PAPER • **OPEN ACCESS**

Robotic systems implementation into law enforcement practice and peculiarities of decision-making models in such systems

To cite this article: K M Kholostov 2021 *J. Phys.: Conf. Ser.* **1958** 012021

Robotic systems implementation into law enforcement practice and peculiarities of decision-making models in such systems

K M Kholostov

Moscow Aviation Institute (National Research University), 4, Volokolamskoe shosse, Moscow, 125993, Russia

E-mail: hkm_tula@mail.ru

Abstract. The proposed directions of artificial intelligence technologies use in maintenance of order and public safety are presented. One of the major directions is the introduction of robotic systems into law enforcement practice, with the respect to certain problems related to the development of models and algorithms for the operation of automatic and semi-automatic robotic means are considered. Possible directions to create models and decision-making methods in control systems of security robots are proposed. As a basis for model development, the experience of creating and operating combat robots, including unmanned aerial vehicles (UAVs) is proposed. In the proposed models and methods, the emphasis on ensuring the safety, reliability and lawful (legal) operation of the created robotic means is emphasized. to ensure safety and reliability, manufacturers and developers of security robotic equipment are to create a unified knowledge base, including rules, prohibitions, and restrictions, with the help of which it is supposed to combine the experience of using security robots and unify approaches to their development and creation.

1. Introduction

Many spheres of modern society witnessed the widespread use of artificial intelligence technologies that has led us not only to a technological leap, but also to the emergence of new types of threats, including in the field of public safety and crime prevention. We are no longer talking about trivial telephone fraud and theft of funds using electronic payment systems, but about more sophisticated forms of crime and offenses where artificial intelligence technologies, including autonomous robots and self-learning software and hardware, play an increasingly active role. In these conditions, law enforcement agencies should have their own plan to introduce and use actively modern artificial intelligence technologies in their activities.

When considering possible directions to introduce artificial intelligence technologies [1], questions related to the problems associated with the implementation arise inevitably. Common problems in any organizational structure [2], like finding sources of funding and planning costs for the acquisition of new technical means, training personnel to use it, ensuring the life cycle of this equipment can be found, but there are also specific ones. The specific problems include the problems of safety ensuring, lawful (legal) use of self-learning and self-managing systems, for example, security robots.

Since the use of robots in maintaining public order, preventing and suppressing crimes, involves the part of the functions of police officers[1]—people, the question of the use of coercive measures legality by such robots (physical force, special means, not to mention the use of weapons) arises inevitably. In this connection, before the implementation stage, it is necessary to determine the boundaries of the use of coercive measures by robots, models and methods of their safe and legal use in the new public security system.

2. The main directions of artificial intelligence technologies use to protect and maintain order

Based on the analysis of the technologies available nowadays, it is possible to define the following *general directions* to use artificial intelligence technologies in law enforcement activities:

- increasing the efficiency of security systems management by improving the analysis, forecasting and decision-making processes;
- autonomous intelligent equipment and robotic systems use to improve the safety of employees by reducing the level of direct human participation in processes associated with an increased risk to their life and health;
- automation of routine (repetitive) operations to reduce the burden on security personnel and increase the reliability of functions;
- optimization of personnel selection and training, drawing up the optimal work schedule for personnel;
- intelligent means of logistics management use, including resource support for the activities of security organizations.

It is necessary to highlight basic technologies that are advisable to apply directly in the interests of ensuring the maintenance of public order and combating crime.

- Image recognition algorithms and systems built on their basis, capable of:
  —to detect and highlight in traffic flows and crowds of people who are on the wanted list or suspected of committing crimes, both in full and in partial images;
  —suspicious behavior of people;
  —suspicious objects, things, hijacked or stolen vehicles.
- Algorithms of recognition (identification) of human speech, operating in real time.
- Means of content and semantic analysis of texts, allowing to assess the psychological state of their author, as well as hidden information contained in messages.
- Intelligent systems that allow to analyze heterogeneous information to proactively identify weak signals, including those indicating a possible increase in crime, a surge in social tension, signs of riots and other acts of public order disturbance.
- Biometric systems to identify people by fingerprints and palms, facial images and iris, tattoos, scars, voice samples.
- Automated intelligent systems to search and analyze Internet content according to specified parameters, establishing the primary source of information on the Internet.
- Technologies to create autonomous robots and robotic systems that ensure the performance of checkpoint functions, patrolling, solving problems of inspecting the scene of crime, especially dangerous objects (including objects with the presence of explosives, toxic substances).

