CHINA AND International Cybersecurity

CHINA AND International Cybersecurity

Translated by WANG Chunbo

Tianjin Foreign Studies University

China Intercontinental Press

Farmington Hills, Mich • Andover, UK • Chicago • Mason, Ohio • Meriden, Conn • New York
San Francisco • Singapore • Waterville, Maine

GALE
A Cengage Company

China and International Cybersecurity

Vice President:
Seth Cayley

Senior Regional Director:
Steve Matsumura

Publishing Manager:
Yang Liping

Project Editor:
Rebecca Chiew
Emery Pan

Senior Product Manager:
Vincent Cheah
Morisawa Masaki

Senior Regional Manager, Production and Rights:
Pauline Lim

Production Executive:
Rachael Tan

Translator:
Wang Chunbo

Proofreader:
Wu Xueting
Susan Amy

Cover Designer:
ST Leng

Compositor:
diacriTech, India

ISBN: 978-981-4839-31-0

This title is also available as an e-book:
ISBN: 978-981-4839-32-7

Cengage Learning Asia Pte Ltd
151 Lorong Chuan
#02-08 New Tech Park
Singapore 556741

Cengage Learning is a leading provider of customized learning solutions with office locations around the globe, including Singapore, the United Kingdom, Australia, Mexico, Brazil, and Japan.
Locate your local office at **www.cengage.com/global**

Cengage Learning products are represented in Canada by Nelson Education, Ltd.

To learn more about Gale product information, visit **www.gale.com**

Printed in Singapore
Print Number: 01 Print Year: 2019

TABLE OF CONTENTS

LIST OF EXHIBITS

PREFACE

Text To Come

Chapter One

INTERNATIONAL CYBERSECURITY GOVERNANCE AND A COMMUNITY OF SHARED FUTURE IN CYBERSPACE

International cybersecurity has become an important issue affecting global peace and security, posing threatening challenges to national governments and the international community. Following the incident of Edward Snowden exposing top-level secret information about the US National Security Agency's surveillance activities (hereinafter referred to as the Snowden Leak) in June 2013, the international community made considerable progress in promoting the governance of international cybersecurity in the face of these challenges (*see* Exhibit 1.1). Governments published their strategy reports on cybersecurity and formulated and implemented cybersecurity policies. However, neither international nor national efforts in governing the cyberspace have successfully reversed the deteriorating situation under the ever-changing and intensifying cybersecurity threats.

In the past five years, the international community has been unable to reach a consensus on the set of rules governing cybersecurity, or build an effective governance mechanism. Therefore, it is necessary for the international community to rethink the theory and practice of international cybersecurity, to explore the root causes of existing problems and seek effective solutions, and jointly build a community of shared future in cyberspace.

Exhibit 1.1 Edward Snowden, a former CIA employee who exposed the US National Security Agency's PRISM (surveillance program), in an interview with NBC Evening News in May 2014

Source: Visual China

1.1 Analyzing the Concept of International Cybersecurity Governance

Cybersecurity is one of the key areas of concern for the international community. Massive cyber surveillance, cyberspace arms race, ransomware, and attacks on critical infrastructure related to financial services and energy supply, are several of the unstable factors jeopardizing the international security system. National governments, including the Chinese government, are beginning to focus on cybersecurity issues, investing large amounts of resources in cybersecurity and establishing corresponding

governance mechanisms. At present, although some achievements have been made, the international community is still facing severe challenges. Compared with traditional global issues, cybersecurity is a complex frontier global governance issue that is multilevel, cross-domain, and interdisciplinary. The advent of the Age of Artificial Intelligence and the rise of the Information Society have expanded the connotations of cybersecurity, making the concept even more difficult to grasp.

From the perspective of international practice, cybersecurity comprises three layers of security—infrastructure, data, and content. The first two layers involve critical infrastructure security and key data protection, which are supported by international cybersecurity cooperation and the national cyberspace strategies, policies, and norms of behaviors formulated by governments. Content security is built on the governance of information, being made even more complicated as countries do not agree on many issues. While countries have reached a consensus on the governance of issues such as fake news, child pornography, and hate speech, they continue to disagree on other ideological issues. Some religious countries impose stringent controls on religion-based speech online. Some developing countries, including China, have an urgent need to govern ideological content for the purpose of maintaining social stability, while most Western countries began paying attention to their cyber ideology only after the hacker interference in the US presidential campaign. Prior to this incident, these Western countries would usually blame the Internet policies of other countries in the name of Internet freedom. In general, content security falls under domestic Internet public policy, with little relevance to international cybersecurity.

From a research perspective, the study of cybersecurity is an interdisciplinary field that requires a background knowledge in information and computer technology (ICT), international relations, international law, journalism, political science, economics, and sociology. Given the complexity of international cybersecurity governance, it is insufficient to simply apply prior knowledge of governance from other fields. To study international cybersecurity governance, one must pay particular attention to the practice of international cybersecurity governance and analyze it from different perspectives. The multilevel, cross-domain, and interdisciplinary nature of international cybersecurity has made it very difficult to comprehend, and equally difficult to build effective governance mechanisms. Any theory and practice relating to international cybersecurity governance issues, actors, and mechanisms must take into consideration the special nature of ICT.

1.1.1 Major Issues in International Cybersecurity Governance

As a subfield of global cyberspace governance, international cybersecurity governance focuses on cybersecurity issues from the perspective of global peace and security, and emphasizes the role of sovereign states in global governance and domestic policy formulation. At the international level, the cooperation of sovereign states in national cyber defense, intelligence, law enforcement, and policy, lies at the core of cybersecurity governance. Specific governance issues include: establishing international rules of cyberspace and norms of responsible state behavior, applying international laws to cyberspace through confidence-building measures, combating cybercrime and cyberterrorism, and promoting cooperation in technical assistance and information-sharing. Although these governance issues have different focuses, there are many overlaps. Therefore, unless we adopt a comprehensive perspective and strengthen the interactions between the mechanisms for handling the different issues, it will be difficult to uncover the problems and find effective solutions.

Aside from international governance mechanisms, the capacity of national governments is the foundation and guarantee for achieving international cybersecurity. In recent years, governments have focused on cybersecurity issues and increased their investments correspondingly. At the domestic level, governance issues cover the following aspects: the strategic planning of cybersecurity; the establishment of related laws, policies, standards, and systems; the specific practices in critical infrastructure protection, personal data protection, and cross-border data transfers; and the planning for upgrading the cybersecurity industry especially in terms of technology and personnel. Due to the borderless nature of cybersecurity, the improved capabilities of national governments for safeguarding cybersecurity will boost international cooperation. Countries ought to strengthen interstate policy coordination, share information and knowledge, and provide technical assistance to one another in the abovementioned areas, with a view to setting up a unified and standardized set of policies, and building a community of shared future in cyberspace.

1.1.2 Main Actors of International Governance

The issues of international cybersecurity governance determine that national governments and intergovernmental organizations are the main actors involved in such

governance. Compared with multistakeholder governance, multilateral governance is more applicable to the building of mechanisms for international cybersecurity governance. Therefore, national governments and intergovernmental organizations such as the United Nations are the main actors in international cybersecurity governance. However, compared with traditional international governance issues, the multilevel, cross-domain, and interdisciplinary nature of cybersecurity increases the complexity of the actors in such governance.

First, due to the extensive nature of international cybersecurity issues and the involvement of various government departments—such as foreign affairs, defense, intelligence, law enforcement, judiciary, trade, industry, and education—its coordination is more difficult than in traditional international governance. Moreover, since cybersecurity is an emerging security issue, the missions and responsibilities among different agencies are still not clearly defined at the domestic level. International cybersecurity governance issues are overseen by multiple administrations, leading to duplications and overlaps and making it difficult to find the right counterpart in international cooperation and negotiations.

Second, international cybersecurity governance involves a multitude of complex international organizations. These include global intergovernmental organizations, such as the United Nations, multilateral organizations with a focus on governance such as the G20, the G7, and the Organisation for Economic Cooperation and Development (OECD), and regional organizations such as the ASEAN Regional Forum (ARF), the Asia-Pacific Economic Cooperation (APEC), and the African Union (AU) (*see* Exhibit 1.2). These intergovernmental organizations also partially overlap in terms of issues they focus on.

Finally, given the complexity of international cybersecurity, non-state actors (including private sector and academia) can also be an integral part of the governance mechanisms and play a role in the international governance of cyberspace. One example is The Internet Corporation for Assigned Names and Numbers (ICANN), an international NGO.

1.1.3 The Development of an International Governance Mechanism

International cybersecurity governance is mainly carried out at the UN, and at multilateral, regional, and bilateral levels. At present, the United Nations Group of Governmental Experts (UN GGE) on Information Security is one of the most

Exhibit 1.2 The First China–ASEAN Cyberspace Forum, Nanning, China, September 18, 2014

Source: CNSphoto

influential mechanisms globally. It was established by the Disarmament and International Security (First Committee) of the UN General Assembly as a consultant to the secretary-general in 2004, in accordance with the UN secretary-general's mandate, to study emerging security issues and put forth measures. The main purpose of the UN GGE is to serve the UN in establishing "an open, secure, stable, accessible, and peaceful ICT environment," and promoting norms of behavior that can enhance the security and stability of international cyberspace.

The UN GGE encourages the UN member states to report annually on their use of ICT, in accordance with General Assembly Resolution A/53/576. The Group

prioritizes and facilitates dialogue on normative issues that have garnered limited agreement, and promotes multistakeholder participation to achieve the establishment of norms in cyberspace governance. As a critical platform, the UN GGE facilitates discussions on the non-binding norms of state behavior concerning the state use of ICT, ranging from the application of existing international law to state responsibilities and obligations in cyberspace. These involve protecting critical infrastructure, preventing cybersecurity incidents, building trust and capacity, and upholding human rights. The framework resulting from the discussion of these issues has been put into practice by bilateral, multilateral, and by specialized agencies in different regions or sub-regions. Although the final reports of the expert group are non-binding, they are seen as a foundation for enhancing the security and stability of cyberspace. The complementary initiatives generated by these reports at global, regional, and bilateral levels have helped disseminate the consensus reached at the UN GGE, strengthened trust between countries and other stakeholders, and enhanced the capacity of developing countries in international cyberspace.

Until 2016, the United Nations has appointed five expert groups, but only the 2010, 2013, and 2015 groups have drawn up a *Report of the Group of Governmental Experts*, respectively. Among them, the 2015 expert group report reached a consensus that emphasized the role of cyber norms in fostering the peaceful use of communications technology and strengthening global societal and economic development through these technologies. Based on the previous reports of 2010 and 2013, the Group has put forward a clearer and more comprehensive definition of the norms of responsible state behavior. For example, it is regulated that a state must not allow others to use its own territory or its communications technology to intentionally commit unlawful acts. A state must respond appropriately to requests for assistance from another state whose critical infrastructure is under attack by malicious communications technology. The report also stipulated additional requirements on enhancing confidence-building measures.

In addition, the 2015 Report includes the application of international law for the use of communications technology, and clearly demonstrates that the basic principles of the *UN Charter* apply to cybersecurity issues. Such principles include protecting the sovreignty of all states, the peaceful settlement of international disputes, refraining from the threat or the use of force against the territorial integrity or political independence of any state, respect for human rights and fundamental freedoms, and non-intervention in the internal affairs of other states.

1.1.4 The Dilemma of Cybercrime Governance and the UN Expert Group on Cybercrime

Cybercrime has become one of the most urgent cybersecurity problems, and the focus of international cybersecurity governance. The ever-changing situation of cybercrime has posed new challenges to investigation, criminalization, and the use of digital forensics. Moreover, as cybercrime is increasingly transnational, the international governance mechanism against cybercrime has become key to effectively curbing the growing trend of cybercrime. Current competing mechanisms at the international level mainly exist between the United Nations and the Council of Europe, but the fight against cybercrime requires a new impetus for international cooperation.

Cybercrime as a Major Challenge of Global Cyberspace Governance

Currently, there are two different research perspectives on cybercrime. One is to treat cybercrime as a new form of crime and the Internet as a means to an end. The other is to emphasize the interdependent relationship between cybercrime and cybersecurity. In practice, people often combine both perspectives when tackling cybercrime. With the acceleration in the innovation and application of cybersecurity technologies, a comprehensive understanding of cybercrime is crucial to the development of international and national mechanisms for international cybersecurity governance.

UN Expert Group Meeting (EGM) on Cybercrime

Established by the Commission on Crime Prevention and Criminal Justice (CCPCJ) in 2010, and in accordance with *UN General Assembly Resolution 65/230*, the Open-ended Intergovernmental Expert Group Meeting on Cybercrime (UN EGM on Cybercrime) is the most important international mechanism for combating cybercrime at the UN level. Its main purpose is to conduct a comprehensive study of the problem of cybercrime and collate responses from member states, the international community, and the private sector. The Group's task also includes the exchange of information on national legislation, best practices, technical assistance, and international cooperation, with a view to examining options for strengthening existing legislation and proposing new national

and international laws, or other strategies to combat cybercrime. Fully recognizing the work of the expert group, the Chinese government promoted the establishment of the expert group and also actively participated in its working process.

From April 3 to 5, 2018, the Fourth Session of Intergovernmental Expert Group Meeting on Cybercrime was held in Vienna, Austria. The Chinese government sent a delegation comprising officials from the Ministry of Foreign Affairs, the Ministry of Public Security, the Ministry of Industry and Information Technology, and the Ministry of Justice. At the session, the expert group first adopted the 2018–2021 work plan. These experts from five continents then conducted group discussions on cybercrime legislation and criminalization, presented their research findings and professional experiences in these matters, and interacted closely with representatives of national governments.

The First Session of the Intergovernmental Expert Group Meeting on Cybercrime was held in Vienna from January 17 to 21, 2011. The group reviewed and adopted a collection of topics for the study and set specific procedures for the group's working mechanism. In 2012, the secretariat of the expert group organized the distribution of questionnaires to various countries. Based on the feedback, the expert group thoroughly studied cybercrime issues and drew up the *Comprehensive Study on Cybercrime*. The report consists of eight chapters, whose coverage includes global connectivity and cybercrime, the global cybercrime picture, cybercrime legislation, criminalization, law enforcement and investigations, electronic evidence and criminal justice response, international cooperation, and cybercrime prevention, respectively. For a comprehensive understanding of the global cybercrime situation and the current difficulties faced by countries, this report is an important resource. In 2013, the Second Session of Intergovernmental Expert Group Meeting on Cybercrime focused on discussing the *Comprehensive Study on Cybercrime*. At the Third Session of Intergovernmental Expert Group Meeting on Cybercrime in 2017, the representatives exchanged views on the *Comprehensive Study on Cybercrime*, and on many other issues, such as legislation, best practices, technical assistance, and international cooperation in combating cybercrime.

The Open-ended Intergovernmental Expert Group Meeting on Cybercrime and the Group of Governmental Experts on Information Security under the United Nations General Assembly (First Committee) are two important mechanisms on international cyberspace governance at the UN. Therefore, the rules and mechanisms are undoubtedly the focus among the major actors.

The Contest for Establishing an International Governance Mechanism against Cybercrime

Prior to the formation of the United Nations expert group on cybercrime, the Council of Europe formulated the *Budapest Convention on Cybercrime*, a regional convention on combating cybercrime, in 2001. The Council of Europe continually invited non-EU countries to participate in the formulation and implementation of this Convention through aid cooperation, so as to elevate it to a global legal standard for combating cybercrime. So far, in addition to the EU countries, the signatories of the Convention include 57 member states and 15 observer states, such as the United States, Japan, Australia, and Sri Lanka. *Budapest Convention on Cybercrime* is the first and only international convention on cybercrime in the world so far.

In the past, regional laws would normally be implemented and practiced before being turned into international laws by international organizations. However, Western countries believe that the *Budapest Convention on Cybercrime* may be directly applied internationally without the United Nations having to enact another international law on cybercrime. This places the Council of Europe above the UN, and rules out its role of the United Nations in combating cybercrime. Therefore, China, Russia, Brazil, and other developing countries hold that the *Budapest Convention on Cybercrime* is a regional convention formulated by a small number of countries. It does not have the true openness and broad representation typical of global conventions, and therefore cannot reflect the general concerns of other countries, especially the majority of developing countries.

For example, the Convention has a limited scope, focusing only on crimes targeted at computer hardware systems and neglecting cyberterrorism or other traditional crimes committed using the Internet. Furthermore, it has stringent requirements and high standards for cybercrime investigation procedures, and its wide-ranging provisions on cross-border investigation and evidence collection violate judicial sovereignty. Therefore, it is generally difficult for developing countries to accept and implement the Convention. Instead, developing countries such as China and Russia have promoted the development of a global convention against cybercrime within the UN framework, and facilitated the establishment of the UN EGM on Cybercrime in 2010, by the CCPCJ to study cybercrime and put forth proposals.

The fundamental problem is that the UN remains the most legitimate and authoritative international organization in international affairs since the Second World War. It must not be replaced by any regional organization. Otherwise, there will be a serious impact on the post-war security system, thereby threatening global security and stability.

1.2 The International Cybersecurity Dilemma

The Snowden Leak of June 2013 is an important milestone in the history of international cybersecurity. It raised the curtain for an intelligence-oriented and militarized cyberspace, changing the course of international cybersecurity and triggering a cybersecurity crisis worldwide.[1] After the leak, interstate strategic competition in cyberspace has been intensified and global efforts in cyberspace governance is on the verge of collapse. Several factors of cybersecurity technology, commerce, and political security have combined to drive global cybersecurity into a dilemma.[2] Thus, an in-depth analysis ought to be conducted on these factors and well-targeted governance mechanisms ought to be established, so as to get out of the current dilemma (*see* Exhibit 1.3).

1.2.1 The Snowden Leak and the Global Cybersecurity Dilemma

The Snowden Leak has aggravated the global cybersecurity scenario, causing international conflicts to arise one after another in the realm of network. The danger of an outbreak of a cyber arms race is imminent. In the meantime, cyberspace governance has fallen into trouble and the current international security architecture has been incapable of dealing with challenges it has confronted. This has created a cybersecurity dilemma.

---

1 Chuanying Lu, "Analysis of the Predicaments of Current Global Cyberspace Governance," *Contemporary International Relations*, no. 9 (2013): 44–47.

2 Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations* (Oxford: Oxford University Press, 2017).

Exhibit 1.3 The 2017 China Internet Security Conference with the theme of security governance issues, such as cybercrime, government, enterprise security, and artificial intelligence held in Beijing, September 12, 2017

Source: Visual China

As is seen in reality, the current cybersecurity dilemma has grown out of three difficult scenarios. Specifically, ongoing changes in the realm of global cybersecurity have given rise to competition in the field among major powers. Also, global efforts in cyberspace governance are on the verge of collapse, failing to deal with crises and the escalation of conflicts. Moreover, characteristic as it is, international cybersecurity leads to low-intensity confrontations among the major powers in cyberspace. Tricky as they are, the three scenarios—strategic competitions among global powers, the international institution in a mire, and conflicts and confrontations—have finally driven cybersecurity into a dilemma.

Cybersecurity as a Contest among Major Countries

Since the Snowden Leak, the concept of cybersecurity has undergone fundamental changes from the original concepts of network security and information security. National governments have generally raised cybersecurity to the level of comprehensive national security. Prior to this, the international community's perception of cybersecurity was confined to cybercrime, computer network security, and information security. The Snowden Leak triggered major discussions on cybersecurity issues, gradually changing the perceptions of cybersecurity globally.[3] The concept and connotation of cybersecurity is expanding and new security issues such as big data and national security, Internet ideology, cyber warfare, and personal data protection, are emerging on the Global Cybersecurity Agenda. The current concept and connotation of cybersecurity demonstrate the trend of cybersecurity permeating politics, economy, culture, society, and military.

The *National Cybersecurity Strategy* issued by the Chinese government defines dozens of cybersecurity threats in five major aspects: the harm of network penetration to political security, the threat of cyberattacks to economic security, the erosion of cultural security by seditious information on the Internet, the destruction of social security by cyberterrorism and cybercrime, and the intensifying international competition in cyberspace (*see* Exhibit 1.4).[4] In a sense, cybersecurity is not only integral to a comprehensive view on national security, but also further enriches its connotation. Therefore, national governments are placing a greater emphasis on cybersecurity in a bid to respond to the threats and challenges to national security.[5]

---

3 Joseph Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2017): 44–71.

4 Office of the Central Cyberspace Affairs Commission, Cyberspace Administration of China, "National Cybersecurity Strategy," accessed March 19, 2019, http://www.cac.gov.cn/2016-12/27/c1120195926.htm.

5 Editorial Note: The comprehensive national security concept was proposed by the Chinese national leaders at the First Plenary Session of the Central National Security Council on April 15, 2014. Cybersecurity is closely related to ten other security-related areas and has enriched the connotation of information security. It is a comprehensive security concept with comprehensive security concept at the top, the other 10 security-related areas in the middle, and cybersecurity interlinked with those 10 areas at the bottom.

Exhibit 1.4 Wu Jianping, vice chairman of the China Internet Association, stressing China's proposal on anti-cyber wars at the Fifth China–US Internet Forum, Washington DC, December 7–8, 2011

Source: CNSphoto

The rising awareness of cybersecurity issues has further prompted major countries to increase their investment of resources in cybersecurity, focusing on cybersecurity as a key area for strategic competition. The international community has also upgraded cybersecurity to the strategic level of comprehensive national security. Major countries including China, the United States, and Russia, have issued national cyber strategies, reorganized their cybersecurity governance structures, and raised the importance of cybersecurity on their national agenda. The Chinese government stated in the *National Cybersecurity Strategy* that "cybersecurity has a bearing on the shared interests of mankind, on global peace and development, and on the national security

of all countries."[6] Russia has clearly stated that it will strengthen its military prowess in cyberspace. The 2016 edition of the *Doctrine of National Information Security of the Russian Federation* pointed out that information plays an important role in achieving goals in their prioritized development strategy.[7] The US government formulated the *Cyberspace Policy Review* as early as 2009 and defined cyberspace as the fifth strategic space after land, sea, air, and outer space.[8]

Cyber forces, intelligence, law enforcement, and administration have become important means of supporting national strategies and responding to cyber crises. With the widespread application of information technology, the size and importance of critical infrastructure on which the operations of economy, finance, energy, and transportation depend are correspondingly on the rise. Under this general trend, cybersecurity has become a new source of risk in the political, economic, cultural, social, military, and more fields. Faced with the increasingly complex cybersecurity environment, countries have tended to enhance their cyber military forces to meet new tasks and challenges. Statistics show that nearly 100 countries have built cyber forces and an increasing number of countries are beginning to focus on the building of cyber defence capability.

The Chinese government stated in the *International Strategy of Cooperation on Cyberspace* that

> "enhanced defense capability in cyberspace is an important part of China's endeavor to modernize its national defense and armed forces, which complies consistently with its strategic guidelines on active defense. China will give full play to the important role of the military in safeguarding the country's sovereignty, security, and development interests in cyberspace. It will expedite the development of a cyber force and enhance its capabilities in situational awareness, cyber defense, in supporting state activities and international cooperation, and in preventing

6 Office of the Central Cyberspace Affairs Commission, Cyberspace Administration of China, "National Cyberspace Security Strategy," accessed March 19, 2019, http://www.cac.gov.cn/2016-12/27/c1120195926.htm.

7 Jie Ban and Chuanying Lu, "The Adjustment of Russia's Cyberspace Strategy Seen from the Federal Government Information Security Doctrine," *Information Security and Communication Secrecy*, no. 2 (2017): 81.

8 The White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," accessed November 28, 2019, https://www.energy.gov/sites/prod/files/cioprod/documents/Cyberspace_Policy_Review_final.pdf.

major cyber crisis. China will also advocate safeguarding cybersecurity and maintaining national security and social stability."[9]

In the *Doctrine of National Information Security of the Russian Federation*, the Russian government stated that it is necessary to "strategically suppress and prevent military conflicts arising from the use of information technology, and at the same time improve the information security system of the armed forces of the Russian Federation, and other armed forces, military units, and institutions, including reinforcing their power and improving their approaches when facing conflicts in the information sphere."[10]

The development of a cyber military power is an emerging strategic field, and the loss of its balance can easily trigger an arms race. Recently, the United States, the United Kingdom, and other countries have actively developed offensive cyber forces, pursued absolute security in cyberspace, and implemented cyber deterrence strategy. This is likely to drive a new form of arms race in cyberspace. In particular, the United States and the United Kingdom have announced high-profile offensive cyber operations in Afghanistan and Iraq and are constantly seeking international and domestic laws that support such operations. This has further accelerated the development of an arms race in cybersecurity.[11]

Confrontation over Building an International Mechanism Aggravates the Cybersecurity Dilemma

The evolution of the concept of cybersecurity and the intensification of the national strategic rivalry have brought new challenges to the establishment of mechanisms for international cybersecurity governance. After the Snowden Leak, the international community attempted to reach a consensus on rules governing international cyberspace. In 2014, NETmundial, the Global Multistakeholder Meeting on the Future

9 Office of the Central Cyberspace Affairs Commission, Cyberspace Administration of China, "National Cyberspace Security Strategy," accessed March 19, 2019, http://www.cac.gov.cn/2016-12/27/c1120195926.htm.

10 Jie Ban and Chuanying Lu, "The Adjustment of Russia's Cyberspace Strategy Seen from the Federal Government Information Security Doctrine," *Information Security and Communication Secrecy*, no. 2 (2017): 81.

