiles of currents through the water column allow better dead-reckoning, through computation of likely set and drift; access to these pre-mission planning data increase the probability of a successful rogue UxV mission.

Availability of real-time observing systems are increasingly accessible and public world-wide, for example the Physical Oceanographic Real-Time System (PORTS) operated at 21 ports by the U.S. National Oceanographic and Atmospheric Administration (NOAA) as an aid to commercial shipping ([18], Fig. 1). Such systems protect the environment by reducing the likelihood of ship grounding by reporting salinity, temperature, currents, water level, and meteorological conditions. These systems allow mariners to safely utilize every available inch of draft in dredged channel, which can translate into tens to hundreds of thousands of dollars (US) savings per transit [18]. Data available from such systems vary by location. An example data set is show in Fig. 2. These data would allow a UxV to be properly ballasted several km from the target, with very accurate predictions of transit times. The UxV could also interrogate data from such systems during the execution of the mission, if the UxV can access a cellular wireless network. This could allow the UxV to make mid-mission adjustments, and redirect to a new target or abort if conditions change.

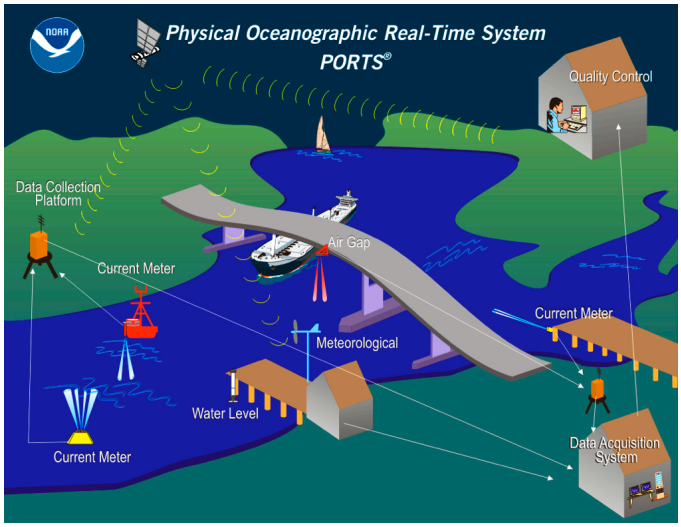

Figure 1. Example of an ocean observing system infrastructure, PORTS, developed by NOAA to reduces the risk of ship grounding and increase economic efficiency. (Credit NOAA).

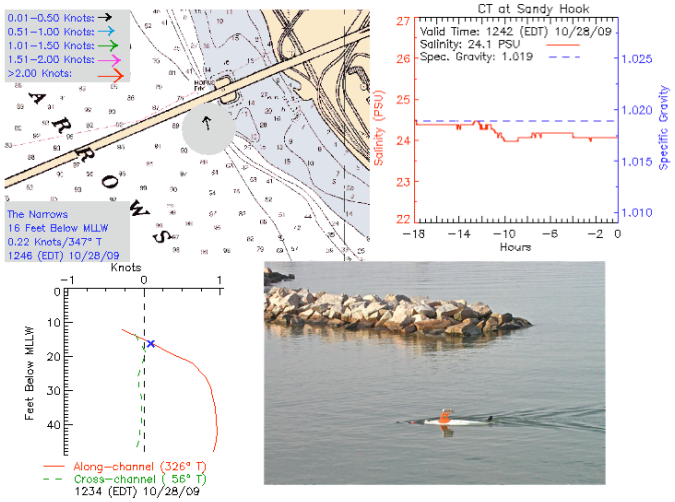

Figure 2. Examples of oceanographic data (top left: current direction, top right: water density, bottom right: water column profile of current speed) available in real time from an observing system that would be useful in planning and executing a rogue UxV mission. (Line figures: Credit NOAA; UxV photo: Credit Virginia Institute of Marine Science)

As will be discussed below, availability of such data needs to be factored into a probabilistic model of credible UxV attack. In particular, a simulated mission generator using such real-time data could be used to generate likely arrival times for rogue UxV missions from likely launch footprints. Likely launch locations include areas removed enough from the port or harbor so as not to have constant surveillance from the waterside, or conversely, areas so close to the port that the security personnel would have little time to react to a UxV attack, even if the launch was observed.

