

Robotics as good machineries outside the factory in changing lives over the coming decades.

Muhamad Momodou

Faculty of Information and communications Technology, University of Gambia.

ABSTRACT

Robotics deals with the design, construction, operation, and use of robots, as well as computer systems for their control, sensory feedback, and information processing. These technologies are used to develop machines that can substitute for humans and replicate human actions. Most of the robots that have been tested to determine the nature of their security protocols did not require sufficient authorization to protect their functionality, including critical functions such as installation of applications in the robots themselves or updating of their operating system software. This article investigates the social significance of robotics for the years to come by studying robotics developments in five different areas: the home, health care, traffic, the police force, and the army. Our society accepts the use of robots to perform dull, dangerous, and dirty industrial jobs. In the coming decade a combined breakthrough of home automation and tele-care is expected, which will place the caretaker and patient in a technological loop.

Keywords: Robotics, technology and cybersecurity.

INTRODUCTION

Until recently, robots were mainly used in factories for automating production processes [1]. In the 1970s, the appearance of factory robots led to much debate on their influence on employment. Mass unemployment was feared. Although this did not come to pass, robots have radically changed the way work is done in countless factories. Robots can store sensitive information, including encryption keys, user social media, e-mail accounts and vendor service credentials, and send that information to and from mobile applications, Internet services, and computer software. As a result, encryption is mandatory to avoid data compromises, yet most robot manufacturers use the same passwords for most or all of their products, leaving consumers vulnerable to hacking if they fail to change them. Robots also receive remote software updates, so proper encryption is necessary to ensure that these updates are trusted and have not been modified to include malicious software [2]. A 2017 study found nearly 50 cybersecurity vulnerabilities in robot

ecosystem components, many of which were common in home, business, and industrial robots, as well as the control software used by other robots tested. Although the number of robots tested was not a large sample, the fact that dozens of vulnerabilities were uncovered, in such a broad spectrum of robots, is concerning. Most of the robots evaluated were using insecure forms of communications, with mobile and software applications connected to the Internet, Bluetooth, and Wi-Fi without properly securing the communication channel [3]. Although some had weak encryption, most of the others sent data to vendor services or the cloud without any protection. Most of the robots that have been tested to determine the nature of their security protocols did not require sufficient authorization to protect their functionality, including critical functions such as installation of applications in the robots themselves or updating of their operating system software [4]. This enables cyberattackers to install software without permission and gain full control over them. Most of

the robots tested were also either not using encryption at all or improperly using it, exposing sensitive data to potential attackers. Furthermore, many robot manufacturers have generally failed to ensure that either users are instructed to change passwords, or updates are routinely provided when changes in the product security protocols are made. Certain robot features are common, intended to improve accessibility, usability, interconnection, and reusability (such as real-time remote control with mobile applications) [5]. Unfortunately, many of these features make robots more vulnerable from a cybersecurity perspective, with both critical- and high-risk cybersecurity issues present in many of the features. A hacked robot has many of the same vulnerabilities as computers, and can suffer the same consequences. A hacked robot operating inside a home might spy on a family via the robot's microphones and cameras. An attacker could also use a robot's mobility to cause physical damage in or to the house [6]. Compromised robots could even hurt family members and pets with sudden, unexpected movements, since hacked robots can bypass safety protections that limit their movements. Hacked robots could also start fires in a kitchen by tampering with electricity or potentially poison family members and pets by mixing toxic substances with food or drinks, or by utilizing sharp objects to cause harm. While there are of course nefarious potential connotations to a robotic future, such capability also opens up fantastic possibilities in areas as broad as search and rescue operations, disaster relief, ambulatory services, and oil spill containment [7]. They may, of course, also be used for more nefarious purposes. In 2014 some researchers at Harvard University created the largest robot swarm at that time using 1,024 tiny robots the size of a penny that could find one another and collaborate to assemble themselves into various shaped and designs, like a mechanical flash mob. Some defense contractors have already developed drones that can fly into enemy territory, collect intelligence, drop bombs,

and defend themselves against attack [8]. In the Korean demilitarized zone, South Korea has deployed border control sniper robots that detect intruders with heat and motion sensors, and can automatically fire on targets up to one kilometer away with machine guns and grenade launchers.