11 Joseph Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2017): 44–71.

of Internet Governance, was held in Brazil. The meeting discussed the international governance mechanisms in response to large-scale network surveillance and offensive cyber operations. The 2014–2015 UN GGE reached a consensus on cyber norms, such as the norms of responsible state behavior, the application of international law in cyberspace, and confidence-building measures.[12] However, the Net Mundial meeting was soon stopped, and the 2016–2017 UN GGE failed to issue a final consensus report due to differences among the parties in terms of state responsibility and countermeasures. As a result, the efforts of the international community in building an international governance mechanism for cybersecurity have stagnated.[13]

In addition, the difficulty in building the governance mechanism is also reflected in the fact that existing norms have not been effectively implemented. For example, in the *Report of the UN GGE 2015* member states reached a consensus that "a state ought not to conduct or knowingly support any ICT activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure." However, incidents such as the attack on Ukrainian power plants occurred repeatedly. The 2015 Report also proposes that in considering the application of international law to state use of ICTs, national governments should follow the principal of sovereignty of all states, the principal of settling international disputes by peaceful means, and the principle of non-intervention in the internal affairs of other states. In practice, however, the cyber sovereignty of many countries has been repeatedly violated and interference in the internal affairs of other countries has occurred frequently. In particular, when dealing with cyber conflicts, unilateral sanctions are often used rather than peaceful means.[14]

---

12 General Assembly, United Nations, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/70/174), (New York, 2015).

13 Michele G. Markoff, "Explanation of Position at the Conclusion of the 2016–2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Tele-communications in the Context of International Security," accessed March 19, 2019, https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm. See also Krutskikh Andrey, "Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in This Sphere," accessed March 19, 2019, http://www.mid.ru/en/foreign_policy/news//asset_publisher/cKNonkJE02Bw/content/id/2804288.

14 General Assembly, United Nations, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/70/174), (New York, 2015).

The contest among countries is one of the main causes for the failure of international governance mechanisms. This can be seen in the differences in the governance concepts and policies held by different countries. Developing countries emphasize cyber sovereignty, uphold the main role of national governments in cyberspace governance, and support the central position of the UN in the development of international rules. Developed countries highlight Internet freedom, advocate the multistakeholder model, and query the effectiveness of the UN platform on cybersecurity governance. As the cyberspace rulemaking process intensifies, the differences between developing and developed countries are increasingly difficult to bridge in the short term. In turn, the opposition has exacerbated the confrontation between the developed and developing countries in international governance mechanisms.[15] The United States and other Western countries promoted like-minded states through the G7 platform, while BRICS and the Shanghai Cooperation Organization (SCO) have become the main platforms for developing countries to promote their governance concepts and policies.

The failure of the international governance mechanisms has not only left the relevant mechanisms of cyber crisis management and dispute settlement at the international level in a limbo, but has greatly affected some important bilateral dialogues and cooperation. For example, the US–Russia Cyber Working Group was suspended because of the Snowden Leak, and recovery in the short run was difficult. The China–US Cybersecurity Working Group was also suspended indefinitely after the US prosecution of Chinese military personnel. Later, jointly promoted by the leaders of the two countries, the China–US High-Level Joint Dialogue on Combating Cyber Crimes and Related Issues was established, and was later upgraded to China–US Law Enforcement and Cybersecurity Dialogue (*see* Exhibit 1.5). The China–US dialogue is mainly focused on combating cybercrime and does not involve cyber military issues.[16] Therefore, in the absence of the mechanisms for crisis management and dispute resolution, conflicts between countries in cyberspace can escalate easily. This encourages unilateral counter-attacks, thus exacerbating the cybersecurity dilemma.

---

15 Chuanying Lu, "Analysis of the Current Dilemma of Global Governance in Cyberspace," *Contemporary International Relations*, no. 9 (2013): 44–47.

16 The White House, "FACT SHEET: President Xi Jinping's State Visit to the United States," accessed March 19, 2019, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

Exhibit 1.5 The Second China–US High-Level Dialogue on Combating Cybercrime and Related Issues, held in Beijing, June 14, 2016

Source: Visual China

The Low-Intensity Confrontations Being Normalized and Taking Place Frequently

Under existing conditions, cyberattacks are less violent and lethal compared with real wars. In military science, violence refers to the physical and psychological harm done to the human body—the first target of violence. The nature of cyber weapons and cyberattacks determines that they are far less violent than traditional weapons and wars. As cyber weapons lack the symbolic attributes of physical weapons, their hidden or low-key attributes make them very different from traditional weapons, such as

warplanes and artillery shells used in physical wars.[17] Therefore, most cyber operations are considered low-intensity conflicts below the threshold of war. Thus, even if cyber operations conducted by one state may endanger the national security of others, the existing international laws do not have clear regulations on such behaviors, as these operations are not serious enough to trigger a war. Consequently, cyber war can be regarded as a new type of special warfare, and thereby, no consensus has been reached on its definition, connotation, or influence.

The aforementioned features of cyberattacks only serve to encourage more cyber operations in various forms, triggering further cyber conflicts. After the end of the Cold War, overall peace has been maintained among major countries, and direct confrontation is extremely rare. The PRISM surveillance program, Stuxnet, the Sony Pictures hacking, Russian hacker interference in the US presidential election, and other cybersecurity breaches have all shown that state actions in cyberspace are increasingly frequent, while the means, targets, and motives of such actions are becoming more diverse, triggering intensifying conflicts. Therefore, some scholars define network interactions between cyber warfare and intelligence-gathering as low-intensity cyber conflicts. Although these actions are not regarded as a form of war, this type of cyber conflict is much more intense than intelligence-gathering.

On the surface, low-intensity cyber conflicts do not have serious consequences to national and international security. However, high-frequency low-intensity conflicts may have accumulative effects, and eventually cross the threshold at a trigger point, causing fierce conflicts that endanger international security.[18]

For example, the sanctions imposed by the United States on Russia against the Russian hacking of the US presidential election indicate the United States is changing its original perception of cyber operations. In response to the hacking, the United States imposed cross-domain sanctions on Russian entities and individuals, and exerted diplomatic pressure on Russia, by expelling Russian diplomatic officials, and closing the Russian consulates in the United States (*see* Exhibit 1.6).[19] Such low-intensity cyber conflicts must be a focus of the rules in international cyberspace governance.

---

17 Thomas Rid, *Cyber War Will Not Take Place*, trans. Xu Long Di (Beijing: People's Publishing House, 2017), 58.

18 Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (Oxford: Oxford University Press, 2015), 20–23.

19 Chuanying Lu, "The Difficulties and Mechanisms of Cybersecurity Governance from the Perspective of International Politics—with the Hacker Gate in the US Presidential Election as an Example," *International Outlook*, no. 4 (2016): 33.

Exhibit 1.6 Senior US intelligence officials at a congressional hearing to testify that Russian hackers intervened in the US election, Washington D.C., January 5, 2017

Source: Visual China

1.2.2 The Reason behind the Security Dilemma

The international cybersecurity dilemma and the three phenomena—the contest among major countries, the failure of the international governance mechanism, and the constant low-intensity cyber conflicts—influence each other reciprocally, causing a systemic security predicament that is seemingly impossible to resolve. To reach a solution, we ought to analyze the reasons behind it, study the technical characteristics of cybersecurity and the attributes of Internet products and services, and further examine the logic of international cybersecurity on this basis.

China and International Cybersecurity

The Logic of Cyber Technology Security

Technology has always been an important part of the study in international relations. The advancement of science and technology has directly or indirectly transformed international relations. From the perspective of international cybersecurity, the logic of cyber technology security has led to two new problems—attribution and cyber defense. These have a direct impact on the strategic choices of major powers in cybersecurity and international cyberspace governance.

Cyberspace is characterized by anonymity, openness, and insecurity. Anonymity and openness are related to Internet architecture. Anonymity means that the identity of Internet users remains anonymous and users can avoid being traced by using encryption and proxies. Openness means that the Internet is connected by a unified standard protocol system and all devices linked to the Internet are interconnected. Insecurity means that as all devices and systems are designed by people, in theory, errors, major ones and minor ones alike, can be found in any device or system, and these may be exploited. Cybersecurity originally referred to the damage to and protection of the confidentiality, integrity, and availability of computer systems and devices. Hence, two important goals of national cybersecurity strategies are the protection of data and critical infrastructure.

Based on the abovementioned features of cyber technology, cybersecurity faces issues of attribution and cyber defense. The resulting logic is that cybersecurity favors the cyber attackers, and rational decision makers tend to strengthen capacity building and increase resource investment to defend their own cybersecurity, so as to gain strategic competitive advantage.

1. **Attribution**. The openness and anonymity of cyber technology makes it difficult to trace the original attacker. It is hard to use existing cyber technology to detect the real attackers of the Advanced Persistent Threat (APT) and punish them. Attribution is the core technology and the most controversial area in international cybersecurity. Using this core technology, we can determine the original attacker, thereby understanding the nature of the international cybersecurity incident and deciding what legal measures to take.[20] Due to the anonymity and openness of the Internet along with various identity-hidden technologies, attackers often camouflage their behavior and identity, and this

20 Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009).

increases the difficulty of cyber attribution. In the many cybersecurity incidents that have occurred, almost no evidence could be provided to identify the original attacker. Therefore, it is difficult for the international community to take its position between the attacker and the attacked and punish the attacker.

This can be illustrated by the Stuxnet incident. The United States and Israeli intelligence agencies that developed the virus have never publicly commented on it, and nobody knew the truth until it was exposed by the media many years later. The Stuxnet virus and its variants have since infected many power plants around the world, becoming one of the major threats to national critical infrastructure. However, there is no mechanism that can spur the international community to condemn or sanction the cyber criminals exposed by the media.[21] Similar cybersecurity incidents, such as the attacks on Ukrainian power plant and the Estonian banking system, still occur frequently, further reducing the confidence of governments and peoples in international cybersecurity (*see* Exhibit 1.7).

2. **Cyber Defense.** In theory, cyber technology is replete with vulnerabilities because networked devices and the codes that run them are designed by humans, and error is unavoidable. Since a device naturally has defects and no device is fully secured, all devices connected to the Internet may become targets of cyber attackers. With increasing informatization, countries are faced with the urgent task of protecting their critical infrastructure.

In practice, vulnerabilities are widespread in the critical infrastructure of different industries and enterprises, and the costs of government protection are enormous. For example, the United States divides its critical infrastructure into 17 categories, but the actual coverage of this infrastructure has never been publicly announced. To fully ensure the security of its critical infrastructure, a country needs to expend enormous amounts of manpower, technology, and financial resources. As operators of many critical infrastructure systems are enterprises in the private sectors, they have limited resources and are also unwilling to disclose information on the cyberattacks. Meanwhile, because of the complexity of cyber technology, these cyberattackers

21 New York Times, "Obama Ordered Wave of Cyberattacks against Iran," accessed March 19, 2019, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

Exhibit 1.7 Experts trying to solve the large-scale cyberattack at the Ukrainian airport in June 2017

Source: Visual China

hide behind the cloak of anonymity, making it even harder for the targets to actively defend themselves.

The Logic of Business Security

Businesses are a major driving force for the evolution of the international system. Structural liberalism holds that interdependence theory has been created side by side with the development of international trade. From the perspective of international security, commerce and trade are important factors. For example, the control of high-tech exports by the Wassenaar Arrangement is an important mechanism for affecting international security through commerce and trade.

From the perspective of international cybersecurity, as more and more cyber technologies and Internet products and services are dually used by the military and civilians, national security and politics are gradually changing the logic of business security. This has led to discussions on "technological nationalism." Therefore, business security logic is an important factor contributing to the international cybersecurity dilemma. Only by recognizing the nature of the problem and implementing corresponding international governance measures from the perspective of supply chain security can the cybersecurity dilemma be effectively alleviated.

The application of Internet products in the military and by civilians is gradually changing the traditional logic of business based on the concepts of competition, openness, and cooperation. In network technology, the dual-use technology in products and services is becoming widespread, and thus has a greater impact on traditional business logic. Internet companies, such as Microsoft, Google, Twitter, Facebook, and Amazon, have cooperated with the US National Security Agency to provide massive amounts of user information to US intelligence agencies without the knowledge of consumers and other countries.[22] Furthermore, US cyber military and intelligence agencies, including the National Security Agency and the Cyber Command, have tried to discover vulnerabilities in the Internet services and products of large technology enterprises, and develop them into weapons for cyber operations. Therefore, military and government networks are not the only targets, and civilian critical infrastructure are also not exempted from cyberattacks.

Due to the dual use of Internet products and services, large Internet companies have found it difficult to maintain neutrality in their business operations. The military and security departments also need to use advanced Internet products and services to enhance their capabilities. For example, Amazon provides a cloud service platform to several US military and intelligence agencies to raise the informatization level of the US military.[23] In this case, governments do not trust the products and services provided by foreign Internet companies. As a result, they are more inclined to use the equipment and services provided by domestic companies to ensure that Internet companies do not collude with their governments to endanger national cybersecurity.

---

22 The Guardian, "NSA Prism Program Taps in to User Data of Apple, Google, and Others," accessed March 19, 2019, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

23 The Sputnik News, "Amazon Collects Another US Intelligence Contract: Top Secret Military Computing," accessed March 19, 2019, https://sputniknews.com/military/201806011065023768-amazon-collects-another-us-intelligence-contract.

Consequently, governments have begun to reexamine the commercial activities of these US companies in their countries and have strengthened their security review on the products and services of foreign Internet companies (*see* Exhibit 1.8).

As the cybersecurity dilemma continues to intensify, a new business logic is emerging in the international cybersecurity arena, which is becoming a new challenge for companies, countries, and even the international economic and security systems. This trend will undermine the security of the supply chains, leading to serious consequences

Exhibit 1.8 A public hearing on China's Huawei and ZTE's role in obstructing US national security investigations held by the US House Intelligence Committee, September 13, 2012

Source: Imagine China

for global trade. For example, a large part of the China–US trade disputes is related to cooperation in the digital economy between the two countries. The "Section 301 Investigations" conducted by the United States specifically addressed cybersecurity issues. The US government also seeks to expand the power of the Committee on Foreign Investment in the United States (CFIUS) and advocates further restrictions on Chinese investment, personnel exchange, and cooperation in science and technology, such as integrated circuit chips and artificial intelligence.

The Logic of International Political Security

In the post-Cold War era, international political security has largely fallen into two main interaction modes of the major state actors: power politics and economic interdependence. As for great power relations, it has seen power struggles as well as economic interdependence and cooperation.[24] As a new territory, cyberspace has yet to build an established regime, and thus, safeguarding security in this field is subject to state capacity. Accordingly, the interaction mode of the major powers in the new-borne field of cybersecurity tends to incline toward power politics instead of cooperation.[25] Although global cybersecurity has both offensive and defensive sides, it seems that the offensive has outweighed the other in the present situation, and this has trapped the great powers in the interaction mode of power struggles. On the one hand, cybersecurity lays the foundation to gain advantages in national security. Thus, national capacity is both a necessity to safeguard cybersecurity and crucial for gaining more advantages in national security.

Accordingly, the logic of political security featuring power politics gains popularity in cyberspace, such as hegemony, absolute security, unilateralism, and preemptive strike. On the other hand, cybersecurity threats are pervasive, regardless of national boundaries. Thus, countries are objectively required to strengthen cooperation and make a joint effort to cope with such threats. Liberalist theories of interdependence, collective security, and multilateral cooperation play a significant role in solving the cybersecurity dilemma. However, after the Snowden Leak, governments have focused

24 Robert Keohane and Joseph Nye, *Power and Interdependence*, trans. Men Honghua (Beijing: Peking University Press, 2012).

25 Jian Yang, *Power and Wealth of the Digital Frontier* (Shanghai: Shanghai People's Publishing House), 67–88.

on cyber threats, and the realist logic of political security wins the upper hand of liberalism. Global cybersecurity is then falling into a strategic game and an arm race.

From the national level, cybersecurity, as a sort of non-traditional type, imposes challenges on governments as well. Traditionally, security is a state affair and national strength plays the decisive role. Accordingly, a country that surpasses others in fields of military strategies, operations, and science and technology definitely feels more secure. This turns out to be a different situation in terms of cybersecurity. As a type of non-traditional security, cybersecurity and informatization tend to be negatively correlated. That is, the higher the level of informatization of a country, the more threats it faces. However enormous an effort an advanced country has made in safeguarding its cybersecurity, threats are never reduced, but keep increasing as there are too many networked devices and critical infrastructures. Consequently, a government has little confidence in its cyber defense and threats have continuously been present. This leads to an absence of transparency in the national cybersecurity policy of major countries. Preferring the realist logic of political security, states find it more difficult to cooperate in the field.

1.2.3 Building a Governance Mechanism for International Cybersecurity

The global cybersecurity dilemma involves multilevel factors as mentioned before. At present, the governance on this issue has been mainly restricted to the field of international politics, without touching the roots of the dilemma. A well-targeted global governance mechanism is to be built for technological, business, and political security to alleviate the dilemma in global governance on cyberspace.

Governance in Attribution and Cyber Defense

Technologically, cybersecurity is plagued with difficulties in attribution and defense. Attribution is actually an issue of accountability. As no objective or neutral international organization takes charge of investigation in the case of a cybersecurity leak, the overwhelming majority of state-level cyberattacks have ended up with inconclusive outcomes. Consequently, more cyberattacks are being plotted, disturbing the international security order. Some scholars believe that a UN body that is in charge of

attributing cyberattacks and conducting investigations in the case of a cyberattack would definitely be a great deterrent on attackers in cyberspace, so that frequent cyberattacks may be brought under control. However, this solution has not been practical so far, as attribution technology is monopolized by some powers that are unwilling to share it nor assist the UN in building attribution capabilities. The international community should be clearer on this issue, remove obstacles faced by the small number of countries, and help the UN advance its work in attribution.

The problem of cyber defense can be overcome by establishing a comprehensive defense system and by formulating a higher security standard. The Wooden Bucket Theory is also applicable to the development of international cybersecurity.[26] From the perspective of Internet products, the short board of any component may affect the overall safety level of the product. Thus, the international community must raise the standards for Internet products and services.

Due to the borderless nature of cybersecurity, countries with relatively weak defense capabilities are also the most vulnerable targets of anonymous cyberattackers. At the national level, such countries are important links that determine the international cybersecurity situation. Therefore, solving the problem of cyber defense depends not only on improving the cyber capabilities of national governments, but also on upgrading overall global cybersecurity defense. Countries must be encouraged to establish a comprehensive cybersecurity protection system, and to cooperate in the protection of critical infrastructure and other related fields. It is also necessary for countries to prioritize capacity building in cybersecurity as a task in governance, and to improve the cybersecurity of developing countries.

Governance in Supply Chain Security

Dual-use goods and technologies for military and civilian are changing the traditional business logic, resulting in the rise of techno-nationalism. The relationship between national security and the economy shall be addressed properly and fundamentally. To avoid impacts from nationalism, supply chain security is a reasonable and professional

26 Editorial Note: The Wooden Bucket Theory (also known as the Cannikin Law) explains how the capacity of a bucket is determined not by the longest wooden stave but by the shortest. When applying this concept to cybersecurity, the most vulnerable link in cybersecurity (the weakest country) determines the overall global network security.

perspective from which to approach the issue of global governance of dual-use network technologies for military and civilian purposes.

Technological nationalism is mainly exhibited as follows: trusting only in domestic products and excluding the use of foreign products, impeding the normal investment activities of other countries, and refusing to sell corresponding technology and products to other countries. This is done by maintaining the monopolistic advantages in core technologies and products so as to generate a deterrent effect. At present, all the major countries have shown a tendency toward technological nationalism in their cybersecurity policies, especially the Trump administration that first prohibited the Federal government from using Russia's Kaspersky Internet security software and then increased its review of Chinese investment in the United States.[27]

Technological nationalism may distort international trade and undermine the principle of fair trade. At the same time, the security concept that upholds the belief that domestic products and services are safer than foreign products and services cannot withstand scrutiny. Under normal circumstances, product safety depends on its product quality, and not country of origin. Only in specific circumstances can there be a situation where national security is threatened by foreign products. For example, a manufacturer may cooperate with a country's security department to deliberately set up loopholes and backdoors to undermine the cybersecurity of other countries. Strengthening the international governance of supply chain security is an effective solution to the problem of dual-use technology by the military and civilians.

First, the international community ought to furnish a more secure standard system for network equipment and products. Second, governments must agree to not implant backdoors and loopholes in cybersecurity products for civilians. In the *Digital Geneva Convention*, Microsoft of the United States advocated governments to "refrain from attacking technology companies, the private sector, and critical infrastructure."[28] Finally, countries ought to focus on the review of cybersecurity and services rather than reject foreign products and investments that violate trade rules. The state must enhance its ability to conduct security reviews of ICT devices and services in order to build public confidence in their network products and services. When restoring trust in enterprises, a country can build

27 Jeanne Shaheen, "The Russian Company that is a Danger to Our Security," accessed March 19, 2019, https://www.nytimes.com/2017/09/04/opinion/kapersky-russia-cybersecurity.html.

28 Kate Conger, "Microsoft Calls for Establishment of a Digital Geneva Convention," accessed March 19, 2019, https://techcrunch.com/2017/02/14/microsoft-calls-for-establishment-of-a-digital-geneva-convention.

a certain degree of deterrence. For example, the Chinese government issued the *Measures on the Security Review of Network Products and Services* to improve its control of security over network products and services, reduce cybersecurity risks, and maintain national security.

Confidence-Building Measures

Confidence-building measures help redirect the course of political security thinking. Enhanced governance at technological and business levels makes a country less perceptive to threats and thus, it can help redirect the interaction mode of major powers on cybersecurity governance from power politics to economic interdependence. Confidence-building measures were initially formed between military alliances during the Cold War and have now expanded to include other non-military areas. The UN GGE has always regarded confidence-building measures as an important component in establishing cyber norms. Confidence-building measures in international cybersecurity include measures in three aspects—stability, cooperation, and transparency. Stability measures include strengthening mechanisms for crisis management, conflict prevention, and hotline establishment. Cooperation measures include sharing data and information, conducting anti-cyberterrorism drills, and fighting cybercrime. Transparency measures include providing information on cyber strategy, national defense strategy, organizational structure, and personnel roles. Confidence-building measures are an area where countries have relatively fewer differences. The difficulty lies in their implementation. Based on previous achievements, the Fourth UN GGE (2014–2015) proposed a higher level of confidence-building measures, including the identification of points of contact at the policy level, the establishment of crisis management mechanisms, the sharing of information, and the exchanging of best practices. It also proposed strengthening the technical, legal, and diplomatic mechanisms on bilateral, sub-regional, regional, and multilateral bases, enhancing cooperation on law enforcement, and expanding the coordination, exercises, and best practices among computer emergency response teams (*see* Exhibit 1.9).[29]

Given the current situation of cybersecurity and its risks and threats, the confidence-building measures proposed by the UN GGE are targeted at and conducive to

29 General Assembly, United Nations, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/70/174), (New York, 2015).

Exhibit 1.10 The Eighth China–US Internet Forum at Microsoft headquarters, Seattle, United States, September 23, 2015

Source: CNSphoto

group has been disrupted since Russia accepted Snowden's request for asylum. The Russian hacking interference in the US presidential election resulted in the suspension of confidence-building measures and worsened relations between the two countries. It will be difficult for both countries to restore their dialogue on cybersecurity in the short term, demonstrating that it is difficult to foster trust in cyberspace.[30] Therefore, from the perspective of bilateral relations, confidence-building measures are key to resolving the cybersecurity dilemma. All parties need to reach a consensus so as to overcome difficulties and advance together.

30 Clint Watts, "How Russia Wins an Election," accessed March 19, 2019, https://www.politico.com/magazine/story/2016/12/how-russia-wins-an-election-214524.

1.3 Building a Community of Shared Future in Cyberspace

To solve the current cybersecurity dilemma, Chinese President Xi Jinping proposed the idea of building a community of shared future in cyberspace.

1.3.1 Five Proposals to Build a Community of Shared Future in Cyberspace

In December 2015, President Xi stated at the opening ceremony of the Second World Internet Conference that

> Cyberspace is the common space of activities for mankind. The future of cyberspace should be in the hands of all countries. Countries should step up communication, broaden consensus, and deepen cooperation to jointly build a community of shared future in cyberspace.[31]

In line with the concept of building a community of shared future in cyberspace, President Xi put forward five proposals. First, accelerate the building of global network infrastructure and promote interconnectivity. Second, build an online platform for cultural exchange and mutual learning. Third, promote the innovative development of the digital economy for common prosperity. Fourth, maintain cybersecurity and promote orderly development. Fifth and finally, build an Internet governance system to promote equity and justice (*see* Exhibit 1.11).

The five proposals put forward by President Xi to build a community of shared future in cyberspace is of great significance in the following three aspects. First, it highlights the systematic nature of a community of shared future in cyberspace. These proposals comprise specific tasks and objectives, as well as challenges and solutions in five aspects—infrastructure construction, online cultural exchange, the development of digital economy, the maintenance of cybersecurity, and Internet governance. Second, it expounds the path China has taken to build a community of shared future in cyberspace. At the Second World Internet Conference, President

31 Jinping Xi, "Speech at the Opening Ceremony of the Second World Internet Conference," accessed March 19, 2019, http://www.xinhuanet.com/politics/2015-12/16/c_1117481089.htm.

