CHAPTER 12

EMERGING TECHNOLOGIES AND NATIONAL SECURITY

DR IMRANUR RAHMAN
ASSISTANT PROFESSOR
LUCKNOW PUBLIC COLLEGE OF PROFESSIONAL STUDIES
Email: drimranlpcps@gmail.com

KEYWORDS

EMERGING TECHNOLOGIES, NATIONAL SECURITY

ABSTRACT

Under the background of a new round of scientific and technological revolution, the governance of emerging technologies has become a hot topic of great concern to all countries. It is not only related to whether we can seize the development opportunities and enhance national strength in the future, but also to whether we can effectively maintain national security and gain international competitive advantages. Therefore, it is of great strategic significance to grasp the development laws of emerging technologies, explore the internal logic of governance, and achieve effective governance. Starting from the characteristics of emerging technologies, this paper reveals the "insecure" attributes contained in its development laws and the systemic security risks it brings. Based on the comparative perspective of traditional technology governance, it deeply analyzes the changes in security preferences in the governance logic of emerging technologies and explores the forward-looking governance path of building "nested" national security.

12.1 INTRODUCTION

The governance of emerging technologies is a hot topic of concern to the international community. However, both in terms of theoretical construction and practical advancement, the governance of emerging technologies faces huge challenges: First, the growth and application of emerging technologies have unique laws, and it is difficult to completely copy the traditional technology governance concepts, models and measures; Second, with the intensification of international geopolitical games, the "national security" dimension in the governance of emerging technologies has become unprecedentedly prominent, becoming an important factor affecting the governance process, increasing the complexity and uncertainty of governance. Therefore, on the basis of grasping the characteristics and development laws of emerging technologies, fully considering the impact and shaping of the current international geopolitical game on them, and better understanding the national security concerns in the governance of emerging technologies, it will help explore more effective and pragmatic emerging technology governance paths.

12.2 CHARACTERISTICS OF EMERGING TECHNOLOGIES

12.2.1 DESCRIPTION AND DEFINITION OF EMERGING TECHNOLOGIES

There is currently no accurate definition or consensus in either the academic or policy circles on what emerging technologies are. The term frequently appears in national strategies related to scientific and technological development in relevant countries and in reports of international organizations, but it is mostly explained in the form of lists, and there is rarely a direct definition of emerging technologies themselves. Typical representatives include the new version of the List of Critical and Emerging Technologies (CET List) released by the United States on February 7, 2022, which lists 19 critical and emerging technologies that are vital to the national security of the United States, involving supercomputing, communications and network technologies, artificial intelligence, semiconductors and microelectronics, hypersonic capabilities, directed energy, renewable energy generation and storage, nuclear energy and finance.

For example, in the India-US Initiative on Critical and Emerging Technologies (iCET) recently announced by the US and Indian governments, it is also made clear through enumeration that the two governments and their industry, academia and research departments will strengthen cooperation in the fields of artificial intelligence, semiconductors, 5G/6G, quantum computing, biotechnology and space technology in the future.

Government departments choose to define the scope of emerging technologies by listing rather than interpreting them. First, to list the key points more concisely, so as to better play the role of policy guidance and concentrate resource investment in practice; second, because emerging technologies are in dynamic development, they need to be adjusted in time; third, countries are at different stages of development, and there are real gaps in the understanding and application of emerging technologies, which are difficult to be completely consistent. Therefore, from the perspective of policy operation, it is difficult and unnecessary to accurately or uniformly define the connotation and extension of emerging technologies. However, for the academic community, it is crucial to define emerging technologies from the perspective of interpretation, because clarification of concepts, as a prerequisite for research, determines the boundaries and focus of research, and is also a further study of the characteristics, laws, and governance of emerging technologies.

The research is the basis and starting point of the topic. Given that research comes first and theory guides practice, the exploration of the above issues will help improve the effectiveness of emerging technology development strategies, policies and measures. As early as the 1990s, the academic community began to conduct a series of studies on emerging technologies, such as Wharton on Managing Emerging Technologies, published by the Wharton School of the University of Pennsylvania in 2000. As an international research group that has paid attention to the development and impact of emerging technologies earlier, the author team of this book mainly explores how to effectively avoid the risks brought by emerging technologies from the perspective of management science, that is, from the perspective of industrial development and company operations, and explores the potential of emerging technologies such as the Internet and biotechnology to create new industries and change existing industries, but the discussion on "Identification and Evaluation of

New Technologies" is of great reference value for defining emerging technologies. This research result has an important impact on the subsequent research on emerging technology management. From the perspective of management, the book chapter defines emerging technology as "a technology that is based on the development of information technology, biotechnology and other disciplines, has potential industrial prospects, has a high degree of uncertainty in its development, demand and management, is emerging and may lead to great changes in industry, enterprises, competition, management thinking, business processes, organizational structure and business model".

