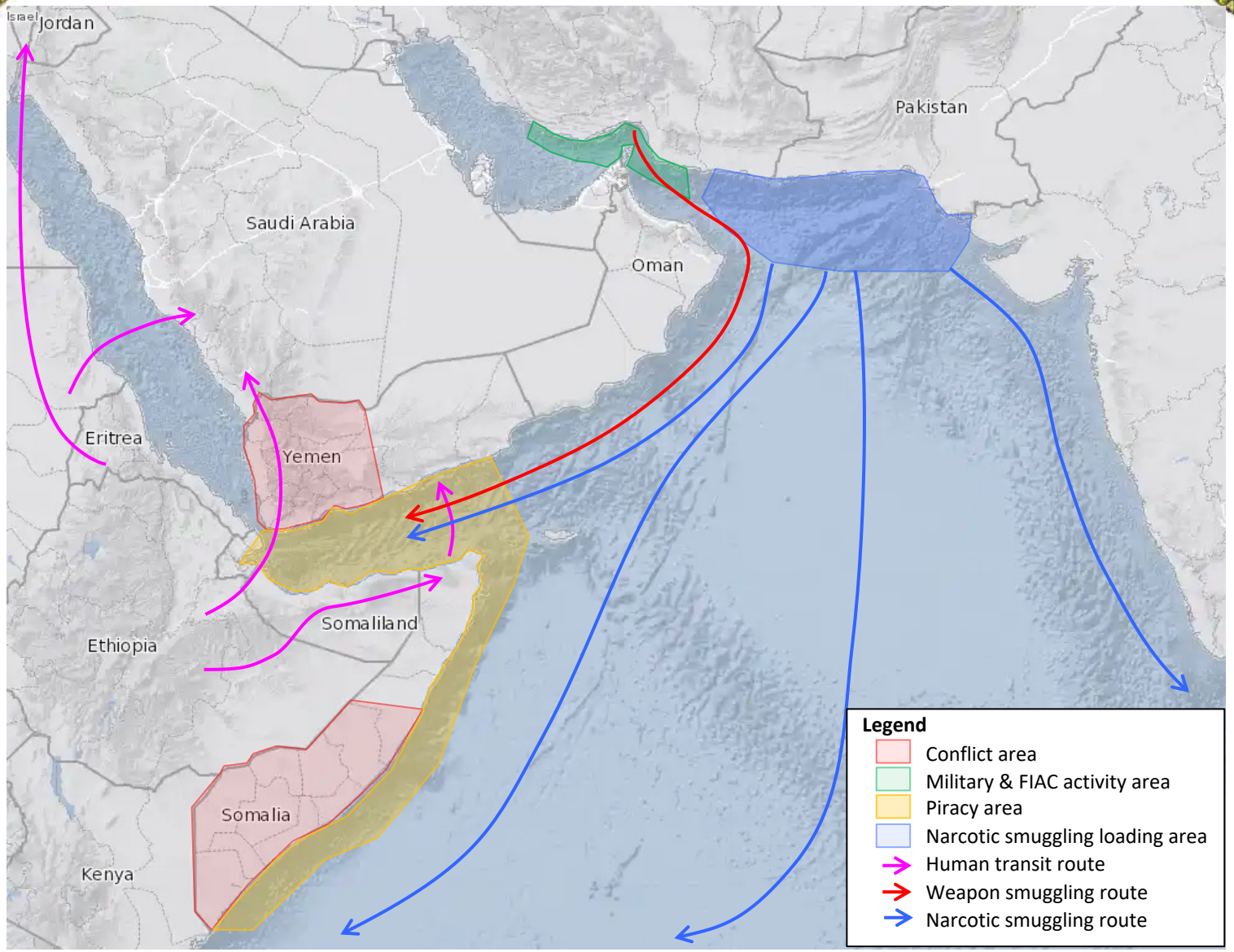
MARSEC THREAT

REGIONAL OVERVIEW



PIRACY

(U) Currently, piracy is suppressed in vicinity of Somalia and there has been no reported incident for more than 1500 days. That being the case, there is a legal distinction between piracy and armed robbery, which according to the IMO is location based. Piracy would happen in international water and armed robbery would happen in territorial water. Because of jurisdiction and the lack of information sharing agreement, there is little to no information available with regards to incidents in territorial water, but they likely happen in countries facing internal conflicts.