[1] According to Art. 18 of the Federal Law No. 3-FZ "On Police", a police officer has the right to use physical force, special means and firearms personally or as part of a unit (group) in cases and in the manner provided for by Federal Constitutional laws, Federal Law No. 3-FZ "On the Police" and other Federal laws.

- Management decision support systems, including measures to determine the optimal options to conduct operational-preventive and operational-search measures.
- Systems of intellectual support to form investigative versions, model the events of crime based on its traces and determine the algorithms for investigating actions.
- Predictive analytics systems that include search and retrieval of data to predict future criminal actions.
- Creation of cyber-physical systems based on the integration of computing and physical synergistically linked resources.
- Recognition of illegal actions in financial transactions, transactions and investment transactions that have signs of money laundering, abnormal behavior of legal entities and individuals in the field of finance, trading and investment.

The implementation and use of the above technologies will allow to adequately counteract modern and promising threats in the field of public security and combating crime, and technologically prepare the internal affairs bodies for the effective implementation of their activities.

One of these main areas of application of artificial intelligence technologies in law enforcement involves the use of autonomous robots and robotic systems, the use of which is impossible without the creation of data management systems for robots based on models containing rules for the safe and lawful behavior of autonomous systems in various environmental conditions.

3. Decision making production model in control systems of security robotic equipment

The accumulated experience in the creation and operation of combat robots, including UAVs [3–5], makes it possible to develop on their basis security robotic means (security robots) of a similar purpose. At the same time, the difference in the nature of the tasks performed, and target settings requires the use of fundamentally different solutions, firstly, in terms of the methods and algorithms used for decision-making in control systems of autonomous and semi-autonomous robots. Control systems for security robots, undoubtedly, must implement special models and algorithms that form the intellectual core of such systems, and that allows obtaining reliable assessments of the current situation, making *strategic, safe, reliable*, and fully *legitimate* (that is, legal) decisions on the implementation of certain security and protective actions.

For further consideration, we will clarify the possible options for the implementation of security robots and the scope of their application. According to the degree of autonomy, such robots can be divided into the following types:

- manipulators, that is, robots fully controlled by an operator (a human);
- autonomous systems, in the activity of which the operator interferes only at the stage of forming a service (for a UAV-flight) assignment and conducting a posteriori analysis [4];
- mixed systems with manual and automatic controls.

For the first of these classes, automatic control systems have a sound regulatory nature, which only maintain the operating modes of their own robot supporting systems (movement systems, thermoregulation, power supply, etc.).

The second and third classes of robotic equipment must have a control system that allows to make decisions independently, without the participation of an operator. The difference in classes is associated with the level of complexity and the degree of responsibility of the decision taken autonomously.

The peculiarity of the models and algorithms implemented in control systems of security robots is determined by the fact that decisions are made in conditions of uncertainty, unreliable and/or incomplete information about the real situation [5]. In this, security robotics

fundamentally differs from military ones, for which the goals and objectives are clearly, reliably, and well defined by the combat mission.

Let us dwell on the content of special conditions of security robots functioning. Unlike hostilities, law enforcement implies that the offender can be among law-abiding citizens and not manifest his illegal aspirations until a certain point. On the other hand, active actions or noisy communication by children or adolescents can be perceived by an outside observer as aggressive, dangerous, or potentially dangerous actions. In such conditions, the control system of the security robot may make an inadequate decision on action (or inaction), which may have unintended consequences. The change in role models of behavior when the same person demonstrates the behavior of the victim and the behavior of the aggressor will cause difficulty for the analysis of human behavior by the control system. In such conditions, for the functioning of the control system, reliable models and response algorithms are especially needed to ensure high reliability and stability of the system.

