Rogue Aquatic Drones

By VS Suguna and Faizal A. Rahman

Synopsis

Drones can facilitate terrorism and crime. As maritime technologies particularly aquatic drones progressively grow, it is a matter of time before new threats emerge.

Commentary

THE APPLICATION of drones for tactical purposes was the preserve of security agencies. As technology becomes increasingly commercialised for myriad purposes, malicious non-state actors such as terrorists and criminals could circumvent international trade regimes that restrict the transfer of potentially dual-use technologies including drones.

Terrorists have reportedly retrofitted aerial drones to conduct attacks and surveillance. The proliferation of aquatic drones may plausibly widen the terrorists' capabilities and opportunities for attacks to coastal cities.

Drone Tech Proliferates

A report on "Jihadist Terrorism 16 Years After 9/11" by New America highlighted the use of armed (aerial) drones as a growing threat as exemplified by reports of ISIS building drones from scratch in Iraq. In Southeast Asia, the Maute Group reportedly deployed commercial off-the-shelf drones to gain a tactical advantage in urban warfare in Marawi city, Philippines.

While the misuse of aerial drones (UAVs) for urban terrorism is a current security concern, it would also be of strategic importance to monitor the developments of aquatic drones for surface and underwater operations. Although aquatic drones have not proliferated at the speed of aerial drones, the technology is increasingly being explored for security and commercial purposes. For example, the Australian start-up

Abyss is developing aquatic drones with data-collection capabilities for industries. In Singapore, the Police is exploring the use of unmanned surface vehicles (USVs) for autonomous coastal patrols.

Over time, the aquatic drone technology would expectedly become more commercially viable and affordable. In highly digital societies (such as smart cities), rogue individuals with access to the Internet and commercially available hardware would be able to assemble aquatic drones with relative ease and speed.

Next Tide of Tech-Enabled Terror

In the foreseeable future, terrorists could deploy aquatic drones similar to how aerial drones are exploited for malicious purposes. This possibility would mark an emergent concern for vibrant coastal cities with busy waterways for two primary reasons.

Firstly, aquatic drones could shift the maritime terrorism landscape by reducing terrain challenges and enhancing terrorists' capability to launch seaborne attacks. Such attacks could be aimed at strategic and soft targets such as civilian passenger vessels, port facilities, tourist and sea sports hubs, and large-scale public events by the sea. For example, the targeting of USS Cole in October 2000 at the port of Aden demonstrated the terrorist intent to hit strategic maritime targets. The 2005 Al Qaeda-inspired plot to attack Turkey-bound Israeli cruise vessels using explosive-laden small boats demonstrated the terrorist intent to hit soft maritime targets.

Secondly, past attacks underscored the importance of coastal cities in the terrorist playbook even if the incidents did not begin at sea. For example, the 2008 Mumbai attack demonstrated terrorists' exploitation of the sea as a staging point to evade security forces on land. The attacks on Barcelona, Spain (August 2017) and Nice, France (July 2016), although land-based, pointed to the attractiveness of coastal cities as soft targets given the wider opportunity for attack due to vibrant tourism scene and a high number of vulnerable civilian targets.

Attack Outcomes

Essentially, the use of aquatic drones by terrorists to target coastal cities could lead to substantial human casualties as well as economic and environmental damages to the coast. Several scenarios are possible but some are perhaps more noteworthy.

First, aquatic drones could be retrofitted to function as remotely controlled or autonomous waterborne improvised explosive devices (WBIEDs). These drones could then be discreetly launched against civilians at sea (such as during sea sports events) or against important port and coastal facilities. Second, the aquatic drones could be deployed for hostile surveillance against critical infrastructure at sea such as marine transportation networks, military and law enforcement installations, and water desalination plants.

Third, aquatic drones could constitute unconventional threats to critical water resources located inland such as reservoirs and other water catchment areas. They could be deployed to disperse harmful chemical and biological agents thus contaminating water supplies, or to cause physical damage to dams. The impact of

such threats could be fatal and will challenge the psychological and social resilience of the affected communities.

Prevention and Response

Strategies to prevent threats involving aquatic drones should factor in how the technology undergoes advancement and commercialisation. In this respect, it would be crucial for security agencies to plan and prepare for possible terrorist (and criminal) scenarios involving the use of not only aerial but also aquatic drones. This step requires the anticipation of plausible risks – known and new - that could emanate from the confluence of drone technology and maritime terrorism.

In addition, security agencies would have to assess the regulations necessary to ensure safe and responsible use, giving security agencies the powers to monitor and interdict potentially rogue aquatic drones. Certain considerations (e.g. operating range, weight and restriction zones) in existing efforts to regulate the ascending aerial drone economy may be useful for the regulation of aquatic drones too.

Strategies to respond to threats involving aquatic drones require both technical capabilities and coordination among the maritime agencies. While security agencies currently have surveillance and offensive tools – unmanned surface vehicles (USVs), unmanned aerial vehicles (UAVs) and coastal closed-circuit television (CCTV) cameras – to guard against coastal intrusions, the tools should also include capabilities to detect and intercept small aquatic drones moving surreptitiously on the waters. Inter-agency procedures should be in place to facilitate collaborative investigations and coordinated response following aquatic drone-related incidents.

Overall, strategies for prevention and response to threats involving aquatic drones would require public-private cooperation in anticipating the challenges in regulating the technology's proliferation and intelligence-sharing between security agencies and other maritime stakeholders.

VS Suguna is an Associate Research Fellow and Faizal A. Rahman is a Research Fellow with the Homeland Defence Programme at the Centre of Excellence for National Security (CENS), a unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore.