**1. Features and attack procedures of aerial targets**

**1.1. Background**

a. Threat missiles include BMs, CMs, and ASMs (not including short-range, nonnuclear, direct fire missiles, bombs, or rockets such as Maverick or wire-guided missiles). Their targets are within a given theater of operations. Threat missiles have unique capabilities that must be considered when planning countermeasures. For example, no other target system can put a warhead into the theater JSA or threaten friendly population centers and neutral countries in a matter of minutes. Other target systems do not create public panic and a political situation each time a launch is broadcasted on television worldwide by reporters wearing gas masks. Effectively countering this threat, coupled with the somewhat elusive nature of some threat missile systems, requires the dedicated attention of determined, knowledgeable professionals.

b. Modern threat missiles can have very long ranges, deliver a variety of warheads, including high explosives and WMD, and can be difficult to counter. Because they arerelatively cost-effective weapons, BMs are weapons of choice for many developing nations. Such weapons provide an offensive capability and, when mated with a WMD, may give a nation the ability to deter a potential adversary by holding population centers and/or military forces at risk. Rogue nations believe missiles provide them with a counter to sophisticated land, air, and naval forces. As a result, nations around the world are actively pursuing missile capabilities.

c. Threat missiles may be used alone or in conjunction with other weapon systems. Their targets can vary from political to military, such as population centers, ports, airfields, headquarters, AD sites, C2 elements, communications nodes, and logistics centers. They can quickly put key civilian facilities at risk, such as power and water stations, petroleum pumping and storage sites, and industrial complexes. BMs and CMs also present a serious threat to merchant shipping, critical sea-lanes, and maritime operations in the littorals. ASMs also have proven to be effective weapons against point targets, and they are difficult to defend against.

**1.2. Generic Architecture**

Although there are many variables between the different types of threat missiles, they generally share a common architecture. Missile programs may have one or more of the following aspects:

*a. Research and Development.* If a country is developing its own missile system or adapting a system purchased from another country, there will be a center, institution, and personnel responsible for the research and development (R&D) effort. However, if a country purchases the complete missile system, there may be no R&D effort unless they attempt to improve the design. R&D efforts should provide some signatures for intelligence sources.

*b. Manufacturing.* Countries that develop their own systems or adapt those produced by other nations require dedicated manufacturing and testing facilities. They also may have to develop or refine the fuel for the missile systems. Although the fuels are of a specific type, they are commonly available on the international market from several sources. The manufacturing process should produce signatures and products (the missiles) that intelligence sources should recognize.

*c. Purchase and Import.* Countries that purchase systems from other nations will have prepared sites for receipt of missile system components and fuels. These ports of entry may be air-, land- (road or rail), or sea-based. These locations may have receipt, inspection, and storage capabilities. If the equipment requires assembly, there may be facilities created nearby to support these activities.

*d. Transportation.* Missile components move from their manufacturing or importing site by rail, road, air, and/or sea to permanent storage sites. In some cases, the missiles may be carried by their transporter-erector-launcher (TEL) unit. The combination of purchasing and transportation should provide signatures or some trail or recognition for intelligence sources.

*e. Missile Storage.* Missile storage locations are required at the point of manufacture, at the point of receipt, in missile unit base locations, and at training installations. Missile storage sites are likely to be constructed and developed within projected operational areas as well. If not mounted on a TEL, storage may include innocuous containers or special canisters that house the missiles until they are launched.

*f. Warhead Storage.* Warhead storage sites are usually located in ammunition areas and may not be easily discernible from bunkers holding other munitions. However, WMD warheads require specialized storage, handling, and, most notably, higher security. WMD generally have telltale signs for not only storage but for movement as well.

*g. Basing.* Missile units are usually located at military bases for OPSEC and safety purposes. Most training and equipment maintenance occurs at these locations. Land-based units likely will move from their garrisons to conduct combat operations. Air units with CMs and ASMs conduct training and wartime operations directly from their home air bases or from dispersal fields. BM units are likely to utilize passive AD measures such as mobility, dispersal, and concealment to complicate their being targeted. Naval units generally have their missiles aboard ships for added mobility and movement to potential firing locations. Normally, intelligence sources should be able to identify adversaries with missile-capable aircraft and ships.