(U) Pirate vessel

(U) Historically, although piracy attacks have occurred at various times during the day, they have been more frequently reported during the early morning. They usually involve more than one skiff, sometimes a mothership if far away from the coast. Pirates use weapons and RPG to intimidate and coerce the vessel operator into slowing down, allowing for boarding. Once on board, they get control of the bridge. Most often, they will not steal nor utilize excessive violence. Their goal would be to get in contact with the vessel owner or financial authority, then relay the process to a third party negotiator on land.

Comment: (U) BMP5 and onboard security guards are the two most effective ways to defend against piracy attempts. Although there was no reported piracy attack, there have been attempts or suspicious approaches in the past few years. There are indication that pirates likely have retained their capabilities to conduct operations and would resume given the right circumstances.

SKIFF APPROACHES IN THE SRS

(U) There were incidents at the end of 2022 and beginning of 2023 with regards to skiffs approaching smaller vessels like yachts and sailing boats in the Southern Red Sea. Those incidents occurred close to the Eritrean territorial waters. Two of those incidents involved an exchange of fire between the skiffs and the yacht.

(U) It is common practice for smaller vessels to sail close to territorial waters to avoid meteorological pattern with high wave or wind which funnel through the BAM during monsoon seasons.

(U) The Eritrean Navy is known to operate vessels that resemble skiffs in that area. The crew may not wear uniforms. This area is routinely patrolled by CMF and EUNAVFOR, which greatly reduces the risk of piracy.

(U) Vessels transiting in the Southern Red Sea, especially near Assab, may expect to be approached by the Eritrean Navy, which could be construed as hostile acts.

(U) Incident related to skiffs in the SRS


(U) Eritrean Navy patrol vessel

Comment: (U) At this time, there has been no report of such incidents happening to larger vessels or merchant vessels. The high presence of foreign military vessels patrolling this area for CMF and EUNAVFOR reduce greatly the risk of piracy.

WEAPON SMUGGLING

(U) There are currently very few weapon smuggling events reported over the past year. That is not to say that they do not happen, but mostly that the legal framework to prosecute this type of activity is difficult to apply. Weapons smuggling is also very difficult to detect and track.

(U) Weapons that were smuggled, mostly drones and missiles, to groups such as the Houthis, Al-Shabaab and AQAP have been observed to be used against vessels near Yemen territorial waters.

(U) Weapon smuggling route

Comment: (U) In the area, the Houthis are the group that has demonstrated their willingness to attack vessels in the past. They have seized or attack vessels inbound to Saudi Arabia with the objective to deprive them of economic gains. Currently, there is a cease fire between the two parties, which reduce the risk of attack on the merchant vessels.