Proposed Domestic uses of Robot

New robotics no longer concerns only factory applications, but also the use of robotics in a more complex and unstructured outside world, that is, the automation of numerous human activities, such as caring for the sick, driving a car, making love, and killing people [9]. New robotics, therefore, literally concerns automation from love to war. The military sector and the car industry are particularly strong drivers behind the development of this new information technology. In fact they have always been so. The car industry took the lead with the introduction of the industrial robot as well as with the robotisation of cars. The military, especially in the United States, stood at the forefront of artificial intelligence development, and now artificial intelligence is driven by computers and the Internet. More precisely, robotics makes use of the existing ICT infrastructure and also implies a continued technological evolution of these networks. Through robotics, the Internet has gained, as it were, 'senses and hands and feet' [10]. The new robot is thus not usually a self-sufficient system. In order to understand the possibilities and impossibilities of the new robotics, it is therefore important to realise that robots are usually supported by a network of information technologies, such as the Internet, and thus are often presented as networked robots. New robotics is driven by two long-term engineering ambitions. Firstly, there is the engineering dream of building machines that can move and act autonomously in complex and unstructured environments. Secondly, there is the dream of building machines that are capable of social behaviour and have the capacity for moral decision

making [11]. The notion that this may be technologically possible within a few decades is referred to as the 'strong AI' view (AI: artificial intelligence). It is highly doubtful that this will indeed happen. At the same time, the 'strong AI' view prevails in the media and is highly influential in the formulation and public financing of IT research. It is beyond dispute that this technology will strongly influence the various practices researched. This also puts many societally and politically sensitive issues on the political and public agenda. For example, according to Peter Singer, the robotisation of the army is 'the biggest revolution within the armed forces since the atom bomb' [12]. The robotisation of cars, too, appears to have begun causing large technological and cultural changes in the field of mobility. Netherlands Organisation for Applied Scientific Research (TNO) describes the introduction of car robots as a "gradual revolutionary development" [13]. Through robots, the police may enjoy an expansion of the current range of applications for surveillance technologies. Home automation and robotics make tele-care possible and will radically change health care practice over the coming years. Finally, we point to the fact that over the past years, 'simple' robotics technologies have given the entertainment industry a new face: think of Wii or Kinect. New robotics offers numerous possibilities for making human life more pleasant, but it also raises countless difficult societal and ethical issues. The debate on the application of robotics to distant battlegrounds is very current, while the application of care robots is just appearing on the horizon. Prompted by the arrival of new robotics, the Rathenau Instituut in 2011 and 2012 investigated the social meaning of robotics for the years to come in Europe and the US by studying robotics developments in five application domains: the home, health care, traffic, the police, and the army [14].

Household Robots

In relation to household robots, we see a huge gap between the high expectations concerning multifunctional, general-

purpose robots that can completely take over housework and the actual performance of the currently available robots, and robots that we expect in the coming years. In 1964, Medith Wooldridge Thring [15] predicted that by around 1984 a robot would be developed that would take over most household tasks and that the vast majority of housewives would want to be entirely relieved of the daily work in the household, such as cleaning the bathroom, scrubbing floors, cleaning the oven, doing laundry, washing dishes, dusting and sweeping, and making beds. Thring theorised that an investment of US\$5 million would be sufficient for developing such a household robot within ten years. Despite a multitude of investments, the multifunctional home robot is still not within reach. During the last ten years, the first robots have made their entry into the household, but they are all 'one trick ponies' or monomaniacal: specialised machines that can only perform one task. According to Bill Gates [16]: '[w]e may be on the verge of a new era, when the PC will get up from the desktop and allow us to see, hear, touch and manipulate objects in places where we are not physically present.' It is unlikely that households will start using in droves the monomaniacal simple cleaning robots such as vacuum cleaner robots, robot lawn mowers, and robots that clean windows with a chamois leather. These robots can only perform parts of the household tasks, and they also force the user to adapt and streamline part of their environment. The study by Sung et al. [17] showed that almost all users of a robotic vacuum cleaner made changes to the organisation of their home and their home furniture. The more tidy and less furnished the household is, the easier it is to make use of that robot vacuum cleaner. This process of rationalising the environment so that the robot vacuum cleaner can do its job better is known as 'roombarization' [18], referring to the vacuum cleaner robot Roomba. Typical modifications are moving or hiding cables and cords, removing deep-pile carpet, removing lightweight objects from the

floor, and moving furniture. An inhibiting factor for the rise of the commercial vacuum cleaner robot probably lies in this need for a structured environment. The history of technology research shows that the interest in new devices quickly decreases when existing practices require too many changes [19]. The expectation that the new generation of robots will operate in more unstructured environments will not work in the household. This is not only a matter of time and technological innovation and development, but it is also an issue that comes up against fundamental limitations. Housework turns out to be less simple than expected [20]. Closer inspection shows that many situations in which a household task must be performed do require a lot of common-sense decisions, for which no fixed algorithms exist. The degree of difficulty is shown by research from the University of California at Berkeley, which aims to develop a robot that is able to fold laundry. Eventually, a robot was developed that took 25 minutes to fold one towel [21].