12.2.2 IDENTIFICATION AND EVALUATION OF EMERGING TECHNOLOGIES

The most influential article on the identification and evaluation of emerging technologies is "What is Emerging Technology" published in Research Policy in 2015. b The author of this article, through text analysis, sorted out the academic papers on emerging technologies over the years, trying to find the commonality of the definition of "emerging technology" under various contextual interpretations. Through comparative analysis, the author proposed five key elements for evaluating and identifying "emerging technologies".

The first is novelty. Compared with existing technologies, it presents completely different technical ideas and principles. The second is rapid growth. Compared with non-emerging technologies, it has obvious growth advantages. This growth is difficult to quantify, but it can be observed through capital investment data, industry data, and alternative metrics (Al metrics). The third is coherence.

Most emerging technologies are not "out of nowhere", but are based on existing technology paths, or may be "new" technologies generated by the combination of multiple technologies. A typical example is artificial intelligence. In fact, artificial intelligence technology was born as early as the 1960s, but due to the limitations of the technical conditions at the time, it did not begin to develop rapidly until the 21st century with the improvement of computer "computing power" and the great abundance of data.

Fourth, it has a significant impact. Its impact is not limited to a specific field, but has a significant impact on the entire social and economic system, changing the behavioural subjects, operating mechanisms and interaction modes of social life, and even the process of knowledge formation.

Fifth, uncertainty and ambiguity. The application scenarios and results that this technology may bring are uncertain, and it may even bring some "unintended" or even "undesirable" results; and ambiguity means that the boundaries of responsibility of different social entities for technological development, especially security, will be difficult to clearly define for quite some time.

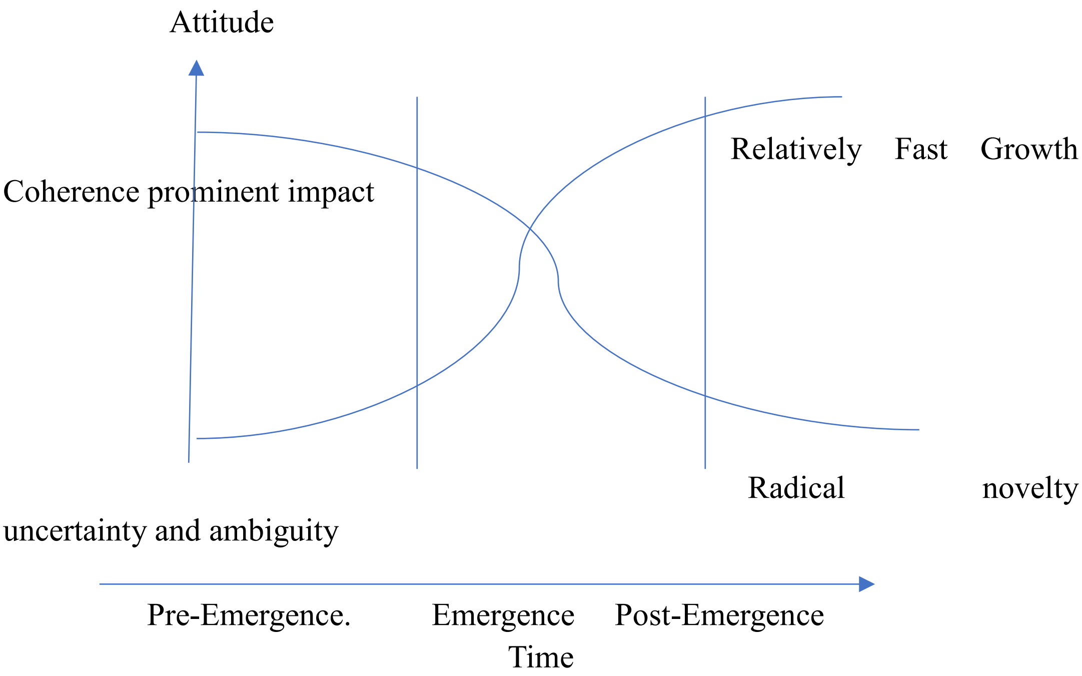

FIGURE 1 THE LIFE CYCLE OF EMERGING TECHNOLOGY DEVELOPMENT

Given the above five key elements, if a technology is "quite novel, relatively fast-growing, will show a certain degree of coherence over time, and has the potential to bring considerable impact to the social and economic fields, change the subject of behaviour, operating mechanism, interaction mode and even the process of knowledge generation, these impacts will emerge significantly in the future, but will show a certain degree of uncertainty and ambiguity for a long time", then it can be called "emerging technology". Of course, the significance of clarifying the five key elements is not limited to better understanding what emerging technology is, but more importantly, on this basis, through the dynamic changes of these elements, we can roughly grasp the development and evolution of emerging technologies. As can be seen from Figure 1, the "life cycle" of an emerging technology development generally includes three stages:

- **Pre-emergence,** which is characterized by prominent novelty and uncertainty, limited corresponding growth rate, and the socio-economic impact it brings has not yet been demonstrated. In practice, it is reflected as a new technical idea or is still in the experimental development stage, with unclear social application scenarios and quite limited actual applications.