Exhibit 1.11 Chinese President Xi Jinping addressing the Second World Internet Conference in Wuzhen, Zhejiang Province, December 16, 2015

Source: CNSphoto

China and International Cybersecurity

Xi proposed to speed up the construction of infrastructure and stressed the following points:

> The essence of the Internet is connectivity, and herein lies the value of information. We should strengthen the building of IT infrastructure for information to travel on a smooth road. Only in this way can we narrow the digital gap between different countries, regions, and communities, and ensure the free flow of information resources.

Cultural exchange was also emphasized at the conference: cultures and civilizations are enriched through exchange and mutual learning. The Internet is an important carrier to spread mankind's cultures and promote positive energy. President Xi advocated the development of the digital economy and pointed out that the global economy is on a difficult path to recovery, including the Chinese economy which is also under downward pressure. Solutions lie in innovation-driven development, which will open up new horizons. He attached great importance to cybersecurity by saying that

> security and development are like the two wings of a bird or the two wheels of a cart. Security ensures development, and development is what security is aimed at. Cybersecurity is a global challenge. No country can stay aloof or remain immune from it. Maintaining cybersecurity is the shared responsibility of the international community.

He proposed to build an Internet governance system in the following:

> International cyberspace governance should feature a multilateral approach with multiparty participation. It should be based on consultation among all parties, leveraging the role of various players, including national governments, international organizations, Internet companies, technology communities, non-government institutions, and individual citizens. There should be no unilateralism. Decisions should not be made with one party calling the shots, or [by] only a few parties discussing among themselves.

Third, President Xi proposed the China Solution and the main areas for multilateral cooperation, which are as follows:

> In the construction of infrastructure, China is now implementing the Broadband China Strategy. It is estimated that by 2020, the broadband network in China will basically cover all the villages. The "last kilometer" of Internet infrastructure will be linked thanks to this strategy, and more people will have access to the network. China stands ready to work with all parties concerned to come up with more investment and technical support to jointly advance the building of global Internet infrastructure, and enable more developing countries and their people to share in the development opportunities brought by the Internet.
>
> To promote online cultural exchange, China is willing to build through the Internet a bridge of cultural interaction for the cultures of the world to learn from each other and for people of all countries to share their feelings and enhance mutual understanding. We will work with all other countries to leverage the strength of the Internet as a communication platform, so that people of other countries will come to know more about China's culture and the Chinese people will learn more of theirs. Together, we will promote the prosperity and development of cyber culture, which will enrich people's minds and thinking, and advance human civilization.
>
> To develop its digital economy, China is now implementing the Internet Plus action plan, advancing the building of Digital China, developing the sharing economy, and supporting Internet-based innovation in all forms, with a view to improving the quality and efficiency of development. The robust growth of China's Internet has provided a large market for international enterprises and business start-ups, and we are ready to step up cooperation with all countries. Through the development of cross-border e-commerce and the building of information-economy demonstration zones, we will be able to spur the growth of worldwide investment and trade, and promote the global development of the digital economy.

> To safeguard cybersecurity, China will work with all other countries to step up dialogue and communication and effectively manage differences. We should push for the formulation of international cyberspace rules accepted by all parties, as well as an international convention against cyberterrorism, improve the legal assistance mechanism to fight cybercrime, and jointly uphold peace and security in cyberspace.
>
> To build an Internet governance system, all countries should step up communication and collaboration, improve the dialogue and consultative mechanism on cyberspace, and study and formulate global Internet governance rules, so that the global Internet governance system becomes fairer and more reasonable and reflects in a more balanced way the aspiration and interests of the majority of countries. This World Internet Conference was held precisely for the purpose of building a platform for global Internet to be shared and governed by all, and for working together for the healthy development of the Internet.[32]

1.3.2 Basic Principles for Building a Community of Shared Future in Cyberspace

The effective implementation of the aforementioned five proposals requires the dialogue and cooperation of the international community. Further, it also requires the adherence to the spirit of mutual respect and mutual understanding, and the guiding principles of peace, sovereignty, joint governance, and shared benefit.

The Principle of Peace

As a newly created territory, cyberspace has diverse actors and interests. However, since the governance mechanism and rulemaking system in cyberspace have not yet been established, conflict and confrontation arise easily among the different parties. Therefore, adhering to the principle of peace as the main guiding principle for dispute settlement is the basis for maintaining peace in cyberspace. The international community must abide by the purposes and principles of the *UN Charter*, especially the

32 Jinping Xi, "Speech at the Opening Ceremony of the Second World Internet Conference," accessed March 19, 2019, http://www.xinhuanet.com/politics/2015-12/16/c_1117481089.htm.

principle of not using or threatening to use, force, and peacefully resolving disputes to ensure peace and security in cyberspace. At the same time, under this principle, a series of related measures and regulations are needed to constrain the violation of the principle of peace, ensuring that the international community can jointly benefit from the peaceful settlement of disputes, by constraining the actions that undermine this principle.

The Principle of Sovereignty

The principle of sovereignty established by the *UN Charter* is the basic norm of contemporary international relations. It covers all aspects of state-to-state relations including cyberspace. All countries ought to respect each other's choice of cyber development path, network management model, Internet public policy, and equal participation in international cyberspace governance. Countries must not pursue cyber hegemony, nor interfere in other countries' internal affairs, nor engage in, connive in, or support network activities that endanger the national security of other countries.

Governments have the right to have a law-based management of the Internet and jurisdiction over infrastructure, resources, and activities within their own territory. They also have the right to protect their information systems and resources from threats, interference, attacks, and destruction, and the legal rights of citizens in cyberspace. Each country also has the right to develop their own Internet public policies, laws and regulations without any foreign interference. While countries exercise their rights in accordance with the principle of sovereignty, they also need to fulfill their obligations. Countries ought not to use ICT to interfere in the internal affairs of other countries. Nor should they use their own advantages to damage information, security, or communication technology products to harm the service supply chains of other countries.

The Principle of Joint Governance

As a common space for human activities, cyberspace needs to be jointly governed and developed by all countries. The diverse cyberspace actors make multilateral participation the primary means of governance for a wide range of issues in cyberspace. However, at present, some scholars and officials absolutize and generalize the multistakeholder governance model, leading to unnecessary disputes. Multilateral governance and multistakeholder governance must not be seen as two conflicting models. Instead, different governance approaches ought to be adopted in accordance with the

attributes and realities of different issues. For example, when it comes to international security, the state ought to play a leading role with the UN as the main governance platform. However, when it comes to issues involving technology, culture, and economy, the technological community, private sector, and social organizations would be more effective in improving international cyberspace governance.

The Principle of Shared Benefit

Cyberspace is the outcome of human intelligence and civilization, and humans ought to enjoy the convenience and benefits of cyberspace. At present, there are vast differences among countries in the development of their networks. The digital gap, especially the new type of digital gap caused by network technologies such as artificial intelligence and big data, has brought great challenges for developing countries. The international community ought to strengthen bilateral, regional, and international development cooperation in line with the *2030 Agenda for Sustainable Development Goals*. In particular, it ought to increase financial and technical assistance to developing countries in cyber capacity-building and help them seize opportunities to close the digital gap (*see* Exhibit 1.12).

1.3.3 The Ideological Origin of Building a Community of Shared Future in Cyberspace

First, the idea of a community of shared future in cyberspace was put forth by China to help shape international relations in cyberspace and address common challenges. Undertaking joint responsibility is a prerequisite for building such a community. This embodies win-win cooperation, joint responsibility, equal-footed consultation and mutual understanding, concerted efforts in managing disputes, and a development prospect that is open, innovative, and inclusive, featuring mutual reciprocity, harmony, and diversity. [33]

Based on human development, cyberspace faces problems such as the rapidly widening digital gap, rising cybersecurity risks, and the insidious infiltration of traditional hegemonic thinking and the Cold War mentality. In the light of these new trends, China's idea of building a community of shared future in cyberspace appeals

33 Xiaodong Zuo, "A New Chapter in International Relations in the Information Era," *People's Daily*, March 3, 2017.

Exhibit 1.12 A foreign student experiencing VR racing at the computer network technology training courses attended by 75 trainees from 20 developing countries in Guiyang, China, June 30, 2017

Source: CNSphoto

increasingly to people around the world, because it puts forth a scientific definition of cyberspace and addresses methods of cyberspace governance. This is China's major theoretical contribution to the development of cyberspace, which ought to become the guiding ideology for international cyberspace governance.[34]

Second, it is an extension of the idea of building a community of shared future for mankind. In September 2015, at the summit to celebrate the 70th anniversary of the

34 Lipo Shan, "International Responsibility of a Responsible Big Country," *People's Daily*, March 3, 2017.

founding of the United Nations, President Xi Jinping comprehensively expounded the concept of a community of shared future for mankind. He first referred to the teachings of Confucius in the *Book of Rites*, and explained that the ideal is to create a world shared by mankind—the ultimate goal of global governance. The president went on to state that peace, development, equity, justice, democracy, and freedom are common values of mankind and the lofty goals of the United Nations. This is the basis for the values cherished to build a community of shared future for mankind, among peoples of different countries and backgrounds. At present, these goals are far from being achieved and we must continue our endeavors. To this end, President Xi proposed that the international community ought to promote the building of a community of shared future for mankind in five aspects, namely, partnership, security architecture, economic development, inter-civilizational exchange, and ecological system.[35]

On January 17, 2017, President Xi Jinping delivered a keynote speech titled "Work Together to Build a Community of Shared Future for Mankind" at the UN Headquarters in Geneva, and systematically explained the concept of a community of shared future for mankind. He stated that China proposed to build a community of shared future for mankind so as to achieve win-win development and realize the aspirations of peoples from countries all over the world. He stated that a series of widely accepted principles that emerged in the evolution of international relations, such as the Four Purposes and Seven Principles enshrined in the *UN Charter*, and the Five Principles of Peaceful Coexistence championed by the Bandung Conference more than 60 years ago ought to guide the world in building a community of shared future for mankind.

President Xi proposed that to build a community of shared future for mankind, China must stay committed to building a world of lasting peace through dialogue and consultation. It ought to build a world of common security through joint efforts, a world of common prosperity through win-win cooperation, and an open and inclusive world through exchange and mutual learning.

Finally, the president mentioned that China ought to make the world clean and beautiful by pursuing green and low-carbon development. These five aspects constitute

35 Jinping Xi, "Working Together to Forge a New Partnership of Win-Win Cooperation and Create a Community with a Shared Future for Mankind—Speech at the General Debate of the 70th Session of the UN General Assembly," *People's Daily*, September 29, 2015. See also Zhang Hui "The Community with a Shared Future for Mankind: The Contemporary Development of the Social Basic Theory in International Law," *China Social Sciences*, no. 5 (2018).

the basic connotation of the community of shared future for mankind, and pave the way to achieve this goal.[36]

Third, it is the crystallization of traditional Chinese culture. The idea of a community of shared future for mankind is the continuation and development of Chinese civilization. Chinese Taoists emphasize "Tao takes naturalness as law," and attach special importance to the relationship between man and nature in accordance with objective laws. The core idea of Taoism is compatible with the modern-day concept of sustainable development. When using natural resources, we ought to take only the appropriate amount rather than "draining the pond to get all the fish."

The ancient Chinese viewed the world as an interconnected system, rather than as opposing individual components. The governance idea of building a community of shared future for mankind, which embodies the concepts of "the unity of man and nature" and "harmonious co-existence" in Chinese civilization, is the result of applying Chinese wisdom to contemporary global problems. The core idea lies in taking into account collective and individual interests, balancing immediate and long-term interests, attaching importance to sustainable development, and forging mutual support for man and nature. This is the core value that is most needed to solve today's global problems, especially in the governance of cyberspace.[37]

36 Jinping Xi, *ibid*.

37 Jian Yang, "Guide the International Governance of the New Territories with the Concept of a Community with a Shared Future for Mankind," *Contemporary World*, no. 6 (2017).

Chapter Two

CHINA'S PARTICIPATION IN INTERNATIONAL CYBERSECURITY GOVERNANCE

Since China made its connection to the Internet, the country has been a major force in promoting the application of the Internet and an active participant in international cyberspace governance. China's ideas and practices jointly constitute its roadmap for participation in cyberspace governance. With the increasingly critical role of Internet technology and its application as a double-edged sword, security issues have become not only an important factor affecting the overall stability of cyberspace, but also the primary obstacle to its development. Presently, to strike a balance between development and security, the governance of cyberspace is focused on upholding security. To this end, China has participated extensively in international cyberspace governance, explored the path for effective governance in cooperation with the international community, and committed to the building of a peaceful, secure, open, cooperative, and orderly cyberspace.

2.1 International Cyberspace Governance at a New Stage: Highlighting Security Governance

The international governance of cyberspace has always centered on the themes of development and security, and equilibrium between the two themes is a goal of cyberspace governance. However, absolute equilibrium is an ideal state to be jointly pursued by the international community, and yet practice proves that both development and security are always in relative equilibrium. Throughout history, the focus of the

international governance of cyberspace has constantly swung between development and security, depending on the primary concerns at the time. Presently, there are signs that the international governance of cyberspace has entered a new stage of development and the balance is shifting in favor of security under the influence of different factors. With the overriding concern over cybersecurity, the international governance of cybersecurity has thus become increasingly important.

2.1.1 The Development-Driven Technology and Application

Internet architecture was originally intended for development and worked toward global interconnectivity and growing inclusiveness, rather than security. From its advent to the first decade of the 21st century, the Internet had undergone rapid commercialization and socialization, becoming a critical information infrastructure to the world. Continuous innovation and progressive application of technology were the characteristics of this stage, and the international community had focused on maximizing the transformative impact that the Internet exerted on society. Although some cybersecurity issues had begun to emerge, most of them were mainly reflected at the technical level, such as spam and the Conficker virus. Even when some of those issues did induce certain social problems such as rising cybercrime, they were not taken seriously by the public as everything seemed to be controllable. This explains why the international community's priority in cyberspace governance then was leaning toward development, as seen from the 2003 World Summit on the Information Society (WSIS) Geneva Conference and the 2005 Tunis Agenda. Although the international community's understanding of Internet governance was beginning to shift from technology-oriented governance to comprehensive governance, it was still believed that a "working definition of Internet governance was the development and application by governments, private sectors, and civil society in their respective roles of shared principles, norms, rules, decision-making procedures, and programmes that shaped the development and use of the Internet," indicating a clear focus on development and application issues (*see* Exhibit 2.1).[1] The agenda of subsequent Internet Governance Forums (IGF) were focused on development.

1 The World Summit on the Information Society, "Tunis Agenda for the Information Society," accessed March 1, 2019, http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

Exhibit 2.1 The then Secretary-General Kofi Annan addressing the World Summit on the Information Society in Tunis, November 16, 2005

Source: Xinhua News Agency

However, the situation has changed in recent years and the security risks of technology have become apparent. The development of Internet technology has entered a new stage with the emergence of Internet-based technologies and applications such as the Internet of Things (IoT), big data, cloud computing, artificial intelligence, and blockchain. Such trends and developments in Internet technology applications are presented as "interconnection of networks," "interconnection of network and things," and "interconnection of people and things." Compared with the initial technology pursuing interconnectivity, these new technologies and their applications have a distinctive feature. From the origin to application of the technologies, the international community has paid close attention to the security risks involved and factored such risks into its design and production.

2.1.2 The Catalytic Effect of Major Emergencies

The far-reaching effects of the Snowden Leak five years ago are still being felt, the most important of which is the international community rethinking cybersecurity in a comprehensive and strategic way. Security concerns have come to be deeply rooted in the minds of people, and countries now regard cybersecurity of core interest. With the increasingly fierce strategic competition among states in cyberspace, particularly the integration of the cyber and real worlds, the cyberspace situation has become highly complicated. Coupled with non-state actors continually increasing their participation in cyberspace by taking advantage of their "low threshold" and "asymmetric power," cybersecurity has become seriously endangered by cybercrime and cyberterrorism.

The international community has begun to realize that security is essential for development. Thus, at the UN High-Level Meeting marking the Tenth Anniversary of the World Summit on the Information Society (WSIS+10 HLM) at the end of 2015, when the international community explored the development goals of the Information Society for the new decade (2016–2025), security concerns were highlighted, as reflected in the *Outcome Document*. The document affirmed the leading function of government and emphasized the role of international law, especially the *UN Charter*, in cybersecurity affairs. It also stated that cybercrime, cyberterrorism, and cyberattacks are major threats to cybersecurity, and called for the improvement of international cybersecurity culture and the strengthening of international cooperation. It appealed to member states to fulfil more of their international obligations while enhancing their domestic cybersecurity, especially by helping developing countries build their capacity in cybersecurity.

2.1.3 The Rising Awareness of the International Community

At this stage, the international community's understanding of the importance of security governance is in line with the cognitive process: awareness of security issues needs a certain period of time to form and develop. On the one hand, the cognitive process has a lagging effect. The primary driving factor for the development of the Internet is the development and application of its technology. In application, technology is often a double-edged sword—promoting development while bringing along its own set of problems. While some of these problems may be technical, most trigger social security risks or regulatory problems. However, these problems will arise only after the

technology is applied. That is why the international community's awareness of security issues has had a time lag—one of the reasons why security issues were not evident in the early stage.

On the other hand, considerable impact is required before any cognitive change can be effected. Many security issues are not addressed and solved even when there is awareness in the international community. It is only when problems hinder development, due to a lack of timely and adequate response, and thus have an impact on society will they eventually receive global attention.

In short, security threats and incidents must have sufficient frequency and intensity to prompt an effective response from the international community. For example, the global ransomware Wannacry affected nearly 200,000 computers in 150 countries around the world in 2017, and most of these computers were used in areas critical to people's

Exhibit 2.2 The electronic timetable at the Leipzig train station in Germany malfunctions due to the Wannacry virus, May 13, 2017

Source: Xinhua News Agency

livelihoods, such as health care and energy (*see* Exhibit 2.2). More importantly, the investigation results of this incident were inconclusive and provided no clear picture of the truth. The problem of cyber arsenals and their hidden security risks, such as in the US–DPRK cyber conflict, are worrying. The international community's handling of such incidents changed from addressing hacker intervention to managing cyber arsenals and defending against risks posed by cyber conflicts and real-world politics. In 2017, large-scale data breaches became the new normal in cybersecurity, and data security concerns rose to an unprecedented height. These issues not only involved citizen privacy and national security, but also has had a major impact on political and social stability. For example, in July 2017, the leakage of sensitive citizen data in Sweden triggered a political crisis. The impact of these burgeoning large-scale cybersecurity incidents has raised the international community's concerns about security governance to a new level (*see* Exhibit 2.3).

Exhibit 2.3 Facebook CEO Mark Zuckerberg at a joint hearing of the US Senate's Commerce Committee and Judiciary Committee to testify on the data breach, April 10, 2018

Source: Imagine China

To draw conclusions about this new stage, we need to further explain two points. First, this is not an absolute point of view. Emphasizing security does not mean neglecting development. Rather, security issues have become the main contradiction, or the main aspect of the contradiction, in cyberspace development. If not effectively addressed, these security issues will also pose formidable obstacles to development. Therefore, the international community is now paying more attention to security issues and investing more resources in security governance. Second, this is not a pessimistic view. Focusing on security governance does not deny the achievements of development and is also not an alarmist view of the future. In fact, raising safety concerns at the current stage is inevitable in the development of cyberspace governance. These concerns conform not only to the objective laws of the development of technology and its application, but also to the cognitive laws of all parties in the international community.

2.2 China's Participation in International Cybersecurity Governance

China's participation in international cybersecurity governance is a phased process. In general, China's cyberspace governance is compatible with both the development of international security governance and its domestic Internet development and application. Therefore, the focus, methods, and influence of China's participation have different features at different times—from participating in the technology-centered global security governance (early stage of Internet development) to actively contributing to the comprehensive security governance (rapid development stage of the Internet). In recent years, China has been playing the role of a major power and bearing its corresponding responsibilities by putting forward the strategic concept of building a community of shared future in cyberspace. It is beginning to put forth the China proposal and the China solution for international cyberspace governance and is leading the international community toward shared security and common development.

2.2.1 Early Stage of Internet Development: Participating in Technology-centered Security Governance

Strictly speaking, international cyberspace governance began in the 1990s. The landmark event was the emergence of a series of Internet governance institutions that

maintained Internet technology and formulated standards. In particular, the US Department of Commerce decided to set up the Internet Corporation for Assigned Names and Numbers (ICANN) to be responsible for the allocation and management of Internet infrastructure resources. At that time, the international community's perception of the Internet was focused on technology. The Internet was regarded as a technology architecture for transmitting and sharing information, and its inherent features were openness, freedom, equality, and sharing. Thus, cyberspace, based on this technical architecture, was inherently characterized by decentralization and virtuality and its development depended on the laws of endogenous development. Therefore, more attention was paid to the materialization of global interconnection and intercommunication via the development in technology. At this stage, any response to the so-called security problems was technology-centered—that is, ensuring the security and stability of the network architecture by implementing programs, standards, and protocols.

With the increasing popularity and accessibility of the Internet across the country, China gradually stepped into the Internet governance process (*see* Exhibit 2.4). In this early stage of Internet development, the focus was on expanding access and securing operations. At that time, governance practices were mainly concentrated in the technical field domestically and internationally, in terms of the physical layer (the Internet's physical architecture) and logical layer (Internet transfer protocols)—that is, to achieve interconnectivity and ensure smooth operations. Therefore, China introduced connection technology and protocol standards domestically. In May 1994, the Computer Network Information Center (CNIC) of the Chinese Academy of Sciences (CAS) completed the setup of China's national top-level domain server (CN). In September 1996, China Golden Bridge Information Network (CHINAGBN) began to provide access to specific group users as well as individual users. In April 1996, the Ministry of Posts and Telecommunications issued the *Measures of the People's Republic of China on the Management of International Access of ChinaNet*. In May 1997, the Information Work Leading Group of the State Council issued the *Interim Administrative Measures for the Registration of Internet Domain Names* in China. In May 1999, the first computer emergency response team (CERT) in China was established at the Network Engineering Research Center of Tsinghua University.

Internationally, China participated in and followed up on the work of Internet governance institutions. Right after the establishment of the ICANN in 1998, China Internet Network Information Center (CNNIC), the registration authority for the ".cn," participated in ICANN-related activities. Qian Hualin, the then technical

Exhibit 2.4 According to China Internet Network Information Center, the Internet penetration rate in China has reached 55.8% as of December 2017, exceeding the global average by 4.1 percentage points

Source: Visual China

director of CNNIC, attended the first ICANN meeting. In October 1999, Professor Wu Jianping of Tsinghua University was elected as a member of the committee of the Address Supporting Organization (ASO), which was affiliated to ICANN. Chen Yin, deputy director of the Telecommunications Administration of the Ministry of Information Industry, attended the Governmental Advisory Committee (GAC) Conference of the ICANN as a China representative. In March 1996, the unified transmission standard for Chinese characters submitted by Tsinghua University (adapted to Chinese codes for use in different countries and regions) was approved by the Internet Engineering Task Force (IETF), becoming the first Chinese protocol recognized as a Request for Comments (RFC) file.

2.2.2 Rapid Development Stage of the Internet: Actively Contributing to Comprehensive Security Governance

The first decade of the 21st century saw the rapid development of the global Internet industry, especially with its commercialization and socialization in full swing. At this stage, the concept and practice of international Internet governance underwent significant changes marked by the two phases of UN-sponsored WSIS. Its first phase took place in Geneva in 2003 and the second phase took place in Tunis in 2005. Since the beginning of the 21st century, the Internet has become a critical information infrastructure globally and has penetrated all aspects of society deeply, involving public policy coordination and geopolitics in many fields. The technology-centered governance concepts and the corresponding institutional settings were increasingly unable to cope with non-technical issues. Therefore, the United Nations promoted the WSIS process and established the UN Working Group on Internet Governance (WGIG) and the Internet Governance Forum (IGF). These showed that the international community had started to conduct intensive and detailed discussions on comprehensive governance. Internet governance, defined by the WGIG in its report delivered in June 2005, as "the development and application by governments, the private sector, and civil society in their respective roles of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."[2]

Since then, the international community has developed a broader perspective of international Internet governance, especially on the subject and content of international security governance. Security no longer refers only to the maintenance of the security of technical architecture but involves all security-related issues, both technical and social, which occur in Internet usage and application. For instance, in addition to spam and the Conficker virus, security-related issues also include threats such as cybercrime. Those issues also involve problems whose impact goes beyond the Internet itself. These include international trade disputes arising from network intellectual property rights and network economy, and other Internet-related issues, such as the digital gap and the "short board" in network capabilities of developing countries that were widely discussed at the time. As explained in Chapter One, from

2 Kofi Annan, "The Working Group on Internet Governance," accessed April 1, 2019, http://www.wgig.org/docs/Desai-SGletter.pdf.

the development and security perspectives and according to the Wooden Bucket theory, the overall level of network security depends on its shortest board. The lack of network security capabilities in developing countries will become an important factor restricting the overall security of cyberspace.

The Internet of China entered the stage of rapid and comprehensive development at the beginning of the 21st century, in keeping with international developments. In May 2000, China Mobile Internet (CMNET) was put into operation and officially launched the Global WAP (Wireless Application Protocol). In 2001, China Telecom provided Internet-based international roaming services. At the same time, other Chinese Internet companies also developed rapidly. In March 2005, Baidu was listed on NASDAQ in the United States (*see* Exhibit 2.5). In August of the same year, Yahoo's entire business in China was handed over to Alibaba. Meanwhile, the concept of Web 2.0 represented by the blog, promoted the development of China's Internet and catalyzed a series of new social applications.

