DOI 10.15302/J-SSCAE-2021.03.007

Artificial Intelligence Security in Multiple Unmanned Systems Cooperation

Shi Wen [1], Wang Kaiwen[1], Yu Chengpu [1], Sun Jian [1], Chen Jie [1, 2]

1. School of Automation, Beijing Institute of Technology, Beijing 100081, China
2. Tongji University, Shanghai 200092, China

Abstract: Multiple unmanned systems cooperation is an important component of China's new-generation artificial intelligence (AI) planning, which is a transformative technology for future national defense construction and social development in China. Although significant achievements have been made regarding the technological research and system integration of multiple unmanned systems cooperation, research on AI security is still in its infancy. Promoting multiple unmanned systems cooperation enables AI applications and risk control. In this article, we propose a four-in-one strategy to promote the collaborative and secure development of multiple unmanned systems, investigate potential challenges and countermeasures for multiple unmanned systems cooperation at the endogenous and derivative security levels, and propose several suggestions regarding the security of intelligent unmanned systems. Specifically, a national unmanned system verification platform should be established to promote the construction of talent teams, services need to be upgraded for the unmanned system industry to develop a next-generation AI security ecology, and the advantages of multiple unmanned systems cooperation should be maximized to improve the livelihoods of people.

Keywords: multiple unmanned systems cooperation; artificial intelligence (AI) security; security risk prevention and control

1 Introduction

An intelligent unmanned system has a variety of types, covering different spaces of land, sea, and air. Such systems are moving comprehensively into all fields of national security and social life, and a new round of industrial transformation and high integration of related technologies is being promoted. As a subversive technology of artificial intelligence (AI), the cooperation of multiple unmanned systems organically connects the distributed unmanned systems in space to realize the effective cooperation of multiple systems in time, space, mode, and task, eventually forming a complete chain of target detection, tracking and recognition, intelligent decision-making, autonomous control, and effectiveness evaluations. With the continuous improvements of the technical levels, the missions of multiple unmanned systems will continue to expand, which will greatly change daily life and military operations.

There are many hidden dangers in the process of creating value for society, such as traffic accidents of unmanned vehicles, navigation disturbances and terrorist attacks on unmanned aerial vehicles (UAVs), and the unemployment of workers caused by the use of robots. The cooperation of multiple unmanned systems may bring about new challenges to national security in military operations, industrial upgrades, government regulations, social governance, and ethics [1].

At present, research on multiple unmanned systems cooperation in China is still in its infancy, and its basic theoretical framework is playing a crucial role in the future development and technological breakthrough of

Received date: February 15, 2021**; Revised date:** April 29, 2021

Corresponding author: Yu Chengpu, professor of C School of Automation of Beijing Institute of Technology. Major research fields include system identification and machine learning, distributed optimization and control, sensor networks and indoor positioning. E-mail: yuchengpu@bit.edu.cn

Funding program: CAE Advisory Project "Strategic Research on the Secure and Independent Development of New-Generation Artificial Intelligence" (2019-ZD-01)

Chinese version: Strategic Study of CAE 2021, 23(3): 082–089

Cited item: Shi Wen et al. Artificial Intelligence Security in Multiple-Unmanned System Cooperation. *Strategic Study of CAE*, https://doi.org/10.15302/J-SSCAE-2021.03.007

unmanned systems [2]. Therefore, in this study, forward-looking research on this blank field was conducted, aiming to reveal the significance of AI security in multiple unmanned systems cooperation, and countermeasures and suggestions for the corresponding problems are proposed for reference to the secure development of unmanned systems in China.

2 Significance in promoting an enabling application and risk prevention of multiple unmanned systems cooperation

2.1 Sustainable and high-speed development of research into multiple unmanned systems cooperation

In July 2017, the State Council described a rich strategy for achieving a new era of AI, pointing out the direction for a security reform of AI in China's multiple unmanned systems, and further clarified the medium- and long-term development goals [2]. Since the implementation of a strategy for the new era of AI in China, significant progress has been made; however, there is still no clear solution to the security problem of AI in multiple unmanned systems [3]. The search for solutions to various problems and the promotion of a steady development based on the safety foundation of multiple unmanned systems are conducive to the achievement of AI used in multiple unmanned systems.