C. *Asymmetric Warfare Scenarios*

UxVs offer some significant advantages to a terrorist group. UxVs provide a great stand-off distance from the target. They potentially allow a sequence of attacks over time, a campaign that could provide very disruptive to a waterside facility. The nature of the technology also allows swarming attacks that can overwhelm defensive systems. The cost per UxV unit is relatively low (thousands to tens of thousands US dollars). The technology lends itself to "person in the loop" control via wireless, but can switch to a fully autonomous attack should the person controlling the UxV be compromised. Fully autonomous ("fire and forget") missions allow the actor to observe results with operational pressure during the attack. They also allow the terrorist group more flexibility in initiating additional indirect attacks on responses to the initial attack, during the ensuing chaos.

UxVs were developed by national defense agencies for ISR missions [19]. A rogue UxV also provides a useful platform for terrorist ISR. A waterside facility could be penetrated and surveyed prior to using the technology to attack infrastructure. ISR from a rogue UxV could also be useful to a terrorist group prepared to use a suicide boater, or shore-side delivery of an agent or explosive by more conventional means like a car or truck. Repeated penetrations of a waterside facility by a terrorist UxV to gather ISR greatly increase the chances of success when a real attack is initiated. Data collected by the UxV in the form of imagery or sonar would useful in psychological warfare against the waterside facility, e.g., pictures of commercial or military ships taken at or below the waterline provided to the media would showcase the capabilities of the group to act at will.

Explosive payloads likely to be carried by UxVs range from the suicide bomber size [9 kg C-4 equivalent] to small car bomb size [100 kg C-4 equivalent]. We base this assessment on the high likelihood that a terrorist group would design a direct-attack UxV to be portable by two persons, thus limiting the mass of the platform. While these platforms would not be capable of sinking a modern warship, they could be used to attack more vulnerable infrastructure such as pipelines, floating piers, large and small commercial vessels, and docks and transportation tunnels that often pass underwater at geographic choke points.

Because UxVs are so small, and potentially could be present in small numbers, they offer a significant advantage in asymmetric warfare by sowing uncertainty, the perfect example of "something lurking out there". Attack by a single UxV would compel a waterside facility to assume more UxVs were present and another attack imminent. The economic chain reaction from a slowing or stopping of port traffic has been examined and is substantial [20].

D. *Need for Risk Mitigation*

UxV technology, and modes by which it would used to attack a port or harbor, have significant differences to threats already identified by the waterside security [21]. Without planning in place for such an attack, the likelihood of an inappropriate response based on other threat scenarios increases. Risk mitigation is possible for any threat including unmanned systems. We now present some thoughts on how to achieve this.

III. Risk Mitigation from Terrorist Unmanned Systems

Our scheme for reducing risk involves analysis of several steps in the "supply chain" for a terrorist UxV attack (Fig. 3). This involves reverse engineering how the UxV will actually be used, developing methods of predicting threat levels within a waterside facility for the use of security personnel, employing technical measures in close proximity to stationary targets, instituting movement and path tactics when transiting, and properly training all waterside personnel to recognize an unmanned system attack.

A. *Reverse Engineer Terrorist CONOPS*

A decision must be made at an early stage by a terrorist group as to whether to deploy a USV (robotic boat) or UUV (robotic underwater vehicle). A USV allows delivery of a bigger payload (e.g., explosives) but carries significant costs among them: 1) a USV of significant size is large and hard to transport without attracting attention (e.g., it requires a boat trailer), 2) during its operation it would be necessary to convince a casual observer that a person was at the helm, and 3) there are

