Technology in Society 44 (2016) 39–47

Contents lists available at ScienceDirect

Technology in Society

journal homepage: www.elsevier.com/locate/techsoc

Consideration of the use of autonomous, non-recallable unmanned vehicles and programs as a deterrent or threat by state actors and others

Jeremy Straub

Department of Computer Science, University of North Dakota, 3950 Campus Road, Stop 9015, Grand Forks, ND 58202-9015, USA

ARTICLE INFO

Article history:
Received 18 October 2014
Received in revised form
21 December 2015
Accepted 23 December 2015
Available online 2 January 2016

Keywords:
Autonomous control
Non-conventional warfare
Deterrence
State & non-state actors

ABSTRACT

This paper considers the use of a non-recallable control technology (either for craft control or to command weaponized software) as a deterrent or threat mechanism by state and non-state actors. It considers the efficacy of this approach in modern war fighting (including in limited war-like scenarios), comparing it to the mutual assured destruction phenomenon created by atomic weaponry and the Zanryū Nipponhei ('Japanese holdout') scenario. The deterrent, immediate and long-term impacts of the non-recallable control technology are considered from a warfighting perspective. The ethical and societal implications of the development of this technology and the proverbial opening of Pandora's Box that its development represents are also considered.

1. Introduction

Continuing advancements in autonomous control technology are changing the nature of warfare. In the physical world, control approaches have advanced from human-at-the-helm (where the human makes every decision and directly controls actuation), to human-in-loop (where the human makes command decisions, but actuation is left to software) to human-on-loop (where the human focuses on strategy and oversight, leaving command and actuation to the software). Command and control systems to completely operate a craft in, for example, the case of communications failure have also been defined.

In the cyber realm, computer malware and its control has advanced to a point where military action with it is routinely contemplated in threat assessment and multiple cyber-attacks have been launched. The high level of reliance on electronic systems means that a cyber-attack may be as crippling as a one by a robotic or human warfighter. While a robotic attack may be confined to a single region, a cyber-attack might simultaneously cripple systems across a nation-state or around the world.

Like the nuclear weapons of the Cold War, either type of attack may render a combatant unable to respond and retaliate; thus, to ensure deterrence, a nation-state must be able to launch an attack that doesn't depend on continued operation of its systems to complete. The mutual assured destruction concept from the Cold War, however, fails to fully capture the complexity of the modern era. The entrance of non-state actors, who may have a similar interest in deterring against their own destruction or making threats to achieve their desired ends, introduces additional complexity. These non-state forces may, similarly, seek to be able to deploy a (perhaps less than decisive) attack that will complete irrespective of the continuance of their control capabilities. A fighting force similar to the Zanryū nipponhei (Japanese holdouts), which continues to cause local or regional problems, potentially fighting a long-over war and exacting continued casualties in retaliation on behalf of a dead movement may be seen as a mechanism to ensure against attack against a non-state actor.

This paper considers the use of a prospectively-soon-available technology, discussed in the context of robotics in [1], that is able to make friend-versus-foe determinations autonomously and command the already existing control algorithms of surface and aerial robotic warfighters as well as cyberspace attacks. It continues by providing background on autonomous vehicle command and weaponized software technologies and with a discussion of the laws of war. Then a picture is painted of the prospective technology, its capabilities and the limitations that currently exist to its implementation. Following this, the benefits and drawbacks of the

E-mail address: jeremy.straub@und.edu.

http://dx.doi.org/10.1016/j.techsoc.2015.12.003
0160-791X/

development and deployment of this type of a system are discussed. The examples of mutual assured destruction and Zanryū nipponhei are considered and ethical and moral considerations are discussed before concluding.

2. Background

An understanding of the relevant technologies, and related non-technical considerations, is necessary to inform this analysis. This section, thus, provides background in several relevant areas. First, work on autonomous vehicle command technologies is presented. Next, weaponized software and its control is discussed. Then, a brief discussion of the laws of war is provided. Finally, previous work on the combination of autonomous control and the laws of war is considered.

2.1. Autonomous vehicle command technologies

Significant prior work exists in developing command and control technologies for robots operating in real-world environments. This work does not, generally, seek to create a general purpose artificial intelligence [2] (which can be applied to any circumstance, in a way mirroring human intelligence). Instead, these efforts focus on individual areas of command needs. Typically, multiple technologies are required to successfully operate a robot in a real-world environment. These include collision avoidance (see, e.g., [3.4]), pathfinding (see, e.g., [5–7]) and low-level control. These needs vary by craft type, with UAVs, for example, having to continuously exert energy (and maintain movement, for fixed-wing units) to remain in flight, while ground vehicles have greater levels of terrain [8] dependence and consideration. Both must consider factors such as obstacle and target movement [9.10] and the need for both long-term and reactive planning [11]. In addition, more generally, technologies for testing (either using hardware [12], autonomous test systems [13] or simulation [14]) and craft-to-craft and craft-to-base communications are required.