- **Rapid growth (Emergence),** which is characterized by a gradual decline in novelty and uncertainty, and a continuous increase in growth rate and influence. In practice, it is reflected as a technology moving from research and development to application, with relatively clear and extensive application scenarios.
- **Late growth,** which is characterized by a peak growth rate and influence, the technology is mature enough to lose its novelty, and its uncertainty and ambiguity are also eliminated to the greatest extent. In practice, it is reflected as a mature technology application that has reached a considerable degree of industrialization and scale, and the corresponding development strategy, policy and governance mechanism have also been improved accordingly.

To grasp the laws of emerging technology development, it is necessary to clarify the following two points: First, emerging technologies are always in dynamic development. Specifically, it includes two meanings. On the one hand, technology itself has a certain life cycle, and a technology cannot always be an "emerging technology"; on the other hand, the judgment of emerging technologies is also dynamically adjusted. Different countries will change the evaluation criteria for the "novelty" and "significant impact" of emerging technologies. For example, compared with the "National Strategy for Critical and Emerging Technologies" released in 2020, the latest CET list in the United States has removed data science and storage technology, blockchain technology, advanced traditional weapons technology, medicine and public health technology, and agricultural technology. However, it should be noted that the overall overlap in the cognition and judgment of "emerging technologies" in various countries during the same period is still relatively high. For example, the OECD's Science, Technology and Innovation Outlook published in 2016 lists 40 emerging key technologies that will have a significant impact in the next 10 to 15 years based on the official technology frontier predictions of Canada, Finland, Germany, the United Kingdom, Russia and other countries and the European Union, and divides them into four groups: digital technology, biotechnology, energy and environmental technology, and advanced materials. Each group further lists relevant important technologies.

More importantly, from the development laws of the above-mentioned emerging technology life cycle, it can be seen that since most of the time of the emerging technology life cycle is in a highly uncertain and ambiguous process, but at the same time it will have a profound and comprehensive impact on the social and economic system, this means that the risks brought by uncertainty and ambiguity will inevitably penetrate into all aspects of the social and economic system and form systemic risks. In addition, compared with traditional technologies, the "implementation" and "expansion" of emerging technologies are often extremely rapid, and even "research and production are synchronized", which results in very limited time for governance to discover problems and respond effectively, bringing great difficulties to security governance. In this sense, the security risks brought by emerging technologies are bound to be complex and systematic, and their security maintenance and effective governance are bound to face huge challenges. On November 16, 2020, the official website of the World Economic Forum released the "Future Series: Cybersecurity, Emerging Technologies and Systemic Risks" report, focusing on the increasingly serious threats posed by inherent hidden dangers and systemic risks in the emerging technology environment. The report stated, "Looking forward to the development trend of technology, it presents a picture of increasing complexity, speed, scale and interdependence.

The emerging technology environment will "overwhelm" many of the risk mitigation measures currently deployed. If we do not intervene now, it will be difficult to maintain trust in and completeness of emerging technologies on which future global growth depends." Therefore, in a sense, the development of emerging technologies itself contains "insecurity" characteristics. In summary, after understanding the definition of emerging technologies and their development laws, the next question is how to govern emerging technologies to effectively maintain security and promote development? Can the concepts and models of traditional technology governance be applied to the governance of emerging technologies?

12.3 LOGIC OF GOVERNANCE OF EMERGING TECHNOLOGIES: THE PROMINENCE OF SECURITY PREFERENCES

To explore the governance of emerging technologies, we can use a comparative perspective, that is, to compare them with traditional technology governance concepts and models because after years of theoretical and practical development, traditional technology governance is relatively formed, and although emerging technologies have distinct characteristics, in essence, as technologies themselves, they must follow the internal logic of general technology governance to a considerable extent, although their own characteristics will bring impacts, challenges and even changes to traditional technology governance to a certain extent. This process is not only an exploration of emerging technology governance, but also a enrichment and improvement of overall technology governance.