In connection with the specified features of the considered control systems, it is proposed to apply production models of decision-making based on rules for them. The decision-making model R, using set-theoretic relations, can then be formalized in the following form:

$$R \xrightarrow{t} \langle X, S, W, Z, P \rangle,$$

where X—is a factorial set of basic parameters characterizing the situation $(x_1, x_2 \dots x_i \dots x_n)$, n is the number of basic parameters; S—a set of typical standard scenarios $s_j \in S$; W is the set of production rules $w_m \in W$ included in the knowledge base; Z is the set of prohibitions and restrictions $z_k \in Z$, also included in the knowledge base; P is the set of service assignments $p_s \in P$.

This model can be described as follows. The control system, operating with a list of available basic parameters from the set X, based on one of the received service tasks $p_s \in P$ (this can be a particular task, or only one performed function), determines one of the typical standard scenarios from the set S, and using the knowledge base in the form of a set of production rules W and a set of prohibitions and restrictions Z, he can make a decision R in time t. In this case, it is assumed that the control system will make the necessary decision, allowing it to complete the task received by the robot, in time $t \leq t_{\max}$, where $t_{\max}$ is the maximum time determined to make a decision.

4. Unified knowledge base of manufacturers and developers of security robotic equipment

The presented model assumes the presence of W—a set of production rules and Z—a set of prohibitions and restrictions included in the knowledge base of the intelligent robot control system. The inclusion of the necessary rules, prohibitions and restrictions in the knowledge base can provide the requirements for the robot control system for making *safe, reliable, and most importantly*, completely *legitimate* decisions [7, 8]. At the same time, an equally difficult task arises—to form, as well as legally enshrine those rules, prohibitions and restrictions that can ensure the "embedding" of the robots being created into the new public security system.

In this direction, it is absolutely inevitable to cooperate between developers and manufacturers of robotic security equipment to create a unified knowledge base that includes a set of W_Σ—an integral set of production rules developed in the process of developing, configuring and training intelligent control systems for security robots. It should be borne in mind that the unified knowledge base being formed is not a simple algebraic sum of private knowledge bases, and the set W_Σ—will not be equal to the sum of private sets W_i, that is, $W_\Sigma \neq \sum_{q=1}^{Q} W_q$. This is due to the fact that, firstly, individual elements of w_{mq}—production rules from various private knowledge bases coincide in meaning with similar rules from other knowledge bases, and, therefore, do not increase the total number of rules. Secondly, and such situation should

be accepted, the rules from different bases may contradict each other, that leads to a conflict and the need to resolve it. To resolve such collisions, it is necessary to create an expert group of specialists who, after studying the collision, must make one of two decisions:

- accept as true one of the rules, while the second is recognized as false;
- both rules are considered false.

Based on the results of the decision made, adjustments are made to the integral set of production rules W_Σ, and thus a "working version" of the knowledge base with production rules is formed. Such a base is subject to mandatory certification and is subsequently used in the creation of new and modernization of existing robotic systems, thereby ensuring their safe, reliable and lawful operation, regardless of the operating conditions X and the specified service tasks P. The base should also include universal rules to ensure the exit of the system of their conflict (unknown, contradictory) situation. It is obvious that the accumulation of production rules in the knowledge base should be ensured by the openness of the system and the presence of machine learning mechanisms in it. The new production rules obtained during operation in the training mode are subject to analysis by a special expert community, and after their approval, they are included in the certified knowledge base in a strictly regulated manner, ensuring the responsibility of the persons made the decision.

In general, at all stages of the creation, modernization, and operation of both the security robotic systems and the models, algorithms and information bases that ensure their operation, it is necessary to ensure the collective adoption of responsible and balanced decisions, since, ultimately, it concerns rights and freedoms of a person recognized as the highest value [9, 10].