DRONES

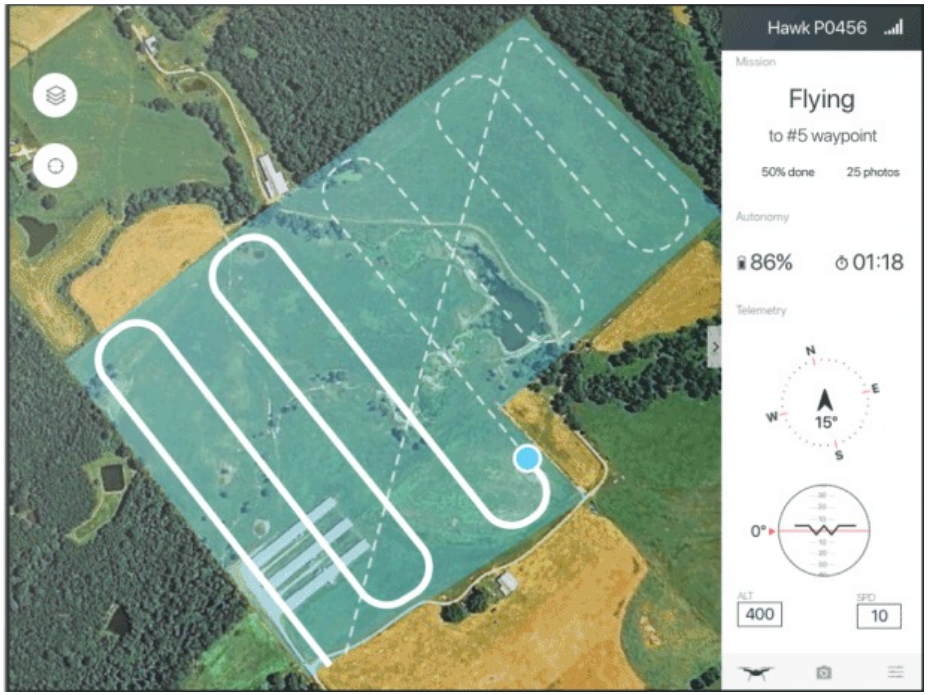
DRONE CONTROL

GPS controlled (waypoints)

(U) Used mostly against static vessel either moored or at anchor. The GPS coordinate is programmed in the drone prior to launch. Interfaces are usually fairly simple to utilize and does most of the work with regards to navigation for the user. They can show mission progress accurately and sometimes be modified during flight. This is mostly used for reconnaissance.

Operator controlled

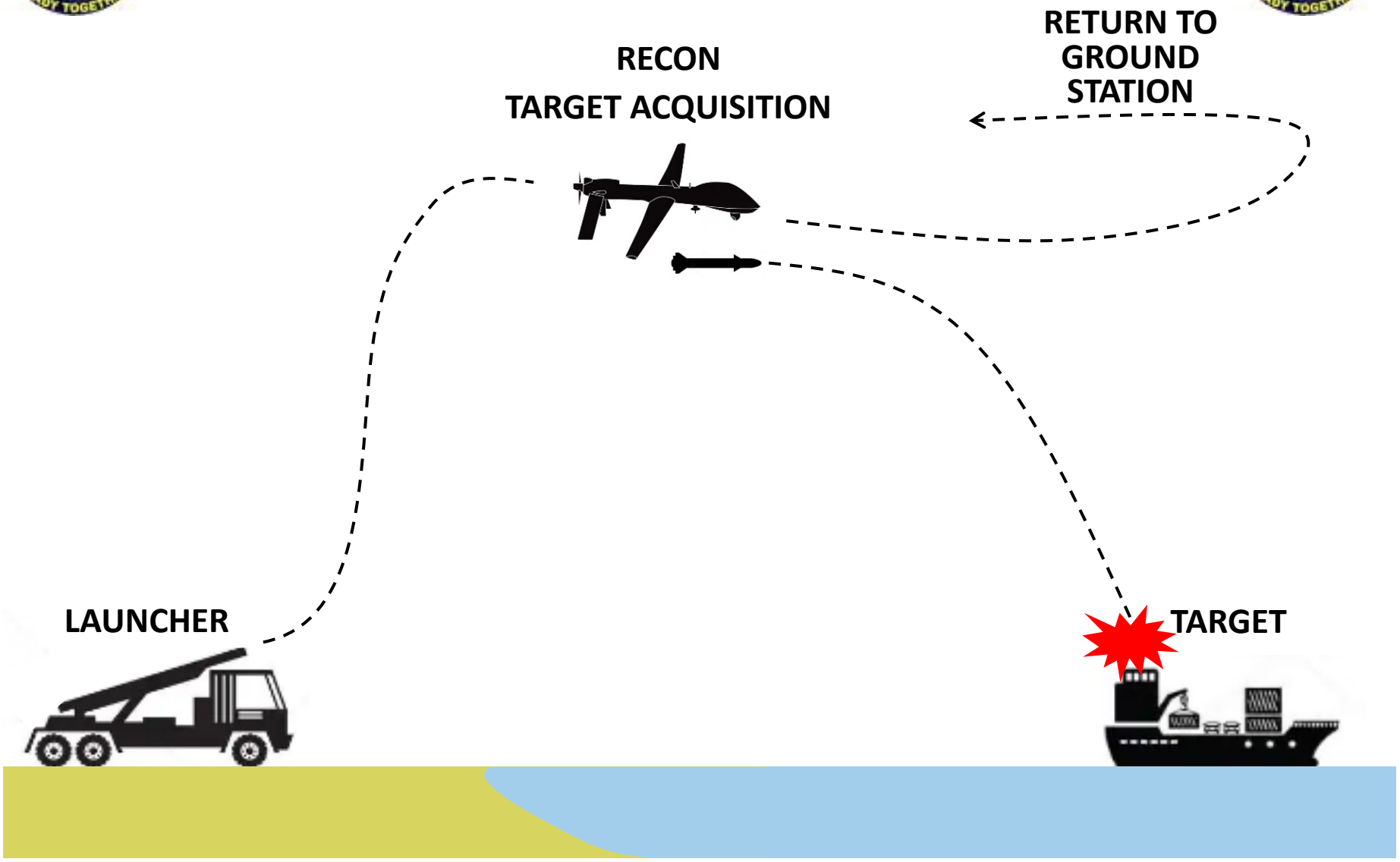
(U) Usually the preferred method to strike moving targets, but require a good connection between the UAS and the ground station. Most often, the operator will be within visual range of the target for smaller vehicle or use alternative communication methods for larger UAS (military).