*h. Assembly Areas.* In cases where BMs and warheads are shipped and stored separately, one of the final stages of preparing the weapon for operations is mating the warhead to the missile body. This may be a training event so it can be efficiently done for combat operations. For aircraft, the loading process could be an indication and warning for intelligence sources, as would the assembly of BMs.

*i. Launch Areas.* Missile attacks normally take place from planned launch areas. The characteristics of the launch areas are dependent on missile type. Historically, BMs usually start from a hide position then move to the launch point. ASMs must be flown to a launch point within range of the target.

*j. Launch Preparation*. After arrival at a launch area, most BMs require some prelaunch preparation. These activities may involve fueling and testing the missile and warhead components along with some assembly operations. Launch preparations for liquidfueled missiles generally require longer setup/checkout time than do solid fuel missiles. For CMs and ASMs, these activities likely will occur at an airfield or port and may involve simply moving the missile from a storage area to the delivery platform (aircraft or ship).

*k. C2.* Planning missile operations is normally a highly centralized process with tight control over the employment and selection of targets. Execution of missile operations may be either centralized or decentralized. The degree of centralization is generally determined by the degree of control desired by senior civilian or military leaders, the capability for secure communications, the ability of the opposing forces to detect or locate transmitters, and the tactics employed. WMD-armed missiles will be tightly controlled because of their political sensitivity and the possibility of retaliation. Thus, WMD-associated missile units normally will require robust communication links or constant communication with national leadership for launch authorization.

*l. Support Units.* Most missile systems require a support system. Support units provide a variety of functions to include maintenance, rearming and refueling, personnel replacement, etc. They also deliver replacement warheads and missiles and conduct all the electronic testing and repair. During peacetime, these units probably will be colocated with the missile firing units in garrison. For employment, they may move to FOBs or dispersal/staging airfields. For naval units the support is likely organic to the ship.

**3. Ballistic Missiles**

*a. BMs* (or SSMs) are characterized by their trajectory, having one or more boosters and an initial steering vector.

*b. Threat Employment Concepts*

(1) Prime targets for BMs are large, soft, or heavily defended facilities, critical to a nation’s warfighting ability, that are normally located in rear areas. Examples include airfields, AD sites, transportation centers (ports and airfields), logistic hubs, and major C2 nodes. Additionally, key population centers are prime targets whose attack might create panic and foster a political crisis. BMs also may be used in a tactical sense to affect battlefield logistics and operations, although this is less likely given the strategic importance of such weapons to smaller or less developed nations.

(2) TBMs normally are carried on a TEL so mobility enhances BM survivability and, conversely, complicates their being targeted. Their long range affords the enemynincreased options in selecting operating areas and determining potential targets. For example, BMs have been exported by many nations and can be set up and fired in less than 45 minutes and relocated within minutes. Missiles often present multiple tracks, either from staging or from their tendency to break up during terminal phase descent, thereby further complicating defensive efforts.

(3) SAM systems have been modified into SSMs in some countries, and this trend likely will spread to other nations. As missile systems and missile technology proliferate, nations will acquire or be able to produce missile systems using solid fuels. This will significantly reduce the dwell time required for system checks and fueling during launch preparation. This reduced dwell time will significantly reduce the missile’s signature and the time available for attack operations.

*c. Threat Employment Operations.* TBM operations generally are broken down into five major phases. These include readiness, deployment, employment, sustainment, and reconstitution.

(1) Readiness Phase. The readiness phase encompasses normal day-to-day peacetime operations. During this phase, BM forces train on wartime tasks and practice doctrinal employment in the local training areas or in garrison. This normally entails TEL operation, missile erection, site preparation, and missile maintenance. Support units will perform maintenance on firing units and conduct resupply operations.

