The problem of robotic activity in qualifying criminal acts

Puchkov D.V.
Ural State Law University
Yekaterinburg, Russia
d.puchkov@loys.law

Abstract — The article describes the main directions of the emergence of the problem of robotic activity and its resolution in qualification of criminal acts. This problem is largely accounted for by the fact that robots that are able to fully adapt to the conditions of work and production have the ability to automatically collect and process information. Management is carried out by an industrial computer with a heuristic program, where the operator sets only the final goal, while the actions and their order are determined by the program. The author of the article studies potentially criminal robotic activity with a wide range of its application: from trading operations to the use of military robots by terrorist organizations.

Keywords — crime, criminal law, cybertechnologies, cybercrime, robots, military robots, criminal groups, financial operations.

A robotic revolution is seen to be another major revolution both in military or civilian spheres, and its significance can be compared with the invention of powder or nuclear weapons. However, there is one important aspect that makes it different from the earlier revolutions: the use of robotic devices will inevitably impoverish not only the quality of technological systems, but it will also change the identity of those who use them. With time, the difference between robotic vehicles and people will gradually disappear, because such systems will make autonomous decisions themselves on their own use.

Today, a decision to apply technological power is to be made by a man and as a result it is rather subjective (a man has to bear responsibility for certain losses). It is true for both an armed conflict and any industrial process. The delegation of such a process to machines will dehumanize the industrial process and will exclude the moment of deliberation in such cases when it seems practically possible. Machines are deprived of morality and mortality and therefore should not possess the power over people in solving the matters of life and death [5, p.14].

In this case, most legal, moral and other codes are based on the fact that when life, health, and other important consequences for people are a priority, decisions must be made by people. For example, as for military robots, we refer to the Hague Convention (IV), under which any combatant shall be under “a command responsible …for the conduct of its subordinates”. The MartensClause, which for a long time is considered a binding rule of international humanitarian law, provides for a necessity to apply “the principle of humanity” in an armed conflict. Should a man be exempt from the process of making decisions, there is a risk that such a process will lose its “humanity”. Therefore, though robotic systems (RS) are able to a certain extent to assess the situation more quickly and more accurately, their abilities are rather restricted since they fail to interpret the context and make predictions relying on the system of values.

At present, more technologically advanced are third generation robots: integral or intelligent robots, which are able to fully adapt to the conditions of work and which possess the ability to automatically collect and process information. Management is carried out by an industrial computer with a heuristic program, where the operator sets only the final goal, while the actions and their order are determined by the program.

Apart from the sensory system, intelligent robots (with artificial intelligence) have a system of processing external information, thus having an ability to behave intelligently, similar to the behavior of a man. Therefore, if some information on vulnerabilities in critically important infrastructures or their systems of management is available or is likely to be at the disposal of terrorist organizations, extremist groups or criminal syndicates, the consequences can be unpredictable. Moreover, it is worth saying that nowadays national security units do not possess the means to prevent such consequences and to promptly identify the perpetrator.

The Trend Micro report (May, 2017) shows that there are more than 83 thousand industrial robots available on the Internet and 5 thousand of them do not possess such a function as the authentication of their users [7]. The researchers found 65 vulnerabilities in robots, including the ones which enable to avoid the mechanism of authentication, modify the key settings and change the mode of the device operation. The above said concerns only robots available via the Internet. However, the report underlines that perpetrators can also get access to devices not connected to the Internet by hacking industrial routers used at high-tech enterprises.

Robots are very often depicted as mechanisms which functioning is based on a simple paradigm “sensing – thinking – acting”; they have sensors which to a certain extent enable to assess the situation; processors, or artificial intelligence, “making a decision” on how to respond to the impulse received; and effectors which execute such “decisions”. The degree of autonomy, which robot processors have, should be considered as the continuum between a significant involvement of a man, on the one hand, like in case with unmanned devices when a man is involved in the management process, and complete autonomy, on the other hand, like in case with robotic systems when people are “outside the circuit
of management’. In accordance with the offered plan, operators will remain at least an element of the so-called ‘expanded circuit of management’: they will program the end goals in robotic systems and make a decision on their activation or, if necessary, on their de-activation, while autonomous systems will modify such goals into tasks and will accomplish them without the involvement of the operator.

The development of cybertechnologies happens in a non-linear manner; therefore it is difficult to predict how robotics will further develop. In this connection, we can soon witness fully autonomous robots ready for application. But the use of robotic systems raises some difficult questions, the list of which is not limited to:

- Robotic systems can become an object of appropriation as well as an object of a hacker’s attack and spoofing [14]. States have no longer monopoly over the use of force. RS can be intercepted by non-state subjects such as criminal cartels or private persons and applied against the state or other non-state subjects, including civilian population [12, pp. 261-263];
- There might be malfunctions in their work. Autonomous systems can be “fragile” [8, p. 8]. Unpredictable mistakes can lead to disastrous consequences;
- It is difficult to foresee future developments in the IT sphere. A permission to use RS can open a Pandora’s Box;
- Matters of regulating the use of RS can even further exacerbate the existing uncertainty in this sphere;
- A possibility of involving a robot can significantly increase the concern, at least, among the civilian population.

