Towards a Taxonomy of 'Capturing Countermeasures'

Patrick Van Hoeserlande

There is no doubt in my mind that autonomous systems are a thing of the future. These systems are being introduced in today's battlefield and their introduction will only increase with time. The question is not if they going to change our way of fighting but how they will do that. We should look ahead and answer the question on how to organize ourselves to exploit fully the opportunities offered by the employment of these systems. However interesting and necessary, this article is not about finding that answer. This Thinkbox concerns a more basic problem than the conceptual reflection on war robots.

Sending out Unmanned Autonomous Systems (UASs) means risking losing them. They can be shot down - in a manner of speaking because not all UAS are flying as some are riding, sailing or diving, but you get the point – or captured. That last things happened in December 2017 when the Chinese took an US Unmanned Underwater Vehicle out of the water just before the USNS Bowditch was about to retrieve it. True, the Chinese returned the precious drone to its owner; nevertheless, the incident raised the question about the protection of UAS. At the eve of the introduction of Unmanned Air Vehicles (UAVs), users feared the scenario of drone returning home rigged with a bomb. A very simple tactic, although much harder to implement, to wipe out the people and infrastructure 'controlling' the drone.

Of course, like all things UAS are also susceptible to unintentional destruction. A passing plane can hit an UAV or a big cargo ship might overrun a small surface vessel. The result will be the same as the intentional act: the loss of the UAS. Not only an adversary has an interest in capturing your technology; somebody may think to receive a finder's fee when returning your 'lost' UAS.

There is clearly a need to safeguard our unmanned systems out there. Before we can tackle the how-question, we should consider the what-element. What do we want to protect? The first reaction is: the vehicle. Is that really the case? Protection in whatever form means extra weight, extra energy consumption and even extra risks. To optimize the whole system, we must make sure that we know what we want to protect. A cheap system may be expandable, but we may want to keep the technology, or only part of it, a secret. Maybe there is nothing new about the hardware, but the collected data may be worth protecting. In addition, I can imagine situations wherein the knowledge of the origin of the equipment or space the system is operating in is the most important to protect.

The decision of what to protect is not a static element. It may evolve over time making the countermeasures more difficult to implement.

The proposed taxonomy below is a first attempt to categorize the different methods to safeguard our autonomous secrets. I invite all to help to improve and complete it. It may well be that some application covers more than one method. With the taxonomy, I want to offer a framework to think about

countering the risk of captured unmanned vehicles. Choosing one or more measures is about striking a balance between protection and mission effectiveness.

Avoidance

The best way to defy capture (or destruction) is avoiding a possible incident, passively or actively.

Passive

Extreme: An UAS can be relatively safe if it operates at the extremes. This will be a burden on the vehicle, but it may be a too much a burden on the system attacking it making the costs too great for the potential benefits. The other side knows very well that they are there but is quasi incapable of destroying or capturing them. Example: Satellites and very deep-water vehicles are an example of such systems being relatively safe.

Camouflage: An old trick that still works. Color schemes, restriction of movement or radiation … make it harder to detect a vehicle, now and in the future.

Stealth: Although a subset of camouflage, the absence of any kind of reflection (radio waves, sound. light) deserves a category on its own because these techniques are harder to implement and may have a serious design impact.

Mimicry: This kind of passive approach has a big impact on the design of the vehicle. The idea is to assimilate an aspect of the environment. Example: A micro-UAV with an exterior design to look like an insect, the shell of an intelligent mine 3D printed to be similar as a rock …

Active

Detection: An UAS may be equipped with a subsystem detecting possible danger and alter the risky action. This ability to detect danger is a condition for all active measures because these are a reaction to an event is the environment. Example: An Underwater Vehicle may stop its ascent to the surface if it detects the sound of a surface vessel nearby. An UAV may adapt it flight pattern if it detects another airplane.

Escape: The next possibility is not limited to avoiding the risk of being captured but running away from the danger. The UAS must of course be equipped with a sensor that triggers the escape subroutine. The action following the detection of a risk is not limited to stopping the procedure, but to actively engage in activities in order to make capturing difficult.

Hiding: A UAS may opt to hide where it is harder to get.

Flight: One way to escape is to run away at high speed, preferable to safety. This approach may be short-lived as speed will possible drain the vehicle's internal energy resources.

Transfer to another medium: An interesting type of escaping is to transfer from one medium to another. There are only a limited number of systems that can go from water to land, from land to air, etc.

Screen: Like the maneuver of an octopus, a change in direction combined with a screen that reduces the effectiveness of the adversary's sensor may increase the likelihood of escape.

Emulation: A bit similar like mimicry, but in an active way. Example: A small UUV may emit a sonar reflection like a submarine.

Decoy: An UAS may launch a decoy to trick its hunter following the decoy instead of the actual vehicle. Although effective, it is limited in its application.

Confrontation

If avoiding capture is not possible or not preferred, the unmanned vehicle can be equipped to tackle the danger head-on.

Self-destruction: If all above do not help or are too cumbersome to implement, a limited or a full-blown self-destruct mechanism may do the trick. The self-destruction must be designed in such a way that it destroys the parts we want to keep a secret. If the vehicle itself or most of the equipment needs protection a complete destruction may be consider. In some cases, this will be a hard thing to accomplish. Parts of a destroyed vehicle may be enough for a reconstruction. Self-destruction does not necessarily mean that it must be an explosion, a strong acid may be better to erase a memory card. Having a self-destruction mechanism aboard may prove a supplementary weakness. It may be hard to define when an UAS is compromised. What are the criteria to initiate the self-destruction? A cyber-attack may initiate the self-destruction mode when the adversary only wants the vehicle out of operation.

Deterrence: The ability to self-destruct may be used as a deterrence. In that case, this ability must be clearly marked to have an effect. Example: The skin of the vehicle may carry a warning that the vehicle will explode if tempered with.

Self-defense: Although a possible legal nightmare, an UAS may be equipped with a self-defense capability. Instead of flight, this system may opt for a fight. This capability must not necessarily be aimed at human soldiers, it may well be exclusively against other UAS.

Against LARS detection

A last category that stands apart from the rest is the protection against Launch and Recovery Systems (LARS) detection. UAS and its operators are extra vulnerable during launching or recovering a UAS. This weakness may offer the opportunity to attack the UAS and its operators at the same time.

Wait: There is no rule that a UAS must be launched just before its employment or recovered directly after it has finished its mission. There may be a period of inactivity between those steps. This forces the other side to spend time and resources in waiting for things to happen.

Change or variation: As there is no rule about the time between activity and L&R, there is no need to have a direct approach from the zone of activity to the L&R activity. The more variation, the harder it will be to follow the UAS and detect the L&R moment.

Speed: The quicker the L&R happens the harder it will be to hit during that vulnerable moment.

This taxonomy is certainly not complete, but I think it may help further development and discussion about protecting our systems. The sooner this aspect receives thought, the better the design of the necessary measures will be.