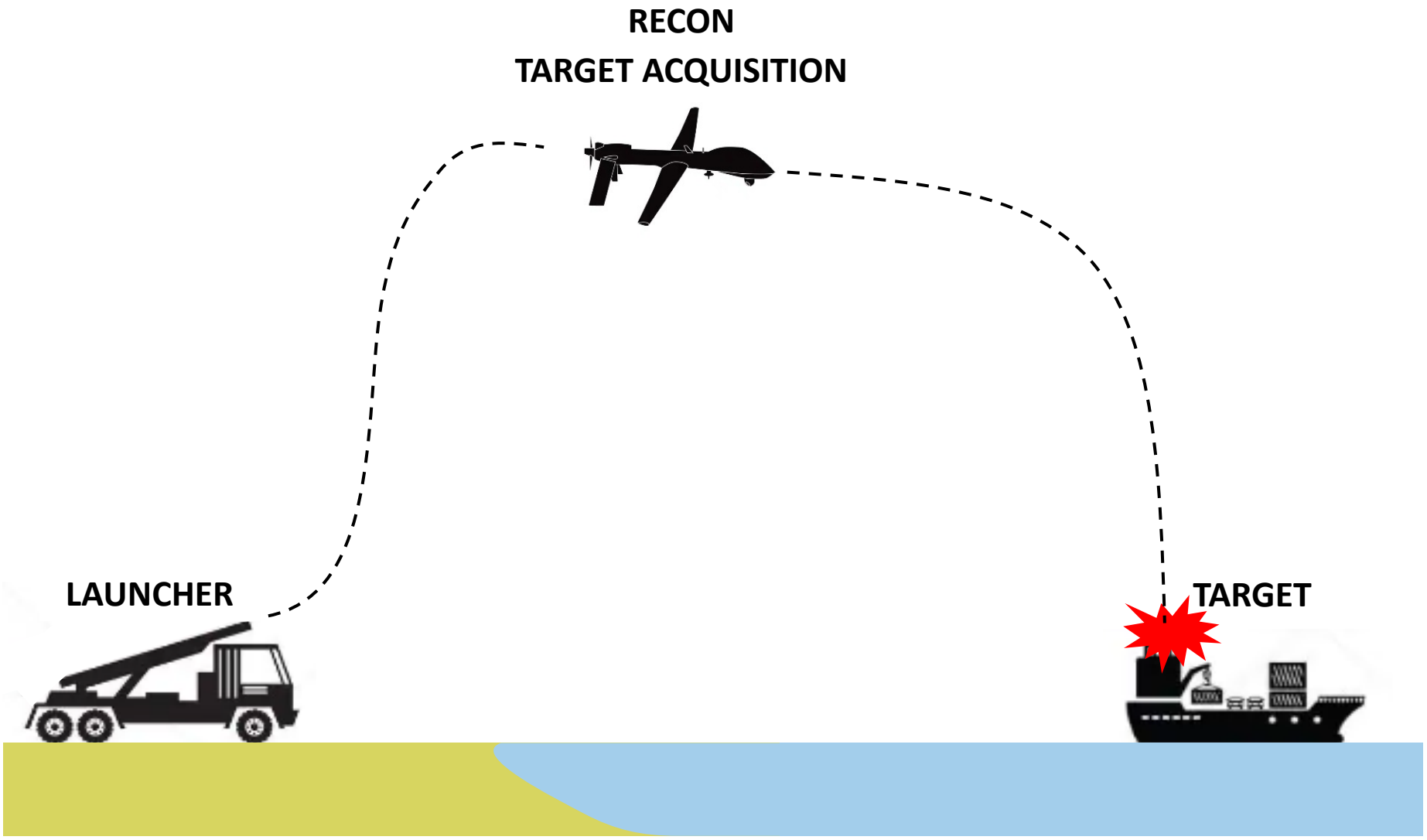
(U) Example of a control interface from an IPAD