12.3.1 THE INTERNAL LOGIC OF TRADITIONAL TECHNOLOGY GOVERNANCE

- **About the goal of governance:** It is generally believed that no matter what kind of governance, its overall goal must be a balance between development and security. Of course, absolute balance is a perfect goal and is difficult to achieve in practice. The process of infinite approach is crucial. Therefore, the goal of so-called technology governance is to minimize various security risks and hidden dangers brought about by the development process while ensuring that the innovation and development of technology are in line with social goals, improving productivity and obtaining corresponding social benefits.
- **About the governance framework:** In fact, technology involves many categories, and the application scenarios and social impacts of each technology are different. Therefore, the understanding of the technology governance framework is often based on the characteristics of "layer-based", "domain-based" or even "issue-based". The so-called "layer-based" means that the problems brought about by technology and its application will involve problems at different levels, some of which are physical levels (technical hardware problems), some are logical levels (technical software problems), and some are application levels (social problems brought about by the industrialization and social application of technology); the so-called "domain-based" means that from the perspective of the social impact of technology, a specific technology will bring about problems in different fields such as politics, economy, culture, military, and society; and "issue-based" means to focus more subdivided and specifically on a specific problem brought about by a certain technology.
- **About the content of governance:** The pacing problem refers to the fact that the speed of scientific and technological innovation has greatly exceeded the speed of updating laws and regulations. This term first appeared in Larry Downes's book "The Law of Disruption" published in 2009: "Technology grows exponentially, but social, economic and legal systems grow only slowly” Therefore, the overall traditional technology governance is characterized by "lag". It should be pointed out that this "lag" is not negative or derogatory. It is essentially in line with the law of technological development. The effectiveness of governance also depends on whether it can maximize the gap in pace and try to keep up with the pace of technological evolution. Like the pace problem, this is also a professional term in technology governance, which further describes the dilemma faced by technology governance from a methodological perspective. It

specifically includes two constraints: one is the information dilemma, that is, the social consequences of a technology cannot be predicted in the early stage of its life; the other is the control dilemma. When the undesirable consequences are discovered, the technology has often become part of the entire economic and social structure, making it very difficult to control it. This term was first proposed by David Colling ridge of Aston University and published in the book "Social Management Technology". Colling ridge once said that when an easy thing is changed, the result will be difficult to predict. When obvious changes are needed, the method of change becomes expensive, difficult and time-consuming.

Therefore, governance practice is to find ways to obtain information, intervene early and achieve control over the best results. Of course, in practice, there is no ultimate perfect solution to this problem itself, but the continuous improvement of governance is essentially to reduce the adverse effects of the "pace problem" or "Colling ridge dilemma" as much as possible. At present, both the "pace problem" and the "Colling ridge dilemma" have become the basic logical starting point for discussions on technology governance. Taking Internet technology as an example, its development process fully confirms this point. The initial design and application concept of Internet technology is "connection" rather than security. Therefore, from the perspective of the technical architecture itself, it is inherently "unsafe".

At the same time, with the continuous popularization and social application of the Internet, the social problems and risks it brings have gradually emerged and been recognized by society, and then response and governance have been put on the agenda. From the perspective of "pace", governance always lags behind the development of technology itself; from the perspective of "dilemma", the "information dilemma" in the early development of the Internet and the current "control dilemma" are obvious. It was impossible to foresee the many governance challenges that would be brought about by later development, from cybercrime to cyberterrorism, from cyberattacks to national behavioural norms, and so on. When the international community realized these problems and began to invest in strengthening governance, Internet technology had already surpassed technology itself and became a "ubiquitous" and "nested" technology that has penetrated all areas of society. Any governance measures may come at a high cost to social development.

12.4 THE INTERNAL LOGIC OF EMERGING TECHNOLOGY GOVERNANCE

Following the traditional technology governance goals, frameworks, content and other ideas, combined with the characteristics and practices of emerging technologies, through comparative analysis, it is concluded that emerging technology governance has the following internal logic:

12.4.1 GOVERNANCE GOALS HIGHLIGHT SECURITY PREFERENCES

In the current new round of scientific and technological revolution, emerging technologies such as information technology, artificial intelligence, life sciences, and digital technology are driving the global scientific and technological revolution into a new historical stage of superposition explosion. Especially in the context of the current international situation and intensified geopolitical games, in view of the experience and lessons of the international community in the governance of information communication and network technology over the years, compared with the situation in the early stage of traditional technology development that emphasized development and security considerations were relatively lacking, the relevant parties' cognition of emerging technology governance was no longer limited to technology and its development itself from the beginning, but attached great importance to it from the perspective of national security and strategic competition, and the security preference was obvious.

For example, the report "Beyond Technology: The Fourth Industrial Revolution in Developing Countries" released by the Center for Strategic and International Studies (CSIS) in 2019 believes that developing countries have latecomer advantages in the application of emerging technologies, especially China is using this to surpass the United States and expand its influence in the world. a Immediately afterwards, CSIS published a report in 2020 titled "Twin Towers: Maintaining National Security and National Innovation in the Governance of Emerging Technologies", which further emphasized that in an era of global technological competition and innovation diffusion, the United States must maintain the two pillars of national security and national innovation, and proposed relevant governance measures in emerging technology leadership, public-private partnerships, innovation and security, emerging technology workforce, extensive and sustained diplomatic engagement, and preparation for inevitable friction and threats.

