Foreign Counter-Unmanned Aerial Systems: Developments in the International Arms Markets

Andrew Hull and David Markov

The Problem

The numbers and capabilities of unmanned aerial vehicles (UAVs) are growing. Many have attributes that make them formidable military tools and threats to homeland security. Consequently, a growing number of counter-UAV systems are being offered by foreign vendors.

Overview

Over the last decade the numbers, types, and capabilities of unmanned aerial vehicles (UAVs) available to military forces, domestic security forces, non-state actors, commercial interests, and even private citizens have grown substantially. Offerings range from large, expensive fixed-wing high-altitude/long-endurance UAVs, which are affordable only to nation states, down to low-cost, low-flying small and micro vertical take-off-and-landing (VTOL) models available to everyone. Both armed and unarmed models are marketed. Some unarmed models are being upgraded with aftermarket lethal capabilities by third parties or private individuals using do-it-yourself techniques. Today, some kind of UAV capability is available to virtually all nations, non-state actors, commercial interests, and individuals. Availability is now generally a function of the price point, rather than technological or regulatory constraints. UAVs are becoming ubiquitous.

Today, some kind of UAV capability is available to virtually all nations, non-state actors, commercial interests, and individuals.

The capabilities of both large and small UAVs are constantly evolving. They are becoming faster, capable of carrying heavier and more diverse payloads, have longer endurance, and are more autonomous. At the same time, economies of scale are driving down costs of both large and small UAVs.

UAVs offered in the international arms market have attributes that make them formidable military tools. They can distract, disorient, and disrupt military operations, as well as provide direct and indirect support to destroying military equipment and structures. Likewise, some individuals and groups have taken advantage of the wide-scale availability of small commercial UAVs for malicious purposes. The Islamic State of Iraq and the Levant (ISIS), for example, has weaponized small commercial drones using improvised grenades as a lethal payload. Other individuals and groups have used small UAVs to overfly sensitive military and infrastructure facilities, fly in restricted airspace around airports, and spy on famous personalities and their neighbors. Two years ago, an individual

even landed a small UAV carrying a bottle with traces of radioactive material onto the roof of the Japanese Prime Minister's office.

Predictably, demand from military, police, and homeland security agencies for technical counters to UAVs is growing. Counter-UAV systems are now a major marketing thrust at international arms and homeland security exhibitions. Options offered encompass a wide variety of approaches, including (1) destroying the UAV, (2) deceiving or evading on-board sensors, (3) disrupting/jamming navigation systems and data links, (4) third-parties taking control of the UAV, and (5) catch/capture systems. A few systems combine several of those approaches. International arms shows offer the full spectrum of countermeasures designed to deal with both large and small UAVs, but with a heavy emphasis on kinetic approaches that destroy UAVs. Security exhibitions, on the other hand, generally concentrate on non-kinetic/not-destructive counters targeted at small, low-flying UAVs.

Destroying UAVs

A large number of counter-UAV systems advertised at international arms shows employ kinetic kill mechanisms. Some are traditional air defense systems (guns, missiles or a combination of both) that have been rebranded as counter-UAV systems or whose capabilities have been modified or enhanced to make them more responsive to the UAV threat. China North Industries Corporation (NORINCO) has displayed the truck-mounted LD-2000 30mm close-in-weapon system (CIWS), originally designed for naval applications as an anti-ship missile defense for use against UAVs, at several editions of AirShow China (see Figure 1). The LD-2000 is designed to engage air targets (including UAVs) with a radar cross section (RCS) of at least 0.1m^2 in a dense electronic counter counter-measures (ECCM) environment. Thales, a European company, offers RAPIDFire, which combines a 40mm anti-aircraft gun with STARStreak very short-range air defense missiles, the same missile used as a man-portable air-defense

(a) (b)

Figure 1. (a) NORINCO's LD-2000 30mm CIWS at AirShow China 2016 in Zhuhai, China; (b) Thales' RAPIDFire 40mm AAA Systems at Eurosatory 2012 in Paris, France

system (MANPADS) to destroy multiple types of air targets, including UAVs (see Figure 1). Thales advertises that RAPIDFire, an anti-aircraft artillery system (AAA), is addressing "the new threats being encountered by armed forces today and in particular the low-cost targets which can attack in swarms and can saturate conventional missile defenses" (Thales Group 2017).