2.2 Effective way to continuously enhance China's military power

In the context of multiple unmanned systems that are widely used in the military field, the importance of security issues has become more prominent. On one hand, an increasing number of countries have developed intelligent weapons, and the ability to realize the cooperative operation of multiple unmanned systems is becoming increasingly stronger. Future wars will be dominated by such systems. Therefore, ensuring territorial sovereignty and homeland security in an intelligent war is of great significance. On the other hand, in an intelligent war, the self-protection of multiple unmanned systems is also of great significance. How to ensure the security of the system and ensure that the data are not leaked, control is in hand, and that the task can still be completed in the face of an attack are major topics of research on multiple unmanned systems.

2.3 Key premise to improve the level of social security in China

AI security is a strategic issue related to China's economic and social development. The cooperation of multiple unmanned systems will be widely used in the fields of industry, agriculture, economy, and national defense, which will also bring profound changes to national security. Owing to a low threshold of abuse, multiple unmanned systems are easy to be exploited by extremist organizations and criminal gangs, and their management difficulty is far greater than before [4]. Strengthening the legislation of multiple unmanned systems in the new era of AI; forming a series of relevant laws and regulations such as for data, models, and applications; and improving the formulation of standards for the use of AI will help improve the overall level of national social security.

2.4 Construction of a highly intelligent society in the future

Traditional unmanned systems have been applied to the intelligent construction of society, intelligent express sorting, unmanned supermarkets, and traffic violation identification, among other areas, saving significant manpower. In the future, the wide application of multiple unmanned systems cooperation will guarantee and further improve people's livelihoods. However, compared with a traditional unmanned system, the application of multiple unmanned systems with communication and interaction capabilities may cause more serious public and ethical security issues, among others [5]. Therefore, it is extremely important to focus on strengthening the problem research and risk prevention in the application of multiple unmanned systems. Only by dealing with the above problems can we ensure that multiple unmanned systems will contribute to society in a safe and reliable manner in the future, and promote the healthy development of a new generation of AI in China.

3 Overview of security of multiple unmanned systems cooperation

With the maturity of multiple unmanned systems cooperation theory systems, the corresponding products and applications have shown rapid development momentum. From the perspective of the application field, multiple unmanned systems products mainly include unmanned vehicle, UAV, and unmanned ship clusters. Unmanned vehicle clusters can not only liberate all types of vehicle drivers, greatly reducing the workload, they also reasonably arrange road resources through intelligent optimization algorithms, relieve traffic pressure, and reduce the

DOI 10.15302/J-SSCAE-2021.03.007

occurrence of road traffic accidents. The application of UAV clusters covers military use (e.g., attacks, harassment, and investigation tasks) and civil use (e.g., disaster rescue, monitoring and inspection, environmental monitoring, and agricultural plant protection). Unmanned ship clusters are mainly used to perform dangerous, boring, and other tasks that are unsuitable for manned ships, including water quality monitoring, channel mapping, and maritime patrol [6]. Compared with traditional manned systems, multi-agent systems have many advantages, including lower operation thresholds, lower operation and maintenance costs, wider application fields, a more stable operation, and more efficient resource allocation. In the military, multiple unmanned systems can guarantee the safety of operators and reduce casualties. At the offensive end, they can also use a number of advantages to form a saturated strike with long distance, large scale, and high precision, which can even change the mode of modern war.

With the rapid development of multiple unmanned systems, many developed countries are actively promoting research on the security framework and legislation of intelligent versions of such systems. In the United States, AI security research and policy issues in multiple unmanned systems are quite frequent. In June 2019, the United States updated the *National Artificial Intelligence Research and Development Strategic Plan*, which listed the security of the AI system as one of its strategic objectives [7]. *Guidance for the Regulation of Artificial Intelligence Applications* published in January 2020 puts forward ten principles for the regulation of AI [8].The *National Artificial Intelligence Initiative Act of 2020*, passed in March 2020, supports research on the moral, legal, social, and other security issues of unmanned systems [9]. In the *Artificial Intelligence and National Security* plan updated in November 2020, the military development and ethical security of intelligent multiple unmanned systems are specified in detail [10].

