International Journal of Cyber Warfare and Terrorism
Volume 10 • Issue 3 • July-September 2020

Deceiving Autonomous Drones

William Hutchinson, Edith Cowan University, Joondalup, Australia

ABSTRACT

This speculative article examines the concept of deceiving autonomous drones that are controlled by artificial intelligence (AI) and can work without operational input from humans. This article examines the potential of autonomous drones, their implications and how deception could possibly be a defence against them and /or a means of gaining advantage. It posits that officially, no truly autonomous drone is operational now, yet the development of AI and other technologies could expand the capabilities of these devices, which will inevitably confront society with a number of deep ethical, legal, and philosophical issues. The article also examines the impact of autonomous drones and their targets in terms of the power/deception nexus. The impact of surveillance and kinetic impacts on the target populations is investigated. The use of swarms can make deception more difficult although security can be breached. The Internet of Things can be considered as based on the same model as a swarm and its impact on human behaviour indicates that deception or perhaps counter-deception should be considered as a defence. Finally, the issues raised are outlined. However, this article does not provide definitive answers but, hopefully, exposes a number of issues that will stimulate further discussion and research in this general area.

KEYWORDS

Artificial intelligence, Consciousness, Counter-Deception, Deception, Drones, Internet of Things (IoT), Power, Robots, Security

1. INTRODUCTION

In the last two decades, the term ‘drone’ usually meant a flying robot, but this has been expanded to include any mobile robot. In this paper, ‘drone’ and ‘robot’ are used interchangeably. They are now found in the aerial, terrestrial, aquatic and space environments. Combined with artificial intelligence and a myriad of sensors, they have become formidable weapons and surveillance platforms (see Dougherty, 2015 for the range involved). In fact, defence against them is difficult for all but the most well-resourced entities. This phenomenon stimulated the start of this research, which concentrates on autonomous rather than just automatic robots. The US Department of Defence (US DOD, 2014, p. 15) gives a simple explanation that an autonomous robot as: “when the aircraft [drone] is under remote control, it is not autonomous. And when it is autonomous, it is not under remote control.” In other words, it is independent of humans for its operating actions.

When considering the ‘intelligence’ and ‘knowledge’ aspects of this topic, it is useful to look at the types of systems that have been developed as these types of systems. Cummings (2017) states there is a hierarchy of knowledge systems starting with skills-based behaviours, then rules-based, then

DOI: 10.4018/IJCWT.2020070101

knowledge-based and finally expertise-based. Skills-based relies on the perception-cognition-action loop and can be automated without much difficulty. As the need for complexity increases, multiple and compound processes can be accomplished by Rules-based learning. The next two levels of system require a higher level of learning where Knowledge-based reasoning is needed where the stored set of rules does not match the existing environment, so a new set of rules have to be created. Expert-based systems use judgement and intuition. Although the move from automated to autonomous systems changes at the rules-based level, it is really at the Expert level that solutions to the ambiguities in the environment can start to be trusted. Cummings (*ibid*) contends that, there are no truly reliable autonomous systems relying on Knowledge-based or Expert based systems, in operation currently. Hence, whilst there are many automated systems there are not truly, fully autonomous ones.

The other underlying rationale and emphasis of this paper is human 'security'. Security is fundamentally based on two approaches – overwhelming the opposition ('force') or deceiving them. Defensive security can involve such passive approaches as obstacles (ranging from physical obstructions to nested passwords) to more dynamic factors such as 'honeypots' in computerised networks. Offensive approaches can be physical defence or active deception. This paper examines the latter. An assumption is made that almost all security measures, both offensive and defensive, involve some deception. Such is the surveillance capability (and increasingly weaponization) of drones that the security function of their targets can often be severely compromised. Thus, to protect a targeted asset means the drone and its sensors, and command and control systems (C2) must be compromised by destruction or such means as manipulation of parts, hacking the C2 systems or physical approaches such as dazzling: see (Bennett and Waltz, 2007, pp. 17-66 for the various methods that can be used). However, on the surface, deception as a strategy would appear to be a plausible approach despite the dominance of the drone in its system's sensory range. The drone's sensors and digital systems would probably have a much faster decision processing than that of a human controller. However, if a human pilot was involved then the known deceptive techniques could be employed to fool the pilot, the drone and, ultimately, thwart its mission. These techniques would partially rely on the corruption of the data coming from the sensors and the manipulation of the cognitive abilities of the human controller if present. The latter techniques have been documented widely (examples are: Harrington, 2009; Malin et al., 2017). However, the potential advent of autonomous drone systems with no human mission control would give the advantage to the drone system with its superior sensory and processing speeds. It should be noted that although that some truly autonomous drone systems (with simple parameters of action) are in existence and deployed, few will admit their operational status. Autonomous drones are increasingly attractive. To the military and industry, they are a source of 24/7 workhorses without the expensive costs of pilots and associated problems of trauma with their human controllers observing the results of their activities. Certainly, there are humanitarian concerns, but the economic and strategic/tactical viewpoints seem to be increasingly over-riding these issues (Walsh, 2018).

The willingness for political and management systems to consider human-less controlled systems of massive destructive capability can be illustrated by a Cold War example (Smith, 2008). This plan was considered by the Soviet system and 'nearly' implemented. It consisted of a crewless ship, packed with nuclear material and a cobalt nuclear device (effectively a globally effective radiation enhanced 'dirty bomb') and was to cruise Arctic waters. Sensors on this ship would register any excessive radioactivity and when the level of radiation passed a predetermined measurement, it would be assumed by the system that the Soviet Union, its leadership and its population had been destroyed. This would cause the ship-based control system to detonate the cobalt bomb, and contaminate the whole globe with radioactivity (Smith, 2008). Even at a superficial level, holes in this system are apparent. Evidently, it was not implemented but was seriously considered. It should be pointed out that certain commentators note that this doomsday machine is still in existence, and armed and ready to go. Some say that it was a double bluff by its creators to control internal power groups who might be tempted to attack the West (Keim, 2007; Torchinsky, 2017). Like the mutually assured destruction