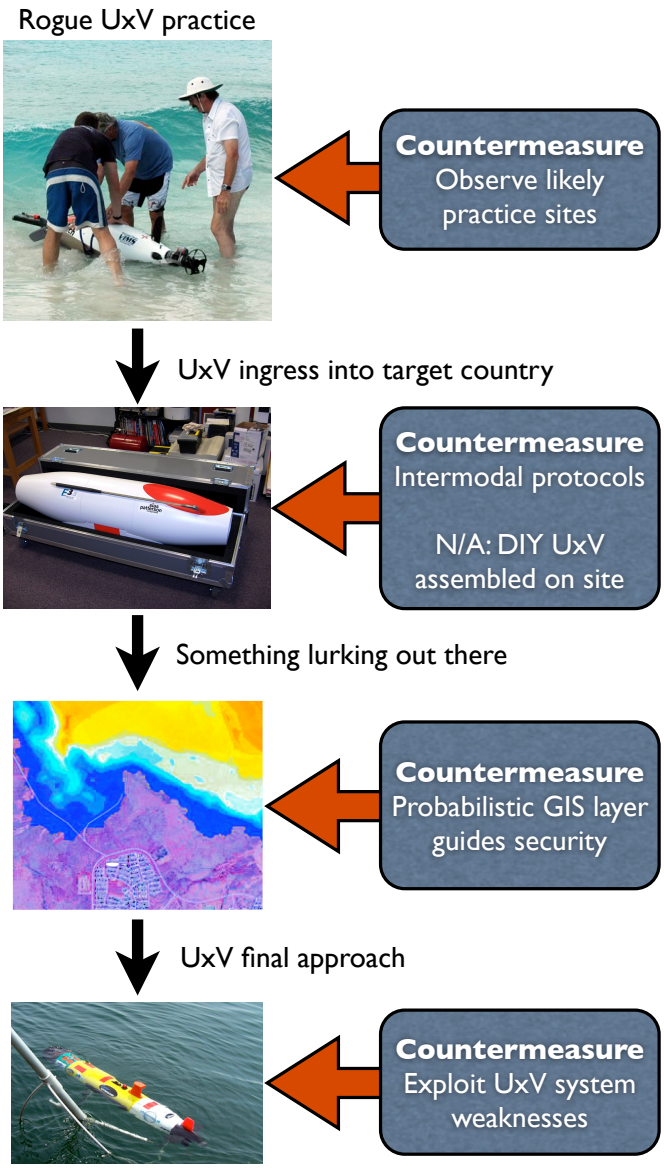

Figure 3. Defeating a rogue UxV entails several opportunities for countermeasures. (Credits: Top, bottom: NOAA)

significant investment of resources in the development of algorithms that detect the approach of suicide boaters, driven in part because of the successful attack on the USS Cole [22]. These measures would need to be overcome to reach the target.

In contrast, a UUV offers almost complete stealth, especially if no active sonars (altimeter, Doppler Velocity Log (DVL) used to measure speed and direction over the bottom) are employed during transit. UUV detection could only be achieved through active sonar, e.g., a swimmer detection system, or by detection of hydrodynamic flow noise from the propeller or the body of the UUV itself, a daunting task in the noisy, reverberant acoustic environment of a working port or harbor. The disadvantages of a UUV include 1) the need to come to the surface to obtain GPS corrections, unless a more advanced navigation system is used, and 2) an inability of the rogue operator to receive data from the vehicle, thus making this kind of attack a "fire and forget system".

It is likely that rogue UxVs will rely heavily on GPS receivers for accurate mission execution. For a UUV, this requires the vehicle to be periodically on the surface. Although the use of DVLs and Inertial Motion Units (IMU) onboard the vehicle cannot be discounted, it is unlikely that these payloads will be incorporated. In the case of the DVL, power, stealth (because it emits sound energy that can be detected), and space for explosives would be sacrificed by its inclusion as a sensor. IMUs carry less of a payload space and power penalty, but would only be of use for time scales of a few minutes during the final target approach because less-than-weapons grade systems exhibit quick loss of accuracy [23]. Military grade systems are very difficult to obtain because of International Traffic in Arms Regulations (ITAR) controls; such weapons-grade units are larger and heavier than the less accurate commercial models, and would need to be procured through theft.

One tactic that melds advantages of the two kinds of UxVs would be for a rogue UUV to operate in USV mode for most of the approach to the target, and only operate as a UUV during final approach, or at other points where stealth outweighs losing GPS positioning. Most of the craft would be submerged below the waterline, and its signature above the waterline signature could be made biomimetic in appearance, e.g., to look like a fish fin. Such a UxV could use GPS to perform complex transits that would allow it to travel from a launch point far removed from the target. The disadvantages of this tactic include the possibility of still being spotted at the surface by radar or imaging systems, both of which can be trained using neural networks and related algorithms to detect the wake of the fin, and its appearance. A USV making its final approach risks being entangled in surface nets or booms placed around waterside assets. Because a hybrid UxV can submerge during this phase, defenses such as the above could be defeated.