Based on this concept, on October 15, 2020, the U.S. State Department released the "National Strategy for Critical and Emerging Technologies", which details the United States' emphasis on developing "critical and emerging technologies" in order to maintain global leadership. The positioning of these technologies is essentially "critical and emerging technologies that are vital to U.S. national security." The European Commission also released the "Key Technology Roadmap for Security and Défense" in February 2022, stating that "staying at the forefront of technological development is essential to ensuring Europe's prosperity, security and lifestyle." The European Commission believes that the decentralization of Europe's security and defence forces has led to economic inefficiency, weakened operational capabilities and increased strategic dependence, and the development of emerging technologies provides an opportunity to change this situation. "Avoid making past mistakes." It is not difficult to see from the above statements that European countries believe that "security" issues have seriously affected economic development and social prosperity and must become their primary concern.

12.4.2 THE GOVERNANCE STRUCTURE PRESENTS A MORE DISTINCT "PAN-SECURITY" FEATURE

The current practice of emerging technology governance has shown that the boundaries of "layering" and "domaining" in traditional technology governance have become more blurred, and the characteristics of "layer" integration and cross-domain" collaboration are obvious; more importantly, national security factors have been highlighted as never before, making the governance of emerging technologies present the characteristics of "pan-securityization." Taking the current rapid and relatively mature AI governance as an example, its governance purpose is to give full play to the advantages brought by AI and effectively reduce the risks caused by AI. From the very beginning, it has shown distinct characteristics of "layer" integration and cross-domain collaboration. Although it is divided into three levels, namely, technical level, ethical level, social and legal level, according to different focuses, the levels are actually interrelated. For example, when considering security at the technical level, ethics is a necessary factor, emphasizing the concept of secure technology design (Secure by Design); similarly, the ultimate goal of governance at the social and legal level is to achieve the ultimate technological ethics for the benefit of mankind, that is, to build responsible artificial intelligence (RAI) by integrating political, economic, cultural, military, legal, and social resources.

In this process, national security factors are the focus of relevant countries. For example, the Belfer Center for Science and International Affairs at Harvard University published a research report entitled "Artificial Intelligence and National Security" in 2017, pointing out that "the advancement of artificial intelligence will achieve national security by promoting changes in military advantages, information advantages and economic advantages." The US strategic community has basically reached a consensus on the following two aspects: First, artificial intelligence is the core variable that affects and shapes the future national security of the United States; second, effectively overcoming the negative effects of artificial intelligence is the key to ensuring the future national security of the United States. In particular, the United States believes that the Chinese government is trying to achieve a "leapfrog" development of military capabilities through the development of artificial intelligence: "China's investment in artificial intelligence may "weaken" the United States' military advantage, "undermine" the free and open international order, and "challenge" American values and traditions in human rights and personal freedoms", which will eventually "challenge" the United States' relative advantage and leadership in the field of artificial intelligence and globally, and pose a serious "threat" to US national security. It can be seen from this that national security factors can be said to run through the governance of artificial intelligence from a strategic height. For example, the report "Cybersecurity, Emerging Technologies and Systemic Risks" released by the World Economic Forum pointed out that quantum technology may change the rules of the game for national security. Some countries are making major investments in quantum technology and skill development and have included quantum technology in the control list. In the future, if a few developed countries gain quantum hegemony, it will have geopolitical implications. In addition, competition and protectionism will also affect international cooperation and fairness, resulting in the inability to release the full potential of quantum technology into economic and social development. If countries cannot ensure fair access to quantum technology, countries with quantum capabilities will gain strategic advantages, while other countries will fall into "quantum poverty."

12.4.3 GOVERNANCE PRACTICES EMPHASIZE "SECURE BY DESIGN" OR "ZERO TRUST SECURITY MODEL"

As mentioned above, one of the characteristics of emerging technologies is rapid development and widespread application, which shortens the time left for decision makers and governance to understand their potential uses and impacts. Future

development and security are highly uncertain and ambiguous. Therefore, the traditional cognition of development first and security later
is obviously unable to adapt to the needs of the development of the situation, and the security “port” must be continuously moved forward. Some security concepts such as “security-based design” and “zero trust” architecture have begun to be recognized and paid attention to. The former means that any technology and application should consider its possible security issues at the beginning of design, and the control of security must be reflected in the corresponding design. The latter was originally a new security model in the field of network security. It is a method of designing a security protection architecture. Its core idea is that by default, all interactions are untrustworthy.