Comment: (U) GPS controlled UAS are far too unreliable to provide the desired effects. It is easy to miss and provide little control over the operation, which restrict the flexibility required to affect vessels. It is, still, very effective for reconnaissance mission. Operator controlled operation is often preferred for military operations.

UAS WITH PAYLOAD



LOITERING AMMUNITION



MULTI ROTOR UAS

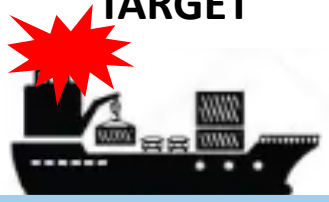
RECON

TARGET ACQUISITION

RETURN TO GROUND STATION

LAUNCHER

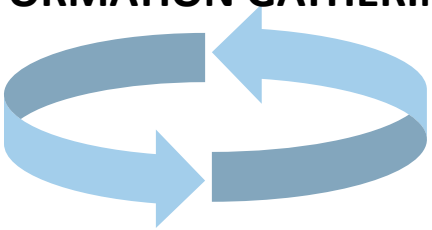
TARGET



RECON UAS

RECON

LOITERING
INFORMATION GATHERING



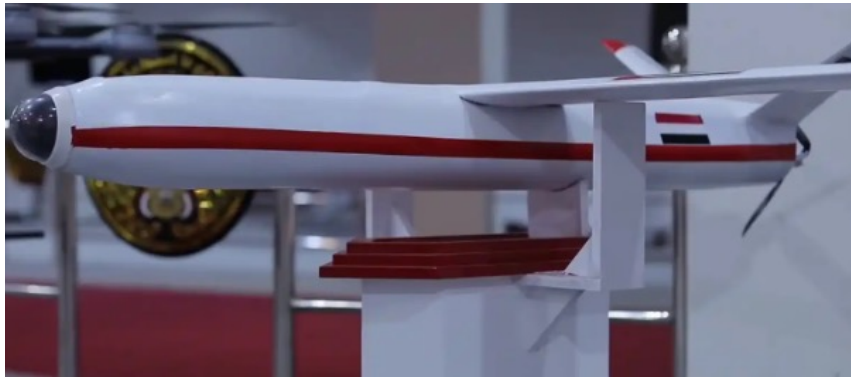
LAUNCHER

TARGET

FIXED WING ATTACK UAS

(U) Wa'aed

(U) Samad 4



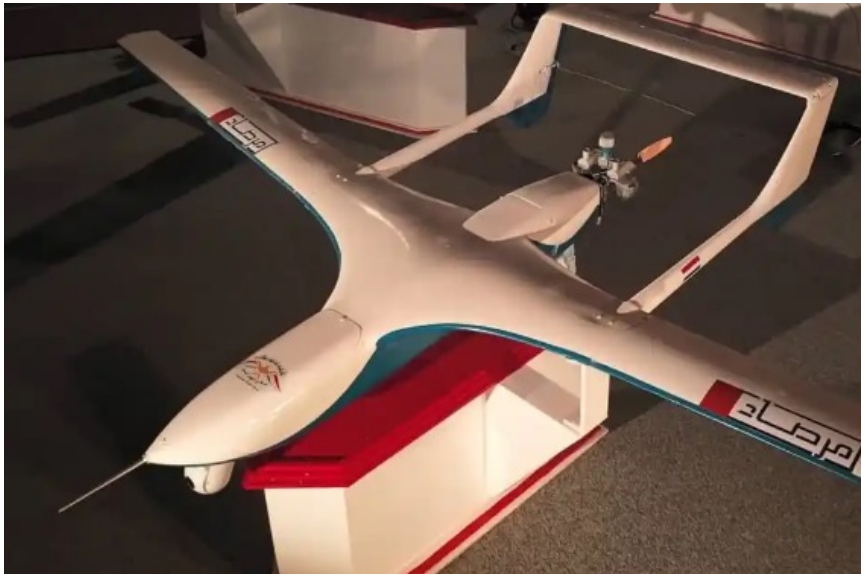
(U) Khatif

(U) Samad 3

Comment: (U) Fixed wing attack UAS are very efficient compared to aircraft due to the low cost/damage ratio and they are difficult to detect. They require a certain amount of technological knowledge to produce the ammunition and require expertise to be used efficiently.