More innovative "kill" concepts include directed energy weapons (DEWs) (systems such as high-power microwaves (HPM), electro-magnetic pulse (EMP), and various kinds of lasers). HPEMcounterUAS from Diehl Defense, a German company, uses HPM to attack semiconductors inside the control systems of UAVs. Targets become inoperable upon the impact of HPM pulses triggering a fail-safe mode. Diehl Defense literature offers scalable ranges up to several hundred meters and the capability of engaging swarms of mini-UAVs simultaneously. Russia's United Instrument Manufacturing Corporation also discussed a microwave gun with military specialists at a closed event at the ARMY-2016 exhibition held in a venue outside Moscow, Russia. Company officials said the weapon is capable of firing super-high-frequency electromagnetic waves, a kind of EMP approach to suppress equipment on board low-altitude aircraft. Researchers at China's Air Force Engineering University published a paper in *Laser & Infrared* in 2013 that discussed advantages of using lasers against small, slow targets, including target detection and destruction with a laser weapon. Four years later, NORINCO displayed such a system, called Silent Hunter, at the International Defense Exhibition and Conference (IDEX) 2017 in Abu Dhabi, United Arab Emirates (UAE) (see Figure 2). It is primarily designed to destroy small, low-altitude UAVs using variable power (5kW to 30kW) lasers mounted on a truck or in a fixed stand-alone box at ranges up to 2 kilometers. NORINCO claims that Silent Hunter is capable of destroying more than 30 UAVs with a 100 percent success rate during the system's state acceptance testing.

Rheinmetall, a German company, showed the Oerlikon Skyshield turret equipped with a high-energy laser effector at IDEX 2017 to deal with low, slow air threats (see Figure 2).

(a) (b)

Figure 2. (a) Silent Hunter and (b) Skyshield on Display at IDEX 2017

Skyshield employs multiple high-energy laser beams superimposed and focused on one spot on the target. Rafael Advance Systems, an Israeli company, has also marketed its Iron Beam high-energy vehicle-mounted laser for dealing with very short-range small airborne targets and as a counter rocket, artillery, and mortar system (C-RAM). Iron Beam uses two separately located high-power fiber-optic lasers working in tandem.

Disrupting/Jamming Navigation Systems and Data Links

Electronically jamming a UAV's links to space-based navigation systems like GPS and jamming radio links passing data are perhaps the most popular non-kinetic approach to countering UAVs. Several such systems were displayed by various Russian firms at ARMY-2016. One in particular was the United Instrument Manufacturing Corporation's Shipovnik-AERO Electronic Warfare System (see Figure 3), which requires about 25 seconds for detecting a UAV and jamming its control signal. It employs wide-band countermeasures to jam all signals, narrow-band countermeasures to jam a certain frequency band, or information countermeasures to distort information.

At Airshow China 2016, held in Zhuhai, China, a number of counter-UAS solutions from Chinese companies were introduced. Three of those solutions included (1) Xinxing Cathay International Group's Counter-UAS System, which is designed to jam the on-board navigation, ground control, and video datalink systems, (2) CETC's JN3141 Remote Control UAV Jammer, which is a rifle-style counter-UAV system that jams the on-board satellite navigation system, and (3) ZR Aerospace's Counter-UAS System, which jams the on-board navigation and ground control systems. See Figure 4.

Deceiving or Evading On-Board Sensors

Some counters concentrate on defeating the UAV's sensors, rather than the platform. These approaches range from rather simple, do-it-yourself (DIY) methods to purpose-built systems being offered in the

Source: HoangSa.net (2016).

Figure 3. Shipovnik-AERO Electronic Warfare System Discussed at ARMY-2016

(a) (b) (c)

Figure 4. Three Types of Counter-UAV Jammers Displayed at AirShow China 2016: (a) Xinxing Cathay International Group's Counter-UAS System, (b) CETC's JN3141 Counter-UAS System, and (c) ZR Aerospace's Counter-UAS System

international arms market. Western anti-drone activists, for example, have developed the technique of using high-power spotlights or commercial lasers to blind on-board electro-optical (EO) sensors of low-flying UAVs by concentrating light on the forward lower portion of the small UAV's nose where these sensors are located.

Companies from many countries are selling multi-spectral camouflage nets. China's Suzhou SHCB Camouflage Net and Tent Company, for example, offered the JF-Leaf Multi-Spectral Camouflage Net, made from nano-composite materials and structures, at IDEX 2015. Company literature claims its design provides a stealthy camouflage net structure that achieves a full band reduction in optical (0.4 to 1.2μm), infrared (3 to 5μm and 8 to 14μm), and radar (Ka, Ku, X, C, S, and L bands) signatures.