Traditional networks are built on trust, and later the corresponding network security protection also adopted the "trust but verify" method. Even in the face of increasingly severe security situations, it also adheres to the principle of "differentiation between inside and outside", that is, by establishing a security boundary (firewall or physical isolation) to retain internal trust and external defence. However, with the continuous upgrading of new technologies and application methods, cyber criminals are constantly looking for new ways to break through traditional security protection architectures. Advanced hacking tools and commercial ransomware are becoming increasingly accessible, making it increasingly difficult to ensure security needs with this method. Therefore, in the 2010 Zero Trust Report of Forrester Research, a well-known market research company, analyst John Kindwig called for adjusting the network security protection method to a "verify but not trust" strategy. These concepts and measures have "spill over" to the governance of emerging technologies. For example, the report "Cybersecurity, Emerging Technologies and Systemic Risks" released by the World Economic Forum clearly proposed the governance strategy of "safe development" for quantum technology, calling on countries to regularly review the security of quantum plans and monitor their risks when formulating quantum development plans or strategies. In addition to strengthening adversarial security defense algorithms, in order to address the "accuracy", "falsification" and "manipulability" of AI abuse and malicious attacks, a guiding cybersecurity operation framework is also needed to automatically detect, investigate and formulate defence plans for emerging AI threats. These concepts and architectural experiences, which benefit from existing technology governance, will have an initial and directional impact on the governance architecture system.

Future development and security are highly uncertain and ambiguous. Therefore, the traditional cognition of development first and security later is obviously unable to adapt to the development needs of the situation, and the security "port" must be continuously moved forward. Some security concepts such as "security-based design" and "zero trust" architecture have begun to be recognized and paid attention to. The former means that any technology and application should consider its possible security issues at the beginning of design, and the control of security must be reflected in the corresponding design. The latter was originally a new security model in the field of network security. It is a method of designing a security protection architecture. Its core idea is: by default, all interactions are untrustworthy. Traditional networks are built on trust, and later the corresponding network security protection also adopted the "trust but verify" method. Even in the face of increasingly severe security situations, it also adheres to the principle of "differentiation between inside and outside", that is, by establishing a security boundary (firewall or physical isolation) to retain internal trust and external defence. However, with the continuous upgrading of new technologies and application methods, cyber criminals are constantly looking for new ways to break through the traditional security protection architecture. Advanced hacking tools and commercial ransomware are becoming more and more easily available, making it increasingly difficult to ensure security needs with this method.

Therefore, in the 2010 Zero Trust Report of Forrester Research, a well-known market research company, analyst John Kindwig called for adjusting the network security protection method to a "verify but not trust" strategy. These concepts and measures have "spill over" to the governance of emerging technologies. For example, the report "Cybersecurity, Emerging Technologies and Systemic Risk" released by the World Economic Forum clearly proposed the governance strategy of "safe development" for quantum technology, calling on countries to regularly review the security of quantum plans and monitor their risks when formulating quantum development plans or strategies. In addition to strengthening adversarial security defence algorithms, in order to address the "accuracy", "forgery" and "manipulability" of artificial intelligence abuse and malicious attacks, a guiding network security operation framework is also needed to automatically detect, investigate and formulate defence plans for emerging artificial intelligence threats. These concepts and architectural experience of existing technology governance will have an initial and directional impact on the governance architecture system.

12.5 EMERGING TECHNOLOGY GOVERNANCE PATHS: BUILDING FORWARD-LOOKING GOVERNANCE WITH “NESTED” NATIONAL SECURITY

Currently, the theoretical discussion and practical promotion of emerging technology governance are still in the early stages of development, but their importance and urgency are increasing day by day. Given the inherent insecurity of emerging technology development laws and the security preferences in governance real needs, how to build a governance framework that can improve the “pace problem” and “Colling ridge dilemma” and promote the healthy development of emerging technologies, while balancing the increasingly prominent national security concerns, is the starting point for further improving the governance path of emerging technologies. Therefore, this chapter proposes forward-looking governance based on “national security”, that is, “nesting” national security elements in the framework of forward-looking governance.

12.6 CONCEPT AND FRAMEWORK OF ANTICIPATORY GOVERNANCE

This concept is widely used in the field of emerging technology governance, originating from the US government and academia's attention to nanotechnology. In 2003, the US Congress passed the "21st Century Nanotechnology Research and Development Act", authorizing the "National Nanotechnology Initiative" (NNI) established in 2000 to promote the development and governance of nanotechnology. According to data from the official website of NNI, it is funded by multiple federal agencies, with more than 80% of the funds being funded by the National Science Foundation, the Department of Défense, the Department of Energy, and the National Institutes of Health. One of the overall goals of the subsequent series of research and development activities is to explore anticipatory governance.

Anticipatory governance is a technical decision-making method that takes precautions and prevents social risks of emerging technologies in advance. Some scholars define its connotation as a technical decision-making method that arranges appropriate scope of participants and adjusts specific communication processes, so that governance participants change or enhance their awareness of emerging technology risks, promotes or slows down the pace of development of certain types of emerging technology applications, and ultimately achieves collective action to resolve social risks of emerging technologies, different from the governance model, forward-looking governance emphasizes cross-domain capacity building, allowing researchers from different disciplines to interact with industry, government, community and the public, and jointly establish various scenarios for technological development before technology research and development is transformed into practical applications. Forward-looking governance also emphasizes managing collective expectations and reflecting on the development environment and social impact of emerging technologies. Unlike technology prediction and technology foresight, forward-looking governance attaches great importance to building the ability of the whole society to deal with unexpected consequences and risks of technology, rather than just predicting the results of technology implementation.

