What if I had to put my safety in the hands of a robot?

Will intelligent robots bring us benefits in relation to security and safety, or will the vulnerabilities within these systems mean that they cause more problems than they solve?

Cyber-physical systems (CPS) are currently found in a wide range of services and applications, and their numbers are rapidly increasing. CPS are intelligent robotic systems linked to the Internet of Things. They make decisions based on the ability to sense their environment. Their actions have a physical impact on either the environment or themselves. This is what sets CPS apart: they are not solely smart systems, but rather, they have physical aspects to them. These robots are likely to infiltrate our everyday lives in the coming years. Due to this, we must look at what impact they will have on citizens' safety and security. The question remains, how safe are these technologies?

© Shutterstock / Willyam

Potential impacts and developments

Such systems often work as part of a network in which information is exchanged, normally using wireless connectivity, which can be vulnerable to hackers and criminals. These networks may be seen as the coupling of information technology (IT) and operational technology (OT) systems, known as IT-OT integration. Issues arise due to the diminished level of security of the OT compared to that of the IT system. Should someone infiltrate these systems they could potentially access the data gathered by the CPS and corrupt the system itself. Although this is a sobering thought, we are seeing the development of technologies which promise to better protect these systems and hence individuals' information, such as through the creation of quantum cryptography, which will (at least in theory) be impossible for a hacker to defeat.

Robots can have positive impacts on our safety. For example, they can aid disaster relief workers. Automated vehicles with the ability to make autonomous decisions can access dangerous sites to help save victims, and keep workers themselves safe and out of harm's way. Driverless cars are another example of autonomous robots that are becoming more commonplace and are expected to be safer for citizens. This is based on the fact that the systems will not tire or suffer from road rage, and that they are better at calculating manoeuvres. The taxi company Uber is in fact already planning on replacing 160 000 drivers with driverless cabs. However, the recent Tesla case, where a driver was killed as the car in autopilot mode did not recognise another car against a bright sky, shows that more work needs to be done to increase their safety. Robots can have medical applications too. CPS can effectively monitor the body and provide the correct medication when needed, ensuring the safety of the patient. However, possible safety concerns can arise should the system malfunction or, as is the case with other technologies, they could be hacked to deliver a fatally high dose to patients.

Another type of robot increasingly being used are drones. They have been used by governments for security, for example in civil surveillance tasks such as border patrols to minimise numbers of illegal immigrants entering countries. Concerning refugees, the ability to closely monitor flowz of people will mean that better relief and aid can be provided, assisting in their safety. Citizens are also increasingly using drones as they are becoming cheaper to purchase and their range is increasing. These drones, in the hands of civilians, while often used for leisure, can also be used for nefarious and criminal purposes, such as the delivery of munitions.

EPRS | European Parliamentary Research Service
Author: Lieve Van Woensel with Sarah McCormack
Scientific Foresight Unit (STOA)
November 2016 - PE 581.923

They can also be fitted with guns or used to fly explosives or dangerous materials into areas, as was seen when a drone carrying radioactive sand was flown onto the roof of the Japanese prime minister's office. Drones are also a threat to conventional aircraft. Thus, we may need to look at counter-drone technologies, as have been seen in Tokyo, where the police catch rogue drones in nets.

Another possible safety concern is the misinterpretation of the signs from CPS by humans, leading to negative consequences. Most fatal accidents in factories with CPS happen when the robot is undergoing maintenance and moves in a way that the human worker did not expect. The ability to predict the systems' movement and behaviour is vital to ensure control over them and the safety of humans who come into contact with them.

A large amount of data on individuals will be stored on databases through the increased use of CPS. The information gathered will range from that regarding individuals' identity to that regarding their purchases, habits and journeys. However, it is not yet known whether this information will end up being linked together and analysed by either unofficial or official bodies. Regardless of the motivation behind the monitoring we may see that it results in altering individuals' behaviour. With the continuous monitoring of individuals by CPS controlled by both government and non-state bodies, could this lead to an Orwellian scenario, where people change their behaviour out of fear of being watched? This idea poses a threat to CPS, as it can turn public opinion against them.

The ability to control CPS needs to be studied. Robot ethics is difficult to harmonise, as judgments of what is and what is not ethical involve knowledge of the context in question. The robots' way of deciding which action is ethically correct in given circumstances will be similar to how a human would make this decision. The ability to make this decision will depend on how it is programmed, and we must therefore ask ourselves who should be responsible for programming these ethical guidelines.

Anticipatory law-making

In a world increasingly being shared with robots we will face legal questions regarding data ownership, privacy, safety and liability. Changes in and perhaps even the introduction of legislation to accommodate for the risks that robots pose will be required to ensure that citizens remain safe and secure.

CPS can improve the management of power and materials leading to a more secure environment. Systems' abilities to shut down when not in use will help to reduce energy waste. Governments will in most cases need to introduce legislation to ensure that this is implemented.

The main legal question, which will arise alongside the development of autonomous robots, will be that of liability. Should an accident occur with a driverless car, who will be held responsible? Will it be the driver, the car or the manufacturer? Currently, some car manufacturers are taking responsibility for accidents that occur with their driverless cars. In Germany, Sweden and the UK, legislation has already been reviewed to allow for the testing of driverless cars on public highways. As it is expected that driverless cars will become commonplace in the future, countries will need to put in place appropriate legislation to protect their citizens.

With the large amount of information collected by CPS, improved and broader data protection laws should be sought. We will also need to examine who owns the data and within what framework it can be shared. Who amongst the individual, the organisation collecting the data and political institutions should be responsible for ensuring that the data is kept safe must also be agreed. We will need to examine existing and emerging data practices, and assess the risk of increased surveillance. The concept of privacy may need to be re-worked, and the concept of vulnerability in the context of CPS will need to be specified in this context.

Robots can increase our safety as seen through driverless cars, drones used for monitoring, embedded medical devices and robots used for disaster relief. Yet safety and liability concerns remain. Overall, the world should not become more unsafe due to the increased use of robots, but adequate legislation will be needed to ensure that the possible negative effects do not outweigh the positive ones.

A study on the 'Ethics of Cyber Physical Systems' has recently been published by the Science and Technology Options Assessment (STOA) Panel. A chapter of that study, written by Professor M. Henshaw (Loughborough University, UK) and J. van Barneveld, MSc (Technopolis Group, The Netherlands), has provided inspiration for this publication.