(2) Deployment Phase. The deployment phase may include initial movement from the garrison location(s) to the initial war fighting positions to support subsequent launch operations. BM force deployment will depend on the range to the target, missile capability, terrain, and survivability considerations. Firing units will move to either hide positions or directly into launch positions. Support units likely will move to a forward base and conduct support to include reloading operations. Deployments may or may not convey hostile intent, depending upon the circumstances.

(3) Employment Phase. The employment phase encompasses initial combat operations. During this phase, TELs move missiles to their initial firing positions from a hide site and then, after launch, move to another hide site or directly to reload operations. The support unit will establish that location based upon doctrine, terrain, the BM force commander’s firing schedule, and the threat.

(4) Sustainment Phase. During the sustainment phase, support units likely will use a forward base/location to conduct the necessary repair/replacement operations to sustain the BM force. Sustainment operations require support units to use lines of communications from garrison locations, field storage areas, and/or the manufacturing infrastructure/import facilities to the forward bases and onward.

(5) Reconstitution Phase. The reconstitution phase encompasses continuous operations between firing units, support units, and higher echelon logistic locations to regenerate BM forces.

*d. Threat Employment—Tactics, Techniques, and Procedures*

(1) TEL Operations. TELs can serve as the transporter and launch platform for missiles. TELs present a small, extremely mobile target with very short dwell time. TELs generally travel only short distances between hide sites, launch sites, and transload sites, unless required to return to a forward base for additional maintenance. A TEL will be in launch configuration for a very short period of time and can displace to a new hide site in a matter of minutes.

(2) Transload Site. The transload site is where fueled, ready missiles are loaded onto TELs. Support unit personnel, vehicles, and equipment from the forward base or location will rendezvous at this site with firing unit TELs. At this site there generally are a number of vehicles: missile resupply vehicles (with one to three missiles), a crane (possibly attached to the resupply vehicle), and other ground support equipment as required by the missile type. The transload site usually is an open area large enough to allow the crane to lift/pivot the missile onto the TEL, approximately 50 by 50 meters. This operation can occur in large buildings or underground facilities with sufficient height, approximately 20 meters. When detected, this site will remain vulnerable throughout its established dwell time.

(3) FOL. The FOL is typically where warheads and missiles are mated, missiles are fueled, and missiles are loaded onto the resupply vehicle. The FOL remains in place from half-a day to 3 days. The FOL usually contains warheads and missile airframes, transporters, cranes, checkout vehicles, fuel trucks (vehicle and missile fuel), and resupply and other support vehicles. FOLs can be located in rural or urban settings and may be hidden in a building complex or underground facility. The FOL has a larger footprint than TEL or transload operations, but is still difficult to locate. Some countries may not employ FOLs, preferring to conduct these operations out of the FOB.

(4) FOB. The FOB is the main missile unit supply and storage activity and will be spread out over a large geographic area for survivability. The number of FOBs will depend on the size of the missile force (targets selected and acceptable travel distances for support units). In situations where a country’s geographic area is small, it is possible that operations typically associated with the FOB could be conducted from garrison.

(a) A typical FOB contains warhead, missile, and propellant storage sites; transporters and cranes; checkout vehicles; fuel trucks (vehicle and missile fuel); and resupply and other support vehicles. An FOB can be established in an urban environment hidden in large buildings, in underground facilities, or in the field. The FOB normally will deploy support equipment to FOLs and/or transload sites as needed to sustain launch operations. FOBs require robust lines of communications (primarily roads and rail lines) to support continuous operations.

(b) The FOB cannot be easily hidden but may be difficult to distinguish from other logistic facilities. Once established, the FOB probably will not be moved in total, but certain components may be moved to complicate detection, create a deception, or facilitate launch operations.

**4. Cruise Missiles**

a. A *CM* is a guided missile, the major portion of whose flight path to its target is conducted at approximately constant velocity and depends on the dynamic reaction of air forblift and upon propulsion forces to balance drag. CMs are unmanned, self-propelled vehicles that sustain flight through the use of aerodynamic lift over most of their flight. CMs usually navigate autonomously to targets and, depending on their sophistication, can position themselves through a number of update methods along extended flight routes. CMs are capable of delivering the full complement of warheads from conventional to WMD.

b. *Threat CMs*

(1) Very few nations currently possess sophisticated CMs such as the Navy TLAM or the Air Force conventional air launched cruise missile (ALCM). Employment by developed nations has been limited. The majority of CMs in potential threat nations are short-range anti-ship/coastal defense CMs with ranges in excess of 100 nautical miles. Some countries are modifying anti-ship CMs for a land attack role.