Operating a UxV platform is a frangible skill. A rogue UxV operator will need significant experience with his or her vehicle. This provides an opportunity for detection by intelligence agencies during the practice phase. UUV practice will be harder to detect through surveillance as the period when the vehicle itself might be observed is much less than that for a USV. However, realistic practice will need to take place in the open (not a covered workshop), in a body of water subject to tides and currents. Likely practice arenas for rogue UxV operations probably share some of the same characteristics as the target waterside facility. These could be pre-identified and monitoring through a variety of remote sensing means available to security agencies. Such practice activities are likely to occur in water bodies with significant numbers of other users that can be assayed using human intelligence assets. Operating a robotic vehicle invariably attracts some attention.

Is it likely that rogue operator would operate the UxV as a "human in the loop" mode during an attack? Such a possibility cannot be ruled out and it fits in with the conservative nature of many terrorist groups as they adopt a new technology. While a UxV might be operated using a direct wireless connection,

modern cellular data networks offer a stealthier alternative. If the UxV has a wireless data device (smartphone, tablet computer, etc.) integrated into the vehicle it would be straightforward to communicate to the robot using social networking sites like Facebook, or via Twitter messages. The operator could easily issue real-time commands (turn left, stop, accelerate, etc.) that could be encoded as innocuous statements using these social media, and sent via smartphone, or tablet computer. This control protocol is impossible to detect without prior knowledge of the perpetrators' web identities. This approach would make the system immune to jamming unless the waterside facility is willing (and legally able) to locally disrupt local cell phone data service within a certain footprint around the waterside. SMS messaging to a specific phone number could also be used as real-time control, but the latency of this approach is now greater than that used in social media.

One possible countermeasure to combat UxVs exploiting connections to the Internet via the cellular network would be to localize all active signals in a footprint around a waterside facility, and compare all signal locations to objects seen in a live video feed at those spots.

For "person in the loop" control of a rogue UxV, the operator would need to be positioned close enough to the target to observe the approach to the target. Unfortunately, given the innocuous, ubiquitous activity the operator would be engaged in (texting, interacting with a small computer), detecting such an individual through behavior seems unlikely.

B. Probabilistic Threat Prediction and Reduction

Data fusion strategies for harbor protected have addressed video surveillance methods [24], ship detection and characterization [25], and developing situation and threat assessment [26]. Geospatial Information Systems (GIS) are used routinely as a decision-making tool for enhancing security in a port or harbor [27], and there has been concern about publicly available datasets aiding terrorist planning [28]. We propose that an additional GIS layer would provide a benefit to assessing the real-time risk of attack by unmanned systems. Fig. 4 shows a notional image of this probabilistic threat at a waterside facility. This layer presents a real-time estimate of risk of attack by an unmanned system.

The risk value would be presented in a color-coding scheme similar to that used for other threat indicators. The risk value is generated using a model that uses the following as inputs: 1) The target area for a UxV attack is assigned a value based on its value to a rogue operator. The value is generated by assuming that if an attack occurs there, the area is removed from the traffic pattern of a working harbor for some period of time. For example, if a port has a "choke point" e.g., all traffic must pass through a specific channel, between a bridge's supports, etc., a successful UxV attack there has a high value. 2) Similarly, when a moveable asset like a ship arrives at a specific location, its attractiveness and degree of protection by technical countermeasures located near the asset influence the location's value temporarily. 3) The location's risk value is also weighted by the location's distance from likely UxV launch locations, each of which is assigned a value that