FIXED WING RECON UAS

(U) Rased-1



(U) Mersad

Comment: (U) Fixed wing recon UAS generally carry a heavier payload at the front, usually camera and optic sensors, sometime accompanied by antennas or other sensors. Their shape are usually optimized to reduce unwanted movement and are constructed lighter to augment time on station.

MULTI ROTOR UAS

(U) Rujum

(U) Nabaa

Comment: (U) Multi rotor UAS sacrifice endurance for maneuverability and ease to launch. They can be operated practically everywhere and have the capacity to hover, which is not available to fixed wing UAS. They can carry limited payloads that most often need to be manually released and aimed with an optic camera.

CYBER ATTACKS

TYPE OF CYBER ATTACKS

(U) **Untargeted:** Seeks to find potential weak spots over a large amount of companies or ships to be exploited by a targeted approach at a later time.

(U) **Targeted**: A focused action aimed towards a single ship or company. They are much more difficult to detect and deter as the attacker likely have all the information they needs to conduct such operation.

(U) **Malware**: Software designed to damage the computer of the target without it's knowledge either by exploiting system bugs or by creating one. Often acquire through links and email.

(U) **Phishing**: Usually aimed at a mass group of people, where the goal is to gain informations. Usually this happens through email where there are requests to click on links or to send data.

(U) **Brute force**: Mostly seen as programs that attempt to forcefully crack passwords by using algorithms.

(U) **Distributed Denial of services (DDOS)**: Achieved through overloading a server with many requests, which denies the user access to the service by slowing the connection down or forcing the server to shut down.

(U) **Social engineering**: Attempts to contact or influence a person to give information that could be harmful through the use of social media.

STAGES OF CYBER ATTACK

(U) **Reconnaissance**: The hacker will attempt to gain information about the target through multiple means such as social media, technical forums or websites to identify a vulnerability in the system. It is also possible that the interception of data from the ship to outside sources is conducted.

(U) **Delivery**: Attempts to access the ship system.

(U) **Breach**: The attacker can tamper with the ship system by either stealing data or taking control of the system. There is an entire spectrum of activities in between those two actions that could be harmful to the vessel.

(U) **Pivot**: With the previously acquired data and access, the attacker can gain access to more sensitive data or systems and can install software that will allow them to gain constant access to the systems.

IDENTIFYING SYSTEM VULNERABILITIES

(U) Is the system stand-alone or is it connected to other systems?

(U) Is the system connected externally, either directly or via other systems?

(U) Does the system have effective, built-in risk mitigation measures such as encryption?

(U) Does the system require regular software updates? Obsolete systems are easier to access.

(U) Does operating the system involve connecting removable devices, for example to obtain diagnostic information?

(U) Is the system easy to physically access?

(U) Is the system lacking security protocols?

(U) Is the system mismanaged by the employee. Example: sharing accounts or passwords?

VULNERABLE SYSTEMS

(U) **ECDIS** (Electronic chart display and information system)

(U) **VDR** (Voyage data recorder)

(U) **EPIRB** (Emergency position indication radio beacon)

(U) **VPMS** (Vessel performance management system)

(U) **CTS** (Container tracker system)

(U) **PMIS** (Port management information system)

(U) **AIS** (Automatic identification system)

POSSIBLE OUTCOME

(U) Changes in ship data, including its position, course, cargo information, speed and name;

(U) Creation of "ghost ships", recognized by other ships as a real ship, in any location in the world;

(U) Sending false weather information to specific vessels to force them to change course to avoid a nonexistent storm;

(U) Activation of false collision warnings, which can also cause automatic correction of the course;

(U) The ability to make an existing vessels "invisible";

(U) Creation of non-existent search and rescue helicopters;

(U) Falsification of EPIRB signals, which activate alarms on nearby ships;

(U) The possibility of carrying out a DDoS attack on the entire system by initiating an increase in the frequency of transmission of AIS message