As for the use of robots by criminal organizations, there are certain prerequisites that it is highly likely to happen very soon. It can be confirmed by the fact that, technically speaking, any military robot is a complex combination of a “civilian” robot with some elements of military or double use functions with the necessary systems of management and control. Asarule, their elements are produced separately and can be sold either legally or illegally. In this connection, terrorist, criminal or extremist organizations face practically no hurdles to get access to the whole set of elements of military robots as well as to the experts in creating and operating such complexes.

We can assume that robots created in such a manner will be less efficient at the initial stage than legal robotic systems; however, later we will see their equal potential, since terrorist and other criminal groups will never cease their efforts to compete with state national security units.

As for the production of chemical and biological weapons with the use of robotics, at present there are no possibilities to promptly detect and identify such processes which are separately allocated in laboratories and in rather “peaceful” organizations such as universities, research centers, etc. In contemporary conditions, it is one of the most urgent threats of the use of robotics by criminal elements. Possessing such weapons, criminal groups can successfully blackmail state bodies to demand a considerable ransom. Directly related to the risk of producing chemical and biological weapons is a possibility to create military robots able to deliver chemical warfare agents.

As known, any automated systems and robots consist of hardware and software, each of them having their own trends and changes. Unfortunately, almost all of them lead to expanded possibilities of their use by terrorists, criminals and extremists.

One of the most difficult issues that many legal, moral and religious codes seek to solve is the attitude to killing a man by another man. The perspective of such a future where completely autonomous robots will be able to solve life-and-death matters raises a set of additional concerns. It can lead to a split among the countries and significantly undermine the rule of law and the system of international security [11, p. 5]. For example, the “Threats and Risks of Using Autonomous Automated Systems and Robots by Criminals, Extremists and Terrorists” report - prepared in 2015 by a group of U.S. researchers on the basis of MTI by the order of the U.S. federal bodies – determines possibilities, risk degrees and various threats of the use of robotics by criminals, terrorists and extremists [3].

Therefore, though robots are quite effective in assessing quantity, their abilities to assess quality, especially when it comes to the protection of human lives, are quite limited. Mechanical calculations are often complicated by some controversial aspects which are so typical for decision-making in military activities. Another uneasy question is the ability of robots to differentiate between legal and illegal orders.

In this situation, individual responsibility and responsibility of a state are of primary importance for securing liability for criminal acts, human rights abuses and international humanitarian law. If there is no liability, prevention and deterrence of such activities will be significantly reduced, thus, decreasing the protection of the civilian population and increasing risks of committing war crimes [1, pp. 42-45]. Robots are not able to make moral decisions and, as a result, even if they deprive somebody of their lives, which naturally leads to criminal liability for people, robots cannot be held liable any way.

However, a question arises concerning the object of liability. A complex character of RS and multi-level decision-making potentially leads to a gap or a vacuum in the issues of liability. Among potential candidates to bear legal liability might be software developers, inventors or sellers of hardware components, combat leaders, their subordinates applying such systems and political leaders.

Traditionally, criminal liability is, first of all, to be borne by leaders: their liability will be one of possible decisions made in connection with RS application [4]. Sincetheleadercan be held liable for independent actions of their subordinate, there might be a parallel in case of liability for the actions of a robot. However, criminal liability is to be imposed only when the leader knew or should have known that their subordinate was planning to commit a crime and did not take any measures to prevent such a crime or if a crime was committed, the leader did not take any measures to punish
the guilty [2]. Therefore, before making leaders criminally liable, it is important to establish whether leaders will understand, in particular, a very complicated character of RS programming.

At the same time, we should mention that liability for the harm inflicted to the civilians shall be borne, at least, by software developers and equipment producers, following the model of imposing strict liability in products liability cases. However, the efficiency of national provisions on the quality of goods has not been checked in respect to robotics [10, p. 8]. The production of RS involves many people, and no person alone will be able to understand a complex combination of constituent parts of RS [13, p. 194]. It is rather doubtful that it would be just to empower victims to file a lawsuit, since they will have to do it in a foreign jurisdiction and will often have no remedies available.

At present, the international community has not yet elaborated a uniform terminological approach to this sphere, especially when it comes to the application of “robots” and “autonomous automated systems”. In particular, the UN instruments contain such notions as “autonomous automated systems” (AAS) and “lethal autonomous weapon system” (LAWS). At the same time, you can hardly see such notions as “robots”, “robot-killers”, “robotic weapons”, etc. in public life, mass media, and official documents of the EU and NATO.