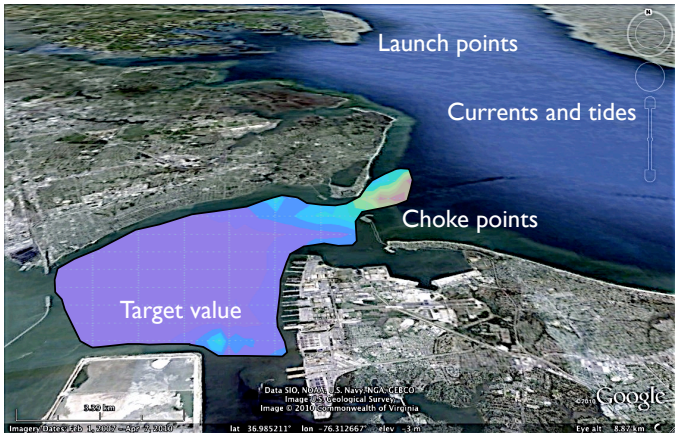

Figure 4. A real-time engine for the assessment of risk from UxV attack would use a cost function involving likely launch locations, cost of transport affected by currents and tide, features dictated by geography (e.g., choke points), presence of surveillance assets above and below the waterline, and the value of specific classes of waterside assets to a terrorist group. The resulting risk value would appear in a GIS layer as conceptualized here.

changes dynamically with the state of the tides, and other hydrodynamic conditions. 4) A location's risk is also weighted by the presence/absence of surveillance assets present. A scheme similar to that in [29] can be used to generate quantitative estimates of coverage and hence protection. 5) An attack at a given location would increase risk as more than one terrorist UxV would be assumed to be present.

Note that this layer will change appearance with a time scale of minutes to hours and provide a dynamic view of where a robotic attack would be most successful. In the event of an attack the GIS layer would help security personnel plan escape routes for vessels in transit, and help guide decisions on movements of ships in the immediate aftermath.

C. Counter-measures During Final Approach to the Target

All UxVs have weaknesses that can be exploited. Our group has developed some proprietary methods that can take advantages of these weaknesses. Some of these countermeasures exploit the type of navigational sensor that is likely to be used during the final approach, e.g., a UUV using a flux-gate compass can be diverted and isolated without the UUV knowing it has been effectively trapped. Robust methods for detection of underwater moving objects now exist [30]. While targeted at the threat of swimmer, these systems could be adapted to recognize a UxV attack. If a surface surveillance or underwater sensing system detects an object congruent with a UxV, a physical barrier is probably the best means to ensure mission failure. Mechanisms that cause fouling or entrapment, e.g., monofilament netting at an appropriate stand-off distance would stop both UUVs and USVs, and could be emplaced on harbor bottoms are critical locations. These methods are equally effective against a swarm of vehicles.

However, during transit these methods could not be as used as easily. Transiting ships have the advantage of speed acting to reduce their vulnerability to more slow-moving UxVs. An attack on a transiting ship would probably have a person in the loop. One tactic to make such an attack harder would be to

vary the speed and course of traffic in harbor. This could be driven by the threat predictions generated by the probabilistic model described above.

A swimmer detection system could potentially detect an evolving attack and the boat operator could be alerted to the approach. The boat operator might have a small window of time to launch a fouling net over the side that stymie the USV/UUV during its final approach.

D. The Importance of Trained Personnel

Training of waterside personnel is an effective countermeasure. Personnel may be the first to recognize that an unmanned systems attack is underway, rather than a sensor network. Training can also prepare personnel for how to prevent indirect attack, e.g., it may be counter-productive to move a high value target through a choke point during or immediately after an attack. Most waterside personnel have no experience with unmanned systems, i.e., how they might appear and behave. Red cell exercises, where real (friendly) UxVs penetrate a waterside facility while security personnel attempt interdiction should be observed by all personnel waterside. A dockworker or crane operator is a valuable sensing system for protection against unmanned systems; training should not be limited to just security personnel. Training is also necessary to implement post-event protocols that deploy limited resources most effectively to prevent property damage or loss of life. In addition to dockside personnel, ship crews need similar training, and additional training in tactics to reduce risk during transit and how to respond appropriately if attacked when away from the dock or anchorage.

FUTURE PROSPECTS – AN EVOLUTIONARY ARMS RACE?