The communication requirements, constraints and techniques used have (in addition to the autonomous control technique used) a significant impact on the operations of a robotic system. They determine the extent of its resilience to failure, how the system will operate in a partially or fully communications-denied environment and under partial-cluster failure conditions. Techniques have been proposed that use a hierarchy [15] to transmit data (and thus are reliant on the availability of relevant hierarchy members) as well as dynamically reconfigurable approaches [16], which may be more resilient. Lucas and Guettier [17], among others, considered and proposed solutions for dealing with constrained communications, while Rogers et al. [18] discussed human-robot mission collaboration techniques.

While the communications approach may determine how craft interact (particularly under less-than-ideal conditions), the priorities of the autonomous command decision-making system drive how the system functions. Duan [19], for example, proposed a predator-prey biogeography method for unmanned combat aerial vehicle control. Wang et al. [20], alternately, suggested the use of the (potentially less aggressive) Firefly Algorithm for this same purpose. Approaches based on bats and mutation [21] and ant [22] and wolf colonies [23] have also been demonstrated. Decision making can also be thought of as a path-planning challenge to arrive at a desired goal, and thus a derivative of the well-known A* (optimal path finding) algorithm [24.25] has also been utilized for this purpose.

Another key consideration for autonomous robots is where data processing will occur. Onboard processing may be required for local decision making in a communications or control-station denied scenario (such as would be applicable to non-recallable craft after the loss of their controllers). However, it also requires local processing capabilities sufficient to this work. Local processing also impacts the ability to balance robot workload [26], and perform mission optimization [27]. One key area of processing need is the identification of targets and their suitably accurate characterization. This ability is critical to the development of a non-recallable system, as otherwise human controller assistance would be required for this function on a recurrent basis (eliminating the non-recallability of the craft). A variety of techniques exist that are relevant to this challenge. Techniques based on rule-based algorithms [28], genetic-algorithms and fuzzy logic [29], and point-clouds [30.31] have been proposed. Consideration must also be given to factors which may impair identification including camouflage and obstruction [32].

2.2. Weaponized software and its control

While robots exist and operate in the physical realm, attack and defense capabilities are also relevant to cyberspace. These attacks may be against robotic control systems or numerous other prospective targets. The term weaponized software (or weaponized code) has been used, largely, to refer to non-physical attacks where a virus or other malware is utilized to attack an electronic system. Herr [33] utilizes the term cyber weapon for this purpose, as well, and defines it as including "digital objects" that "depend on the use of information systems" which "can have both digital and physical effects". The term weaponized software is used in this context in this section (despite the fact that a limited number of sources have used the term in the context of autonomous control software, which was covered in the previous section).

Weaponized software can prospectively be used in a variety of contexts. Tyugu [34] proffers that the deployment of autonomous weaponized software and centralized control thereof "in a unified setting" is problematic. Concerns about this approach include a defect in the agent code resulting in unexpected results, insufficient situational awareness for decision making, an agent reaching an inaccurate understanding of a situation, an agent incorrectly interpreting its instructions, the loss of contact with an agent and the "formation of unwanted coalitions". Tyugu proffers that, for long running software, a situation similar to insubordination is possible and the use of formal methods to guarantee control across any prospective scenario is "practically impossible". It is suggested that advanced autonomous agents will consider benefits, desires and interactions and reflect on their own state. The use of "strict constraints" is proposed along with "careful testing" thereof.

However, despite the potential peril, the speed of warfare may dictate a need for autonomous control, Caton [35] contends. Scenarios under which the speed of attack and response could outpace humans' ability to make defense and counter-attack decisions necessitate autonomous countermeasures. This would require autonomous attack identification and assessment, the determination of who to respond against and what response is appropriate. Numerous considerations abound with this type of a system including what role allies (and/or their computer systems) should have in decision making, whether a counter attack runs the risk of starting an autonomous cycle of escalation, and ethical considerations. Caton also notes that this type of system would make prior notification of weapons tests and immediate notification regarding other incidents, which could be perceived as hostile, critical.

The use of autonomous agent-controlled software as part of an "active cyber defense" (defined as a set of "protective measures that are launched to defend against malicious cyber activities") is suggested by Heinl [36]. While extoling the virtues and benefits of active cyber defense, Heinl cautions that policy and legal