It was during this period that the Internet became an important economic engine and social platform in a real sense. At the same time, the severity of various security issues brought about by the Internet began to emerge. Domestically, China urged the ministries and commissions involved to work hard to promote various cybersecurity policy measures. Internationally, China also actively participated in corresponding work on comprehensive governance. In December 2003, China sent a government delegation headed by Wang Xudong, the then minister of the Ministry of Industry and Information Technology, to attend the first phase of the WSIS. He delivered a keynote speech titled "Strengthening Cooperation, Promoting Development, and Jointly Moving towards the Information Society," elaborating on issues such as the Internet management of information, communications and network security, human rights and freedom of expression, and closing the digital gap. During the summit, China also participated as one of the major movers in the discussions on global Internet governance centered on the management of the Internet key addressing system. It also took part in drafting the WGIG report and provided the opinion of the Chinese government and those gathered from the public.

In November 2005, Huang Ju, the then member of the Standing Committee of the Political Bureau of the CPC Central Committee and the then vice premier of the State Council of China, attended the second phase of WSIS as head of the Chinese government delegation and delivered a keynote speech titled "Strengthening Cooperation and Promoting Development for a Better Tomorrow for Information Society." Huang Ju detailed China's governance concepts and propositions in four aspects—promoting

Exhibit 2.5 The official listing of Baidu Online Network Technology Co., Ltd. on NASDAQ, New York, August 5, 2005

Source: CNSPhoto

coordinated development, strengthening international cooperation, and fully respecting differences in social systems and cultural diversity.

In addition, the Tunis phase of the WSIS established the IGF as a multilateral, multistakeholder, democratic, and open forum to advance international Internet governance. As one of the major achievements of WSIS, the IGF has become the main arena for global Internet governance with the broad participation of various stakeholders. In 2011, the Multistakeholder Advisory Group (MAG) was set up to advise the UN secretary-general on the organizational structure and routine work of the IGF. From its inception, the IGF has become an important and globally-recognized Internet governance platform and China has always been an active participant. The

Chinese attendees to previous IGFs include government delegations dispatched by the Ministry of Industry and Information Technology, the National Internet Information Office, and the Ministry of Foreign Affairs; representatives from industry associations and research institutions, such as China Internet Association, China Association for Science and Technology (CAST), China National Computer Network Emergency Response Technical Team (CNCERT), China Communications Standards Association (CCSA), China Information and Communication Research Institute, and CNNIC; and from Internet companies such as Baidu, Qihoo 360, AdChina, Yibao Payment, and Tencent. China is highly recognized for its achievements in anti-spam measures, industry self-regulation, information accessibility, cybersecurity, and cultural diversity.

2.2.3 Recent Years: Security Governance under the Vision of Building a Community of Shared Future in Cyberspace

The Snowden Leak in the summer of 2013 became an important trigger for the reform of international cyberspace governance. Prior to the incident, progress in governance had been in slow and gradual reform. The Snowden Leak accelerated related agendas and practices, especially as the international community's concerns on cybersecurity rose to an unprecedented height. In October 2013, the Internet governance agencies jointly issued the *Montevideo Statement on the Future of Internet Cooperation*, condemning the global monitoring and surveillance conducted by the US government. In 2014, ICANN and the Brazilian government jointly hosted the Brazil Internet Conference (NETmundial), calling for reform of the existing governance mechanism. Subsequently, the international community actively promoted the reform of the governance mechanism, starting with urging the internationalization of ICANN and changing the US-regulated Internet basic resource allocation and management system. The US government made a commitment to delegate its power in March 2014 and fulfilled its commitment on October 1, 2016.

At the same time, forums and conferences on governance at various levels were held, and multilateral, regional, and bilateral international organizations, including G7 and G20, incorporated cybersecurity governance into their agenda. From December 14 to 16, 2015, the WSIS+10 HLM was held in New York (*see* Exhibit 2.6). The work of the UN GGE followed and the Fifth UN GGE was held in 2016. At this stage, all these organizations tackled cybersecurity issues from a strategic level.

Exhibit 2.6 Ban Ki-moon, the then UN secretary-general addressing the WSIS at the UN General Assembly, December 15, 2015

Source: Imagine China

First, security has been set as an important goal and direction of governance. The WSIS+10 High-Level Meeting clarifies the development goals for the new decade of the Information Society (2016–2025). The *Outcome Document* puts forward the basic framework and principles for development and governance of the Information Society. In particular, it has established a series of new governance objectives and key areas, with security governance as one of the most prominent features. For example, it affirms the "leadership of the government in cybersecurity issues affecting national security;" emphasizes the role of international law, especially the *UN Charter*; points out that cybercrime, cyberterrorism, and cyberattacks are major threats to cybersecurity; calls for upgrading international cyberculture and strengthening international cooperation; and appeals to member states to take on more international obligations

while strengthening domestic cybersecurity, especially to help developing countries in cybersecurity capacity building.

Second, the development of cyber norms has become the focus. The international community believes that in addition to the characteristics of the development of network technology and its applications, the root cause of the current severe cybersecurity issue is the lack of norms of behavior. Therefore, developing and strengthening the norms of behavior in cyberspace for both state and non-state actors is key to effective security governance.

The most representative examples of such norms of behavior for state actors are the *UN GGE report* and the *Tallinn Manual*. The report of the Third UN GGE confirms that state sovereignty and international norms and principles based on the concept of sovereignty, apply to the ICT-related activities conducted by national governments, and to their jurisdiction over ICT infrastructure within their territory. In 2015, the Fourth Expert Group enriched the relevant content and incorporated the principles of national sovereignty, non-interference in internal affairs, prohibition of the use of force, peaceful settlement of international disputes, and responsibility for the control and management of domestic network facilities, further improving the normative system.

More importantly, the 70th Session of UN General Assembly unanimously adopted a resolution on information security jointly proposed by 82 countries, including Russia, China, and the United States, and authorized the establishment of a new expert group to continue discussions on the application of international law, norms of responsible state behavior, and rules and principles of Internet usage. In 2016, complying with the new requirements, the work of the newly formed UN GGE steadily advanced, aiming at implementing norms of responsible state behavior and establishing a number of operational measures in confidence building and capacity building. Although the Fourth UN GGE failed to reach a final outcome document, its in-depth and detailed discussions on those issues are valuable.

In addition, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) issued the *Tallinn Manual* (versions 1.0 and 2.0) in 2013 and 2016 respectively, centering on norms of cyber operations in wartime and discussing the application of wartime international laws, such as the *Law of Armed Conflict* (LOAC), to cyberspace. The *Tallinn Manual* (Version 2.0) further expanded the international laws for cyber operations in peacetime. Although the Manual was mainly compiled by Western countries, it was intended to include non-Western countries in order to enhance the Manual's influence. At the same time, although it was an instrument proposed by experts, it constantly sought

government endorsement, by, for example, organizing consultations for government legal representatives. Considering the general practices in the origin and promulgation of international law, even if it is only a proposal by experts, we must not underestimate the influence of its formation process, and of relevant concepts and rules on cyber norms of the future.

As for norms of behavior for non-state actors, the exploration of relevant laws and regulations has been further promoted with the advancement of international cooperation in combating cybercrime. For example, on May 24, 2017, the 26th UN Commission on Crime Prevention and Criminal Justice (CCPCJ) adopted the resolution *Strengthening International Cooperation Against Cybercrime*.

If China's involvement in international cyberspace governance was only limited to participation in the first two stages of Internet development, then it can be said that in recent years merely participating in cyberspace governance no longer meets China's demands domestically and internationally. The reason behind such a change is China's improved network and enhanced international influence, especially after President Xi Jinping's promulgation of the strategic concept of forging China into a network power domestically and building a community of shared future in cyberspace internationally. With unprecedented will and dynamism, China has increasingly invested greater energy and resources in international cyberspace governance.

On the one hand, China continues to participate in and follow up on the building of important governance mechanisms and platforms to make its voice heard. For instance, the UN GGE under the United Nations was established in 2011 with the joint efforts of China, Russia, and other countries to discuss information security issues. China participated in all four sessions of the UN GGE, actively contributed ideas and suggestions, and spurred the international community to reach a consensus on the application of the *UN Charter* and its basic principles for cyberspace. In addition to its increased participation at the UN, China has also increased its involvement in the work on global and regional governance. For example, China promoted the SCO, G7, G20, and BRICS summit, as well as other platforms, to list cybersecurity and related governance issues on their agenda. Moreover, China took the initiative to build bilateral platforms, establish Track One and Track Two dialogue mechanisms with the United States, UK, Germany, and other countries on network issues, urge to reach bilateral agreements, and to start extensive and in-depth discussions on issues of common interest (*see* Exhibit 2.7). At the same time, China has launched non-governmental forces from all parts of the country to carry out multilevel, multichannel international cooperation, such as

Exhibit 2.7 The meeting of public security ministers of SCO member states on information technology and cybercrime held in Astana, Kazakhstan, April 28, 2011

Source: Xinhua News Agency

promoting cooperation between CNCERT and the computer emergency response teams (CERT) of other countries (*see* Exhibit 2.8). Meanwhile, more attention has been paid to the function of think tanks, experts and scholars to encourage them to participate in various conferences and forums on the academics of governance, and to make the voice of China heard around the world.

On the other hand, China has actively advocated agendas and built platforms to lead the international community in building a community of shared future in cyberspace, and to contribute to the joint maintenance of stability and development of cyberspace. Since 2014, China has successfully hosted the World Internet Conference (Wuzhen Conference) for three consecutive years, making the conference

Exhibit 2.8 Suzanne Spaulding, the under secretary at the US Department of Homeland Security, encourages China to cooperate with US–CERT, Washington, DC, September 10, 2015

Source: CNSphoto

an important comprehensive governance platform for the international community to explore governance issues and engage in cooperation. In particular, President Xi put forward the Four Principles and Five Proposals that focus on promoting the reform of the global Internet governance system at the Second Wuzhen Conference. He called on all parties of the international community to:

1. Speed up the building of global Internet infrastructure and interconnectivity;
2. Establish an online platform for cultural exchange and mutual learning;
3. Promote innovative development of cyber economy for common prosperity;
4. Maintain cybersecurity and its orderly development;

5. Build an Internet governance system to advance equity and justice based on the principles of respect for cyber sovereignty, maintenance of peace and security, the promotion of openness and cooperation, and the cultivation of good order.

On March 1, 2017, the Chinese Ministry of Foreign Affairs and the Office of Central Cyberspace Affairs Commission jointly issued the *International Strategy of Cooperation on Cyberspace*. Under the theme of peaceful development, win-win cooperation, and the goal of building a community of shared future in cyberspace, this strategy was the first to outline the China proposal for international cooperation in cyberspace comprehensively and systematically, thus offering the China solution to the problems in international Internet governance.

2.3 China's Proposals for Selected Governance Issues

China has actively participated in cyberspace governance to tackle the core concerns of the international community. Where there is an urgent need for wisdom in the governance of cyberspace, China has been offering its ideas and proposals for building a secure and stable cyberspace. However, due to differences in national conditions and perspectives, and intentional or unintentional misinterpretation, the international community has had some doubts about China's proposals. Therefore, it is necessary to clarify these issues (*see* Exhibit 2.9).

2.3.1 The Multistakeholder Model

For a long time, under the influence of traditional governance, the multistakeholder model has been regarded as the model for Internet and cyberspace governance, and the international community has had a perception that China advocates the government-led model rather than the multistakeholder model. The main reason for this view is that China supports the important role of UN organizations and institutions in Internet governance. However, this perception has been a major misunderstanding.

First, historically the United Nations has always been an important driving force of international Internet governance. It is the UN that has constantly urged the advancement of the WSIS, which is of great historical significance to Internet governance. Anyone familiar with the history of Internet governance ought to know that

Exhibit 2.9 Li Baodong, then Chinese vice foreign minister, expounds China's perspective on cybersecurity at the forum jointly held by the Chinese Ministry of Foreign Affairs and the United Nations in Beijing, June 5, 2014

Source: CNSphoto

even the multistakeholder model was jointly established with the WGIG under the auspices of the UN. The then UN Secretary-General Kofi Annan called on all parties to seek Internet governance in an innovative way due to the uniqueness of the Internet. At the time, the US government supported the private sector-led model, while other countries, including China, realized that the government was indispensable in public policymaking, and thereby advocated the government, the private sector, civil society, and even individuals to jointly participate in Internet governance. That is the reason why the WGIG, together with other multistakeholders, has given a clear working definition of Internet governance, affirming that these actors must all play a role in accordance with their respective functions.

Second, from the practical perspective, the governance of Internet or cyberspace involves a wide range of issues which are complex and diverse. In fact, governance can be roughly divided into the following three different layers according to the nature of the issues involved: physical, logical, and applicability. The former two are mainly technical, while the latter contains many public policymaking issues and expands continuously along with the further deepening application of Internet technologies. According to the hierarchical theory of Internet governance, these issues are interrelated but with very different natures and attributes, and ought to be addressed by different approaches. Therefore, there is no single model that can apply to all layers. Even within the same layer, roles of diverse participants in actual governance are very different. For example, at the technical layer, the private sector and the technical elite ought to play a leading role, while within the public policymaking layer, the government ought to assume greater responsibilities. Hence the multistakeholder model only emphasizes the differences in the procedures for participation and decision-making of each actor, without reflecting the disparity in practicing governance between different actors.

Third, from the intent of the multistakeholder model, there is no unitary definition of this governance model yet. The two main highlights of this model are the participation of all parties and an open process. However, there is no paradigm regulating the positioning and interrelationship of all parties in the specific practice of governance. Even ICANN and IETF, the two international governance bodies that are representatives of the multistakeholder model, differ greatly in their organizational structure and operation. Since all parties have the right to participate in governance, intentionally limiting the role of a certain actor, or even creating opposition and confrontation among various stakeholders, can cause real damage to the multistakeholder model. Therefore, the dispute over the multistakeholder model is unnecessary.

China has never opposed the multistakeholder model, but has advocated its flexible and pragmatic use based on the actual situation. After all, Internet governance itself is complex. In practice, governance should be field-specific or issue-based, and generality has no practical significance. Specifically, in the actual application of the multistakeholder model, attention ought to be paid to fairness and efficiency. All stakeholders ought to be involved to achieve fairness, and the leading role ought to be played by different actors in different situations to ensure efficiency. For example, the technical community and professional institutions must be responsible for maintaining the Internet technology architecture and formulating governance standards, while the government ought to play a leading role in areas such as public policy. In any case,

"leading" is only a division of responsibilities rather than a monopoly. Any complete decision-making process must be consulted with, and negotiated and supervised by all parties.

Unfortunately, cyberspace has long been plagued by the Cold War mentality, dividing countries into different ideological camps based on their attitudes toward the multistakeholder model. In order to address the resulting problems and confrontations, in the *Outcome Document* of WSIS+10, "multistakeholders" and "multilateral" are used interchangeably rather than in contradictory terms, and are regarded as integral parts of cyberspace governance. China uses both terms in its official documents to be in agreement with the *Outcome Document*, and to avoid confusion over the China approach toward the multistakeholder model among the international community.

2.3.2 Cyber Sovereignty

Currently, some members of the international community believe that China's emphasis on cyber sovereignty means that China is separating itself from the unitary global Internet. As such, it will pose a serious threat to openness and interconnectivity as well as to the free flow of information. However, this is not true. China's perception and practice of cyber sovereignty is not fundamentally different from that of other countries.

First, China supports the international consensus that the principle of sovereignty applies to cyberspace. For a long time, cyberspace was understood as a field that transcends physical space, provides immunity against national sovereignty, and is not subject to state control and international rules. However, reality shows that while cyberspace is unique, the development of cyberspace needs to be regulated and requires an international order. To establish an international order within the existing system, the concept of "national sovereignty" must be clarified as one of the core principles for current state and international operations. After extensive discussions, the UN GGE document fully affirmed that the basic principles of the *UN Charter*, including the principle of sovereignty, and international laws must be applied to cyberspace.

Second, China supports the international community to further explore the applicability of national sovereignty to cyberspace. Although the international community has reached a consensus on applying the principle of sovereignty to cyberspace, there are still many problems when implementing this principle. Some arise from having

different understandings of the issue. For example, some scholars believe that given the transnational nature of cyberspace, we ought to consider "sovereignty transfer" from the perspective of cooperation and responsibility when applying the principle of sovereignty. Others hold that before discussing sovereignty transfer, we must first clarify the definition and boundary of sovereignty. Some problems come from the practical level. For example, based on the principle of sovereignty, the state has the right to be free from external interference. However, due to the anonymity and untraceability in cyberspace, the "external" is difficult to define, and protecting such a right is impossible to achieve. Despite all the difficulties, some progress has been made. The most important achievement is to have all parties reach a consensus on the domestic jurisdiction over cyberspace, that is, countries are to have control over their own territorial network infrastructure, network activities, and information flow. Therefore, China believes that in the burgeoning cyberspace, many problems, including the application of the principle of national sovereignty, are still in the process of exploration. Hence, we ought to encourage various theoretical and practical innovations in the spirit of openness, rationality, and innovation.

Third, China's view on cyber sovereignty reflects the basic principle of sovereignty. President Xi has expounded the connotation of cyber sovereignty on various occasions, and he reiterated this at the opening ceremony of the Second World Internet Conference in Wuzhen that

> we should respect the right of individual countries to independently choose their own path of cyber development, model of cyber regulation, and Internet public policies, so as to participate in international cyberspace governance on an equal footing. No country should pursue cyber hegemony, interfere in other countries' internal affairs, or engage in, connive at, or support cyber activities that undermine other countries' national security.[3]

This statement affirms the application of the principle of sovereignty to cyberspace from two dimensions. Internally, China can independently formulate policies and plans for the development of the Internet according to its own situation. Externally, China is to strive for equal participation in Internet governance and to build a fairer

3 Xi Jinping, "Remarks by H.E. Xi Jinping President of the People's Republic of China at the Opening Ceremony of the Second World Internet Conference," accessed April 1, 2019, http://www.chinaembassy.org/eng/zgyw/t1327570.htm.

and more just cyberspace order. Therefore, China has not elaborated on the concept of cyber sovereignty beyond traditional sovereignty, but has followed a consistent understanding and positioning of its own rights and responsibilities within the international community. This approach of applying the principle of sovereignty to cyberspace is a logical necessity.

2.3.3 Cyberspace Rules

In the process of cyberspace rulemaking, questions on China's position are focused on why China adheres to the UN framework and whether China has a government-led mentality underpinning a multilateral framework or governance model. In fact, if we understand China's basic stand on the necessity and importance of current international cyberspace rulemaking, we ought to appreciate that China's emphasis on the UN framework is a responsible, rational, and pragmatic attitude to various platforms and channels for current cyberspace rulemaking.

The current crisis in cybersecurity has two root causes: the security vulnerabilities and hidden dangers in the application of technology, and the lack of norms of behavior. Comparatively speaking, the latter is more serious as technical problems are relatively easier to solve. In most cases, technology and its application in themselves are not the issue; the real problem is the people who abuse technology. Therefore, reinforcing rules that govern cyberspace actors to effectively regulate the behaviors of state and non-state actors is the crux to maintaining the security and stability of cyberspace. From the current rulemaking process, it is obvious that norms of state behavior must be explored under the multilateral framework. For norms of non-state behavior such as combating cybercrime and cyberterrorism, although cooperation among various parties is indispensable, the strong role of government and the investment of its resources are key. Therefore, the UN channel or its framework remains one of the most effective ways to address such issues. Although the current international cyberspace rulemaking is facing some difficulties, China still attaches great importance to it. In particular, China insists that the UN framework ought to be the main channel in the formulation of norms of state behavior, with other models as supplementing channels.

First, norms of state behavior must be formulated under the UN framework. In the current international situation, the UN framework remains the most authoritative and legitimate institution for handling international relations and responding to global security threats. This applies equally to cyberspace. In a certain sense, since the relations in cyberspace are an extension of those in the real world, the regulation of

state behavior in cyberspace must also rely on the UN framework. Practice proves that the UN framework has always occupied a central place in the formulation of norms of state behavior in cyberspace. In addition to the aforementioned UN GGE and WSIS, another example is the International Telecommunication Union (ITU). In July 2017, the ITU released the second *Global Cybersecurity Index* (GCI) and pointed out that cybersecurity has become a vital component of digital transformation. It also encouraged countries to consider making national cybersecurity policies. The GCI pays close attention to the issue of cybercrime, emphasizing the need for governments to undertake measures at strengthening the cybersecurity ecosystem, so as to reduce the threat of cybercrime and boost the people's confidence in the network. The joint efforts of these mechanisms have advanced the formulation of public policies and technical solutions for cybersecurity.

Second, we ought to adopt a positive attitude toward other rulemaking processes. Since cyberspace rulemaking is still in the early stages of development, we ought in general to be open to any beneficial experiment, drawing from theoretical innovation, mechanism reform, or best practices. In recent years, other mechanisms and related actors, in addition to the UN framework, have all made various achievements in this area. At the level of regional intergovernmental organizations, the Group of Seven (G7) and the Group of 20 (G20) summits have actively explored ways to respond to cybersecurity threats. The G7 Leaders' communiqué endorsed the *Declaration on Responsible States Behavior in Cyberspace*, and expressed the leaders' determination to work together with other partners to tackle cyberattacks and to mitigate their impact on critical infrastructure. It stated:

> We endorsed the *Joint Communiqué*, the *Declaration on Responsible States Behavior in Cyberspace*, and the *Statement on Non-Proliferation and Disarmament of the Foreign Ministers' Meeting in Lucca*, and further discussed issues and crises that are most seriously threatening the security and well-being of our citizens and global stability.

At the level of corporations, Microsoft took the lead in calling for the application of a *Digital Geneva Convention* to protect cyberspace, stating that the international community must ensure that civilians in peacetime are protected from cyberattacks, just as civilians in wartime are protected by the *Geneva Convention*. Siemens advocated the *Charter of Trust* to enhance the confidence of all parties in cyberspace.

At the level of thinks tanks, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) issued the *Tallinn Manual* (versions 1.0 and 2.0) in 2013 and 2016 respectively, highlighting the norms of cyber operations in wartime, and discussing the application of wartime international law in cyberspace such as the LOAC. The *Tallinn Manual* (Version 2.0) further expanded the scope of international law for peacetime cyber operations. In February 2017, the EastWest Institute of the United States and the Hague Center for Strategic Studies of the Netherlands jointly launched the Global Commission on the Stability of Cyberspace, to develop norms and policies that advance the international security and stability of cyberspace, by pooling the intelligence resources of the global academic community. Regardless of the views and positions contained in the documents, whenever traditional mechanisms such as the UN GGE met with bottlenecks, these initiatives garnered the attention of the international community and inspired all parties to think about possible methods for rulemaking.

Third, we must face up to the problems that occur during the process of rulemaking. From the problems in the current rulemaking process, an effective system for cybersecurity governance has not yet been established. For instance, even though the UN framework enjoys legitimate authority and facilitates in-principle consensus, actual implementation remains difficult because of limited resources and the unwieldy decision-making processes. This is why after 2017, the international community discussed the next steps of the UN GGE at length and that of making adjustments to the mechanism. The UN secretary-general Guterres is also setting up a team of experts, hoping to get around the bottlenecks.

At the level of regional intergovernmental organizations, geopolitics, and other related issues are factors that hinder the acceptance of proposals initiated by such organizations. Yet rules and initiatives made at the level of corporations and think tanks need to be widely accepted and recognized by the international community before being officially incorporated as norms. However, this is currently hardly the case, as seen from the *Tallinn Manual*. Some people believe that given the current rising trend of boosting cyber arsenals, formulating international laws such as the LOAC for cyberspace would not be conducive to forging trust and stability, and would undoubtedly aggravate the militarization of cyberspace. Another example is Microsoft's proposal for the *Digital Geneva Convention* to protect cyberspace. Many governments state that they welcome wisdom from corporations, but still believe that cyberspace rulemaking is the business of governments who should have the final say. However, since rulemaking is still in its early stage, any discussion is constructive—at least for understanding the concepts of

security and stability in cyberspace, and for raising global awareness. In the long run, it favors the creation of an environment conducive to the development of cyber rules. However, the direction of actual developments and their results still depend on the joint efforts of all parties.

2.3.4 Combating Cybercrime

In terms of China's proposals and practices, and intense determination in combating cybercrime, one of the most frequently asked questions by the international community, especially the United States and Europe, is China's attitude toward the *Budapest Convention on Cybercrime*. In fact, China has repeatedly reiterated its position on international cooperation in combating cybercrime on several international occasions. The main points are as follows.

First, China attaches great importance to the fight against cybercrime. The nation has realized that new forms of organized, industrialized, and transnational crime, are emerging along with the advancement of the Information Society as a result of the integration of traditional crimes with the Internet, causing tremendous harm to cybersecurity and social order. Therefore, China continues to improve its policy and legal frameworks for cybersecurity and considers the fight against cybercrime an important strategic task for maintaining national cybersecurity. For example, China has in recent years successively promulgated laws and regulations, such as the *State Security Law of the People's Republic of China* and the *Cybersecurity Law of the People's Republic of China*. It has also actively promoted the improvement of legislation against cybercrime and established the basic legal framework for criminalization.