When UxVs become part of the countermeasure space, techniques for identification of friend or foe (IFF) must be applied. New techniques for rapid reduction of ignorance about a target such as an unmanned system moving in the harbor are available that use fuzzy sets combined with Dezert-Smarandache theory, an extension of Dempster-Shafer theory that incorporates new rules for combining imprecise, highly conflicting, uncertain data [31]. For example, this approach for paradoxical data analysis shows promising results for robots exploring and mapping a new environment [32], which could be adapted in a straightforward manner to a security patrol by friendly UxVs. The future of countermeasures will include using UxVs to counter terrorist UxVs. Roving perimeters of UxVs around transiting targets may be necessary if UxV attack becomes a preferred mode of asymmetric warfare.

Unfortunately any novel innovative technology has its down side and it is only a matter of time before terrorist UxVs are used in a disruptive manner at a waterside facility. It is imperative that democracies already well-versed in this technology not be complacent about developing counter-measures for attacks by such systems, and recognize the serious nature of this emerging threat.

ACKNOWLEDGMENT

The authors thank the following individuals for insightful discussions: J. Bouchard, D. Doolittle, B. Francisco, E. Hansen, D. Jones, J. Keane, S.M. Patterson, J. Pollack, M. Rodger, I. Rutberg, T. Sedler, J. Sias, A. Trembanis, M. van der Mandele, and R. Yeo.

REFERENCES

[1] G.L. Rogova, "Harbour protection and higher level fusion: issues and approaches", in Harbour Protection Through Data Fusion Technologies, E. Shahbazian, G. Rogova, and M.J. DeWeert, Eds. Dordrecht, Netherlands: Springer, 2009, pp. 109-118.

[2] S. Lambakis, J. Kiras, and K. Kolet, "Understanding "asymmetric" threats to the United States, Fairfax, Virginia: National Institute for Public Policy, 2002.

[3] P.W. Parfomak and J. Frittelli, "Maritime security: potential terrorist attacks and protection priorities", Washington, DC: CRS Report to Congress (Order Code RL33787), 2007.

[4] Department of Homeland Security, United States, "National plane to achieve maritime domain awareness for the the national strategy for maritime security", Washington, D.C: Department of Homeland Security, 2005, available at: http://www.dhs.gov/xlibrary/assets/HSPD_MDAPlan.pdf.

[5] B.P. Hill, "Maritime terrorism and the small boat attack threat to the United States: a proposed response", Master's Thesis, Monterey, California: Naval Postgraduate School, 2009.

[6] R.T. Kessel and R.D. Hollett, "Underwater intruder detection sonar for harbour protection: state of the art review and implications", NATO Undersea Research Center, 2006.

[7] L. Faulkner, R. Granger, P. Hurst, W. Jankowski, D. Steinbrecher, and J. Tattersall, "Harbor shield: a new technique for inspection of vessels below the waterline", IEEE Conference on Technologies for Homeland Security, pp. 221-226, May 2009.

[8] C.A. Pinto and W.K. Talley, "The security incident cycle of ports", National Urban Freight Conference, Long Beach, California, February 2006.

[9] U.S. Customs and Border Protection, "Container security initiative: 2006-2011 strategic plan", 2006, available at: http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/csi/csi_strategic_plan.ctt/csi_strategic_plan.pdf.

[10] B.A. Jackson, D.R. Frelinger, M.J. Lostumbo, and R.W. Button, "Evaluating novel threats to the homeland: unmanned aerial vehicles and cruise missiles", Santa Monica: RAND Corporation, 2008.

[11] Defense Industry Daily, "Hezbollah Mirsad-1 UAV penetrates Israeli air defenses", April 20, 2005, available at: http://www.defenseindustrydaily.com/hezbollah-mirsad1-uav-penetrates-israeli-air-defenses-0386/.

[12] FOX News and Associated Press, "Unmanned Hezbollah aircraft attacks Israeli warship off Beirut", July 15, 2006, available at: http://www.foxnews.com/story/0,2933,203453,00.html.

[13] B.V. Bigelow, "'Do-it-yourself drones' create buzz at S.D. convention", Union-Tribune, San Diego, June 11, 2008, available at: http://legacy.signonsandiego.com/news/military/20080611-9999-1n11drone.html.

[14] FIRST K-12 Robotics competitions, http://www.usfirst.org/.

[15] Association of Unmanned Vehicle Systems International/U.S. Office of Naval Research competitions at undergraduate-graduate school level, http://www.auvsi.org/auvsi/auvsi/Events/AUVSIStudentCompetitions/Default.aspx

[16] D. Barzilay, "The British army in Ulster", Vol. 2, Belfast, Northern Ireland: Century Books, 1975, p. 207.