In short, its core essence is twofold: **first,** it does not pursue predetermined results as a goal, but maintains a dynamic and open attitude towards future technology development and application scenarios, and there are many possibilities in the future; **second,** it emphasizes that the process is not only the continuous deepening of cognition, but also the continuous choice of practice. In order to overcome uncertainty and ambiguity, full information exchange and coordination of all parties are essential. To this end, forward-looking governance emphasizes cross-disciplinary and multi-subject cooperation and the integration of relevant mechanism forces. Different scholars have different understandings and suggestions on the specific governance framework and policy toolbox. Based on the views of all parties, the basic points are as follows:

- **Information and data collection**. Obtain as much relevant information and data as possible to enhance public awareness and help decision-making.
- **Fill in the policy "gaps".** New technologies often bring new problems, some of which require the introduction of new policies, while others require the clarification of new functional departments. Therefore, it is necessary to strengthen the dynamic adjustment of policies and the adaptability of mechanisms.
- **Strengthen the responsibilities of key entities**. Technology governance practices show that professional institutions and industrial departments engaged in technology research and development have a huge influence. Strengthening the responsibilities of these key entities can often achieve good results from point to surface.
- **Adhere to the participation of "multi-stakeholders".** Not only does governance practice require the participation of stakeholders, but more importantly, in this process, a mechanism-based communication platform for

stakeholders can be established, which is conducive to updating information, colliding new ideas, and building public trust, thus forming a good governance ecology. It should be pointed out that the above points run through the entire process of emerging technology governance. Taking the acquisition of information and data as an example, it is generally understood that emerging technologies often face "information dilemmas" in the early stages of development, and it is necessary to predict the future development direction and make corresponding policy choices as early as possible. Therefore, it is crucial to find effective ways to alleviate them. This method can be to encourage information sharing and communication among various industries and institutions, or to use some advanced scientific and technological means, such as the current development of big data and artificial intelligence technology, which provides an opportunity for more efficient scenario simulation and deduction, helping policymakers strengthen prediction and make effective decisions. However, these measures and methods are not limited to the early stages of development. The future of forward-looking governance is uncertain, and each stage is a node that affects the future. Therefore, it is necessary to constantly obtain the latest information, calibrate policies, and even change choices

12.7 SUGGESTION

The significance and benefits of this "nesting" are mainly reflected in the following aspects:

First, it is to enhance public awareness and shape a social policy environment that is conducive to security. For the special historical period in which the development of emerging technologies is currently taking place, the sensitivity of public cognition at home and abroad is limited, and the idea of free development of traditional technologies still exists to a considerable extent. In many cases, the public cannot understand the relevant emerging technology governance policies from the perspective of international strategic competition and national security, and the relevant measures are even controversial. Therefore, it is necessary to consciously embed relevant information points on national security into the collection of information and data, increase the publicity and explanation of relevant policies, and help form a better public awareness and social policy environment.

Second, make more comprehensive policy predictions and decisions. Given that the governance of emerging technologies involves a wide range of fields and multiple departments, it is difficult to comprehensively consider various factors in practice, especially for professional institutions and industrial departments. Information related to national security is relatively scarce. Adding necessary national security information points can help them better improve multi-dimensional information, calibrate policies, and make decisions that balance development and security. Of course, it should be emphasized that "necessary" national security information points can be obtained through internal or special channels, and relevant departments can provide necessary guidance and communication on the premise of ensuring security, so as to avoid making decisions that may affect national security due to information loss or neglect.

Third, promote the formulation of new policies to reflect the necessary national security demands. One of the characteristics of emerging technology governance is to constantly adjust policies according to new problems, especially to fill policy gaps. In order to improve efficiency, new policies should have necessary national security considerations and reflect corresponding national security demands at the beginning of their design, so as to better adapt to the needs of the development of the situation and maintain the stability of policies. This has been proven in practice. In recent years, the strategic documents and laws and regulations on relevant technology development issued by various countries have reflected clear security considerations. However, it is important to pay attention to the fact that the situation is always developing and changing. With the development of technology and applications, the impact of a new technology on national security is also changing. Therefore, the flexibility of relevant policies should be maintained, and timely evaluation and dynamic adjustment should be made.

Fourth, clarify and strengthen the national security responsibilities of stakeholders. Important stakeholders in emerging technologies, including professional institutions and industrial sectors, focus on security issues related to their professions or products. As for social public responsibilities, including national security, either the awareness is not in place or the degree of attention is limited, which is also one of the manifestations of the "ambiguity" of responsibilities in the development of emerging technologies. On the one hand, the governance departments need to further clarify the responsibilities with the help of relevant policies and regulations; on the other hand, it is more important to strengthen policy guidance in practice, refine the operation guidelines and provide supporting policy tools so that relevant parties can better perform their corresponding duties. This will not only help enhance the stable expectations of relevant parties for policies, but also help them build confidence in development.