(2) Future CM technology will build on existing low observable, sensor defeating designs using radar absorbing materials and composite materials such as Kevlar or carbon fiber to further reduce their radar cross-sections and render them more difficult to detect.

CMs generally possess some of the following features:

(a) Radar cross-section under 1 square meter (-10 decibel and lower).

(b) Low infrared signature (varies by type of CM).

(c) Acoustic signature (varies by type of CM).

(d) Cruise altitude of 100 feet to 2000 feet above ground level or 50,000 feet above mean sea level.

(e) Range of 100 to 1000 nautical miles.

(f) Payload of 200 to 1000 pounds.

(g) Speed range of high subsonic (low altitude) or supersonic (high altitude).

(h) Air-, land-, or sea-launched.

c. *Threat CM Employment*

(1) CMs put stress on AD systems because they are difficult for theater sensors and weapons systems to detect, identify, track, acquire, and destroy. CMs are more difficult to detect than the larger BMs because they do not give off as large a heat signature at launch, fly at very low altitudes during their attack legs, and normally have a smaller radar crosssection. Ground-based surveillance radars have a difficult time detecting CMs when in low level flight (following terrain contours) because of line-of-sight restrictions created by radar horizon and terrain masking. Similarly, airborne radar systems may have a difficult time isolating CMs from ground clutter. These traits, when combined with radar evasion techniques and low observable construction methods, cause delays in detection and engagement decisions by engagement authorities and shooters per the ROE. However, once detected in flight, CMs can be engaged by fighters, AAA, and SAMs. The best tactic is to shoot down the aircraft carrying the CMs.

(2) SLCMs and ground-launched cruise missiles (GLCMs) present opportunities for detection as well as challenges for surveillance systems. Surface launch systems normally must be boosted to “cruise” altitude. The boost phase often uses a rocket motor that will produce an infrared signature that could potentially be exploited by space-based or properly positioned theater assets. ALCMs do not have a boost plume since aircraft or UASs deliver them above the cruise altitude. Although the ALCM has a small radar cross-section, it is vulnerable to radar detection during descent to its low-level altitude. Once near the surface and in a terrain following mode, sensors have to filter radar ground clutter to extract a radar signature from these low-altitude profile missiles.

(3) High-altitude, high-mach profiles rely on altitude and speed to overcome defenses. Because the CM is high, ground-based radars will not be obstructed by the curvature of the earth, and airborne radars can discriminate them from ground clutter. As a result, when using the high-altitude profile, CMs are more likely to be detected earlier in flight than when using a low-level profile.

(4) CMs provide a significant standoff range for the aircraft or launch platform and remove the “manned” component of the weapons system from the immediate target area. The release range of CMs from aircraft and other platforms can easily be beyond a defender’s radar and sensor range. The long distance release or launch of CMs and their smaller radar signature increase the possibility that surveillance assets will not detect them. Battle managers require cues to focus their search in detecting CMs in any surveillance area. Combining hostile aircraft attacks with CM and ASM attacks may allow “leakers” to get through. Indeed, CMs may resemble and be misidentified as manned aircraft.

(5) Rapid CID is critical for CM defense. CM defense is complicated by the use of low observable technology and the potential of SOF or other friendly aircraft without IFF transponders operating in the same airspace, thus requiring ID verification prior to engagement. CMs make surveillance and detection difficult because their flight profiles are specifically designed to defeat or confuse radar tracking. As with BMs, the objective is to eliminate as many CMs as possible before launch. CMs in flight may be part of TST target sets designated by the JFC. The challenge for defending against CMs is to find them early, before launch if possible, and engage them before they can navigate to their targets.