The European Union (EU) has also carried out active research and policy-making on the security of intelligent unmanned systems, and EU member states have issued laws and regulations to regulate the operation of UAVs. Since July 2019, France has stipulated that UAVs must register electronic accounts. In addition, Germany has stipulated that the fuselage of all UAVs must be engraved with the owner's name and address. The United Kingdom has also increased the radius of its no-fly zone for UAVs near airports from 1 to 5 km. Moreover, Spain, Portugal, Italy, and other countries have banned UAVs from flying at night. In early 2019, the European Commission released the *European Coordinated Plan on Artificial Intelligence*, which listed AI security as a key field of strength and occupied a leading position in the global field of AI ethics [11]. In April 2019, the European Commission issued its *Ethics Guidelines for Trustworthy Artificial Intelligence*, which put forward seven principles of trusted AI [12]. In June 2020, the new general EU guidelines for UAVs will be officially launched. These guidelines replace the current regulations of EU member states and provide clear and unified rules for the development of the UAV industry in Europe [13].

China's multiple unmanned system-related legislation has also gradually advanced. In July 2017, China's State Council issued for the first time a strategic document titled the *Development Plan for the New Generation of Artificial Intelligence*, which proposed that the scale of the core industry of AI should exceed 1 trillion CNY by 2030 and drive the scale of related industries to exceed 10 trillion CNY. It also defined the basic theoretical framework of AI in multiple unmanned systems cooperation and put forward a plan to "strengthen the research of AI related legal, ethical, and social issues, and establish laws, regulations, and an ethical framework to ensure the healthy development of AI" [2]. However, in the definition of autonomous cooperative control and optimal decision-making theory, the framework focuses more on the realization and optimization of cooperative control, and there has been no further elaboration on the potential security risks in multiple unmanned systems. In December 2020, the Security Research Institute of China Academy of Information and Communication issued its *Artificial Intelligence Security Framework*, which formulated a more comprehensive security framework for AI, although a detailed description of the unique security problems in multiple unmanned systems cooperation is still not provided [3].

4 Challenges of multiple unmanned systems cooperation

In contrast to traditional unmanned system research, the core elements of multiple unmanned systems cooperation include communication interaction, cooperative games, and swarm intelligence evolution. With reference to the above characteristics of multiple unmanned systems cooperation, this study adheres to the problem-oriented analysis of its specific strategic initiatives, and constructs an AI security framework in the cooperation of multiple unmanned systems around the two modules of endogenous security and derivative security, as shown in Fig. 1.

4.1 Endogenous safety

To ensure the reliable execution of multiple unmanned systems tasks, the main consideration of an endogenous security is whether the system itself is stable and reliable, whether it prevents leaking secrets during the process of communication interaction, whether it can ensure that the control right is always in its own hands, and whether it can continue to complete the task after failure. The endogenous security of multiple unmanned systems cooperation should pay attention to all sections of multiple unmanned systems tasks, from ensuring the security of each part to ensuring the overall security, which covers the data security of the interaction between individual unmanned systems, the network security of multiple unmanned systems, the software and algorithm security, and the system architecture security of multiple unmanned systems. The endogenous security of multiple unmanned systems cooperation includes three parts: communication and interaction security, cooperative decision-making and cluster evolutionary algorithm security, and system architecture security.

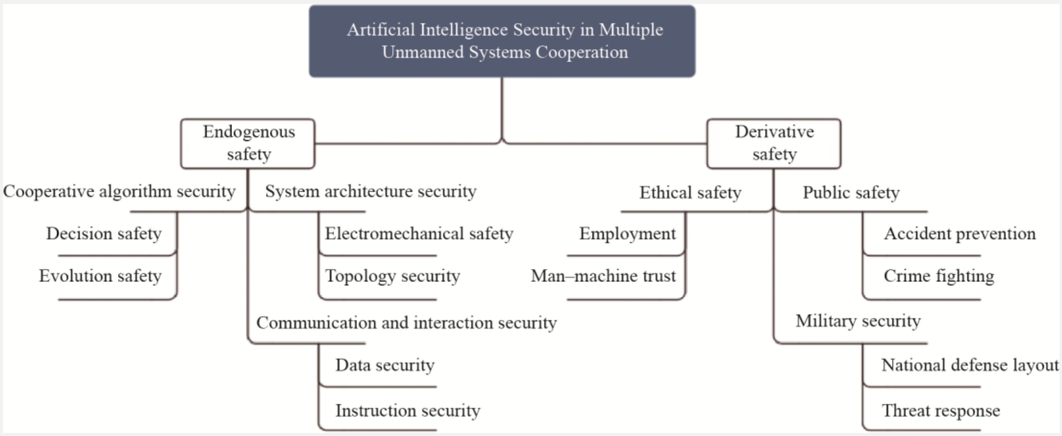

Fig. 1. AI security framework in multiple unmanned systems cooperation.