Furthermore, China has actively carried out extensive international cooperation. As the main organ responsible for cracking down on cybercrime, the Chinese public security organs have continuously strengthened international cooperation in law enforcement and established a cooperative mechanism for annual meetings in the Asia-Pacific region, based on the Interpol Working Group for the Asia-Pacific region on combating information technology crimes. It has also conducted bilateral consultations with the United States, UK, Germany, and other countries, concerning the combating of cybercrime and started bilateral police cooperation with other countries in a series of enforcement operations. Furthermore, the Chinese public security organs jointly established the Asian Cybercrime Technology Information Network System (CTINS) with 14 countries, including Japan and South Korea, to exchange the latest information about cybercrime and to share investigation and forensics technology in a timely manner.

It has formulated the *Agreement on Cooperation in Ensuring International Information Security* between the Member States of the Shanghai Cooperation Organization (SCO), by relying on the SCO to establish a collaborative mechanism for cybercrime investigation and forensics. The *International Criminal Judicial Assistance Law* currently being drafted will provide detailed provisions on international cooperation to further improve the strength and efficiency of judicial assistance in combating cybercrime. During the Fourth World Internet Conference in December 2017, China held the first international cooperation forum on combating cybercrime, demonstrating once more that it attaches great importance to international cooperation in this matter (*see* Exhibit 2.10).

Second, China supports the role of the United Nations and encourages the joint efforts of other stakeholders. The United Nations plays an important role in international cooperation against cybercrime, and China has consistently facilitated the

Exhibit 2.10 Forum at the Fourth World Internet Conference held in Wuzhen, Zhejiang Province, December 4, 2017

Source: Visual China

continuous progress of the discussion on international cooperation against cybercrime under the UN framework, especially the work of the Open-ended Intergovernmental Expert Group Meeting on Cybercrime (UN EGM on Cybercrime). As the only platform under the UN framework to promote international cooperation against cybercrime, the UN EGM on Cybercrime, with the joint efforts of all parties, obtained a new authorization at the 26th Session of the United Nations Crime Prevention Committee and formulated and adopted its *2018–2021 Work Plan*. China promotes the work of the UN EGM on Cybercrime and is willing to work with all parties to develop it into a platform for countries to offer policy guidance, exchange experiences, and share information about international cooperation against cybercrime. Director of the Department of Treaty and Law of the Ministry of Foreign Affairs, Xu Hong, made the following statement at the Forum on International Cooperation against Cybercrime at the Fourth World Internet Conference. He said that cybercrime was an issue at the forefront of discussion and that international cooperation against cybercrime required the effective synergy of multiple stakeholders, such as enterprises, technological community, academia, and netizens.

Third, China has adopted a rational attitude toward various initiatives promoting international cooperation against cybercrime. Europe is taking the lead in combating the ideology and practice of cybercrime. The *Budapest Convention on Cybercrime* is regarded as the pioneer in this field and it has played a positive role in promoting international cooperation against cybercrime. That being so, China believes that the world ought to face up to the existing problems in the Convention. From the formality perspective, as a convention formulated by a regional organization, the representativeness and legitimacy of the Convention are questionable. From the content perspective, the Convention is based on the common law system and has problems docking with the civil law of other countries. In particular, countries still hold different views and have disputes over the provisions on cross-border forensics. In practice, law enforcement faces difficulties.

In addition, the Convention that was formulated about 20 years ago can no longer meet the needs of the current situation. For example, it has difficulty addressing different types of crimes and effectively putting deterrents in place. Moreover, regional organizations such as the Asian-African Legal Consultative Organization (AALCO) and the SCO have conducted relevant discussions and the Russian government has also proposed to establish a comprehensive draft convention. Undoubtedly, these explorations are beneficial to the overall promotion of international cooperation against

cybercrime. However, it is imperative to decide on the mechanism and form, and to remove various practical restraints, so as to improve the efficiency of the corresponding cooperation mechanism, better adapt to the requirements of the situation, and ensure the implementation of these initiatives.

2.4 China's Future Participation in International Cybersecurity Governance

As previously mentioned, China has clearly proposed a strategic concept of forging the country into a cyber power domestically and building a community of shared future in cyberspace internationally. To this end, China has promulgated the *National Cybersecurity Strategy* and the *International Strategy of Cooperation on Cyberspace*. As a major power in cyberspace, China is committed to fulfilling its responsibility and to working together with the international community to promote the international governance of cyberspace. In particular, China is committed to actively responding to the core concerns of the international community about the security of cyberspace and the development of its governance. In the future, China will take a more proactive approach and contribute to international cybersecurity governance by advancing the China solution.

2.4.1 Reform the Governance Mechanism based on the Principle of Sovereignty

The international community has always had a misunderstanding about cyberspace and has been over-emphasizing its uniqueness. Hence, many countries believe that the governance of international cyberspace is separated from that of the real world and that the traditional state-based governance model and mechanism are inapplicable to cyberspace. This is not true, and practice fully proves that cyberspace is an integral part of real space. Although cyberspace has its own particularity that has greatly influenced the political pattern in real space, it has not reached a critical point for qualitative change. The existing international system based on the coexistence of different sovereign states has not fundamentally changed. Therefore, cyberspace governance ought to follow the political logic of the real world and reflect the appeals of sovereign states for national development and international cyberspace strategy.

In fact, the practice of cyberspace development proves that a certain coercive and binding force is necessary for the effective governance of cyberspace. Although national authorities may not be the only source of such a coercive and binding force, it is definitely an important factor in the existing international system. In this regard, China has put forward its concept of cyber sovereignty, which well reflects the reality and is an important contribution to developing a concept of cyberspace governance.

Next, we must take this concept of cyberspace governance as a guide to formulate concrete policies for advancing the reform of the governance mechanism. Such a concept is necessary, but what is more important is other countries' understanding and acceptance, and this depends on China's performance. It is necessary to emphasize that this performance is not only a reflection of China's sovereign concerns and demands. As a major power in cyberspace, China must fully consider the corresponding appeals of other countries so as to resolve misunderstandings and win widespread support.

2.4.2 Strike a Balance between Openness and Stability

On the one hand, the basic end-to-end architecture is the root cause of the Internet's success and value. Internet governance must maintain the basic network architecture of openness and cannot for any reason obstruct its interconnection, intercommunication, or universal access. This is the principle of openness in Internet governance. On the other hand, security is the top priority for Internet development, because it is impossible to avoid the security challenges and social problems it has brought about. This is the principle of stability in Internet governance. As the founder of the Stanford Center for Internet and Society, Lawrence Lessig, has theorized, the Internet is moving from being an irregulable space to becoming a highly regulated one, and Internet governance must consider its tradition of openness and the realistic need for stability.[4] In fact, the current development of cyberspace governance has fully demonstrated the recognition and practice of balance by multiple stakeholders.

China ought to uphold this idea and be attentive to the differences between domestic and foreign policies on this issue. Domestic policy depends on China's actual needs, while foreign policy comprehensively considers the actual needs of multiple stakeholders of the

4 Lessig Lawrence, *Code and Other Laws of Cyberspace* (New York: Basic Books, 2006).

international community, acts accordingly, and avoids unilaterally over-emphasizing a particular issue. It is imperative to convey the concepts of openness and stability to the international community.

2.4.3 Follow the Principle of Keeping Up with the Times

Through a systematic review of international cyberspace governance practices, cyberspace governance is not unchanged. Rather, it is always in the process of continuous adjustment according to developments, to ensure the openness and flexibility of the governance mechanism. As former UN Secretary-General Kofi Annan said in the opening speech at the IGF, Internet governance and traditional governance are essentially different in some aspects. As long as it is conducive to effective Internet governance, any reasonable suggestion and useful attempt ought to be fairly treated. At present, Internet governance reform is comprehensive and ever-changing. Even at the technical level, maintaining effective operation is no excuse to deny any change—whether in the allocation of network resources, or in the formulation of technical standards. The evolutionary governance reform is parallel with, and not contradictory to, the establishment of new institutions, resource integration, and institutional reform. In short, to further improve the governance mechanism, we must continue to make decisions with an open mind according to the current situation.

2.4.4 Promote a Flexible and Pragmatic Governance Model

There is no fixed model for cyberspace governance. While the international community accepts the term "multistakeholder," it is a principle rather than a model. In fact, "multistakeholder," "multilateral, democratic, transparent," or "multiparty" are all open and principled expressions of the role and participation of actors in cyberspace without fundamental differences. China ought to highlight that in the multistakeholder model, we should not have a rigid understanding of the dominant stakeholder, but ought to be flexible and pragmatic based on actual needs. We must be stage-specific and field-specific in determining which stakeholder should play a leading role.

Stage-specific means that governance issues and their focuses differ from one Internet development stage to another. Therefore, the actor playing a leading role must also differ correspondingly. In the early stages, the private sector played a leading role,

while the current Internet governance situation requires the government to play an even greater role. As Joseph Nye of Harvard University stated, although the Internet has to some extent led to the decentralization of power, the government is still the main actor in international politics and ought to assume responsibility for cybersecurity governance. In the face of expanding Internet resources and users, Internet self-governance is an impossible mission. The development of the Internet shows that government power and geographical privileges are still key constraints, and that the Internet relies heavily on the government's coercive power. This can be illustrated by the fact that it is the government who builds infrastructure, promotes education, protects property rights, imposes compulsory measures on cybercrime, controls the market size, and provides public goods. The government-led model, conducive to popularization of the Internet and enhancement of security, among other benefits, is a prerequisite for Internet development of a certain stage.

Field-specific means that even under the government-led model, the government ought not to dominate cyber affairs; the governance of various fields can be dominated by different actors. For example, the maintenance of network operations can be handled by the relevant technical institutions; industrial development can be the responsibility of the industrial sector, and the government ought to play a leading role in cybersecurity and public policy formulation. A complete decision-making process must be consulted with, and negotiated and supervised by multiple actors.

2.4.5 Focuses of Future International Cybersecurity Governance

Future international cybersecurity governance is likely to focus on both perennial problems and emerging hotspots. China must act positively on these security issues to achieve the best possible outcomes in security governance. In addition to the formulation of different norms of state behavior, we ought to focus on the following aspects.

Cybersecurity Capacity Building

The development of the Internet will shift to the Global South. In the future, the development of information infrastructure will mainly be in Asia, Africa, and South America. China has always placed importance on its assistance to developing countries, emphasizing Internet development. Especially after the Belt and Road Initiative was

proposed, building the Digital Silk Road to enhance the Internet infrastructure and promoting safe operations of the affected countries will improve overall cybersecurity (*see* Exhibit 2.11).

Security Issues of New Technologies and Applications

In recent years, the security problems brought about by new technologies, such as artificial intelligence, big data, the Internet of Things, and blockchain, have raised widespread concerns globally. China ought to develop its capabilities in maintaining security and making corresponding rules along with enhancing its existing advantages in technological development and applications, to solve the security problems associated with new technologies and applications.

Exhibit 2.11 Panel discussion at the China–Brazil Internet Conference held in Sao Paulo, Brazil, May 30, 2017

Source: CNSphoto

Norms of Behavior for Non-state Actors

Compared with current norms of behaviors for state actors that have had an internationally agreed formulation and implementation process, rulemaking for non-state actors is lagging. Issues such as combating cybercrime and cyberterrorism in most cases do not involve ideological disputes, and therefore have a great potential for international cooperation. However, it is difficult for the international community to cooperate in those areas due to limitations in the coordination of national laws, policies, and management mechanisms. Therefore it remains difficult to achieve a truly efficient international cooperation mechanism; the resulting overdependence on bilateral frameworks for judicial assistance will cause inefficiency. This is a security problem that must be solved in the future of international cybersecurity governance, so as to achieve full coverage of the norms of behavior for all actors.

Chapter Three

TOP-LEVEL DESIGN OF CHINA'S CYBERSECURITY SYSTEM

3.1 The Correct Outlook on Cybersecurity

A person's mindset determines his behaviors, and the right mindset will lead to the correct actions. President Xi Jinping stated that the correct outlook on cybersecurity ought to be established. China adopts the concept that cybersecurity is holistic rather than fragmented, dynamic rather than static, open rather than closed, relative rather than absolute, and shared rather than isolated. This is the basic principle and methodology China has used for maintaining and practicing cybersecurity.

3.1.1 Cybersecurity: Holistic, rather than Fragmented

In the current Information Age, cybersecurity is closely linked to many other aspects and affects the security of the entire country. The rapid development of informatization and globalization is shaping a future world where everything is controlled by information networks. The fast growth of cyberspace has spawned the rule of whoever controls cyberspace controls everything. Security issues in various spheres—politics, economy, culture, society, and military—are linked to cybersecurity. The emerging color revolution in the political sphere, the rampant cyberattacks in the economic sphere, the rising cybercrime in the social sphere, and the accelerated transformation of methods of warfare in the military sphere—these are the variations of traditional security issues being exacerbated in cyberspace. From China's perspective, cybersecurity is regarded as a strategic component of the concept of holistic national security, inseparable from security issues of other spheres.

3.1.2 Cybersecurity: Dynamic, rather than Static

In the era of the Internet of Things and with the extensive application of new technologies, such as cloud computing, big data, and mobile Internet, decentralized and independent networks have become highly correlated and interdependent, with increasingly blurred systemic boundaries. At the same time, the source of threats and the methods of attacks in cybersecurity are constantly changing. Cyberattacks have evolved from traditional attacks, such as distributed denial-of-service (DoS), phishing, and spam attacks, to advanced persistent attacks (APT) or precision cyber weapon attacks. Hence, the traditional static and single-point protection is no longer valid, and the idea of simply relying on several security devices and software to maintain permanent security is outdated.

Therefore, it is necessary to establish a dynamic and comprehensive concept of protection, and to replace the simplistic mindsets of "divide and conquer" and "fight one's own battles." We ought to be aware of real-time security issues, promptly upgrade the protection system, and continually enhance the protection capability to effectively manage the ever-changing cybersecurity risks.

3.1.3 Cybersecurity: Open, rather than Closed

The Internet has turned the world into a global village, and into a community of shared future in cyberspace. Only in an open environment can we imbibe advanced technologies and continually improve the level of cybersecurity through foreign exchange, cooperation, interaction, and competition. Therefore, China must not "reinvent the wheel behind closed doors," nor must the country close its doors to the outside world and exclude learning. To maintain national cybersecurity, China ought to establish a global vision and have an open mind to seize the historic opportunity created by the emerging technological revolution and maximize the potential of cyberspace development.

3.1.4 Cybersecurity: Relative, rather than Absolute

There is no absolute security in cyberspace, and China ought to ensure its security in a manner that suits its national conditions and avoid blindly seeking absolute security. Otherwise, China may have to bear an excessively heavy burden and be unable to devote its resources to address other concerns. We ought to clearly understand the

cyber threats that we face—which threats are potential, and which are real; which threats are likely to become cyberattacks, and which can be solved by political, economic, or diplomatic ways; which threats should be closely monitored, and which should be eliminated at full force; which threats will cause irretrievable losses, and which can be tolerated to avoid overprotection.

3.1.5 Cybersecurity: Shared, Rather than Isolated

Cybersecurity is for the people and by the people, and maintaining cybersecurity is a shared responsibility of the entire society that requires the participation of all parties—governments, enterprises, social organizations, and netizens. While Internet accessibility promotes global connectivity, a cyberattack on one particular place endangers the entire network and any data breach will jeopardize the security of the entire country. Hence, the government, enterprises, and institutions must bear joint responsibility to safeguard the security of its national network.

Governments ought to be responsible for the top-level design, the formulation of policies and regulations, and the creation of a vibrant environment for Internet development. Enterprises ought to actively play the role of maintaining network security and leading the innovation in security technology. The public ought to build awareness concerning cybersecurity protection and master the skills for upholding cybersecurity. National cybersecurity can be ensured only when all parties work together toward this goal (*see* Exhibit 3.1).

3.2 Strengthening the Strategic Guidance on Cybersecurity

Faced with the increasing complexities of cybersecurity, China insists on prioritizing planning. In July 2016, the *Outline of the National Informatization Development Strategy* was issued. The document stated that it is necessary to adhere to the principle of active defense and effective response, forge cybersecurity defense capabilities and deterrence power, safeguard cyber sovereignty and national security, strengthen the security protection of critical information infrastructure, and consolidate the foundation of the cybersecurity system. In December 2016, the Office of the Central Cyberspace Affairs Commission released the *National Cybersecurity Strategy*, a programmatic document guiding the work on national cybersecurity. It proposed to take the concept of holistic

Exhibit 3.1 The opening ceremony of the Internet Security Volunteers Summit participated by 100 volunteers in Hangzhou, China, January 11, 2016

Source: Visual China

national security as a guide, coordinate development and security, and push for a peaceful, secure, open, cooperative, and orderly cyberspace. It also set out the Four Principles and Nine Strategic Tasks for China's cybersecurity.

In December 2016, the State Council issued the *National Informatization Development Plan for the 13th Five-Year Period (2016–2020)*, requiring equal emphasis to be placed on cybersecurity and IT-based development, and prioritising the improvement of the cybersecurity protection system. It set out major tasks and projects, such as enhancing China's top-level design for cybersecurity, establishing a security protection system for critical information infrastructure, monitoring the cybersecurity situation, and strengthening innovation in cybersecurity capabilities.

3.2.1 Understanding Opportunities and Challenges in Cyberspace Strategically

The Chinese government realized that informatization has brought about a historic opportunity for China that ought to be seized. The *National Cybersecurity Strategy* makes the following point:

> Cyberspace is changing people's production and lifestyles in an all-around way, profoundly affecting the historical development of human society. It is becoming a new channel for information dissemination, a new space for production and life, a new driver for economic development, a new carrier for cultural prosperity, a new platform for social governance, a new bond of exchange and cooperation, and a new territory of national sovereignty.

While cyberspace has catalyzed economic growth and social progress, it has also brought about new security risks and challenges. In this regard, China's *National Cybersecurity Strategy* draws the following conclusion:

> Network penetration jeopardizes political security, harmful information on the Internet erodes cultural security, and cyberterrorism and cybercrime undermine social security. International competition in cyberspace is on the rise.

However, opportunities in cyberspace outweigh the challenges. China upholds the principles of active use, scientific development, law-based management, and ensuring security. It resolutely safeguards cybersecurity, maximizes the potential of its cyberspace development to benefit not only the 1.3 billion Chinese people but also all mankind, and firmly maintains global peace.

3.2.2 Strategic Goals

China ought to take the concept of holistic national security as a guide, pursue the vison of innovative, coordinated, green, open, and shared development, enhance its awareness of risk and crisis, and keep in mind both its national and international imperatives. China also coordinates the two major issues of development and security, promotes the active defense of and effective response to cybersecurity-related issues, urges the building of a peaceful, secure, open, cooperative, and orderly cyberspace, and safeguards state sovereignty, national security and development. This will go toward realizing the strategic goal of building China into a cyber power. The specific goals are as follows:

1. Peace. The abuse of information technology will be effectively curbed. The cyberspace arms race and other related activities that threaten global peace will be effectively controlled, and cyber conflicts will be successfully prevented.
2. Security. The cybersecurity risks will be effectively controlled. A sound national cybersecurity protection system will be established, and core technical equipment will be kept safe and controllable. The network and information systems will be stable and reliable, equipped with enough qualified cybersecurity personnel. People's cybersecurity awareness, basic protection skills, and confidence in using network technology will increase significantly.
3. Openness. The standards, policies, and markets of information technology will be open and transparent; product circulation and information dissemination will be smoother than ever before, and the digital gap among countries will close. Regardless of size, strength, or wealth, countries everywhere, and especially the developing countries, will be able to share in the fruits of Internet development and participate in international cyberspace governance.
4. Cooperation. Countries around the world will cooperate more closely in technology sharing and in their fight against cyberterrorism and cybercrime. The multilateral, democratic, and open international system of Internet governance will be perfected. The community of shared future in cyberspace with win-win cooperation as its core will start to take shape.
5. Orderliness. The legitimate rights and interests of the public in cyberspace, such as the right to be informed, to participate, to express, and to supervise will be fully guaranteed. Privacy in cyberspace will be effectively protected and human rights will be fully respected. The domestic and international legal systems for cyberspace and cyber norms will be steadily established—the rule of law will be effectively applied to the governance of cyberspace. China will foster a credible, civilized, and healthy cyber environment, promote the free flow of information, maintain national security, and develop public interests as an organic whole.

3.2.3 Principles

China advocates the following principles for maintaining global cybersecurity. First, respecting and safeguarding cyber sovereignty. Cyber sovereignty is inviolable, and countries have the right to choose their own development path, network management

model, and Internet governance policy. Equal participation in international cyberspace governance ought to be respected. The cyber affairs of a sovereign state is the responsibility of its people. Each country has the right to formulate national laws and regulations concerning cyberspace. Countries also have the right to take necessary measures to manage their own information systems and control cyber activities in their own jurisdiction, according to their domestic situation and international experience.

Countries ought to have the right to protect their information systems and resources from intrusion, interference, attack, and destruction, and to safeguard the legitimate rights and interests of citizens in cyberspace. They also have the right to prevent and stop the dissemination of harmful information that endangers national security and interests, and maintain order in cyberspace. No country ought to impose cyber hegemony, apply double standards, or use the Internet to interfere in other countries' domestic affairs; or engage in, condone, or support cyber actions that endanger the national security of other countries.

Second, sticking to the peaceful use of cyberspace. The peaceful use of cyberspace is in the common interest of mankind. All countries ought to abide by the *UN Charter's* principle of not using or threatening to use force, and to prevent information technology from being used for the purpose of undermining international security and stability. All countries are also to jointly resist any cyber arms race and prevent cyber conflicts. China ought to adhere to the principles of equality and mutual respect, seeking common ground while reserving differences, and promote inclusiveness and mutual trust. China also respects the security interests and major concerns of other countries in cyberspace, and promotes the building of a harmonious cyberspace. China opposes the use of technological superiority to control the networks and information systems of other countries, or to collect and steal data from other countries on the pretext of national security. A sovereign state must not blindly seek absolute security at the expense of others.

Third, upholding the rule of law in cyberspace governance. China ought to promote the rule of law in cyberspace. Cyberspace must be governed, operated, and used in accordance with the law, so that the Internet can enjoy sound development. China must establish an orderly network in accordance with the law so as to protect the lawful, orderly, and free flow of information in cyberspace, personal privacy, and intellectual property rights. Any organization or individual when enjoying freedom and exercising its rights in cyberspace must, at the same time, abide by the law, respect the rights of others, and be responsible for its speech and behavior on the Internet.

Fourth, coordinating cybersecurity and informatization. Without cybersecurity there is no national security, and without informatization there will be no modernization. Security and informatization are like the two wings of a bird or the two wheels of a cart, and this relationship between the two must be properly handled. Security is the precondition for development, and therefore any development at the expense of security is unsustainable. Development lays the foundation for security and stagnation in development is the biggest safety concern. Without the development of informatizaton, cybersecurity is not guaranteed and existing security may even be lost.

3.2.4 Strategic Tasks

China ranks first in the world in terms of the number of Internet users and scale of network. Hence, maintaining China's cybersecurity not only meets domestic demand, but also contributes to global cybersecurity and peace. China's *National Cybersecurity Strategy* identifies the following key strategic tasks.

First, to firmly defend cyber sovereignty. In accordance with the *Constitution* and other laws and regulations, we shall manage the cyber activities within our jurisdiction, protect the security of our information facilities and resources, and adopt different measures—economic, administrative, technological, legal, diplomatic, military, and so on—to unswervingly safeguard our cyber sovereignty. China resolutely opposes all acts that subvert its political power and undermine its national sovereignty through the Internet.

Second, to resolutely safeguard national security. China will prevent, stop, and punish any use of the Internet for treason, secession, sedition, subversion, or incitement to undermine the people's democratic dictatorship; and for the theft or disclosure of state secrets; or other acts that endanger national security such as the use of the Internet by foreign forces for infiltration, destruction, subversion, or secession.

Third, to protect the critical information infrastructure. China ought to take the necessary steps to protect its critical information infrastructure and key data from attack and sabotage. We must attach equal importance to technology and management, emphasize both protection and deterrence, and focus on recognition, prevention, early warning, response, disposal, and so on. We must also establish and implement critical information infrastructure protection systems, increase investments in management, technology, personnel, and capital. We must also implement comprehensive policies in

accordance with the law, so as to effectively strengthen the security of critical information infrastructure.

Fourth, to strengthen the development of cyberculture. China ought to reinforce the management of its online ideological and cultural stand, vigorously cultivate and practice core socialist values, implement network construction projects, and forge a sound cyberculture. We ought to boost the spread of cyberethics and civilization, give full play to the guiding role of moral education, and use the fruits of human civilization to nourish cyberspace and restore the cyber ecosystem. Moreover, China ought to improve the cyber etiquette of its young people and ensure Internet safety for minors (*see* Exhibit 3.2).

Exhibit 3.2 The Forum on Safeguarding the Future: Online Protection of Underage Users at the Fourth World Internet Conference in Wuzhen, China, December 4, 2017

Source: CNSphoto

Fifth, to crack down on cyberterrorism and cybercrime. China ought to strengthen capability building in cyber anti-terrorism, anti-espionage, and anti-secrets theft, and crack down on cyberterrorism and cyber espionage. We must follow the principles of comprehensive governance, source control, and law-based prevention, and severely curb illegal activities, such as online fraud, cyber theft, gun and drug trafficking, infringement on citizens' personal information, the dissemination of pornography and obscene materials, and hacking.