[17] J. Grabinsky, "Short and unglamorous: the life of a target", Unmanned Systems, August 2010, pp. 61-62.

[18] U.S. National Oceanic and Atmospheric Administration, Physical Oceanographic Real-time System (PORTS), http://tidesandcurrents.noaa.gov/ports.html.

[19] Office of the Secretary of Defense, "Unmanned systems roadmap 2007-2032", Washington, D.C.: Department of Defense, 2007.

[20] J. Bouchard, "New strategies to protect America: safer ports for a more secure economy", Center for American Progress, Critical Infrastructure Strategy Series, June 15, 2005, available at: http://www.americanprogress.org/issues/2005/06/b815195.html

[21] E. Shahbazian, M.J. DeWeert, and G. Rogova, "Findings of the NATO workshop on data fusion technologies for harbour protection", in Harbour Protection Through Data Fusion Technologies, E. Shahbazian, G. Rogova, and M.J. DeWeert, Eds. Dordrecht, Netherlands: Springer, 2009, pp. 337-351.

[22] M. Riveiro, G. Falkman, and T. Ziemke, "Visual analytics for the detection of anomalous maritime behavior", pp. 273-279, 12th International Conference Information Visualisation, 2008.

[23] A.K. Brown, "Test results of a a GPS/Inertial navigation system using a low coast MEMS IMU", Colorado Springs, Colorado: NAVSYS Corporation, 11th Annual Saint Petersburg International Conference on Integrated Navigation System, Saint Petersburg, Russia, May 2004, available at: http://www.navsys.com/Papers/04-05-001.pdf.

[24] L. Snidaro, G.L. Foresti, and C. Piciarelli, "Automated video surveillance of harbour structures", in Harbour Protection Through Data Fusion Technologies, E. Shahbazian, G. Rogova, and M.J. DeWeert, Eds. Dordrecht, Netherlands: Springer, 2009, pp. 223-232.

[25] Y. Allard, M. Germain, and O. Bonneau, "Ship detection and characterization using polarimetric SAR data", in Harbour Protection Through Data Fusion Technologies, E. Shahbazian, G. Rogova, and M.J. DeWeert, Eds. Dordrecht, Netherlands: Springer, 2009, pp. 243-250.

[26] A.N. Steinberg, "An approach to threat assessment," in Harbour Protection Through Data Fusion Technologies, E. Shahbazian, G. Rogova, and M.J. DeWeert, Eds. Dordrecht, Netherlands: Springer, 2009, pp. 95-108.

[27] GeoDecisions, "IRRIS White Paper", January 19, 2007, available at: http://www.tea.army.mil/tools/IRRIS6WhitepaperAward(Jun05).pdf.

[28] J.C. Baker, B.E. Lachman, D.R. Frelinger, K.M. O'Connell, A.C. Hou, M.S. Tseng, D.T. Orletsky, and C.W. Yost, "Mapping the risks: assessing the homeland security implications of publicly available geospatial information, Santa Monica, California: RAND Corporation, 2004, available at: http://www.rand.org/pubs/monographs/MG142/.

[29] A. Caiti, V. Morellato, and A. Munafo, "GIS-based performance prediction and evaluation of civilian harbour protection systems," OCEANS 2007, Aberdeen, Scotland, pp. 1-6, 2007.

[30] T. Clarke, A. Webb, C. Minto, and D. Stanhope, "The Cerberus wideband swimmer detection sonar", Marine Technology Report, pp. 34-40, November 2006.

[31] A. Tchamova and J. Dezert, "Target identification based on DSmT", in Harbour Protection Through Data Fusion Technologies, E. Shahbazian, G. Rogova, and M.J. DeWeert, Eds. Dordrecht, Netherlands: Springer, 2009, pp. 307-316.

[32] X. Li , X. Huang, J. Dezert, L. Duan, and M. Wang, "A successful application of DSmT in sonar grid map building and comparions with DST-based approach", International Journal of Innovative Computing, Information and Control, vol. 3(3), pp. 539-549, June 2007.