4.1.1 Communication and interaction security

During the execution of cooperative tasks of multiple unmanned systems, frequent communication and interaction are needed, including the interaction between each individual of multiple unmanned systems, the interaction between multiple unmanned systems and their owners, the interaction between multiple unmanned systems and various entity task objects, among others. Therefore, communication and interaction security are important aspects of cooperative endogenous security for multiple unmanned systems. The main purpose of communication network security is to prevent attacks on the network, to ensure that the owners of multiple unmanned systems can control multiple unmanned systems safely and reliably and ensure that the data are not stolen or tampered. On one hand, the cooperation of multiple unmanned systems must ensure safe and reliable communication. Once the data dissemination is cut off, or the information content is stolen, decrypted, or tampered with by others, the multiple unmanned systems will be greatly threatened, and our strategic intention will also be seriously hindered. On the other hand, if the security of the communication network cannot meet the requirements, the control rights of multiple unmanned systems will not be guaranteed. Because of the strong behavior ability of multiple unmanned systems, compared with simple data loss, the consequences of unsafe control are often more serious [14,15].

To solve the problems of data leakage and loss of control rights in the above-mentioned multiple unmanned systems, the systems should be equipped with a secure storage space that cannot be directly accessed by the outside world, and the data should be encrypted to ensure data security during the communication process. At the same time, a digital certificate, key and other authentication materials can be used for two-way remote identity authentication to ensure the legitimacy of each individual identity in the system and the credibility of the headquarters [16,17].

4.1.2 Security of cooperative decision making and cluster evolutionary algorithm

In terms of algorithm security, we should consider whether multiple unmanned systems can make correct decisions. We should also consider whether the direction of the collaborative decision-making algorithm and self-learning evolution is autonomous and controllable. An immature decision-making algorithm may lead to a less robust collaboration, and it becomes difficult to realize on-the-spot collaborative decision-making and action. When the system structure is affected by the outside world, if the intelligent collaborative algorithm fails to complete the control and optimization in real time, it becomes difficult to achieve an accurate collaborative control task, which reduces the consistency and stability of the collaboration. Thus, the risk of cooperative mission failure and damage to the multiple unmanned systems increases. In the future, multiple unmanned systems based on group intelligence evolution can learn and be upgraded independently. The security of its evolution direction is more important, and

DOI 10.15302/J-SSCAE-2021.03.007

will become a new challenge for algorithm security in multiple unmanned systems coordination.

To solve the above problems, the training process of the decision algorithm is improved, the cooperative evolution law of the unmanned system cluster is revealed, an active defense mechanism is designed, and a large number of possible confrontation samples are added during the training process. In other words, imaginary enemies are added during the training process to improve the robustness of the algorithm, reduce the possibility of a cooperative control task failure and incorrect evolution direction, and realize cooperative decision-making and evolution in a safer and more reliable manner [18].

4.1.3 System architecture security

System architecture security can be divided into two aspects: electromechanical security and topology security. The electromechanical security should consider whether the information receiving and receiving characteristics and information processing capacity of each individual in the multiple unmanned systems are sufficient, and whether the sensor and communication module can meet the needs of a cooperative task. Topology security is based on the electromechanical security. It considers the overall response speed and cooperative modes of multiple unmanned systems, and the ability to collect, process and exchange information and to get tasks allocated and executed correctly in real time under complex scenarios. It also considers whether a fault can be detected and topology switching can be done to continue the task [19].

The multi-layer clustering framework can effectively solve the security problems of the system architecture. The multi-layer clustering framework can help multiple unmanned systems react quickly in the face of changes. Even in the case of failure, it can achieve topology switching and continue to complete the next task to make the network topology more stable and achieve more robust multiple unmanned systems cooperation [20,21].