Chinese companies are also aggressively marketing high-fidelity inflatable decoys to deceive on-board UAV sensors. China's Obsidian Group (see Figure 6), for example, advertised inflatable military equipment decoys at IDEX 2015. According to marketing brochures, this company uses PVC fabric, split air chamber structure forming, and "realistic modeling" techniques to produce "superior performance and low cost" false targets for the battlefield. Customer decoy options include optical, infrared, radar-compatible, single spectral, and multi-spectral decoys.

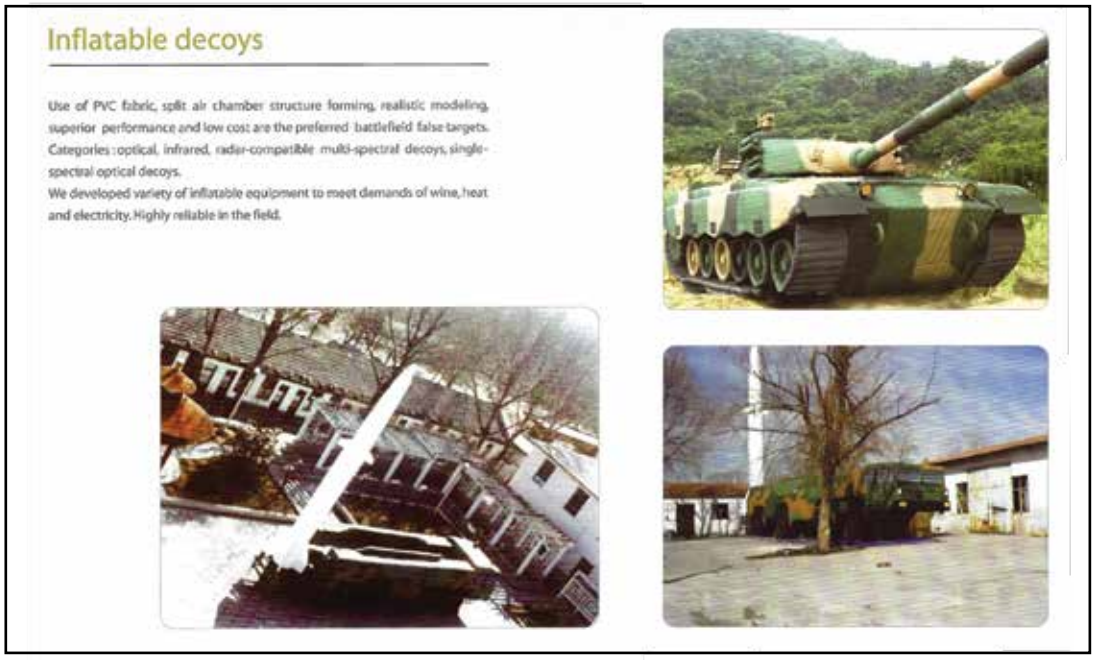
Russian companies like Scientific Production Enterprise RUSBAL also offer a wide range of inflatable decoys. Examples of their products are shown on display at ARMY-2016. See Figure 7.

Taking Control of the UAV

One of the more sophisticated approaches involves third parties taking over the control system of the targeted UAV. The RSA Conference 2016 in San Francisco had a session entitled "Hacking a Professional Drone," which claimed that "professional UAVs are not as secure as one might think" (Rodday 2016). "Serial hacker" Samy Kamkar, for example, designed the SkyJack Counter-Drone System that seeks out other UAVs. The SkyJack system takes over the UAV following these steps:

Note: This brochure has been included for notional purposes only.

Figure 5. Suzhou SHCB Camouflage Net and Tent Company Technical Characterization from Brochure at IDEX 2015



Note: This brochure has been included for notional purposes only.

Figure 6. Marketing Brochure for Inflatable Decoys from China's Obsidian Group at IDEX 2015

Figure 7. Inflatable Decoys Displayed by Scientific Production Enterprise RUSBAL at ARMY-2016

(1) seeks the wireless signal of any other drone in the area, (2) forcefully disconnects the wireless connection of the true owner of the target drone, (3) authenticates with the target drone, pretending to be its owner, (4) feeds commands to the target, and (5) takes control of the target UAV's on-board computer. Kamkar has made public all the technical specifications anyone needs to build an aerial hacker drone of their very own.