As for the prohibitions and restrictions on Z, according to the author, they should be formed by a competent interdepartmental commission from among experts in various subject areas and adopted before the start of industrial use of any autonomous and semi-autonomous robotic systems that perform the functions of ensuring order and safety. The system of prohibitions and restrictions should have a hierarchical structure in which some prohibitions or restrictions take precedence over others. For example, j-levels of prohibitions and restrictions form subsets $Z_1, Z_2 \dots Z_j \dots Z_L$ of the set Z, where L is the total number of levels. If we denote by F_j—the strength of the j-th prohibition (restriction), then the forces of prohibitions of levels form a set F, whose members form a system of priorities: $F_1 > F_2 > \dots F_j > \dots F_L$. Such a condition is urgent for the implementation of the proposed decision-making model since the emergence of several equivalent prohibitions and restrictions at once will lead to internal collisions in the control system of the security robot and consequently to blocking its operation.

One of the problematic and, at the same time, interesting cases in the practice of operating security robots may be such a situation in which the factorial set of the main parameters X, which is currently taking shape, will include factors x_i, the values of which are not provided for by the rules or do not correspond to prohibitions, but at the same time they contain danger. This situation can block the operation of the robot control system due to the impossibility to make a decision. The potential presence of the likelihood of such situations will give rise to a desire among attackers to block the work of security robots, for example, by their paradoxical behavior. In this case, the solution seems to be the development of universal algorithms that allows the system to get out of an unresolved situation, by returning to the previous (previous in time) situation, or by making a random decision that is not critical in the current situation.

5. Conclusion

As it has been shown, the widespread introduction into the system of public relations of autonomous (semi-autonomous) robotic systems capable to make decisions independently affecting to one degree or another human rights and freedoms is associated with problems not only of a technical nature, but also with issues of ensuring safety and legality of use. The

development of intelligent and robotic systems should be simultaneously accompanied by the cultivation of the "ethics of human-machine relations". Only the observance of this condition will ensure the conflict-free coexistence of a person and a robot in the era of their joint coexistence.

References

[1] Decree of the President of the Russian Federation 10.10.2019 No. 490 "On the development of artificial intelligence in Russian Federation"
[2] Romashkova I A and Abolikhina E S 2018 Problems in artificial intelligence developtment and their possible solutions *Youth scientific bulletin* **1** 104–09
[3] Bocharov L U and Reulov R V 2015 Military and Special Purpose Marine Robots: Analysis main development prospects in the USA *Technical problems of the World Ocean development* **6** 16–20
[4] Yevdokimenkov V N, Krasil'shchikov M N and Sebryakov G G 2016 Distributed intellectual control system for the group of unmanned aerial vehicles: architecture & software and mathematical support *Izvestiya SFedU. Engineering sciences* **1** 29–44
[5] Klimov R S, Lopota A V and Spassky B A 2015 Trends of military unmanned ground vehicles *Robotics and technical cybernetics* **3** 3–10
[6] Kholostov K M 2020 Modern information technologies in problems of modeling and analysis of the operational environment *Herald computer and information technologies* **2** 41–52
[7] Kharitonova Y S and Savina V S 2020 Artificial intelligence technology and law: challenges of our time *Perm university herald. Juridical sciences* **49** 524–49
[8] Mamychev A U, Gayvoronskaya Ya V and Miroshnichenko O I 2018 Modern doctrinal-legal and ethical problems of development and application of robotic technologies and artificial intelligence systems (on the example of autonomous uninhabited underwater vehicles) *Bulletin of the Vladivostok State University of Economics and Service* **3** 135–50
[9] Chiappe D, Rorie R, Moran C and Vu K 2012 A situated approach to the acquisition of shared SA in team contexts *Theoretical Issues in Ergonomics Science* **15** 69–87
[10] Hauss Y and Eyferth K 2003 Securing future ATM-concepts' safety by measuring situation awareness in ATC *Aerospace Science and Technology* **7** 417–27