4.2 Derivative safety

The derived security of multiple unmanned systems cooperation mainly considers the impact that people or other objects outside the multiple unmanned systems may face after they are put into use. A system failure, interference, or decision-making error, in addition to the risk of a mission failure or system damage, may also lead to derivative security problems. At the same time, if the owner of the control rights of the multiple unmanned systems harbors malice and gives a targeted task to the multiple unmanned systems with bad intention, it may produce more serious derivative security risks. AI-derived security in multiple unmanned systems cooperation mainly considers public and ethical safety and military security.

4.2.1 Public safety

When multiple unmanned systems are operated, accidents will endanger public security, not only affecting the social order, but also threatening personal safety and property. At present, although multiple UAV cooperative systems are widely used, the safety performance evaluation system is not perfect, and is prone to various accidents, such as a UAV demonstration failure caused by various external interference and road traffic congestion caused by unmanned vehicles. Simultaneously, multiple UAV cooperation has the characteristics of low cost, wide use, low threshold, hidden identity information, large-scale casualties, and so on. Its illegal use seriously threatens the safety of personal and property. The development of multiple UAV systems is bound to bring new forms of crime. Compared with a single UAV system, a multiple UAV system is convenient for organized crime, causing significant harm to public safety [22].

In the face of the impact of multiple unmanned systems on social public security, strengthening the supervision is undoubtedly the most effective solution. Strengthening the supervision of all unmanned equipment manufacturers and holders, strictly checking all production lines, providing algorithms and equipment circulation objects to manufacturers, strictly implementing real name registration management for all privately held unmanned equipment, allowing all legal UAVs to have their own “identity certificate,” and seriously dealing with unregistered UAVs and registered but illegal UAV behaviors are other approaches [4].

4.2.2 Ethical safety

In terms of social ethics, in the civil field, most unmanned systems are faster, more efficient, and more accurate in engaging in repetitive, regular, and programmable tasks. They can not only replace manual labor, but also most mental labor. They play a major role in manufacturing, agriculture, and medical treatment, resulting in many workers changing jobs or leading to unemployment. In the military field, owing to technical failure, misjudgment, and other factors when using multiple unmanned cooperative systems, accidental injury or even death of human beings will occur. In the meantime, the interactions among multiple unmanned systems and between such systems and people are based on trust. Once an intelligent unmanned system has the ability to think independently, it will lead to a conflict between machines and even between people. In the long run, with the continuous improvement of intelligent and autonomous levels of multiple unmanned cooperative systems, there is a risk beyond human control, which may cause harm to human beings.

With the development of AI, the problems of workers changing their jobs and unemployment are inevitable. In the process of an industrial structure transformation, it is unavoidable that old jobs will be replaced by new ones. The success of the industrial revolution was also accompanied by a large number of workers changing jobs. Therefore, from the perspective of new jobs created by AI, we should not avoid the problems of unemployment and job transfer, but increase investment in high-tech fields, emerging industries, and modern service industries, actively promote the transformation and upgrading of industrial structure, and encourage the labor force to shift from primary and secondary industries to tertiary industries. Regarding the problems incurred by the independent thinking of AI and its potential harm to human beings, with the current technology, such harm is only a distant assumption. However, in the future, when facing an AI having the ability of autonomous learning, we can let it learn collaborative cooperation, altruism, and other aspects of human values during the early stage of learning and take the first step of harmonious coexistence with human beings [5,23].

4.2.3 Military security

At present, the state of international competition is complex, and the security risks caused by uncertain factors are sharply increasing. The core of military security is to protect national sovereignty and territorial integrity and to resist the invasion of foreign armed forces. A strong military strength has always been the foundation of China’s stability, and the importance of military security is self-evident. At present, the cooperation of multiple unmanned systems is most widely used in the military, and the future combat mode will be completely changed by the emergence of the cooperation of multiple intelligent unmanned weapons. Militarily, we should not only have the ability to resist the invasion of foreign armed forces but also have the ability to take the initiative to attack foreign threats [24].