TeleRadio Engineering of Singapore has sold SkyDroner (see Figure 8) to clients in the Middle East and Asian Pacific, including Singapore Special Operations Units. TeleRadio designed SkyDroner for used by police departments, defense forces, airports, prisons, and operators of nuclear, water, and power plants. SkyDroner consists of multiple sensors that monitor the UAV's range of radio signals and signature characteristics. It then takes over the command and control frequencies and can issue instructions to the target, causing it to land at a designated area.

Catch/Capture Systems

One of the problems with implementing counter-UAV systems is the shoot/don't-shoot dilemma posed by small UAVs. There are situations in which the goal is not to defeat UAVs by employing kinetic means if it results in collateral damage from their crashing into urban areas or sensitive infrastructure. The answer to that dilemma is systems that ensnare the UAV and take it to another location for disposal. Tokyo's Metropolitan Police Department is now employing a fleet of these net-carrying counter-UAVs.

This approach is exemplified by two British systems: (1) SkyWall from Openworks (see Figure 9) and (2) Net Gun X1 from Drone Defence (see Figure 9). The SkyWall system uses a compressed gas-powered and programmable projectile containing either a net, net and parachute, or net with electronic countermeasures to capture a small UAV. The launcher has a scope to sight the target and an onboard computer to calculate the required launch vector and muzzle

Source: TeleRadio Engineering Pte Ltd (2016).

Figure 8. TeleRadio Engineering of Singapore SkyDroner

velocity for intercept. The intelligent projectile receives continuous flight-update information, and when it reaches the target, a net and parachute are deployed to capture the UAV and bring it back to earth safely. The Net Gun X1 system uses two different kinds of capture nets: (1) a 3×3 meter mesh net with a maximum range of 10 meters, and (2) the smaller 2×2 meter Spider net with a maximum range of 15 meters.

Final Thoughts

The growing UAV market will spark further growth in the counter-UAV market over the next decade. One market forecast estimates that between 2016 and 2026, counter-UAV systems "will be equally attractive to customers in the civilian and military sectors due to the rising security threat posed by UAVs with numerous opportunities for companies wanting to enter the market to offer existing or newly developed C-UAV products" ("Global Counter UAV Market" 2017). Continuing to monitor offerings at international arms and homeland security exhibitions will provide insight into the emerging counter-UAV market as various countries and companies continue to refine and develop their market-driven solutions to satisfy this growing threat dynamic.

Source: (a) OpenWorks Engineering (2017); (b) Drone Defence Services Ltd (2017).

(a) (b)

Figure 9. (a) SkyWall from Openworks; (b) Net Gun X1 from Drone Defense

References

Drone Defence Services Ltd. 2017. "Drone Defence - Net Gun XI." Accessed July 17, 2017. http://www.dronedefence.co.uk/net-gun-x1.

"Global Counter UAV Market." 2017. ADSNews. Accessed July 10, 2017. http://www.asdnews.com/news-67625/Global_Counter_UAV_Market.htm.

HoangSa.net. 2016. "Nga trang bị tổ hợp tác chiến điện tử Shipovnik-AERO, Mỹ "khóc thét" (Russia Equipped with Electronic Warfare Team Shipovnik-AERO, the United States 'cry out'"). Accessed July 17, 2017. http://hoangsa.net/nga-trang-bi-to-hop-tac-chien-dien-tu-shipovnik-aero-my-khoc-thet/.

OpenWorks Engineering. 2017. "SkyWall Capture Drones – Protect Assets." Accessed July 17, 2017. https://openworksengineering.com/skywall.

Rodday, Nils. 2016. "Hacking a Professional Drone." Briefing at the RSA® Conference 2016, San Francisco, CA, February 29–March 4. https://www.rsaconference.com/writable/presentations/file_upload/ht-w03-hacking_a_professional_police_drone.pdf.

TeleRadio Engineering Pte Ltd. 2016. "SkyDroner." Accessed July 17, 2017. http://www.skydroner.com/.

Thales Group. 2017. "RAPIDFire." Accessed June 29, 2017. https://www.thalesgroup.com/en/worldwide/defence/rapidfire.

Mr. Andrew Hull *(left) is a Research Staff Member in IDA's Strategy, Forces and Resources Division. He holds a Master of Arts from the University of Kentucky, William Andrew Patterson School of Diplomacy and International Commerce.*

Mr. David Markov *(right) is a Research Staff Member in IDA's Strategy, Forces and Resources Division. He holds a Master of Arts in international security affairs from the University of Kentucky, William Andrew Patterson School of Diplomacy and International Commerce.*