Amusement Robots

It seems that entertainment robots do meet expectations and social needs. Compared to the household robot, expectations concerning the entertainment robot are much less pre-defined. The goals are just communicating, playing, and relaxing [22]. The need is not set, but arises in the interaction. We see an age-old dream come true: devices that resemble humans or animals, and can interact with us. Examples are the dog AIBO (a robot companion shaped like a dog), the fluffy cuddly toy Furby, the funny My Keepon (a little yellow dancing robot that can dance to the rhythm of music) and the sex robot: all four invite us to play out social and physical interaction. People become attached to the robot and attribute human features to it. This is called 'anthropomorphism', i.e. attributing human traits and behaviours to non-human subjects. People even assign robots a psychological and a moral status, which we previously only attributed to

living humans [23]. Research shows that young children are much more attached to toy robots than to dolls or teddy bears, and even consider them as friends [24]. Nevertheless, we certainly cannot speak of a success story. The social interaction robots that are currently available are very limited in their social interaction and are very predictable, so many consumers will not remain fascinated for long eventually. This motivates researchers to proceed in order to reach a more efficient and effective interaction [12, 29, 45]. There is a lack of knowledge about the mechanisms that encourage communication between humans and robots, how behaviour occurs between humans and robots, and even how the interaction between people actually works. Such knowledge is critical to the design of the social robot, because its success depends on successful interaction [13]. This research discipline of human-robot interaction is still in its infancy. At this time—and probably within the next ten years—we should therefore consider commercially available social interaction robots like Furby and My Keepon as fads and gadgets whose lustre soon fades rather than as kinds of family friends. How the sex robot will develop is still unknown, but the sex industry and some robot technologists see a great future for this robot and consider the sex robot to be a driving force behind the development of social robots and human-robot interaction research (see, for example, [16]). In order to let robots interact with humans in a successful manner, many obstacles must be overcome, especially to develop a social robot which has many of the social intelligence properties as defined by [10]: it can express and observe feelings, is able to communicate via a high-level dialogue, has the ability to learn social skills, the ability to maintain social relationships, the ability to provide natural cues such as looks and gestures, and has (or simulates) a certain personality and character. It will take decades before a social robot has matured enough to incorporate these properties, but modern technology will make it

increasingly possible to interact with robots in a refined manner. This will turn out to be a very gradual process [12].

Expected Social Gains

Robotisation presents a way of rationalising social practices and reducing their dependence on people [18]. Rationalisation can have many benefits: higher efficiency, less mistakes, cheaper products, and a higher quality of services, et cetera. Rational systems aim for greater control over the uncertainties of life, in particular over people, who constitute a major source of uncertainty in social life. A way of limiting the dependence on people is to use machines to help them or even to replace them with machines. As

CONCLUSION

Both in Europe and the United States, the goal of developing robotics for the domestic environment, care, traffic, police, and the army is embraced by policymakers and industry as a new research and societal goal. There is an aim for technology to enable an increasing amount of autonomous moral and social actions. Thus, a radical development path unfolds, namely, the modelling, digitisation, and automation of human behaviour, decisions, and actions. This development is at least partially legitimated by speculative socio-technical imaginaries, such as multifunctional, autonomous, and socially and morally intelligent robots. In the short and

[16] (p. 105) argues: "With the coming of robots we have reached the ultimate stage in the replacement of humans with nonhuman technology." The development and use of robotic systems is often legitimated by the fact that they will take over "dirty, dull, and dangerous" work. Some claim that the 'principle of unnecessary risk' leads to an ethical obligation to apply robotics in certain situations. [18] believes it is morally unacceptable to give a soldier an order that may lead him to suffer lethal injuries if a military robot could perform this same task. This principle of unnecessary risk is also applicable to driving cars and sex robots.

medium term, developments in the field of new robotics are mainly characterised by terms such as 'man in-the-loop' and 'man on-the-loop', which indicate that robotic systems are increasingly advising human operators on which action must be taken. Firstly, this signifies the digitisation of various previously low-technology fields, such as the sex industry and elderly care. For example, in the coming decade a combined breakthrough of home automation and tele-care is expected, which will place the caretaker and patient in a technological loop. The experimentation with care robots must be seen from this perspective.