China should strengthen its layout of multiple unmanned systems in terms of a national defense strategy, consolidate the foundation of coordinated technology development of multiple unmanned systems, and pay close attention to the development trends of world military science and technology and weapons and equipment. It should also strive to seize the strategic commanding height of scientific and technological research and development, firmly grasp the development trend of multiple unmanned systems in the military field, and prepare for various risks and challenges that may exist in future wars, promoting a leap forward in the development of national defense construction, providing a strong guarantee regarding the realization of the Chinese dream of building a strong military, and contributing to the realization of the common aspiration of peace and development of all mankind.

5 “Four-in-one” promotion of coordinated security development of multiple unmanned systems

Constructing a security governance framework of multiple unmanned systems, remaining in line with international standards, and building an ecosystem for multiple unmanned systems are current goals. Based on an innovation-driven development strategy, we should implement the relevant theoretical basis of multiple unmanned systems cooperation, enhance the innovation ability of AI science and technology, maximize the advantages of interdisciplinary integration, vigorously develop the front-end technology of intelligent multiple unmanned systems, and build an intelligent economic and social system. We should also build a legal system of security governance, improve the laws and regulations related to the application of intelligent multiple unmanned systems, establish a sound social responsibility system for AI, and realize the comprehensive rule of law in the new era. In addition, we should formulate ethical standards and improve the research and development standards of AI technology, building a peaceful society with AI to realize a new era of intelligence.

5.1 Promoting the safety and ecological construction of unmanned systems

To ensure the healthy development of AI technology in multiple unmanned systems cooperation, it is imperative to build a perfect security governance framework for multiple unmanned systems. Through international exchanges and cooperation, we should establish a sound safety assessment and supervision system for UAVs, unmanned vehicles, unmanned boats, and other unmanned systems. Aiming at the endogenous safety and derivative safety problems of multiple unmanned systems cooperation technologies, it is necessary to build multiple unmanned systems cooperation risk assessment index systems to strengthen risk control, evaluate the possible degree of harm, divide the risk level, formulate corresponding safety standards and countermeasures, and standardize the assessment procedure. We should also establish a special governance organization, such as a multiple unmanned systems cooperation security committee, to manage the security development of multiple unmanned systems cooperation. We must also evaluate and supervise the security of AI technology in multiple unmanned systems and ensure the implementation of national AI-related security policies put in place, as well as carry out research on social issues such as employment, the lives and property security of citizens, and privacy security, which may be brought about by AI in multiple unmanned systems. We should also conduct extensive exchanges and cooperation with various fields of society, and put forward operable, practical, and practical solutions with constructive policy suggestions.

5.2 Promoting advanced technology construction of unmanned system

International cooperation and independent innovations should be carried out simultaneously, and basic research and applications should be conducted in parallel. We should continue to strengthen the research on basic theories related to multiple unmanned systems cooperation, focus on breaking through the weak links in basic theories and related industries, and take a forward-looking aim at the emerging direction of multiple unmanned systems technologies, focusing on quantum AI cryptography [16], federated learning [17], countermeasure sample generation [18], clustering ad hoc network technology [20], blockchain technology [21], and other basic theoretical research closely related to the architecture, communication, and data security of multiple unmanned systems. Enhancing the innovation ability of AI technology has always been focused on the development trend of multiple unmanned systems around the world, learning advanced knowledge and cutting-edge technologies, firmly controlling the key core technology of AI, enhancing the innovation ability of independent and controllable technology, and ensuring the safety of related technologies and AI in multiple unmanned systems cooperation. Full play should be given to the advantages of interdisciplinary integration, effective ways of interdisciplinary integration should be explored, front-end technology of intelligent multiple unmanned systems should be vigorously developed, and an intelligent economic and social system should be built. Based on three aspects of independent innovation with Chinese characteristics, collaborative development of scientific and technological innovation and institutional innovation, and continuously strengthening basic research, we should implement a new development concept, show our confidence and determination in strengthening independent and controllable technology and innovation, enhance the ability of independent innovation, and speed up the construction of new innovations.