Sixth, to improve the cyberspace governance system. China ought to hold an open and transparent law-based governance of the network to ensure that the law is enforced strictly, administered impartially, and supervised publicly. We will further improve the overall system of laws and regulations governing cyberspace, as well as other related systems, to enhance the scientific and standardized management of cybersecurity. We will speed up the development of a comprehensive cyberspace governance system with laws and norms, combining administrative regulation, industry self-regulation, technical support, public supervision, and social education. We will also strengthen the protection of the confidentiality of communications, freedom of speech, trade secrets, and shield the right to reputation, property rights, and other legitimate rights and interests in cyberspace.

Seventh, to solidify the foundation of cybersecurity. China must persist in innovation-driven development, actively create a policy environment conducive to technological innovation, coordinate resources and strength, and make breakthroughs in core technologies as soon as possible. We ought to establish and improve the national cybersecurity technology support system and strengthen the research on the basic theory of cybersecurity and its major issues. China must lay effective groundwork for cybersecurity, such as classified protection, risk assessment, and vulnerability detection. We also need to strengthen the mechanisms of cybersecurity monitoring and early warning, and establish an emergency response system for major cybersecurity incidents. We ought to carry out cybersecurity talent management projects, professionalize cybersecurity courses, and build first-class cybersecurity schools and innovation parks. We will foster publicity of cybersecurity by vigorously carrying out public education activities to raise citizens' awareness on national cybersecurity issues (*see* Exhibit 3.3).

Eighth, to improve cyberspace protection capability. As cyberspace is a new territory of national sovereignty, we must build a cybersecurity protection system that is commensurate with China's international status and cyber prowess. We aim to make timely discoveries, resist network intrusions, develop cybersecurity defense methods, and forge a strong shield for China's cybersecurity.

Exhibit 3.3 A class activity on Safe Internet Access for Children at a local elementary school in Sichuan Province, China

Source: CNSphoto

Ninth, to enhance international cooperation in cyberspace. On the basis of mutual respect and trust, we will strengthen dialogue and cooperation, and urge the reform of international cyberspace governance. China supports the United Nations in promoting the development of international rules and international counter-terrorism conventions on cyberspace, in improving the judicial assistance mechanism against cybercrime, in deepening international cooperation in policy and lawmaking, technological innovation, standardization, emergency response, and in the protection of critical information infrastructure. China will strengthen its support for Internet technology diffusion and infrastructure construction in developing countries and backward regions, and will strive to close the digital gap.

3.3 Establishing a Sound Legal System for Cybersecurity

The rule of law applies to cyberspace. The use of the Internet to advocate the toppling of governments, propagate religious extremism, or to incite separatism and terrorism, must be resolutely prevented and punished. Under no circumstances can such activities be allowed to go unchecked. The use of the Internet to engage in fraud, circulate obscene materials, commit slander, or sell contraband goods, cannot be left unchecked. Countries of the world ought not to allow such activities to take place.

To accelerate the promulgation of cyber legislation, improve the law-based supervision measures, and mitigate cyber risks, China formulated the *Cybersecurity Law*, which is the basic law of cybersecurity. Based on this law, China continuously improved the system of cybersecurity laws and regulations, increased the enforcement of the *Cybersecurity Law*, and established a sound legal system for cybersecurity with Chinese characteristics.

3.3.1 The Promulgation of *Cybersecurity Law* Forms the Basic Legal Framework

In recent years, various departments in China have formulated departmental regulations and normative documents on cybersecurity. The National People's Congress and the State Council have also promulgated and implemented several laws, decisions, and administrative regulations on cybersecurity. This lays the foundation for cybersecurity legislation and provides a favorable legal basis for the standardization, and a protection system of the healthy and orderly development of China's information industry. In general, however, there are problems in cybersecurity legislation, which can be typified by unreasonable legal structures, the lack of overall planning and coordination, an over-emphasis on principle or generality, and insufficient protection of citizens' rights and interests.

To solve these problems, China legislated the *Cybersecurity Law*, which took effect on June 1, 2017 (*see* Exhibit 3.4). Its guiding ideology is as follows:

> We should uphold the holistic national security concept as a guide, follow the principles of proactive utilization, scientific development, law-based regulation, and security protection, to give full play to the leading and driving role of legislation. We also ought to address the prominent current

Exhibit 3.4 The enactment of the *Cybersecurity Law of the People's Republic of China*, June 1, 2017

Source: CNSphoto

problems in the field of cybersecurity, improve the national cybersecurity protection through institutional improvement, take the initiative in cyberspace governance and rulemaking, and effectively safeguard national cyber sovereignty, security, and development interests.

We ought to uphold the following principles in the formulation of the *Cybersecurity Law*.

First, we must fully learn from work done on cybersecurity in recent years and establish the basic institutional framework to protect cybersecurity, based on China's current situation of cybersecurity and cyberspace-related legislation. We ought to focus on institutional arrangements, make corresponding normative provisions, and establish and improve related systems with Chinese characteristics from the following aspects of cybersecurity: network equipment and facilities, operation, data, and information. At the same time, we must draw on the experience of other countries to ensure that our main system is consistent with international practices, and that domestic and foreign-funded enterprises are treated as equals in China.

Second, we should be problem-oriented. As the country's basic law in cybersecurity governance, the *Cybersecurity Law* highlights the existing cybersecurity problems in China. In recent years, some mature practices have been refined into regulations to provide effective legal protection for the work on cybersecurity. The principled provisions are made for some institutional arrangements that are necessary but lack actual application. Attention ought to be paid to the connection with existing laws and regulations, and to the interfaces reserved for the formulation of supporting laws and regulations.

Third, we should place equal emphasis on cybersecurity and informatization. We ought to pursue a balanced relationship between the two to safeguard cybersecurity and to develop a higher level of informatization. The *Cybersecurity Law* forges a good environment for development by ensuring security. It not only focuses on standardizing cybersecurity regulations, but also attaches great importance to the protection of the legal rights of various parties involved in cyberspace, the free flow of cyber information that conforms to cyber laws, and the healthy development of network technology innovation and informatization.

3.3.2 Prompt Promulgation of Supporting Laws, Regulations, and Policies

After the promulgation of the *Cybersecurity Law*, the Cyberspace Administration of China and other relevant departments have accelerated the formulation of supporting documents and rules for the Law, to promote the continuous improvement of the cybersecurity legislative framework.

For instance, the Cyberspace Administration of China (CAC) promulgated the *National Cybersecurity Incident Emergency Plan* and the *Measures on the Security Review*

of Network Products and Services. Together with the relevant departments, the CAC issued the *Catalogue of Critical Network Equipment and Cybersecurity Products (First Batch)* and the *Announcement on the Issuance of the List of the Institutions Responsible for Safety Certification and Safety Testing of the Critical Equipment and Cybersecurity Products (First Batch)*. This is to ensure that important systems such as cybersecurity emergency response, cybersecurity review, and product testing and certification established by the *Cybersecurity Law*, can be successively implemented. The Supreme People's Court and the Supreme People's Procuratorate jointly issued the *Interpretation of Several Issues concerning the Application of Laws in Handling Criminal Cases of Infringement of Citizens' Personal Information*, which provides an effective legal tool to be used for the protection of citizens' personal information.

In addition, the *Regulations on the Security Protection of Critical Information Infrastructure and the Classified Cybersecurity Protection*, intended to be released as administrative regulations of the State Council, have begun to solicit public opinion.

Several supporting policies, such as the *Measures on Security Assessment of Cross-Border Transfer of Personal Information and Important Data*, and the *Cybersecurity Law*, are also being developed.

3.3.3 Rapidly Carrying Out Inspections to Ensure Effective Law Enforcement

On August 25, 2017, the Standing Committee of the National People's Congress announced that it would carry out inspections on the effective implementation of the *Cybersecurity Law* and the *Decision of the Standing Committee on Strengthening Network Information Protection* (referred to as "one law and one decision") in several provinces, autonomous regions, and municipalities. The inspection aimed to uncover problems, analyze the causes of those problems, and propose suggestions for solving key issues and predicaments when implementing the "one law and one decision."

The inspection of the implementation of the "one law and one decision" has focused on the following aspects:

1. Publicity and education;
2. Formulation of supporting laws and regulations;
3. Strengthening the protection of critical information infrastructure and the implementation of classified protection of cybersecurity;

4. Governance of illegal and harmful network information and the maintenance of a favorable cyberspace ecosystem;
5. Protecting citizens' personal information, and investigating and punishing the infringement on citizens' personal information and related crimes.

The law enforcement inspection is normally conducted one year or several years after the law is implemented, while the inspection of the *Cybersecurity Law* was conducted only half a year after its implementation. The unusual frequency demonstrates the emphasis placed by the NPC Standing Committee on the implementation of the *Cybersecurity Law*. It also reflects the important position of the *Cybersecurity Law* in the development and security of the country.

The results of the inspection show that all localities and departments have thoroughly implemented the strategic plan of the Central Committee of "building China into a cyber power," integrated cybersecurity into the overall socioeconomic development plan, and promoted cybersecurity and the protection of network information. Specifically, the achievements in the implementation of the *Cybersecurity Law* have been to:

1. Carry out in-depth publicity and education to enhance public awareness of cybersecurity;
2. Formulate supporting laws, regulations, and policies, to build a legal system of cybersecurity;
3. Improve security and prevention capabilities to ensure the secure operation of the network;
4. Control and eliminate illegal information to secure a vibrant cyberspace;
5. Strengthen personal data protection and crack down on the infringement on Internet users' personal information;
6. Support the promotion of core cybersecurity technological innovation.

However, there are still some difficulties and problems in implementing the "one law and one decision" and in maintaining network security.

First, the urgent need for public awareness of cybersecurity to be strengthened. Second, the weak cybersecurity infrastructure. Third, existing cybersecurity risks and hidden dangers. Fourth, the inadequate protection of Internet users' personal information. Fifth, the need for the *Cybersecurity Law* enforcement system to be further

streamlined. Sixth, the need for supporting laws and regulations of the *Cybersecurity Law* to be improved. Seventh, a shortage of cybersecurity professionals.

These problems in the implementation of the *Cybersecurity Law* reflect the short board in China's cybersecurity and provide a clear direction for future efforts.

3.3.4 The Digital Economy and the Combat against Cybercrime and Illegal Industry Chains

The *Criminal Law of the People's Republic of China* (1997 Revision) clearly stated the criminal charges for computer crimes, namely, that of illegally invading computer information systems (Article 285), of destroying computer information systems (Article 286), and of using computers to commit traditional crimes (Article 287). However, this definition of the crime of illegally invading computer information systems (Article 285) is too narrow as it applies only to state affairs, national defense, and science and technology. According to Article 286, the suspect can only be charged with the crime if his actions caused the failure of a computer information system. As a result, the People's Courts were often unable to prosecute suspects in cases of cybersecurity infringement.

In order to keep up with the times, the Standing Committee of the National People's Congress promulgated *Amendment VII* to the *Criminal Law of the People's Republic of China* in February 2009, including the criminalization of other behaviors that jeopardize the country's information system, in addition to those related to state affairs, national defense, and science and technology. Article 285 stipulates:

> Whoever provides special programs or tools used for intruding into or illegally controlling computer information systems, or whoever knows any other person committing the criminal act of intruding into or illegally controlling a computer information system, and still provides programs or tools to such a person shall, if the circumstances are serious, be punished under the preceding paragraph.

In August 2015, the NPC Standing Committee adopted *Amendment IX* to the *Criminal Law*, which further reinforced the crackdown on cybercrime. The main amendments were as follows.

First, to further strengthen the protection of citizens' personal information, the Amendment modified the provisions to the crime of selling and illegally providing citizens' personal information, obtained by performing duties or by providing services. It broadened the definition of the crime of illegally invading computer information systems, and added a provision to the criminalization of selling or illegally providing citizens' personal information.

Second, in response to the failure of network service providers to fulfill their security management obligations resulting in serious consequences, the following provision was added to the *Criminal Law*:

> Network service providers shall be prosecuted with criminal liability, if they fail to comply with the security management obligations stipulated by laws and administrative regulations, and refuse to rectify after being ordered to by regulatory authorities, resulting in the dissemination of illegal information or the leakage of users' personal information with severe consequences, or resulting in the loss of evidence in criminal investigations.

Third, the following acts were clearly stipulated as crimes:

1. Establishing websites or communication groups for committing fraud, propagating criminal methods, producing or selling prohibited or controlled items, and so on;
2. Publishing information on the production or sale of prohibited items, such as drugs, guns, obscene materials, controlled items, or other illegal information;
3. Providing information for the purpose of fraud or other criminal activities (*see* Exhibit 3.5).

Fourth, the following provision was added to the *Criminal Law* in response to the increasing number of criminals propagating law-breaking methods, or abetting other would-be criminals in cyberspace:

> Criminal liability shall be prosecuted depending on the severity of the action of providing technical support for Internet access, server hosting, network storage, data transmission and communication, or supporting publicity and payment settlement for abusers of the information network with criminal intent.

Exhibit 3.5 Detention of criminals on a mega-network platform scam in Wuhu, China in October 2018

Source: Imagine China

Fifth, in response to the illegal establishment of pseudo base stations that seriously disrupted radio order and infringed on citizens' rights and interests, the criminalization of disrupting radio communications was modified to reduce the threshold of crime and enhance operability (*see* Exhibit 3.6).

Sixth, the following provision was added to the *Criminal Law*:

> It is a criminal act to fabricate and spread false dangers, epidemics, disasters, and policing on information networks or other media; or knowing that the abovementioned is false information, deliberately spread [them] on information networks or other media, thereby seriously disrupting social order.

Exhibit 3.6 Pseudo base stations uncovered by Guangzhou police in cooperation with companies, such as Tencent, 360, and Baidu, through big data platforms

Source: CNSphoto

3.4 Building a Sound Cybersecurity Standardization System

Cybersecurity standardization is an important part of the system that safeguards national cybersecurity, and plays a fundamental and normative role in building a secure cyberspace and in reforming international cyberspace governance. The Chinese government emphasizes the standardization of cybersecurity, and has set up a cybersecurity national standards body and issued relevant documents to promote national standardization efforts in cybersecurity. Remarkable results have been achieved.

3.4.1 Organization

China's work on the standardization of cybersecurity can be traced back to the 1980s and is easily divided into two phases. Before 2002, cybersecurity standards were formulated by various authorities and industries according to their business needs. There was no unified planning or overall management, or any effective communication and coordination, among the departments.

In 2002, the China National Information Security Standardization Technical Committee (TC260) was established under direct leadership of the National Standards Committee as a counterpart of ISO/IEC JTC1 SC27. According to Document [2004] No. 1 of the National Standards Commission, all applications for the national cybersecurity standard project by the relevant departments must be reviewed, coordinated, and submitted by the National Information Security Standardization Technical Committee from January 2004 onward. Further, in the process of formulating the national cybersecurity standards, the Commission's working groups, or main drafting units, ought to actively cooperate with the National Information Security Standardization Technical Committee responsible for submitting the national standards for review and approval. The establishment of the National Information Security Standardization Technical Committee shows that China's work on the standardization of cybersecurity has entered a new era.

To date, the TC260 has launched seven working groups and a special task force. WG1 is the cybersecurity standardization system and coordination working group. It is responsible for studying the cybersecurity standardization system, tracking the development of international cybersecurity standards, researching and analyzing domestic demands for the application of cybersecurity standards, and proposing new projects.

WG2 is the working group on security and confidentiality standards for the classified information system. Its main tasks are the research, proposal, formulation, and revision of the security and confidentiality standards for the classified information system, to ensure the overall security of the system.

WG3 is the cryptographic technology standards working group responsible for the research and formulation of cryptographic algorithms and modules, and key management standards.

WG4 is the identification and authorization working group. Its main tasks include the analysis, research, and formulation of PKI/PMI standards at home and abroad.

WG5 is the cybersecurity assessment working group responsible for studying and researching the status quo and development trends of domestic and international assessment standards, proposing assessment projects, and developing assessment plans.

WG6 is the communications security standards working group responsible for studying and researching the status quo and development trends of communications security standards, formulating and revising them, and proposing the establishment of related systems.

WG7 is the cybersecurity management working group responsible for the study of the cybersecurity management standardization system and the formulation of cybersecurity management standards.

The Big Data Security Standards Task Force is responsible for the development of security standards related to big data and cloud computing. Its specific tasks include researching the urgent needs for standardization, researching and developing standard formulation roadmaps, setting direction for annual standards research and development, and organizing key standards formulation in a timely manner.

3.4.2 Achievements

Since its inception, the National Information Security Standardization Technical Committee has focused on formulating the key standards urgently needed in the national cybersecurity protection system. The Committee has been adhering to the principle of laying equal stress on drawing from international standards and from independent research and development. It has also conducted research and implemented a revision of the national cybersecurity standards in a planned, step-by-step manner. As of April 2018, it had officially released 215 national cybersecurity standards.

In order to strengthen the management of cybersecurity standardization and provide full service for industries and units, the National Information Security Standardization Technical Committee has established a national cybersecurity standards management and service platform, realized an open and transparent management of the entire development life cycle of cybersecurity standards, and built a resource library for referencing domestic and international cybersecurity standards.

At the same time, the Committee has underlined the top-level design and strategic planning of cybersecurity standardization, and has developed supporting standards for cybersecurity in line with national cybersecurity policies to meet the urgent needs of various cyber authorities. In the development of international standards,

the Committee has actively organized international exchanges on cybersecurity standardization, monitored new international achievements, substantively participated in international standardization activities, put forward several proposals, and made contributions to the formulation of international standards.

The establishment of China's cybersecurity standardization system has provided strong technical support and basis for various cybersecurity protection tasks. These tasks include: the cybersecurity management of cloud computing services; the security inspection of government information systems; the classified security protection of information systems; the testing, certification, and the market accessibility of cybersecurity products; cybersecurity risk assessment; and the protection and confidential security inspection of classified information systems.

3.4.3 Measures

In August 2016, the Office of the Central Cyberspace Affairs Commission, General Administration of Quality Supervision, Inspection, and Quarantine, and the National Information Security Standardization Technical Committee, jointly issued the *Several Opinions on Strengthening National Cybersecurity Standardization Work*. It was proposed in the document that with the rapid development and application of network information technology, and with cybersecurity becoming increasingly complex and severe in this new era, tighter requirements for the work on standardization of cybersecurity are required. To implement the national cyber development strategy, we need to deepen the reform of cybersecurity standardization work, and build a unified, authoritative, scientific, and efficient cybersecurity standardization system. We also need to develop a corresponding working mechanism to support the development of cybersecurity and informatization. We will take the following measures:

1. Establish a coordinated and cooperative working mechanism. We will establish a unified and authoritative national standard working mechanism under the leadership of the National Standards Commission and the National Information Security Standardization Technical Committee. Under the overall coordination of the Office of the Central Cyberspace Affairs Commission, and with the support of the cybersecurity authorities, we will unify the technology, submission, review, and approval of national cybersecurity standards. For other national standards relating to cybersecurity, we ought to seek the opinions of the Office of the Central Cyberspace Affairs Commission and the

relevant cybersecurity authorities, to ensure the coordination of national standards with the cybersecurity standardization system.

We will explore the establishment of a liaison and a consultation mechanism for the cybersecurity industry, to ensure coordination and convergence of industry and national standards, and to avoid any contradiction between differing industry standards. We will establish a standard information-sharing mechanism for major national projects and key science projects. In addition, we will promote the compatibility of military and civilian standards to strengthen military–civilian integration in the cybersecurity and informatization sectors.

2. Strengthen the building of the standardization system. We will build a scientific standardization system to synchronize the planning and development of cybersecurity standards with IT application standards. We will optimize and improve standards at all levels, integrating and streamlining the mandatory ones, optimizing and improving those that are recommended, and developing industry-specific standards and recommendations. In principle, no local cybersecurity standards will be formulated based on locality.

   We will promote the urgently needed formulation of key standards. Focusing on the urgent needs of national strategies, such as the "Internet Plus Action Plan," "Made in China 2025," and "Big Data Development Action Plan," we will accelerate the research and development of standards for different fields, such as critical information infrastructure protection, cybersecurity review, network identity credibility, key IT products, the security of industrial control system, big data security, personal data protection, smart city security, Internet of Things, Next-generation communications network security, Internet TV terminal product security, and cybersecurity information-sharing.

3. Improve the quality and basic capabilities of cybersecurity standards. We will improve the applicability of standards and expand the participation and coverage of standards formulation, to fully and effectively meet the needs of cybersecurity management, industrial development, and those of Internet users. We will raise standards to an advanced level and shorten the cycle of formulation and revision to meet the needs of cybersecurity protection, and those of the development of emerging technologies and industries in a timely manner. We will make the formulation of standards more normative to ensure that they are based on rigorous work procedures. We will strengthen the basic capacity

building in standardization, as well as the research on the strategy and basic theory of cybersecurity standardization.

4. Enhance the publicity and implementation of cybersecurity standards. We will strengthen the publicity and interpretation of standards in cybersecurity management and combine publicity with implementation. We will press ahead with the implementation of the standards, and actively refer to national standards when formulating policy documents and deploying work.
5. Strengthen international standardization. We will participate substantively in standardizing international cybersecurity, to have a say and build our influence. We will persist in the work and build a team of experts who excel in both technical knowledge and foreign languages.
6. Build a team of cybersecurity professionals. We will actively conduct training to develop highly skilled cybersecurity talents and cybersecurity standardization experts.
7. Provide sufficient financial support. All departments and localities must prioritize the standardization of cybersecurity, and encourage enterprises to increase their investments in the research, development, and application of cybersecurity standards.

Chapter Four

KEY FIELDS OF CHINA'S CYBERSECURITY PROTECTION

4.1 Protection of Critical Information Infrastructure

In his speech at a symposium on cybersecurity and informatization on April 19, 2016, President Xi Jinping stated that "as the nerve center of economic and social operations, critical information infrastructure (CII) is the top priority of cybersecurity and may also be the main target of cyberattacks," and he put forward the instruction and requirement of "taking effective and practical measures to protect the security of China's CII."

The *Cybersecurity Law of the People's Republic of China* came into effect on June 1, 2017, and devoted a section to elaborating the operations security for CII. In 2018, the Chinese government officially promulgated the *Regulation on the Protection of the Critical Information Infrastructure* (hereinafter referred to as the "Regulation"), which detailed the requirements stated in the *Cybersecurity Law*. With this, China's CII protection system has been formally established, and various questions from the international community have now been clarified.

4.1.1 The Identification and Scope of China's Critical Information Infrastructure

The effective and complete identification of CII is the logical starting point for establishing a CII protection system. In this regard, Article 2 of the Regulation inherits the provisions of the *Cybersecurity Law* and adopts asset importance as the

criterion for the identification of CII. In other words, all the information infrastructure—whose damage, loss of function, or leakage of data may seriously jeopardize national security, national economy, people's livelihoods, and public interest—will be included in the scope of the protection of CII. Article 9 further outlines the areas or industries of China's CII, which fall into a total of 18 categories—telecommunications, the Internet, radio and television, satellite navigation, banking, securities, insurance, electricity and the power grid, petroleum and natural gas, petrochemicals, civil aviation, railways, water conservancy, education, medical and health, social security, national defense technology industry, and e-government. Hence, it is evident that the logical starting point for China's CII protection system is asset importance.

This criterion is in line with international conventions. For example, in February 2013, the United States issued *Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity* and *Presidential Policy Directive (PPD-21) Critical Infrastructure Security and Resilience*, identifying 16 critical infrastructure sectors. These sectors are: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactor, materials, and waste; transportation systems; and water and wastewater systems. Recently, Singapore released the *Cybersecurity Bill*, in which the CII is defined as a computer or a computer system necessary for the continuous delivery of essential services that Singapore relies on, and the loss or compromise of the computer or the computer system would have a debilitating impact on the availability of the country's essential services. These essential services include national security, defense, foreign relations, the economy, public health, and public safety and order in Singapore. It can be seen that Singapore has also followed the identification criterion of asset importance.

Let's further examine the identification of the CII in a specific field or sector. Article 12 of the Regulation stipulates that the following factors shall be considered in the specific identification of CII. First, the importance of the network facilities and information systems to the core business of the sector or field. Second, the severity of harm that may be caused by the destruction of these network facilities and information systems to the sector or field. Third, the impact on any other related sector or field.

A similar mindset is also embodied in the German *IT Security Act* which came into effect on July 25, 2015. The Act defines critical infrastructure as those whose

failure or impairment would cause significant supply shortage to a large number of users, and therefore are highly important to the public. To further identify the scope of critical infrastructure, the German Ministry of the Interior issued decrees in May 2016 and June 2017, delineating the scope of the critical infrastructure in several sectors and fields such as energy, information technology and communications, water and food, health, finance and insurance, and transportation.

The above two decrees also take asset importance as the criterion based on the following steps: first, identifying key businesses by sector or field; second, identifying the types of supporting facilities necessary for the key businesses; and third, setting sector-specific threshold values according to the key businesses and types of supporting facilities. Those above the threshold values shall be designated as critical infrastructure. For example, in the field of clinical medicine, the threshold is the number of inpatients annually.

In general, from the coverage of sectors and fields to the specific identification of CII facilities, China takes the same approach as international practice (*see* Exhibit 4.1).

4.1.2 The Guideline of CII Protection and Its Differences from the Classified Protection System for Cybersecurity

Since the CII is vital to the country, society, and people, the level of protection ought to be high. From this point of view, the classified protection system for cybersecurity is compatible with the protection of CII. The salient feature of the classified cybersecurity protection system is to classify the protection according to asset importance, and require operators to build a corresponding security protection capability.

Therefore, the *Cybersecurity Law* and the Regulation both stipulate that the protection of CII must be based on the classified protection system for cybersecurity. However, they also stipulate that key protection must be implemented on top of that.