(6) Training patterns or identifiable launch sequence events for GLCMs are rarely observed or practiced in an overt environment. Consequently, the probability is small for conclusively identifying a GLCM TEL using current sensor data. Attacking a CM TEL requires the earliest possible detection of the target and the ability of sensors to discriminate between TELs and other targets. Successfully targeting CMs before launch will depend in great part on pre-hostility JIPOE/IPB efforts. Targeteers will require information on infrastructure, logistic support patterns, movement discipline, and signatures of typical storage and assembly facilities. Identification by signature is key to finding CMs before launch, since detecting the launch itself or tracing the flight path back to the launch site may be extremely difficult when they are launched from maximum range.

d. *CM Target Development*

(1) Procedures for finding and targeting CMs on the ground are no different than for finding other targets using a variety of theater and national sensors. Space-based and theater reconnaissance, surveillance, and target acquisition assets normally will collect intelligence data on these targets prior to armed conflict as part of IPB. Sensors on JSTARS and UASs and SOF pass CM target information to analysts and battle managers by data link or voice. Data collected and fused from multiple sensors will provide the necessary confirmation of the target. Immediate threat data will be broadcast over intelligence processing and transmissions systems such as tactical related applications and tactical data dissemination systems.

(2) When conflict begins, sensors must be used to validate known target information. With proper ISR, aircraft and naval launch platforms for ALCMs and SLCMs provide identifiable signatures and will yield opportunities to detect, ID, track, and attack those platforms. GLCMs will present a more difficult target set. The following is a discussion of targeting methods against each category:

(a) ALCM. Destroying ALCM-capable aircraft on the ground or neutralizing their supporting airstrips/bases is the best means to prevent ALCM employment. In this context, missions against this target system do not differ from other OCA missions in terms of tactics or weapons. The IPB process must focus on providing the intelligence that targeteers need to determine which aircraft and air bases support ALCM activity and task missions against them accordingly.

(b) SLCM. Destroying the launch platform in port is the best means to prevent SLCM launch. The IPB process will provide the naval order of battle information to identify specific SLCM carriers and support bases for targeteers and battle managers to task missions against them. Signatures of naval vessels and their substantial support base infrastructure will facilitate finding SLCM targets by satellite, UAS, and other surveillance platforms.

(c) GLCM. GLCM platforms normally are an adaptation of any available vehicle chassis capable of supporting one to two tons. Any medium-to-large size truck or tracked vehicle could be developed into a CM TEL. These TELs likely will be considerably smaller and less distinct than heavier BM TELs; however, a robust IPB effort can catalog such known and suspected vehicles for exploitation by surveillance sensors. GLCM deployment and training in suspect nations must be collected against and studied for behavioral cues to detection. Long-range GLCM permit the enemy to establish a large number of well-dispersed, fixed-launch locations (both actual and decoys) deep within their own territory. The enemy can be expected to employ camouflage, concealment, and deception for fixed and mobile TELs to reduce probability of detection. Detecting and targeting mobile GLCM platforms or newly built fixed launch sites will depend on a robust IPB, dynamic management of ISR assets, dedicated and trained analysts aided by technology improvements such as automatic target recognition systems, and a responsive C2 architecture.

**5. Air-to-Surface Missiles**

ASMs employment can be expected on all battlefields. Like BMs and CMs, ASMs are capable of delivering a complete range of warheads and can be carried by a variety of rotaryand fixed-wing platforms. Flight profiles, short flight times, and reduced radar cross-section make these missiles difficult to detect, track, and engage. Additionally, their speed and relatively short flight times leave a small window for interception. ASMs increase the survivability of the delivery platform through standoff capability, usually beyond the range of some point defenses. Many of the North Atlantic Treaty Organization and former Warsaw Pact nations are equipped with US and Russian manufactured systems and have exported them throughout the world. The best method for countering ASMs is to target the delivery platforms and related bases and facilities.