5.3 Promoting the legal norm construction of unmanned system

We should keep pace with the times, formulate and improve policies related to AI and laws related to the cooperation of multiple unmanned systems, adhere to the combination of flexible principles and standardized laws, and build a new legal system characterized by AI to provide strong support for comprehensively promoting the rule of law and accelerating the construction of a socialist country ruled by such governance. Research should be carried out on the legal issues related to the application of multiple unmanned systems technologies, such as civil and criminal liability confirmation, personal privacy security, data security, and property rights protection, and the laws, regulations, and ethical framework should be established to ensure the healthy development of multiple unmanned systems cooperation technology. An accountability system should be established and improved, the division of responsibilities be clarified, the implementation of responsibilities, and clarify the power responsibility relationship among regulators, product developers and users. Focus on the professional responsibilities of AI researchers in the field of AI security, and such researchers should be required to ensure the security of multiple unmanned systems through technical means. To lay a legal foundation for the rapid application of new technologies, we should speed up the research and development of relevant safety management laws and regulations around application fields with good foundations, such as autonomous driving and service robots. According to the function, use, and security of multiple unmanned systems, a perfect classification and classification system for multiple unmanned systems should be established. The formulation of technical safety standards should be accelerated, indicators should be refined, and more areas should be covered. The convergence of domestic safety technical standards and international standards should be sped up, while keeping up with the international leaders.

5.4 Promoting the social ethics construction of unmanned systems

Owing to the characteristics of frequent interaction and cooperation operations, multiple unmanned systems can greatly improve the quality of human life; however, there may be uncontrollable security risks resulting from independent consciousness. During the process of collaborative research and development of multiple unmanned systems, an ethical design is added to learn the collaborative cooperation and altruism in human values, and thus the multiple unmanned systems has a certain ability of moral judgment initially. During the actual operation process, the system can follow preset ethical and moral standards of people to eliminate the possibility of harming human society. The specific ethical requirements put forward by the safety management organization of AI are embedded with ethical elements through technical means during product development, and implemented and guaranteed through policy requirements and legal norms to curb the possible risks of AI technology in multiple unmanned systems from the ideological source, realizing the unity of science and technology and humanistic care, and taking the first step for human beings to live in harmony with AI.

6 Countermeasures and suggestions

6.1 Building a national unmanned system verification platform and promoting the construction of talented teams

A public technology verification platform of autonomous unmanned systems should be built with production, education, and research as a whole to provide fertile ground for compounding high-end talent and high-level innovation teams. Full play should be given to the main vitality of governments, industries, universities, and research institutes, introducing and cultivating a group of young talents to provide basic innovative research and a healthy development of the industry, as well as providing full openness and resource support to the platform to solve the concerns of the team. Focus should be placed on the breakthrough and verification of common key technologies closely related to security applications, such as controllable intelligent evolution, trusted sensing interaction, reliable collaborative control, and the guidance and support of all parties to jointly develop and build a common security technology system for autonomous unmanned systems.

6.2 Gradually improving the management of unmanned system industry to develop a new generation of AI security ecology

The establishment of access standards should be promoted for the AI industry as represented by civilian unmanned systems and a comprehensive and in-depth quality inspection system for products. In addition, the management and services should be improved to ensure the safety and reliability of civilian unmanned systems actually put into use, as well as to promote the healthy development of industrial ecology. On this basis, we will gradually refine the laws and regulations for the application of unmanned systems in various subfields, and formulate the qualification standards for personnel related to the design, production, use, and service of unmanned systems in specific fields so as to grasp the opportunities and meet the challenges more intelligently.

6.3 Giving full play to the advantages of multiple unmanned systems cooperation, enabling its application

In-depth research should be conducted on the next generation of AI technology as represented by unmanned systems and the new risks during the process of industrial development, such as social security, employment placement, industrial security, and national defense. In addition, local risk disposal and overall security development plans should be formulated. In the fields of manufacturing, agriculture, justice, education, national defense, and medical care, it is necessary to promote the gradual application of unmanned systems, seek advantages and avoid disadvantages, guarantee and improve people’s livelihoods, and serve to build a community of shared future for mankind. The opportunities should be firmly grasped and challenges calmly dealt with in realizing a smooth transition under the high-speed development and application stage of unmanned systems and their collaborative technologies.

References

[1] Wu Q. Unmanned systems development and analysis of the impact on national security [J]. Unmanned Systems Technology, 2018, 1(2): 62–68. Chinese.

[2] The State Council of the PRC. Notice of the State Council on issuing the development plan for the new generation of artificial intelligence [EB/OL]. （2017-07-08）[2021-04-27]. http://www. gov.cn/zhengce/content/2017-07/20/content_5211996.htm. Chinese.

