Battlefield Asymmetric Robotic Threat

By LTC Christopher Korpela, LTC Daniel Bennett, LTC Paul Maxwell | February 24, 2016

Despite being unmatched technologically on the battlefield, low-cost, asymmetric threats have proven dangerous for US military forces. The proliferation of IEDs (of all types) in the Iraqi and Afghan theaters demonstrated that inexpensive, commercial off-the-shelf (COTS) technology can impact US high tech operations. Robots have the potential to provide a similar destructive impact on our forces given their wide availability including powerful, open-source software, which has been illustrated recently with ISIS coupling IEDs with 'driver-free' vehicles.[1]

There are many robotic systems being developed for a variety of military uses such as transport, personnel recovery, and direct combat. These systems are extremely complex and not affordable, especially in large quantities, for most of the adversaries that the US military is likely to face. However, there has been a rapid proliferation of drone and other robotic and/or custom built machines that, excluding the payloads, can cost well under $25,000. At this cost point, poorly funded adversaries can obtain this capability and perhaps do so *en masse*. Though higher in cost than the low-tech IEDs encountered in Iraq and Afghanistan, the potential increased lethality of these devices and the standoff protection offered to the attacker may encourage their use.

Robotic systems discussed in this paper include ground-based (wheeled, tracked) and air-based (rotor-wing, fixed-wing) systems. Water-based systems exist but are not as significant a threat to US ground forces. These systems can range from completely autonomous to completely command controlled. Threat systems may rely on commonly available communications protocols such as RF, Wi-Fi, cellular, satellite, and Bluetooth. These robots will obtain their processing power from devices ranging from low-end embedded processors and FPGAs to laptop computers to potentially cloud-hosted systems. An intent, enabled particularly by processing power, is that robots could conduct more analysis on their own in order to make decisions and take action while minimizing sustained control communications requirements and the signature it provides. In fact, as discussed in Mayer, "not only will increased autonomy reduce personnel and operating inefficiencies, defence planners view it as a 'crucial' attribute for maintaining tactical advantage on the battlefield."[2] A serious concern from the US military perspective is with respect to the rules of war and engagement, however when you consider many of our adversaries, particularly non-state actors, then many of these considerations will not be made in their decision cycles, thereby making it a simpler process.

The effects these robots are able to achieve against US forces are limited by the payload capabilities of the robots. Most aerial systems are capable of carrying payloads on the order of five pounds or less. Ground-based robots can carry heavier loads but are still limited to tens of pounds at best. Even with this limitation, it is easy to envision robots being able to distract, disrupt, or destroy US forces. Distracting might be in the form or a ruse in one location while an asset able to conduct kinetic effects is being used somewhere else. Robotic assailants could disrupts our forces by degrading our communications or locally spoofing/blocking GPS signals. Destruction may be achieved via the spreading of ICM sub-munitions or through the creation of mobile Explosively Formed Projectiles (EFPs). Given the current range limitations and control methods for robots, these systems are most lethal in urban/sub-urban areas where concealment for the controller is readily found. Additionally, these environments provide better terrain for ground based systems, better communications network support, and ready power for charging the systems. Though possible, marshalling robots and controlling them to their target is much more difficult in open, varied terrain.

Aerial robots are growing in popularity and are widely available. Individuals can purchase systems from a few hundred dollars to thousands of dollars through a variety of vendors such as department stores, hobby stores, and online retailers. These robots are frequently multi-rotor systems though single-rotor and fixed-wing systems are available. Most of these systems are targeted at surveillance missions and all have a very limited payload capability – some more expensive systems can carry up to five pounds.[3] The limited payload capability effects their range and station time. Current systems can achieve 20 minutes of flight time (due to battery limitations) and many are limited to under a mile of range due to command control communications constraints. Flight training for these systems is minimal given COTS autopilots such as the OpenPilot[4] and Ardupilot[5] devices. The limitation on range may soon evaporate as readily available autonomy packages proliferate. Available autopilots such as the Pixhawk[6] combined with open-source software such as the Mission Planner[7] make creating autonomous flight feasible with little experience.

Ground-based robots are also readily available commercially in many form factors. The two most common threat systems are wheeled and tracked robots with simple motorized platforms and added electronics similar to the Traxxis RC systems[8] used by USMA cadets or purposely built robots such as the Fire Bird V[9] or Jaguar v4[10]. These systems have increased operating times (multiple hours) and increased payloads (up to 50 pounds) compared to aerial systems. For command controlled systems, ranges are still limited by the technology employed. Though mobility for these systems may be limited by obstacles, their increased payload allows for more sensors, communications devices, and computing power. Similar to aerial systems, autonomous systems are currently not common but will proliferate rapidly. More expensive systems come with software capable of limited autonomy out of the box. For systems without this capability, open-source software such as the Robot Operating System (ROS)[11] provide ready-made tools to quickly build and field an autonomous system without expert knowledge. This software repository provides free, tested software that allows the quick integration of sensors, actuators, and computers to create custom designed robotic systems. This type of open-source code lowers the technological barrier to entry for complex systems.