**6. Unmanned Aerial Vehicles (UAVs)**

*a. Architecture.* Typically, any UAV or drone architecture consists of three main elements: Unmanned Aircraft (UmA), Ground Control Station (GCS), and Communication Data-Link (CDL). These components are briefly described in the following:

• Flight Controller: it is classified as the drone’s central processing unit.

• Ground Control Station: it is based on an On-Land Facility (OLF), which provides human operators with the necessary capabilities to control and/or monitor UAVs during their operations from a distance. GCSs differ depending on the size, type, and drones’ missions.

• Data Links: are wireless links used to control the information flow between the drone and the GCS. This depends on the operational range of UAVs. Based on the literature review, drones’ control can be categorized based on their distance from the GCS:

* Visual Line-of-sight (VLOS) Distance: allows control signals to be sent and received via the use of direct radio waves.
* Beyond Visual Line-of-Sight (BVLOS) Distance: allows drones to be controlled via satellite communications.

*b. Domain of use.* Drones will play a major role in the near future, by delivering goods and merchandise, or even serving as flying mobile hot-spots for broadband wireless access. In fact, when drones are deployed as hot-spots, the most suitable solution for bandwidth allocation is the Binomial and Poisson cluster processes. The main goal is to serve a massive number of users in a specific area. Moreover, drones can be used to maintain all the needed security and surveillance techniques, which are implemented to ensure the usage of these drones safely, securely and properly.

Therefore, the focus is on the multi-purpose usage of these drones, both in the civilian and military domains. The multi-purpose uses of drones are illustrated in Fig. 1.



Fig. 1 Drone multi-purpose usage

UAVs became the perfect choice for military usage, especially for intelligence and reconnaissance purposes performing Surveillance, Target Acquisition and Reconnaissance (STAR), Joint Surveillance Target Attack Radar (JSTAR), Reconnaissance, Surveillance and Target Acquisition (RSTA) tasks. Their deployment is a key part to counter insurgency and terrorism, offering the ability to Track and Identify Dismounted Personnel (TIDP) in urban environments, especially in Areas of Operation (AO).

Fig. 2 presents a summary about several Drone/UAV types being used in overt/covert military operations, which are described next.

• P-CAS: more efforts are directed to enable UAVs to offer a Persistent-Close Air Support (P-CAS)/Precision Strikes for real-time protection of ground troops, and for a quick target elimination through the use of laser-guided missiles and without waiting for an airstrike-call. This method was applied by the American, (British) and French armed forces in Mali, Somalia and Djibouti, Kenya and Nigeria (mainly against Boko-Haram, and Al-Shabaab); hence, the Unmanned Combat Aerial Vehicle (UCAV). These drones can also be used to help (elite) troops in their covert, overt or clandestine operations by offering guidance, close air-support or currently active/passive enemy movement as part of Surveillance, Target Acquisition, and Reconnaissance (STAR), Reconnaissance Surveillance Target Acquisition (RSTA), and/or Combat, Intelligence, Surveillance, Reconnaissance (CISR), to enhance the Command, Control, Communications, Computers, Intelligence, Surveillance, & Reconnaissance (C4ISR) role and overcoming the limited Intelligence, Surveillance, and Reconnaissance (ISR) role of Unmanned Ground Vehicles (UGVs).

• Precision Shelling: UAVs were also used to conduct precision shelling against terrorist targets. In fact, Russia has been relying on this Guided Artillery Rounds technique as early as July 2015. This technique was also adopted by Pro-Russian separatists against Ukrainian forces in 2014, and by Ukrainian forces against Pro-Russian separatists in 2019.

• Aerial Surveillance/Reconnaissance: unlike the reliance on Human Intelligence (HUMINT), UAVs were also deployed as part of aerial intelligence and information gathering, allowing the identification and tracking of insurgents (i.e training, movement and camps), vehicles (i.e movement, types), weapons, weapon caches, and Improvised Explosive Devices (IED) (i.e factories, equipment, market, and planting), especially in Afghanistan. In fact, they were also used by both Ukrainian forces and pro-Russians for reconnaissance and counter-reconnaissance purposes during the Ukraine war. Recently, a new Russian drones’ footage emerged on February 2020, exposing how Turkish artillery batteries are targeting the Syrian army in support of anti-government rebels in Idlib.