DOI 10.15302/J-SSCAE-2021.03.007

[3] Security Research Institute of China Academy of Information and Communications Technology. Artificial intelligence security framework 2020 [R]. Beijing: Security Research. Institute of China Academy of Information and Communications Technology, 2020. Chinese.

[4] Chen W G. Some thoughts on the governance of artificial intelligence [J]. Frontiers, 2017 (20): 48–55. Chinese.

[5] Du Y Y. Artificial intelligence security issues and their solutions [J]. Philosophical Trends, 2016 (9): 99–104. Chinese.

[6] Wang W J, Zheng Y T, Lin G Z, et al. Swarm robotics: A review [J]. Robot, 2020, 42(2): 232–256. Chinese.

[7] The National Science and Technology Council. The national artificial intelligence research and development strategic plan: 2019 update [EB/OL]. (2019-06-21) [2021-04-27]. https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019-printer.pdf.

[8] The White House. Guidance for regulation of artificial intelligence applications [EB/OL]. (202011-17) [2020-12-03]. https://www. whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memoon-Regulation-of-AI-1-7-19.pdf.

[9] CONGRESS. National artificial intelligence initiative act of 2020 [EB/OL]. (2020-03-12) [2021-04-27]. https://science.house.gov/ bills/hr6216-national-artificial-intelligence-initiative-act-of-2020.

[10] Congressional Research Service. Artificial intelligence and national security [EB/OL]. (2020-11-10) [2021-04-27]. https://crsreports. congress.gov/product/pdf/R/R45178.

[11] Council of the European Union. European coordinated plan on artificial intelligence [EB/OL]. (2019-02-18) [2020-12-03]. https:// www.consilium.europa.eu/en/press/pressreleases/2019/02/18/european-coordinatedplan-on-artificial-intelligence/.

[12] The High-Level Expert Group on AI at European Commission. Ethics guidelines for trustworthy AI [EB/OL]. (2019-04-08) [2020- 12-03]. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[13] Ye C Q. Notice of the European Union on general guidelines for UAVs [J]. Financial Technology Time, 2019, 288(8): 89. Chinese.

[14] Derakhshan F, Yousefi S. A review on the applications of multiagent systems in wireless sensor networks [J]. International Journal of Distributed Sensor Networks, 2019, 15(5): 1–19.

[15] Wang L, Wang P, Yan Z. A survey on secure communication of unmanned aerial vehicles [J]. Cyberspace Security, 2019, 10(9): 13–19. Chinese.

[16] Wang B N, Hu F, Zhang H G, et al. From evolutionary cryptography to quantum artificial intelligence cryptography [J]. Journal of Computer Research and Development, 2019, 56(10): 2112–2134. Chinese.

[17] Yang Q. AI and Data Privacy Protection: The Way to Federated Learning [J]. Journal of Information Security Research, 2019, 5(11): 961–965. Chinese.

[18] Liu X L. Research on generation of adversarial examples based on swarm evolutionary algorithm [D]. Chengdu: School of Information and Software Engineering (Doctoral dissertation), 2019. Chinese.

[19] Wu Y M. Research on secure consensus for multi-agent systems under malicious attacks [D]. Hangzhou: Zhejiang University of Technology (Doctoral dissertation), 2016. Chinese.

[20] Cui Z Y, Sun J Q, Xu S Y, et al. A secure clustering algorithm of Ad Hoc network for colony UAVs [J]. Journal of Shandong University (Natural Science), 2018, 53(7): 51–59. Chinese.

[21] Zang Y H, Li X J. Unmanned cluster operation information sharing [J]. Command Control & Simulation, 2020, 42(4): 19–22. Chinese.

[22] Fan Q Y, Jin M J, Huang L, et al. The safety problems and countermeasures of unmanned vehicles [J]. Scitech in China, 2019 (6): 13–15. Chinese.

[23] Li X Q. Security, privacy and ethical challenges in artificial intelligence applications and their countermeasures [J]. Science & Technology Review, 2017, 35(15): 11–12. Chinese.

[24] Johnson J. Artificial intelligence, drone swarming and escalation risks in future warfare [J]. The RUSI Journal, 2020, 165(2): 26–36.