What does "key protection" mean?

According to the Regulation, key protection means a comprehensive, scientific, and advanced overall design for the protection of CII from the perspective of risk management. In fact, at the Symposium on Cybersecurity and Informatization on April 19, 2016, President Xi Jinping made a speech on the importance of risk management for the protection of CII. Using risk management to coordinate all aspects of protection of CII is one of the most important tasks of implementing key protection.

Exhibit 4.1 The opening ceremony of China's Critical Infrastructure Protection Committee in Chengdu, China, July 16, 2016

Source: CNSphoto

A complete risk management process consists of the following four steps: to identify risks, assess the risks, respond to the risks, and continuously monitor changes in the risks and environments. These four steps form a feedback loop that continually raises the ability of an organization in risk management. We will discuss the four steps one by one.

First, the identification and assessment of risks are of pioneering significance to the protection of cybersecurity and even to CII. President Xi Jinping stated, "As the saying goes, 'with a profound understanding of yourself and the enemy, you can fight a hundred battles with no danger of defeat.' To safeguard cybersecurity, we must first identify where the risk is, what kind of risk it is, and when the risk will occur;

unspotted risk is the greatest risk." If we cannot identify the risk, the only consequence will be our being ignorant of "who comes in, whether he or she is an enemy or friend, and what he or she is doing."

Second, risks can be further categorized as internal risks and external risks. President Xi Jinping stressed that

> By identifying and assessing internal risks, we are able to have a clear understanding of the domestic situation, identify the loopholes, notify the results, and push for rectification. Identifying and understanding external risks allows us to know in which field others in the outside world are fighting with aircraft and cannons, while we are still wielding swords and spears.

Third, risk management has a comprehensive and fundamental guiding role for the overall arrangement and the resource allocation of cybersecurity protection. President Xi Jinping once stated that since there is no absolute security in cyberspace, we ought to ensure security based on the fundamental dimension of our national context and avoid seeking absolute security at any cost. Otherwise, we may bear a heavy burden and be unable to carry out other important work.

Therefore, under the constraints of resources, risk management is the best guide for us to prioritize our work and allocate cybersecurity resources scientifically and efficiently. President Xi said that by identifying and assessing risks, we can keep a detailed and clear account. We will know what must be heavily guarded by all sectors, what must be properly protected by local governments, and what must be safeguarded by market forces.

In fact, risk management is one of the basic guiding principles not only for cybersecurity but also for national security. The *National Security Law* specifically devotes two sections ("Intelligence Information" and "Risk Prevention, Assessment, and Warning") in Chapter 4 titled "National Security Rules" to specify the risk management of national security.

In sum, adhering to the idea of risk management can help us develop a system surpassing the single-facet criterion of asset importance in the protection of CII, and the compliance requirements based on the bottom line and static mindset of security capabilities in classified protection. Moreover, we will be able to effectively understand the changing dynamics between offensive and defensive capabilities. We will be able to scientifically and efficiently allocate finite security resources, thereby gaining the initiative in the dynamic competitive arena to achieve substantial security outcomes.

4.1.3 The Regulation and the Internationally-Accepted Risk Management Principle

The risk management principle in the Regulation is mainly reflected in the following aspects. First, the Regulation followed the instruction of President Xi to establish an "all-weather and all-dimensional cybersecurity situational awareness system." Articles 27 and 28 of Chapter 4 "Protection and Promotion" respectively require the national network information and protection authorities (including the competent supervisory departments of a sector or a field) to establish a cybersecurity information-sharing mechanism at the national, sectoral, and field levels. These articles also require that a cybersecurity monitoring, warning, and information-sharing mechanism for each sector must be built so as to promptly study, aggregate, share, and notify of cybersecurity information to the authorities.

Article 27 also emphasizes that the cybersecurity information-sharing mechanism ought to give full play to the role of operating units and cybersecurity service organizations. It also requires the national network information department to coordinate the establishment of the cybersecurity information-sharing mechanism among government, enterprises, and network service organizations. So far, a multilevel cybersecurity information-sharing network with a complex matrix structure across the public and private sectors has been developed. The ultimate goal of this network is to comprehensively use the data collected from all sources and better understand the latest cybersecurity risks.

Second, Article 30 of the Regulation requires the departments responsible for cybersecurity protection to regularly conduct inspections of and tests on the cybersecurity risks in the CII, and the operators' performance of security protection. This routine inspection is essentially different from the previous "tick for compliance" way of security check. The departments have not only grasped the current situation of the cybersecurity risks in their own sectors and fields, but also deeply understood the nationwide cybersecurity risks through the monitoring and early warning system established by the national network and information authorities. Therefore, they can effectively guide and urge the operators to promptly uncover problems during the security inspection and testing, and propose security protection measures commensurate with the current risk situation. In this way, the sense of risks can be transformed into actual security protection requirements that correspond to the changes in external situation and can be put into practice.

Third, Article 29 of the Regulation stipulates that departments responsible for protection will establish and improve their contingency plans for cybersecurity

incidents in their sectors and fields, regularly organize emergency drills, guide operators to tackle cybersecurity incidents, and provide the necessary technical support and assistance. The emergency drills, based on a comprehensive grasp of the changing cybersecurity risks, will undoubtedly avoid arbitrary decisions to the greatest extent, thus improving the pertinence and timeliness of the drills (*see* Exhibit 4.2).

According to the Regulation, a multilevel cybersecurity situational sensing system will be established for the protection of CII throughout the country. Real-time risk sensing and analysis will be translated into dynamic and targeted security protection requirements through the inspections, tests, and drills organized by competent authorities. In this regard, the security protection obligations for the operators of CII stipulated in Chapter 3 of the Regulation must be understood from the perspective of risk management. One of the most important obligations of the operators for the security protection of CII is to make timely adjustments to the security protection strategy according to the actual risk situation.

Through the abovementioned institutional arrangements stipulated in the Regulation, the risk sensing of government departments can be felicitously involved in the risk management of the CII operators in the process of risk identification and assessment. This mechanism can not only broaden the horizons of the operators, but also effectively prevent them from deliberately and selectively ignoring the impending risks for the development of their businesses.

Planning the security protection of CII through risk management is a core concept in the latest cybersecurity legislation, policies, and standards of the United States, the European Union, and other developed countries and regions.

Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity issued by former US president Barack Obama in 2013 explicitly requires the National Institute of Standards and Technology (NIST) to develop a Cybersecurity Framework, with risk management as one of the core measures to protect the critical infrastructure of the United States. At present, the NIST Cybersecurity Framework has been favored by many US regulatory authorities. For example, the US Securities and Exchange Commission (SEC), the US Federal Trade Commission (FTC), the Department of Homeland Security (DHS), and the Department of Energy (DOE), recommend this risk management-centered framework to their supervised entities.

The *Directive on Security of Network and Information Systems* (the NIS Directive) adopted by the European Parliament in 2016 for basic networks and information systems advocates the establishment of a risk management culture, where operators of

Exhibit 4.2 A network security emergency drill jointly held by the Henan Provincial Communications Administration and the Henan branch of CNCERT in June 2008

Source: Visual China

basic networks and information systems ought to conduct risk assessments and adopt the appropriate security measures proportionate to the risks they face.

In the same vein, Article 32 of the *General Data Protection Regulation (GDPR)* adopted in 2016 stipulates the security protection obligations of personal information controllers, which are as follows:

> Taking into account the state-of-the-art technology, the costs of implementation and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihoods and severity for the rights and freedoms of natural persons,

the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

In fact, many experts and scholars have pointed out that although there are significant differences between the legal systems of the United States and the European Union, their approaches and responses to cybersecurity issues are gradually merging. Risk management is regarded as one of the core issues, and operators are urged to adjust their security measures to adapt to changing cyber risks.

As stated in a report of the President's Commission on Enhancing National Cybersecurity established by then US president Obama in December 2016, global cyber and physical systems are increasingly converging, becoming interconnected, interdependent, and transcending national boundaries. This means that cybersecurity needs to be achieved by coordination at all levels: international, national, organizational, and individual. The recent outbreaks of the Wannacry and NotPetya viruses perfectly typified this. The recognition of risk management as a guide in the Regulation for coordinating security protection of CII paved the way for international cooperation among China, the United States, and Europe.

In short, the protection of CII is based on the classified protection system for cybersecurity. This approach imposes new security protection obligations on the operators of CII. More importantly, it also requires the national network and information authorities, and the departments responsible for security protection, to actively apprehend the security risk situation, and lead the specific protection work accordingly. The protection of CII aims to establish a coordinated and sustainable security protection system with risk management at its core, so as to better respond to the increasingly deteriorating security situation in cyberspace and effectively protect national security, the national economy, people's livelihoods, and public interest.

4.1.4 The Purposes of the Security Review of Network Products and Services

Article 22 of the Regulation states that if the network products and services purchased by operators of CII may affect national security, a security review will be conducted in accordance with national cybersecurity regulations. However, there are various misunderstandings and even misinterpretations about this requirement at home

and abroad. With the promulgation of the laws and regulations, such as the *National Security Law*, *Cybersecurity Law*, and *National Cybersecurity Strategy*, and the successive publications of *Measures on the Security Review of Network Products and Services* and the *Measures on Cybersecurity Review (Draft for Soliciting Opinions)*, China's value orientation, goals, and institutional framework are becoming clearer.

First, the value orientation of the cybersecurity review is to safeguard national security. In accordance with the provisions of Article 59 of the *National Security Law*, in the field of information technology, the national security review will be conducted on matters and activities that affect or may affect national security, including network information technology products and services, with the aim of effectively preventing and resolving national security risks. The *Cybersecurity Law* specifies in Article 35 that CII operators purchasing network products and services that may affect national security, must go through a security inspection organized by the national network and information authorities, and other relevant departments of the State Council.

The two laws are in the same vein. In the section "Protecting Critical Information Infrastructure" of the *National Cybersecurity Strategy*, it is stipulated that a cybersecurity review system for important information technology products and services procured and used by the CPC and government departments in key fields must be established. The criterion for defining CII is precisely the information facilities whose damage, loss of function, or leakage of data may seriously jeopardize national security, the national economy, people's livelihoods, or public interest.

Therefore, we can see from the current *Measures on the Security Review of Network Products and Services* that the value orientation of the cybersecurity review gives full play to the coerciveness and authority of state power, and to safeguarding national sovereignty, security, and development interests. The promulgation of the *Measures on the Security Review of Network Products and Services* marked the full implementation of "two laws and one strategy."

Second, the cybersecurity review is positioned to ensure controllable security. As an important institution focusing on national security, the cybersecurity review is accurately targeted at important network products and services used by information systems related to national security and public interest. Its fundamental goals are to improve the controllability of the security of network products and services, and to reduce the supply chain security risk. The concepts of controllable security and the supply chain security risk can be understood from the following two perspectives.

1. Differences with business performance reviews. The cybersecurity review does not evaluate and assess the business performance of the products and services. Rather, it checks whether operators take action without authorization, or whether the output was illegally tampered, or interfered with, or interrupted in the process. In more general terms, products and services that affect or may affect national security must be absolutely "loyal to the user." However, the function and performance of the products and services is not the focus of the cybersecurity review.
2. Connotation of controllable security. Article 4 of the *Measures on the Security Review of Network Products and Services* lists the four risks that the review ought to focus on: stability (the risks of illegal control, interference, and disruption), supply chain security (the risks in R&D, delivery, and technical support), and users' control over their own information (the risks of using the convenience of providing products and services for illegal collecting, storing, processing, or for utilizing user-related information), and the independence and autonomy of users (the risks of users' reliance on products and services that carry out unfair competition or to harm the interests of users).

Of course, the connotation of controllable security will be updated according to the changing situation. The last provision of Article 4 is added for this purpose.

This principle can be further explained by an analogy with a staff selection process for an important position. During recruitment, a candidate will be assessed on three aspects—ability (through a qualifying certification), health (through a regular physical examination), and loyalty (through a review of their background and continuous user behavior analysis).

The same is true for key network products and services. First, the functions of products and services (through certification and assessment); second, the sustained operational ability of products and services (through security checks); third, the credibility of products and services (through cybersecurity review).

Finally, the institutional framework for the cybersecurity review involves the full participation of various parties. In his speech on April 19, President Xi proposed the incisive conclusion that "cybersecurity is for the people, and by the people." Article 9 of the *National Security Law* details that

> In maintenance of national security, priority shall be given to prevention, and equal attention shall be paid to temporary and permanent solutions.

> Specialized tasks shall be combined with reliance on the masses, and the functions of specialized authorities and other relevant authorities in maintaining national security shall be maximized. Citizens and organizations shall be extensively mobilized to prevent, frustrate, and legally punish any conduct that compromises national security.

Therefore, the cybersecurity review is not something that only concerns a particular department, but an important work for everyone. Specifically, the broad participation in the cybersecurity review is reflected in the following aspects.

The organization and leadership of the cybersecurity review are undertaken by the Cybersecurity Review Committee, which is set up by the Office of the Central Cyberspace Commission and other relevant authorities. Subordinate to the Committee are the Cybersecurity Review Office and a Group of Experts on Cybersecurity Review. These constitute the organization for the top-level design of cybersecurity review. At the initial stage, Article 8 of the *Measures on the Security Review of Network Products and Services* regulates various forms of review application, such as the application of enterprises and of the competent authorities and departments, recommendation from national industry associations, and feedback from the market. During the review, an independent third-party organization will first form an evaluation. Then, the experts will produce a comprehensive assessment based on the third-party evaluation and submit it to the Cybersecurity Review Committee. Following this, the Committee will draw their conclusion of the review. Lastly, after the approval of the Cyberspace Administration of China, the final conclusion will be released or published by the Cybersecurity Review Office.

On May 24, 2019, the Cyberspace Administration of China released the *Measures on Cybersecurity Review (Draft for Soliciting Opinions)*. It improves and perfects the *Measures on the Security Review of Network Products and Services*, and specifically adds new requirements for reviewing supply chain security. Currently, the Cyberspace Administration of China has solicited public opinions and is incorporating these into the draft. Once it is formulated and published, it will replace the *Measures on the Security Review of Network Products and Services*.

In summary, the sectors and areas of CII regulated by the Chinese government, and its specific criterion for the identification of CII, are consistent with international practices. In addition, China's CII protection system consists of two major levels. The first level is the classified protection system for cybersecurity, which specifies the

different security measures that must be taken for each network according to asset importance. The second level focuses on the identification, assessment, response, and monitoring functions of the dynamic security risk management highlighted in the Regulation. China has one additional level of classified protection system more than Europe and the United States, who directly adhere to risk-based legislative requirements. The reason is that Chinese network operators have weaker security capabilities and less experience in implementing security protection, and so there is an urgent need for China to improve its overall security level based on asset importance. After improving their basic security capabilities, the operators of CII ought to adjust and optimize their security protection strategies, according to the concept of dynamic risk management.

4.2 Protection of Data Security

Data has become a national basic strategic resource—this is the common understanding of the two documents guiding China's future socioeconomic development, namely, the *Outline for the Promotion of Big Data Development* and the *Outline for the 13th Five-Year Plan*. The former further states that big data is exerting an increasingly important impact on global production, circulation, distribution, consumption, economic operating mechanisms, social lifestyles, and national governance capabilities.

In fact, in all the documents issued by the State Council and various departments, only data (or big data) and archives are eligible to be called basic strategic resources. "Strategic resources" refer to land, grasslands, rare earths, oil, natural gas, food, water, forests, minerals, coal, and so on. "Basic" literally means more important. Hence, using this word to modify "strategic resources" reflects the high positioning of the data and the deep understanding of its role by the CPC and Chinese government. However, such a comparison also highlights a harsh fact that though China has established a relatively mature protection system for strategic resources, it has apparently not built a scientific and complete system for the protection of the data resources that matches its importance (*see* Exhibit 4.3).

As previously mentioned in Chapter Three, President Xi Jinping repeatedly stressed on many occasions that cybersecurity and informatization must be planned, deployed, promoted, and implemented in a unified way. At the Second Group Study Session of the Political Bureau, President Xi emphasized that China ought to improve its ability to protect critical national data resources. Accordingly, the *13th Five-Year*

Exhibit 4.3 China International Big Data Industry Expo in Guiyang, China, May 26, 2018

Source: CNSphoto

Plan puts forward the requirements of fully implementing the action plan for big data development and accelerating the sharing, openness, development, and application of data resources, to assist industrial transformation and upgrading, and social governance innovation. Under such circumstances, the question of how to effectively protect data as a valuable national basic strategic resource has become a top priority for the Chinese government.

With the official implementation of the *Cybersecurity Law* on June 1, 2017, the basic framework, key tasks, and requirements of China's cybersecurity work have been clarified. As for the specific protection of data security, Article 37 of this law stresses the security assessment system for the cross-border transfer of personal information and important data in a very distinctive way. How do we understand such an institutional innovation? What is the significance of the implementation of this system to the building of China's data resource protection system? These questions are the focuses of the following section.

4.2.1 Overall Design for Data Security in China's *Cybersecurity Law*

According to provisions of the *Cybersecurity Law*, data security protection can be divided into three dimensions. First, the maintenance of the confidentiality, integrity, and availability of network data (acronymized as the CIA of traditional information security), which is clearly stipulated in Article 10 of the "General Provisions" of the *Cybersecurity Law*. Article 21 specifies the security protection obligations of network operators, including the operators of CII, and sets out the requirement of preventing network data from being divulged, stolen, or falsified. Article 31 further defines the scope of CII, focusing on the possible harm caused by data breaches.

Second, personal information protection. The *Cybersecurity Law* not only inherits the main provisions of the existing Chinese laws on the protection of personal information, but includes additional provisions according to the characteristics, development needs, and concepts of this new era. For example, Article 40 clearly holds the network operator that collects and uses personal information responsible for protecting the information. Article 41 adds the principle of minimum sufficiency. Article 42 adds the conditions for personal information-sharing. Article 43 adds the right of an individual to delete and correct his or her personal data under certain circumstances. Article 44 provides for the first time a certain legal space for transactions on personal information transactions. These five provisions on personal information are all innovative not only in the protection of an individual's autonomy and the right of control over his or her own information, but also in full integration in both concept and principle with the current international rules, and the legislation on the protection of personal information in the United States and Europe.

Third, data protection at the national level. Articles 51 and 52 require the national network and information authorities and relevant departments to strengthen the collection of cybersecurity information and demand that departments responsible for the protection of CII to submit cybersecurity information in a timely manner. This means that the *Cybersecurity Law* authorizes the relevant national departments to collect and analyze important cybersecurity information, including those owned by the private sector. Article 37 stipulates that personal information and important data collected and produced by CII operators during their operations within the territory of the People's Republic of China will be stored within China. Personal information and important data provided to anyone outside China will be subject to a security assessment (*see* Exhibit 4.4).

Exhibit 4.4 Three dimensions of the provisions of the *Cybersecurity Law*

Dimension	Provisions
Data Security	Article 10: Maintain the confidentiality, integrity, and availability of network data. Article 21: Prevent network data from being divulged, stolen, or falsified. Article 27: No individual or organization may provide programs or tools for the purpose of conducting activities endangering cybersecurity, such as the stealing of network data. Article 31: The CII that will result in severe damage to state security, people's livelihoods, and public interest if it is destroyed, loses functions, or encounters data leakage.
Personal Data Protection	Article 40–44
Data Protection at National Level	Article 37: Personal information and important data collected and produced by CII operators during their operations within the territory of the People's Republic of China will be stored within China. Article 51: The National Cyberspace Administration will make overall planning and coordinate relevant departments to strengthen the collection, analysis, and public circulation of cybersecurity information. Article 52: The departments responsible for CII security protection shall report cybersecurity monitoring and early warning information according to relevant provisions.

The requirements of the *Cybersecurity Law* for data security protection can be summarized as follows:

Data security = integrity + confidentiality + availability

Personal information protection = data security + basic principles of personal information collection and usage (legal, reasonable, necessary, open, and transparent) + right to delete and correct personal information

Data security protection at national level = data security + right of disposal of important data + security assessment of data export

4.2.2 The Requirements of the *Cybersecurity Law* for Personal Information Protection

Nowadays, the wave of the information revolution and the full-scale development of digitalization have made production and people's lives increasingly integrated with the Internet. As more of real life shifts online, large volumes of personal information can be freed from the constraints of paper and can be directly recorded, transmitted, stored, and used in the form of a binary system. After digitalization and networking, personal information continues to retain its ability to identify a particular individual independently, or in combination with other information. The value of personal information can also be further explored and released with the support of modern computing and storage capabilities. In today's world, personal information has become one of the most important elements in the efforts to improve efficiency and support innovation in the digital economy of the future.

While the world is embracing the digitalization and networking of personal information, cybercriminal groups both at home and abroad have targeted personal information. They have stolen hundreds of millions of pieces of personal information and formed a black market for trading these information. Using the close relationship between individuals and their personal information, these cybercriminal groups have commited a variety of crimes, such as targeted fraud based on personal information. In addition, cyber identity theft may directly cause incalculable economic losses. The death of Xu Yuyu in 2016 due to the leakage and misuse of her personal information serves as a warning to us.

At present, the status quo of personal information protection in China needs to be improved urgently. In 2014 itself, there were data breaches in many well-known e-commerce companies, courier companies, recruitment websites, and test registration websites. Among them is the forum of a well-known mobile phone manufacturer that leaked the personal information of eight million users, including details of their account numbers, passwords, and social media accounts. The *2015 Review of China's Internet and Cybersecurity Situation* shows that there have been serious data breaches in China, such as the leakage of personal information of about 100,000 candidates that sat for college entrance examinations and nearly 6 million users of a ticketing system (*see* Exhibit 4.5).

In his speech on April 19, President Xi Jinping systematically discussed the six key issues of the Internet and informatization. At the very beginning, he put forward the people-centered development of Internet and informatization. Then, he gave the instruction

that cybersecurity is for the people, and by the people. Obviously, there is a wide gap between the actual situation and the requirements stipulated by President Xi. If the situation of unauthorized access, use, disclosure, destruction, and modification of personal information cannot be improved, the future of cyberspace will still be full of thorns and traps. If the Internet is not safe for the people, how can it become a new space for people to study, work, and live in, and a new platform for them to access public services?

In this regard, the fourth chapter of the *Cybersecurity Law*, "Network Information Security," elaborates the norms of behavior for network operators in processing personal information. The five characteristics and innovations are as follows:

Exhibit 4.5 The "Clean and Secure" Internet Operation captured more than 40 cybercrime gangs and identified 120 million pieces of personal information illegally acquired in Guangdong Province from April to May 2018

Source: CNSphoto

First, the *Cybersecurity Law* is the most comprehensive and authoritative regulation on personal information protection in China. At present, China has not yet formulated a unified law on personal information protection. Prior to the promulgation of the *Cybersecurity Law*, the most important laws for the protection of personal information were the *Decision on Strengthening Network Information Protection* passed by the NPC Standing Committee in 2012, the *Decision on the Revision of the Law on the Protection of Consumer Rights and Interests of the People's Republic of China* adopted by the NPC Standing Committee in 2013, and the *Amendment VII* and *Amendment IX to the Criminal Law* adopted in 2009 and 2015, respectively.

As mentioned, the *Cybersecurity Law* includes several new provisions according to the characteristics, development needs, and protection concepts of the new era, such as the following:

1. The principle of minimum sufficiency. Network operators may not collect personal information unrelated to the services they provide.
2. The conditions for sharing personal information. No personal information may be provided to others without the consent of the person whose data is collected, except where the information has been processed in such a manner that it is now impossible to restore and retrace to the particular individual.
3. Data rights of individuals. If an individual discovers any network operator who has violated the provisions of laws, administrative regulations, or bilateral agreements in collecting or using his or her personal information, he or she has the right to request the network operators to delete the personal information. If an individual discovers that the personal information gathered or stored by network operators contains errors, he or she has the right to request the network operators to rectify the error. Network operators will adopt corresponding measures necessary for the deletion or correction.

Second, the *Cybersecurity Law* clarifies the party responsible for the protection of personal information. At the beginning of the chapter "Network Information Security," it puts forward the basic principle that whoever collects the personal information shall be held responsible. The Law sets the network operator that collects and uses the personal information as the party responsible for protecting it. It expounds that network operators must strictly protect the privacy of the users whose information they collect and establish user information protection systems. According to the provisions of this article, the network operator who collects and uses personal

information is the first person responsible—whether it is to prevent internal personnel from selling personal information, or to ensure that the system is not compromised and so would not result in any data breach. Identifying the responsible parties can not only avoid the situation where no one takes responsibility for the serious consequences of any leakage of personal information, but also force network operators to place importance on the protection of the personal information they collect.

Third, the *Cybersecurity Law* is in accord with advanced international concepts. In general, its provisions on the protection of personal information have been consistent with the existing international rules, and US and European legislations. At present, the main globally recognized legal documents for personal information protection include the *OECD Privacy Framework*, the *APEC Privacy Framework*, the *EU General Data Protection Regulation*, the *EU–US Privacy Shield*, and the *US Consumer Privacy Bill of Rights Act (2015)*. These legislations demonstrate the main principles of personal information protection—namely, the principles of clear purpose, consent and choice, minimum sufficiency, openness and transparency, quality assurance, guaranteed security, data subject participation, clear responsibility, and restricted disclosure.