REFERENCES

1. Akrich M (1992) The description of technical objects. In: Bijker W, Law J (eds) *Shaping technology/building society: studies in sociotechnical change*. MIT Press, Cambridge, pp 205-224
2. Aldrich FK (2003) Smarthomes: past, present and future. In: Harper R (ed) *Inside the smart home*. Springer, London, pp 17-39
3. Alley R (2013) The drone debate. Sudden bullet or slow boomerang (discussion paper nr. 14/13). Centre for Strategic Studies, Wellington
4. Arkin RC (2009) *Governing lethal behavior in autonomous robots*. Taylor and Francis, Boca Raton
5. Arkin RC (2010) The case of ethical autonomy in unmanned systems. *J Mil Ethics* 9(4):332-341
6. Arth M (2010) Democracy and the common wealth: breaking the stranglehold of the special interests. Golden Apples Media, DeLand
7. Asaro PM (2008) How just could a robot war be? In: Briggie A, Waelbers K, Brey Ph (eds) *Current issues in computing and philosophy*. IOS Press, Amsterdam, pp 50-64
8. Bacevich AJ, Cohen EA (2001) *War over Kosovo: politics and strategy in a global age*. Columbia University Press, Columbia

9. Birk A, Kenn H (2002) RoboGuard, a teleoperated mobile security robot. *Control Eng Pract* 10(11):1259-1264
10. Borenstein J, Pearson Y (2010) Robot caregivers: harbingers of expanded freedom for all? *Ethics Inf Technol* 12(3):277- 288
11. Breazeal C (2003) Toward sociable robots. *Robot Auton Syst* 42(3-4):167-175
12. Breazeal C, Takanski A, Kobayashi T (2008) Social robots that interact with people. In: Siciliano B, Khatib O (eds) *Springer handbook of robotics*. Springer, Berlin, pp 1349-1369
13. Broggi A, Zelinsky A, Parent M, Thorpe CE (2008) Intelligent vehicles. In: Siciliano B, Khatib O (eds) *Springer handbook of robotics*. Springer, Berlin, pp 1175-1198
14. Butter M, Rensma A, Van Boxxel J et al (2008) *Robotics for healthcare (final report)*. DG Information Society, European Commission, Brussels
15. Checkoway S, McCoy D, Kantor B et al. (2011) Comprehensive experimental analyses of automotive attack surfaces. In: Wagner D (ed) *Proceedings of the 20th USENIX on security (SEC'11)*. USENIX Association, Berkeley. <http://www.autosec.org/publications.html>
16. Coeckelbergh M (2010) Health care, capabilities, and AI assistive technologies. *Ethics Theory Moral Pract* 13(2):181-190
17. Cummings ML (2006) Automation and accountability in decision support system interface design. *J Technol Stud* 32(1):23-31
18. Cummings ML (2010) Unmanned robotics and new warfare: a pilot/professor's perspective. *Harv Natl Secur J*. <http://harvardnsj.org/2010/03/unmanned-robotics-new-warfare-a-pilotprofessors-perspective/>
19. Decker M (2008) Caregiving robots and ethical reflection: the perspective of interdisciplinary technology assessment. *AI Soc* 22(3):315-330.
20. Detert J, Treviño L, Sweitzer V (2008) Moral disengagement in ethical decision making: a study of antecedents and outcomes. *J Appl Psychol* 93(2):374-391
21. Dragutinovic N, Brookhuis KA, Hagenzieker MP, Marchau VAWJ (2005) Behavioural effects of advanced cruise control use. A meta-analytic approach. *Eur J Transp Infrastruct Res* 5(4):267-280.
22. Evans D (2010) Wanting the impossible. The Dilemma at the heart of intimate human-robot relationships. In: Wilks Y (ed) *Close engagements with artificial companions. Key social, psychological, ethical and design issues*. John Benjamins Publishing Company, Amsterdam, pp 75-88.
23. Fong T, Nourbakhsh I, Dautenhahn K (2003) A survey of socially interactive robots. *Robot Auton Syst* 42(3-4):143-166.
24. Gates B (2007) A robot in every home. The leader of the PC revolution predicts that the next hot field will be robotics. *Sci Am* 296:58-65.