Though similar, robots and automated systems are different in applying different software and hardware devices. Most specialists tend to agree that unlike “a robot” which a highly automated system, AAS is a much wider notion including certain software and hardware combination, with different levels of automation.

At the same time, the theory of automated management of as early as 1960s elaborated an efficient and understandable criterion which makes it possible to distinguish a robot in the structure of automated systems. Such a criterion is a method of making a decision from a set of alternatives. The aim of using a certain set of software and hardware is their ability to perform at least two operations: spatial movement and implementation of its function.

Therefore, it would be strange if criminals did not take advantage of such a rapidly developing segment of military and civilian robotics and, in particular, robotic vehicles, let alone the military use of unmanned transport for expedition, evacuation and logistic needs. By the estimates of experts and business analysts, it is expected that till 2020 the automobile industry will have no less than 25 cars produced in developed countries equipped with the “automated driving” option. It is well-known that any high technology has triple designation: military, civilian and criminal; consequently, there are grounds to believe that it is criminals and criminal syndicates that will actively apply robotic transport.

As for terrorists, there is no need to comment. Terrorist groups, including networks and swarms, even at present possess different technological resources which surpass the potential of many state armies. Terrorists make an efficient and active use of all types of weapons and equipment applied in contemporary armies.

As for criminal transnational organizations, the use of robotic transport enables them to solve two most important tasks. On the one hand, it diversifies channels of delivery of this or that type of goods, but, on the other hand, minimizes the human factor in this process. The latter is extremely important. For example, by the data of American law enforcement agencies, not less than 70% of successful crime investigations and failed delivery of drugs in the U.S. is connected with successful covert intelligence work or work of undercover agents. In other words, the more robots and fewer people are involved in criminal activities, the more difficult it becomes for law enforcement agencies to plant a mole or recruit agents among criminals.

Besides, for the last five years, completely robotic systems – trading robots – have become customary in most financial markets of America, Great Britain and Japan. Trading robots are intelligent software and hardware sets which are equipped not only with modules for collecting, processing and analyzing information, but also for independent – without a man - decision-making according to algorithms. The last remark deserves attention. Not only among politicians, military and businessmen, but even among IT experts, there is a misconception that trading robots are a forerunner of artificial intelligence and are very close to it.

On the surface, the situation seems as such that all decisions on share purchases, indexes, currencies, derivatives, etc. are made by trading robots. But if you look deeper, in fact, such decisions are made not by their own rules but following an algorithm set by people – developers, programmers, mathematicians, analysts, etc. Therefore, it is early to speak about artificial intelligence, though decisions in financial markets are made by robots without direct involvement of a man.

If in 2010, not more than one third of operations in American financial markets were conducted by trading robots, at present more than 70% of transactions in stock and over-the-counter financial markets are made not by people, but by trading robots. The expansion of trading robots, which can cost U.S. $10,000 and even more, is justified by two factors. On the one hand, trade in financial markets requires regular processing of big chunks of information. In short-term trading, robots make most part of transactions, because people just fail to process and analyze such diverse and multi-format information. So, robots perform this job more efficiently making decisions based on certain rules.

In this connection, trading robots are successors and more universal variants of computers which used to win in chess championships. In both cases, the programs are based on certain algorithm rules built on the principle of hierarchy in decision-making. On the other hand, a source of profit in financial markets is super-short-term arbitration. If someone is able to respond to some market news quicker than the others, they will make more profit out of such knowledge. If since the Rothschild times till the mid-XX there was a race for speedy reception of information, since the middle of the last century we see a race for a speedy response to information received.
So far, we know only few financial crimes committed with the help of trading robots. However, taking into account clusterization of destruction, there are grounds to beware that the risk of large-scale and, probably, global acts of financial terrorism is likely to increase. Simulation models elaborated by the Massachusetts Technological Institute and the Financial Laboratory in Zurich, Switzerland, evidence that deliberate interception of control over trading robots can make financial markets collapse and cause a collapse of the world financial system as its knock-on effect.

Though in our contemporary life, different devices help us make different decisions, they are mostly used only in such cases when there is a necessity to conduct mechanical surveillance (for example, by a referee in sports competitions), but not in situations when it is necessary to make moral decisions with far-going consequences (for example, in adjudicating a case by a court). The importance of making people contact directly is further proved by the fact that different legal systems do not approve trials in absentia. It is evident that nowadays robots have a considerable impact on our life, including their impact on life and death decisions. However, in none of such cases do robots make any decisions involving a murder; in this respect, robotic systems provide an absolutely new perspective for criminal activity.

References


