New Challenges in Robotics
Cyber Security and Digital Forensics

GIUSEPPE VACIAGO, FRANCESCA BOSCO*

Summary:


1. Introduction

The coming years are certain to be critical for the robotics industry, as it refines the capacity to massively produce robots. As this shift takes place, these robots will increasingly become integrated into our everyday lives. The use of Unmanned Aerial Vehicles (UAVs), also known as drones, is increasing in both the military and civilian sectors. Although we are used to the concept of military drones, commercial and civilian use of the technology is still evolving. Small drones are compact, easy to carry, and can be concealed in a bag or a backpack. In the transportation sector, the development of Google’s Driverless Car, an autonomous motor vehicle, and of Android Auto and Apple CarPlay, provide insight into the future of personal transportation, and alludes to the possibility of greatly reducing accidents and providing vital transport to individuals who could not operate a motor vehicle otherwise.

If there is no doubt about the usefulness of robotics in terms of development of innovation and economic growth for governments or companies that are progressively making an extensive use of it, less known are the possible risks that these inventions may generate to the community. The objective of this paper is certainly not to deal with the captivating and well explored theme of the conflict between humans and robots, but to highlight missing

* G. Vaciago is Adjunct Professor of Legal Informatics at the University of Insubria and a criminal lawyer specialized in ICT Law. F. Bosco is Senior Fellow at the United Nations Interregional Crime and Justice Research Institute (UNICRI). She is co-founder of the Tech and Law Center. The opinions expressed in this article do not represent the views of UNICRI.
scientific literature that specifically deals with evaluating how best to prevent a computer attack to a robot (cybersecurity) and to acquire any digital evidence that the robot contains after the incident has occurred (digital forensics).

Before getting to the heart of the article, however, it is considered appropriate to define what is meant by robot and what are its main features: a robot could be defined as “an artificial agent or other machine that implements some functions requiring autonomous decision making. Such a machine consists of the machine hardware, software, and an additional level of abstraction, the machine cognition”

Starting from these definitions, which are the main aspects of robotics that we need to take into consideration? Robots have three essential characteristics: interactivity, autonomy and adaptability

The robot’s conduct, although attributable at the program set by the programmer or the manufacturer, could not entirely been planned in its specific details because of the increase of experience made by the robot on its own. What happens if damage is not derived from a defect of the robot, but from its behaviour?

With this in mind, digital forensics is a key aspect which should be taken into consideration when ascertaining liability in the event of an accident due to a malfunctioning robot. Digital forensics reconstructs the manner in which the object was designed and the manner in which it operated when the event occurred. Similarly, regardless of the extent to which robot and drone safety requirements provided for by European Community legislation (known as the “Machinery Directive”) are met, it would be advisable not to underestimate the safety of the operating system or applications controlling the robot or the drone, as a potential IT attack against the software could have devastating effects on the manner in which it operates.

---