The US military currently does not anticipate such attack vectors and are unprepared to defend against them. In contemporary combat, the US normally has air superiority, or rapidly establishes it. Furthermore, "Slow-moving and non-stealthy drones are easily targeted by ground-based air defences or an adversary's combat

aircraft."ii However, you can consider a swarm of drones as providing a means to distract, disrupt, as decoys preparing the environment, or simply as the main effort or thrust. "The future, however, may lie in smaller drones. As Work and Brimley have argued, 'large quantities of low-cost, expendable unmanned systems can be produced to overwhelm enemy defences with favourable cost-exchange ratios… making survivability a characteristic not of any individual platform but of a swarm of systems."[12] It can serve as another offset strategy, as with IEDs before and as discussed in Velez-Green's article.[13] Although we have systems like the Phalanx Close-in Weapon System,[14] they are designed for multiple 'dumb' missiles and these robots could be programmed with evasive maneuvers or could be used in places where it would not make sense to have the Phalanx strategically placed or cost-efficient for the limited number of these systems that would be available versus small drones being used *en masse*. Robotic counter-measures may take many forms ranging from new Warrior tasks to allocation of E/W assets to systems being developed by industry.[15] Defeating a robotic opponent may be accomplished via Soldier training that recognizes a threat vehicle(s) and engages with appropriate weapon systems. Home station and CTC training tasks can teach Soldiers the battle drills necessary to defend against robots. More sophisticated defensive means may be to deny portions of the electromagnetic spectrum in localized areas. This may mean jamming commonly used command frequencies or even spoofing GPS signals to confuse autonomous systems as mentioned in Cooney's Airbus article.15 Additionally, emphasizing tested military techniques such as camouflaging assets can improve defenses by increasing the difficulty of identifying targets by systems that use visual or electronic means of target acquisition. Denying pattern recognition algorithms an easy match can defeat a robotic attack.

It is important for the Army to recognize this potential attack vector and to develop counter-measures to protect its assets. Hardware to comprise robotic attackers is readily available and the software is freely available through the open-source movement. Together, these elements create an opportunity for future opponents to attack our forces despite our technological advantage. To understand the threat and prepare for it, it is necessary to survey the threat devices and software and then develop a plan to mitigate them.

Endnotes

[1] Ian Drury, "Inside the jihadi workshop of death: How ISIS is developing driver-free vehicles for bomb attacks in the West and sophisticated new missile technology capable of downing passenger jets." http://www.dailymail.co.uk/news/article-3385968/Inside-jihadi-workshop-death-ISIS-developing-driver-free-vehicles-bomb-attacks-West-sophisticated-new-missile-technology-capable-downing-passenger-jets.html (accessed 5 January 2016)

[2] Michael Mayer, "The new killer drones: understanding the strategic implications of next-generation unmanned combat aerial vehicles." http://onlinelibrary.wiley.com/doi/10.1111/1468-2346.12342/epdf (accessed 10 December 2015).

[3] http://www.turboace.com/matrixbuyingguide.aspx.

[4] https://www.openpilot.org/products/openpilot-Revolution-platform/.

[5] http://ardupilot.com/.

[6] https://store.3drobotics.com/t/pixhawk.

[7] http://planner.ardupilot.com/wiki/mission-planner-overview/.

[8] https://traxxas.com/.

[9] http://www.nex-robotics.com/products/fire-bird-v-robots/fire-bird-v-atmega2560-tank-drive-robotic-research-platform.html.

[10] http://jaguar.drrobot.com/specification_V4.asp.

[11] http://ros.org.

[12] Robert Work & Shawn Brimley, "20YY: *preparing for war in the robotic age"* (Washington DC: Center for a New American Security, Jan. 2014), 8-9.

[13] Alex Velez-Green, "Swarm Robotics and the Future of the Military." http://harvardpolitics.com/world/swarm-robotics-future-americas-global-military-supremacy/ (accessed 21 September 2014).

[14] http://www.raytheon.com/capabilities/products/phalanx/

[15] Michael Cooney, "Not in my airspace: Airbus rolls out anti-drone system." http://www.networkworld.com/article/3019660/security/not-in-my-airspace-airbus-rolls-out-anti-drone-system.html (accessed 6 January 2016).