• Unmanned Airstrikes: were the prime choice of the US as early as 2002, especially in the elimination of Al-Qaeda operatives in Yemen with their use of predator drones, before evolving into their authorised use in their Global War Against Terror (GWAT) along their British counterparts. Moreover, Israel also relied on the extensive use of drones and UAVs to perform unmanned airstrikes against key targets/figures in the West Bank, and military installations in Iraq and Syria. The same goes for Russia and Iran (Shahed-129 drone) using UAVs to counter uprising insurgencies and terrorism in Syria. Recently, after the loss/injury of more than 59 Turkish soldiers by Syrian airstrikes as part of “Dawn of Idlib 2”, the Turkish army extensively used drones in retaliation attacks to target the Syrian Regime’s troops and allies’ military targets and installations in series of well-coordinated drone strikes, before a cease-fire was established, and before risking further escalation with Russia.

• UAV Hijacking: This is done mainly through GPS spoofing/jamming, and it was very effective in the Ukrainian conflict and in countering ISIL’s threat, especially over the city of Mosul, until its liberation in 2017.

• Covert Aerial Surveillance/Reconnaissance: UAVs were being developed and produced as early as world war one, using Archibald Montgomery Low’s radio control techniques to counter the Zeppelins threat, before their covert use in the cold war era for spying purposes, and during the Vietnam war as part of reconnaissance. This included their use by the US-led coalition forces, mainly the British in operation Herrick, Afghanistan.

• Evading Radar-Detection: another military purpose of drones is to avoid radar detection. The Harop IAI, or HARPY IAI 2 along the British ”Fire Shadow”, are classified as anti-radiation drones. They are capable of autonomously reaching their targets without the need to carry a warhead by self-destruction into the main target. However, IAI Harop showed a higher success and accuracy rate compared to the Fire Shadow, yet the British Ministry of Defense (MoD) stated that the project will be extended in the future. This is due to their ability and capability to evade SAMs and radar detection systems, which are either designed to target a much larger aircraft or to intercept fixed-trajectory missiles.

• Interception of Footage: military analysts are capable of analyzing the footage taken and filmed by a terrorist’s drone in an attempt to thwart a domestic terror attack. This allows them to identify their tactics, operational geographical location, along with their skills, weapons, and training.

• Targeted Assassination & Killing: the adoption of this term came as part of the US approval of use of lethal force as part of new rules of engagements for counter-terrorism and counter-insurgency tasks/purposes (i.e Afghanistan, Yemen, Iraq, Syria and Libya). Its adoption can be based on the use of drone strikes or explosive-laden drones. Kamikaze drones/UAVs or loitering munitions might also be used for ”Target Assassination” purposes, as part of the so called explosive-laden drones. This specific concept was demonstrated by the Israeli K1-UAV, which can be adapted and used by intelligence and spying agencies, where Israel Aerospace Industries (IAI) also unveiled their newest Loitering Munitions (LM) called IAI Harpi at the Singapore Airshow in 2016 and the IAI Mini-Harpi in 2019. However, not far from now, on August 4th, 2018, a drone-led assassination attempt was foiled when two drones wrapped with explosives were used to assassinate the Venezuelan president; they were shot down by snipers injuring 8 soldiers and 1 civilian. Targeted killing is executed via drone strikes by what is referred to as ”Killer Drones” such as the case of the Global Hawk, Predator and Reaper Drones, as well as the British ”Protector RG Mk.1” UAV for the elimination of key terrorist figures/targets. However, the adoption of this method resulted into further civilian casualties, and the rise of new insurgencies.

*c. Military countermeasures.* Examples of military techniques to counter drone attacks include the use of old Soviet anti-aircraft weaponry (i.e ZSU-23-4 Shilka, and surface-to-air missiles (SAM S-300/S-400 missiles)), to shoot down Turkish drones over Idlib and Syria. Recent studies revealed how terrorists are shifting towards a new asymmetric warfare called ”drone warfare”. For this reason, four main different military countermeasures were suggested and implemented to overcome the UAV security threats. According to the Cable News Network (CNN), the Pentagon issued new guidelines allowing the military to bring down any drone flying near or over a US military base.