Fifth, relevant departments explore more effective ways of participation. "Multi-stakeholder" participation is more of a principled statement, and often faces certain efficiency issues in practice. Especially considering that national security is often quite sensitive and may have a certain impact on the normal business and activities of other relevant parties, therefore, discussions or cooperation involving national security issues must be cautious and moderate, not only requiring full evaluation and precise grasp, but also continuous exploration and innovation of working methods, while achieving more effective participation, laying a foundation of trust that is conducive to the governance ecology of emerging technologies.

It should be noted that the so-called "nesting" does not mean an excessive security tendency and preference, and its "boundary" and "scale" still need further exploration. For example, how to implement various principles such as necessity, rationality, scientificity, and transparency, how to maintain the real-time nature of policy adjustments, how to build a smooth information feedback channel to help calibrate measures, and how to ensure that there are necessary evaluation and supervision mechanisms during implementation, etc. If these supporting issues are not timely, it will not only be difficult to achieve the original intention of balancing security and development, but will also affect development in turn.

12.8 CONCLUSION

Based on the review of relevant domestic and foreign research, this chapter expounds the characteristics of novelty, rapid growth, coherence, major social impact, uncertainty and ambiguity of emerging technologies, and combines these characteristics to explore the dynamic and unsafe characteristics contained in its development laws from the perspective of "life cycle". Focusing on the intensified geopolitical competition and game in the current new round of scientific and technological revolution, this chapter analyses the security preference in the governance logic of emerging technologies, especially the prominence of the "national security" dimension, and proposes to embed national security elements into the forward-looking governance framework of emerging technologies. Of course, this is just a preliminary idea. The theoretical exploration of emerging technology governance is still in its early stages of development. This article only takes national security as the starting point and attempts to preliminarily deconstruct the governance of emerging technologies from the perspective of theory and analytical framework. Many questions remain to be further studied or answered in practice.

12.9 REFERENCES

- System issues such as a "List of Critical and Emerging Technologies," https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf. (Accessed on February 8, 2022)
- Press Information Bureau, Government of India, "Prime Minister's Meeting with President of the United States of America," https://pib.gov.in/PressReleseDetailm.aspx?PRID=1827885. (Accessed on May 26, 2022)
- Daniele Rotolo, Diana Hicks and Ben R. Martin, "What Is an Emerging Technology," Research Policy, July 7, 2015, p.23.
- OECD, "Science, Technology and Innovation Outlook," 2016, https://www.oecd.org/fr/sti/oecdscience-technology-and-innovation-outlook-25186167.htm. (Accessed on March 2, 2017)
- World Economic Forum, "Future Series: Cybersecurity, Emerging Technology and Systemic Risk," https://www.weforum.org/reports/future-series-cybersecurity-emerging-technology-andsystemic-risk/. (Accessed on November 17, 2020)
- Larry Downes's book "The Law of Disruption" published in 2009,P 23:
- CSIS Report, "Beyond Technology: The Fourth Industrial Revolution in the Developing World," https://www.csis.org/analysis/beyond-technology-fourth-industrial-revolution-developingworld. (Accessed on May 22, 2019)
- CSIS Report, "Twin Pillars: Upholding National Security and National Innovation in Emerging Technology Governance," https://www.csis.org/analysis/twin-pillars-upholding-nationalsecurity-and-national-innovation-emerging-technologies. (Accessed on January 23, 2021)
- White House, "National Strategy for Critical and Emerging Technology," https://www.whitehouse.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf. (Accessed on December 8, 2020)
- "List of Critical and Emerging Technologies," https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf. (Accessed on February 8, 2022)
- European Commission, "Roadmap on Critical Technologies for Security and Defense,"

https://ec.europa.eu/info/sites/default/files/com_2022_61_1_en_act_roadmap_security_and_defence.pdf (Accessed on February 27, 2022)

- Chao Lemen and Yin Xianlong: "The Current Status and Trends of Artificial Intelligence Governance Theory and System", "Computer Science", Issue 9, 2021, pp. 1-8.
- 13-"What Is Zero Trust?" https://www.redhat.com/zh/topics/security/what-is-zero-trust. (Accessed on August 2, 2022)
- Tan Zongying and Gong Xu: "National Nanotechnology Program and National Science Foundation of the United States", https://www.nsfc.gov.cn/csc/20345/20348/pdf/2006/NationalNanotechnologyProgram and National Science Foundation of the United States.pdf. (Accessed on August 5, 2022)
- Chen Yu and Ma Yongchi: "Prospective governance characteristics of social risk resolution of emerging technologies", https://www.cnki.com.cn/Article/CJFDTotal-KJJB202210013.htm. (Accessed on August 10, 2022)