Next, we list a set of the most recent real-time highly accurate anti-drone countermeasures, and in Fig. 2, we highlight the latest generation of high-energy laser weapons targeting UAVs.

• ATHENA: or Advanced Test High Energy Asset, is an upgrade to the Area Defense Anti-Munitions (ADAM) system, which is a 30-KW laser weapon system that uses the 30-KW Accelerated Laser Demonstration Initiative (ALADIN) laser, which combines the power of three 10-KW fiber lasers into a single beam. ATHENA can also operate on 10 and 20 KW levels. This system is funded and tested by Lockheed Martin and it can operate over thousands of meters.

• Rafael Drone Dome: is a counter-UAS operational mobile system 381] used to detect, track and eliminate hostile drones (even when maneuvering) as small as 0.002 m2, at a distance of 3.5 km, using a high power laser beam, enabling a soft and hard-kill. Testing results show its ability to successfully eliminate three drones in a timely manner.

• Boeing Compact Laser Weapons System (CLWS): is used to track and disable UAVs through the use of a laser weapon system to acquire, track, and identify potential targets, or even destroy them. Its main advantages are based on the fact that it is portable and it can be assembled in almost 15 minutes. Moreover, it can destroy a target from 22 miles within 10-seconds, using an energy beam of 2, 5 or 10 KW.

• Anti-UAV Defence System (AUDS): is an anti-UAV system developed by UK defense companies to address the increasing UAV threats. It is classified as a smart-sensor and ”effector” package with the ability to remotely detect small UAVs, track and classify them before providing the option to disrupt their activities. It was used around UK airports and it is now being deployed in New Zealand. Among its characteristics, it contains an electronic-scanning radar aimed at detecting targets, an electro-optical video for target tracking and classification, along with a software known as ”intelligent directional RF inhibitor”. Its detection range is up to 10 km, with a minimum target size of 0.01 m2. Moreover, it is able to operate in various weather conditions, and 24 hours a day.

• Counter-Rocket and Mortar (CRAM): is a missile-based counter rocket, artillery, and mortar defense system developed as part of the US Army Enhanced Area Protection and Surviving (EAPS) technology, with an expansion including threats from unmanned aircraft systems or drones. In fact, CRAM is the land version of Phalanx CIWS. Among its characteristics is the use of a 20mm HEIT-SD (highly explosive incendiary tracer, self-destruct), 30, 50 or 76mm Driven Ammunition Reduced Time (DART) of flight, cannon to launch command guided interceptors using a precise tracking radar interfero-meter as a sensor, a fire Control Computer (CC), along with an RF transceiver to launch the projectile into an engagement ’basket’. Computations are then made on the ground, and the RF sends the information back to the CC.

• Non-kinetic Methods: other countermeasures include non-kinetic methods such as the use of radio waves to disrupt drone flights. However, due to the rules of engagement being classified, it is hard to tell under what options and weapons the army might use them.

• Anti-UAV Zappers: were sent and used by the British forces on the frontline in Iraq and Syria to protect Western and American forces against drone attacks emanating from the Islamic State of Iraq and Syria (ISIS). By 2017, Zapper was responsible for downing more than 500 drones through radar jamming.

• ADS-ZJU: ADS-ZJU stands for Anti-Drone System at Zhejiang University; it was developed and tested on a DJI Phantom 4 drone. The authors combined three detection and surveillance technologies including audio, video, and RF, and the architecture consists of four units:

* Heterogeneous Sensing Unit: it uses various types of sensors to capture information to detect drones.
* Central Processing Unit: it performs drone feature extraction, drone detection, and drone localization.
* Automatic Jamming Unit: it relies on RF jamming against any drone flying over a sensitive area.
* Real-Time Display Unit: it is based on a liquid crystal display that predicts both acoustic signals and real-time trajectory of a drone.



Fig. 2 Military anti-UAV/UAS techniques