These principles are also reflected in the *Cybersecurity Law*. For example, the principle of openness and transparency means that the purpose and scope of collecting and/or using personal information, and the measures of protecting personal information must be publicly disclosed in a clear, understandable, and reasonable manner, and public supervision ought to be accepted. This principle is embodied in the provisions of the *Cybersecurity Law*: network operators ought to disclose their rules for the collection and use of information, and explicitly state the purposes, means, and scope for collecting or using information. Another example is the principle of data subject participation. Compared with other existing legislations in China, one of the unprecedented highlights of the *Cybersecurity Law* is to give individuals the right to request the deletion or correction of their personal information under certain conditions.

Fourth, the *Cybersecurity Law* strikes a balance between the protection and use of personal information. In the era of big data and cloud computing, data, including personal information, ought to flow and be shared and traded freely to maximize its value in the form of agglomeration and economies of scale. However, the free flow of data may cause the individual or the organization that collects and uses such data to lose control over the personal information. Hence, the scope and the use of personal information will become uncontrollable. To achieve the balance between the two is one of the important challenges in the protection of personal information in the new era.

In this regard, the *Cybersecurity Law* first gives a certain amount of space for personal information transactions at the legal level, which is a huge improvement. The *Decision on Strengthening the Protection of Network Information* stipulates that personal information of citizens should not be sold, while the *Cybersecurity Law* stipulates that personal information of citizens should not be illegally sold. In other words, according to the *Cybersecurity Law*, citizens' personal information can be transacted under certain circumstances, giving the green light for legal transactions of personal information and opening the space for developing China's big data industry. Of course, the compliance requirements for such transactions are to be further formulated in detail.

Moreover, the *Cybersecurity Law* further specifies the legal provision of personal information, which is also an important innovation. It regulates that no personal information can be provided to others without the consent of the person whose information is collected, except where the information has been processed in such a manner that it is impossible to restore and retrace to the specific individual. According to the provisions, in at least two cases, personal information can be provided legally. The first is to have the consent of the individual whose personal information is collected, and the second is to anonymize the information so that whether it is used independently, or in combination with other information, it is impossible to identify a specific individual and to recover the information.

Fifth, the *Cybersecurity Law* demands mandatory notification and reporting after the occurrence of personal information security incidents. It stipulates that in the event of the occurrence, or possible occurrence of any personal information breach, damage, or loss, immediate remedies must be taken. The network operator must promptly inform the user and report to the competent authority in accordance with the regulations. Compared with previous legal provisions, the *Cybersecurity Law* adds the requirements of the new mandatory notification and reporting after the occurrence of personal information security incidents.

Globally, the mandatory reporting and notification of cybersecurity incidents, including breaches of personal information, have been a focus of recent legislation. Many countries and regions have further reinforced the awareness of being the main responsible party of organizations and institutions through mandatory informing and reporting to external parties, urging them to earnestly fulfill their obligations to protect personal information. In the United States, the federal-level *Health Insurance Portability and Accountability Act* and the *Gramm-Leach-Bliley Act* in the financial industry provide for the mandatory notification and reporting system of data security incidents. In addition,

47 states in the United States, as well as the District of Columbia, Guam, Puerto Rico, and the US Virgin Islands, have adopted laws on mandatory data notification and reporting. In the European Union, the *General Data Protection Regulations* and the *NIS Directive* also impose mandatory notification and reporting obligations. This time, China's *Cybersecurity Law* has drawn on the advanced experience on personal information protection of other countries.

The *Cybersecurity Law* has strengthened the protection of personal information and enabled people to safely enjoy the dividends brought by the Internet. It is a concrete manifestation of implementing the instructions of President Xi Jinping. The promulgation and implementation of the *Cybersecurity Law* can curb the abuse of personal information, enhance the protection of personal information, and protect users' legitimate rights and interests, and overall public interest (*see* Exhibit 4.6).

4.2.3 The National Standard of the Regulation on Personal Information Security and the International Standards

On August 22, 2017, the Office of the Central Cyberspace Affairs Commission, General Administration of Quality Supervision, Inspection, and Quarantine, and the National Information Security Standardization Technical Committee jointly issued the *Opinions on Strengthening National Cybersecurity Standardization Work* (hereinafter referred to as the "Opinions").

In the second part titled "Strengthening the Standard System," the Opinions puts forward the requirement of promoting the formulation of key standards urgently and clearly sets the formulation of the standards for personal information protection as one of the priorities. As pointed out in the Opinions, the standardization of cybersecurity is an important part of the cybersecurity protection system. It plays a fundamental, normative, and leading role in building a secure cyberspace, and in promoting the reform of the network governance system. In order to substantially improve the behavior of organizations and institutions that collect and use personal information, there is an urgent need for a set of scientific and advanced, and realistic and feasible standards for personal information protection.

At the end of December 2017, the National Standardization Committee officially issued the *Personal Information Security Specification* as the national standard for information security technology, which came into effect on May 1, 2018. The *Personal*

Exhibit 4.6 The Personal Information Protection Forum of the 2018 China Internet Conference in Beijing, China, July 12, 2018

Source: CNSphoto

Information Security Specification provides specific protection requirements for various organizations that deal with personal information including, but not limited to, institutions and enterprises. It was formulated as the basic standard document for the protection of personal information in China, laying a foundation for various activities related to personal information protection, as well as for the formulation and implementation of laws and regulations on personal information protection. In addition, it also serves as the guide and basis for personal information security management and security assessment conducted by national authorities and third-party assessment agencies.

First, in order to implement President Xi Jinping's instruction that cybersecurity is for the people, the *Personal Information Security Specification* manages to balance the following four values. The first value is the control of one's own privacy and personal information. This includes the control over the collection, use, and circulation of personal information, and that of the resulting impact on the individual owner of the data. The second value is the development interests, that is, reasonable appeals of enterprises and industries to make full use of personal information to offer, improve, and innovate their products and services. The third value is public interest, including

the use of personal information by government departments to pursue public administration, the free flow of information necessary for social development, and the public's right to be informed. The fourth value is national interest—that is, the positive and negative impacts caused by the cross-border flow of personal information on state sovereignty, national security and competitiveness.

Second, the *Personal Information Security Specification* is based on China's existing laws, rules, regulations, and standards, including the *Decision of the NPC Standing Committee on Safeguarding Internet Security*, the *Decision of the NPC Standing Committee on Strengthening Network Information Protection*, *Amendment V to the Criminal Law*, *Amendment VII to the Criminal Law*, *Amendment IX to the Criminal Law*, *Provisions on the Protection of Personal Information of Telecommunications and Internet Users*, *Information Security Technology: Guidelines for the Protection of Personal Information in Public and Commercial Service Information Systems (GB/Z28812-2012)*, and *Information Security Technology—Security Criterion on Supplier Conduct of Information Technology Products (GB/T 32921—2016)*.

Third, the *Personal Information Security Specification* refers to the most advanced foreign legislation on personal information protection, including international rules, such as the *OECD Privacy Framework*, the *APEC Privacy Framework*, and the EU and US legislations on personal information protection, such as the *General Data Protection Regulations*, the *Privacy Shield*, and the US *Consumer Privacy Bill of Rights Act*.

Lastly, the *Personal Information Security Specification* manages to be in line with international standards for the protection of personal information. ISO/IEC JTC1/SC27 is a subcommittee of the Joint Technical Committee (JTC1) of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is responsible for the research and formulation of the standardization of information security. SC27/WG5 is responsible for the development and maintenance of the standards related to identity management and privacy protection. Currently, the most representative and systematic standards are ISO/IEC 29100 series standards, including *ISO/IEC 29100 Privacy Protection Framework*, *ISO/IEC 29101 Privacy Architecture*, and the *ISO/IEC 29190 Privacy Capability Assessment Model*, *ISO/IEC 29134 Privacy Impact Assessment*, and the *ISO/IEC 29151 Guidelines for the Protection of Personally Identifiable Information*. In addition, there are the US *Guide to Protecting the Confidentiality of Personally Identifiable Information (NIST SP800-122)*, and the *Security and Privacy Controls for Information Systems and Organizations (NIST SP800-53)*, the *Inventory of Data Protection Auditing Practices (CWA 15262:2005)*,

Self-Assessment Framework for Managers (CWA 16112:2010), and the *Personal Data Protection Good Practices (CWA 16113:2010)* of the European Union.

The rapid development of big data technology and applications poses more challenges to personal information protection. In the process of data collection, the development of mobile Internet and the Internet of Things make the collection of personal information increasingly common and clandestine. In the process of data usage, the combination of personal information from multiple sources creates digital portraits and real-time tracking, and data mining increases the risk of exposure of personal information and the loss of privacy, thereby significantly affecting personal rights. In the process of data disclosure, data flow, transaction chain, diversified information processing subjects, complex methods of data transfer, and the cross-border flow of personal information have become a new normal. With the formal implementation of the *Personal Information Security Specification*, future-oriented personal information protection standards have been proposed to scientifically and effectively reduce the risks in data protection, meet the needs of informatization development, and enrich the content and system of China's personal information protection.

4.2.4 Important Data Defined in the *Cybersecurity Law*

In the *Cybersecurity Law*, the word "business" in the term "important business data" was deleted in the draft of the third review, reflecting the legislator's consideration that "important data" refers to information concerning collective interests—that is, national security, national economy, the people's livelihoods, and public interest. Therefore, as long as the data of the network operator does not involve national and public interest, it is not within the scope of "important data." For example, the minutes of a high-level meeting of an Internet company may be very important to the company, but if it does not affect the state or public interest, it is clearly not in the category of "important data." Such data can be exported without any restriction. However, the stocking and shipping records and inventory data generated from the information system of a company that produces war reserve materials may be identified as "important data," since such records and data are related to national security. The cross-border flow of such kinds of data will be subject to security assessment in accordance with the *Cybersecurity Law*.

The change from "important business data" to "important data" shows that the *Cybersecurity Law* has transcended the relatively familiar method of categorizing data into personal, corporate, and national data. Instead, it considers the value of the spheres

that are impacted. In other words, whether it is personal or corporate data, as long as it is significant to the collective interests of the country, it will be identified as "important data." Therefore, in the *Measures for Network Data Security Management* issued by the Office of the Central Cyberspace Commission, "important data" is defined as "the data which do not involve state secrets, but may jeopardize national security, the national economy, the people's livelihoods, or public interest if it is leaked, stolen, falsified, lost, or illegally used."

The proposal of the concept of "important data" is essentially an objective requirement for safeguarding national security and the public interest in the era of big data. It is also a natural reaction to the new characteristics of the era of big data in the protection of data security at the state level. In the past, the classification of "personal, corporate, and national data" was reasonable in that only the data held by the state can affect collective interests back then. However, in the era of big data, data is collected, accumulated, and circulated in large numbers outside the public sector, and many companies have acquired massive data resources. These data already have the possibility of affecting national and public interest. This can be seen from the case of Alibaba's huge collection of user information. Indisputably, this is both personal and corporate data. However, given its scale, granularity, and accuracy, it can be compared to the basic national population database of public security organs. It is likely to cause serious harm to national security once the basic population data on such a scale is leaked.

Another example is the data generated during the cybersecurity protection provided for critical infrastructure in key industries, such as finance, energy, transportation, and telecommunications. Such information includes system architecture, security protection plans, policies, implementation measures, and vulnerabilities. Although this data is controlled by cybersecurity service providers, once it is leaked, it will significantly increase the cybersecurity risks facing the critical infrastructure. Therefore, at the national level, these data will be regarded as "important data," even if they are in the hands of the private sector.

In summary, we must identify the "important data" according to the value of the potential impact and benefits of the data, rather than by the "owner of the data."

The *Measures for the Management of Network Data Security* also specifies the "important data" with examples. "Important data" includes :

- Data on geography, natural resources, and important reserve materials
- Data on genes, biological traits, diseases, and so on
- Data on economy, such as macro statistics

- Data on the defects, loopholes, and preventive measures in network information systems
- Data on crowd navigation, location of large equipment, mobile data, and so on.

4.2.5 Balancing Development and Security through the Security Assessment of Cross-Border Data Flow

In accordance with the requirements of the *Cybersecurity Law*, the Office of the Central Cyberspace Affairs Commission formulated and promulgated the *Measures on the Security Assessment of Cross-Border Transfer of Personal Information and Important Data (Draft for Soliciting Opinions)* in April 2017. On June 27, 2019, China also released the *Measures on Assessing the Security of Cross-border Transfers of Personal Data (Draft for Soliciting Opinions)*. Those two regulations define China's management of cross-border transfer of personal data. How to develop the system design in the *Measures on Assessing the Security of Cross-border Transfers of Personal Data (Draft for Soliciting Opinions)*? In the Internet era, data naturally flows across borders and gains value because of this mobility; data flow can lead to flows in technology, capital, and talent—this is now a basic consensus. In this context, has the system design of the Measures achieved a balance between development and security? These are the main questions we will discuss in this section.

International Trends of Cross-Border Data Flow Control

Geographically, statistics show that more than 60 countries and regions around the world have proposed requirements for the control of cross-border data flow. The United States Information Technology and Innovation Foundation (ITIF) published a report titled *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?* on May 1, 2017. The report points out that the countries which implement control on cross-border data flow are spread across all continents, including the developed countries and regions, such as Canada, Australia, and the European Union, as well as the developing countries, such as Russia, Nigeria, and India. Of course, countries vary in the range and degree of control on cross-border data flows.

Chronologically, most of the existing data localization regulations were put in place after the year 2000. An interesting point is that the rise of data localization is

precisely in sync with the development of information technology, such as the Internet, distributed systems, cloud computing, and big data.

On the one hand, with the large-scale adoption of cloud computing and distributed systems, the ability of data owners to control data is weakening as intermediate links are increasing. Problems that were very clear in the standalone era, such as the types of data, the size of data, storage facilities, and accessibility, have become more difficult to answer.

On the other hand, the development of big data technology has greatly enhanced the need of data owners for data control. Once the massive data is disclosed, whether by active sharing or by the passive disclosure due to the compromise of information systems, it may be maliciously misused. For example, by combining massive data with other data sets, and by using algorithms in data mining, hostile overseas forces may capture and analyze important data that can threaten national security. It is not difficult to understand from these two perspectives that establishment of control measures for cross-border data flows by the state is largely a response to the above dilemmas.

Reasons for Protecting Cross-Border Transfers of Personal Data

Protection of cross-border transfers of personal data aims to safeguard the legal rights of the data subject concerned when the personal data flows away from the original controller, and across national borders.

Compared with data transfer within a country, cross-border transfers will result in four major changes:

1. The capacity to protect the data varies along with the change of data controller.
2. The applicable laws and regulations vary across borders.
3. The supervisory authorities established in the sender country do not have the jurisdiction over the data recipients.
4. Limited means for the data subject to protect his/her rights.

Therefore, institutional designs (domestic and foreign) for protecting cross-border transfers of personal data ought to focus on the abovementioned four aspects.

The EU *General Data Protection Regulation* (GDPR) came into effect on May 25, 2018. Based on the European Data Protection Directive 1995, the GDPR revised the system for protecting cross-border personal data transfers.

First, the Standard Contractual Clauses (SCC) states the principles for safeguarding the transfer of personal data across borders and determines the level of protection.

The GDPR also holds the data controller and other relevant parties of the same country legally liable. By differentiating their legal responsibilities, the GDPR makes it more convenient for local supervisory authorities to exercise their rights. By way of contracts, the data processor and relevant parties of the same country can affix legal liability to any data recipient residing across borders. Meanwhile, the SCC also regulates that the data subject retains certain contractual rights.

Second, binding corporate rules (BCR). Supervisory authorities of the country where the data controller resides ought to assess the adequacy level of the data protection offered by binding corporate rules (BCR).

For an international enterprise, if the country where one of its branches is located has a lower level of protection, the branch within that country shall still comply with BCR to protect the data.

When submitting its BCR application, the international enterprise must specify the country of origin. The specific branch operating in that county shall be legally responsible for the transfer of cross-border data. This means that the local supervisory authorities and the data subject can affix the liability to that entity.

Lastly, assessing the adequacy of data protection in a country or a territory. Once the adequacy level is approved, it means that the European Commission agrees with the legislation and enforcement powers of the supervisory authorities established in that country or territory. It also means that the convenience and effectiveness of exercising the rights of the individual in that country are acceptable. Thus, the assessment is a prudent process which requires holistic consideration.

Consequently, using the data subject's consent as the sole requirement for the transfer of cross-border data cannot mitigate the risks caused by the abovementioned four changes. According to international practice, personal consent of the data subject is not the prerequisite for data transfer. It can only serve as the requirement for occasional, one-time, and limited situations (such as the the adequacy of the level of protection, the SCC, and the BCR).

Similarly, the approaches to data protection in the *Measures on Assessing the Security of Cross-border Transfers of Personal Data (Draft for Soliciting Opinions)* are also based on the abovementioned four changes. Through institutional design, the new security risks are mitigated. Details are as follows:

1. The *Measures on Assessing the Security of Cross-border Transfers of Personal Data (Draft for Solicitation of Opinions)* requires the network operator and the third-country data recipient to sign a contract before the data transfer takes

place. Meanwhile, it also makes detailed regulations, especially on the protection of recipient data. Moreover, the operator ought to submit a report analyzing the security risks and protection methods when applying for cross-border data transfer protection. One of the focuses of the report is the data protection level of the recipient. Such a design is to ensure that the data recipient in the third country has adequate data protection.

2. Regarding the changes in applicable laws and regulations after the data has been transferred to another country, the *Measures on Assessing the Security of Cross-border Transfers of Personal Data (Draft for Soliciting Opinions)* regulates the contract for such transfers and stipulates that the recipient ought to inform the operator in a timely manner if the contract cannot be executed due to changed laws in the third country. The operator decides if the contract ought to be terminated or if relevant data is to be deleted. This requirement can effectively prevent any loss or damage to personal data, resulting from regulatory changes in the country where the data recipient resides. Before transferring the data, the operator ought to assess the laws and regulations of the country as well.
3. In order to tackle the issue that the supervisory authorities of the country where the data sender resides cannot exercise jurisdiction over the recipient in the third country, the *Measures on Assessing the Security of Cross-border Transfers of Personal Data (Draft for Soliciting Opinions)* covers three aspects. First, it requires that the contract signed by the operator and recipient ought to clarify the legal responsibilities of guaranteeing personal data security. It ought to specify the role and tasks of the operator (accountability by default).

   Second, through the annual reports of operators, national network and information authorities are able to understand the overall situation of the cross-border data transfer of an individual operator. These authorities can also require the operator to demand the data recipient to delete all the data, by way of signed contracts.

   Third, the *Measures on Assessing the Security of Cross-border Transfers of Personal Data (Draft for Soliciting Opinions)* regulates that when international operators offer services directly to the Chinese market, they need to designate legal representatives or organizations in China to execute their legal obligations and responsibilities as a guarantee for effective jurisdiction.
4. Another highlight of the *Measures on Assessing the Security of Cross-border Transfers of Personal Data (Draft for Soliciting Opinions)* is ensuring that the data

subject can protect his or her legal rights after the cross-border data transfer. The operator not only needs to regulate its methods and approaches for the data subject to exercise his or her rights in the contract, but also needs to analyze and assess the effectiveness and convenience of these methods when submitting the security assessment of the cross-border data transfer. It also confers the right to inquire on the data subject in cross-border data transfer. The data subject can refer to the copy of the contract signed between operator and recipient for the basic information of the operator and recipient, and purpose, category, and terms for data preservation. With the precondition of ensuring the right to be informed, the data subject can better exercise his or her rights.

Without regulations on the onward transfer of the personal data, the institutional design for the security of cross-border data transfer will become a mere formality. Thus, the *Measures on Assessing the Security of Cross-border Transfers of Personal Data (Draft for Soliciting Opinions)* specifically makes rules for the onward transfer of personal data. For this purpose, the data subject can choose to either opt-out or opt-in if the data contains sensitive information.

Overall, in China's institutional design for the security assessment of cross-border personal data transfer, approaches to handling security risks, that is, tackling the four changes, are in line with international practices. Such approaches are effectively designed with a clear purpose.

Outlook

As an important part of state-level data security protection designed by the *Cybersecurity Law*, the security assessment of cross-border data flow is a key step in establishing a comprehensive and multilevel data resource protection system in China. However, for a basic strategic resource such as data, the existing design of the *Cybersecurity Law* is insufficient. For example, regarding the control of important data, it only provides the right to dispose cybersecurity information. As for the prevention of the malicious use of important data that may threaten national security, it provides only the security assessment of cross-border data flow. Nonetheless, the promulgation of the *Cybersecurity Law* is a good start and we need to implement the *Measures of the Management of Data Security* so as to ensure that cybersecurity keeps pace with developments in big data.

Chapter Five

CHINA'S CYBERSECURITY CAPACITY BUILDING

5.1 Cybersecurity Technology Industry

The cybersecurity technology industry, comprising mainly cybersecurity enterprises and professional service agencies, meets the information security needs of most individuals and commercial organizations. It also ensures the security of many government departments and several special industries. The cybersecurity technology industry is made up of practitioners engaged in R&D, service guarantees, and business operations. In essence, the cybersecurity technology industry is the basic driving force for safeguarding the national cyberspace and for guaranteeing the healthy development of an information society.

5.1.1 Scope of the Cybersecurity Industry

At present, with the rapid development of information and network technology, the cybersecurity technology industry is continually evolving and the industrial structure is constantly striving for perfection. At the same time, the boundary between software and hardware products is blurring and linkages between products and services are being strengthened.

The industry can be divided into products and services based on the deliverables. Cybersecurity products can be further subdivided into four categories: security protection, security management, security compliance, and other security-related products. Security protection products include firewall, intrusion detection and defense, unified threat management (UTM), web application firewall (WAF), anti-virus, data leakage prevention, and so on. Security management products include identification

and access control, content security management, terminal security management, and security information and event management (SIEM), among others.

Security compliance products mainly include tools for security baseline management, security auditing, testing and assessment, and so on. Other security-related products include industry-specific products that do not belong to the abovementioned three categories (such as botnet, Trojan, and worm detection and protection systems), emerging technologies (such as cybersecurity situational awareness platforms, big data analytics, and so on).

Cybersecurity services can be subdivided into four categories: security integration, security operations and maintenance, security assessment, and security consulting. Security integration services refer to the security integration within information systems engineering projects. Security operations and maintenance services include professional operations services, maintenance and repair services, and others. Security assessment services consist of risk assessment, penetration testing, insurance evaluation, and others. Security consulting services involve education, training, design and planning, and others.

5.1.2 The Development of China's Cybersecurity Technology Industry

As the information technology further develops and the global security situation becomes more complex and diverse, the demands of the cybersecurity industry continue to grow. Given the functions of China's cybersecurity technology industry in both society and economy, it is an essential pillar of the country's cybersecurity.

Since the 18th CPC National Congress in November 2012, cybersecurity has been elevated to the level of national security. A series of incidents threating cybersecurity, such as the Snowden Leak, the cyberattacks on the Ukrainian Power Grid, and the US presidential election confirmed the critical link between cybersecurity and national security. President Xi Jinping emphasized that "without cybersecurity, there will be no national security or stable economic and social operations, and the interests of the majority of people will not be guaranteed." With the frequent occurrence of major global cybersecurity incidents, Chinese people have realized that cybersecurity is not only related to their daily lives, personal and property safety, but also to national security.

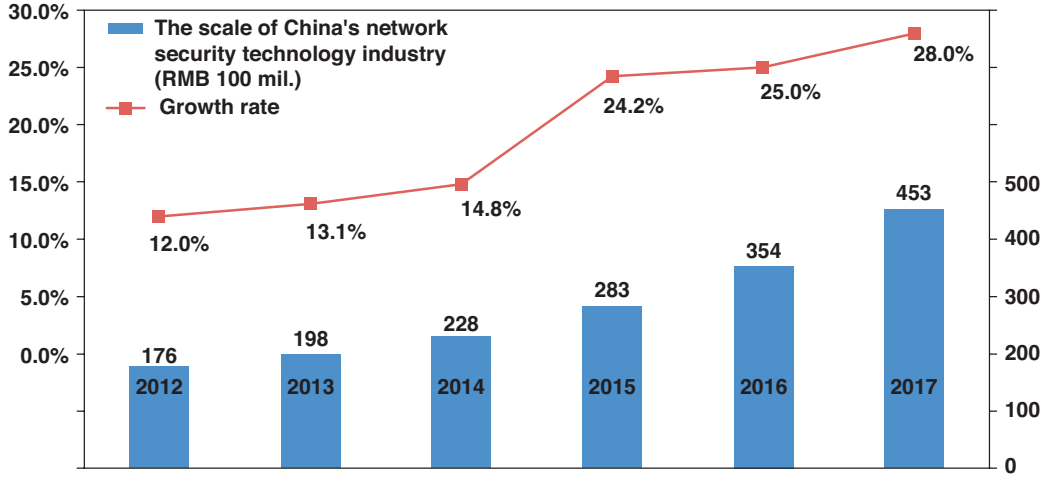
China's cybersecurity technology industry began to develop with the wide diffusion and application of information technology, especially Internet technology. After more than two decades of development, the cybersecurity technology industry has

been continually improving and a relatively sound technology industry system has taken shape. China's cybersecurity enterprises, with their independent intellectual property rights, are active in all major sub-technical fields. At present, there are more than 2,600 Chinese enterprises engaged in cybersecurity-related businesses, including 20 listed companies on the Shanghai and Shenzhen stock exchanges.

According to the statistics from the China Cybersecurity Industry Alliance, the scale of China's network security technology industry reached RMB 28.3 billion (2015), RMB 35.4 billion (2016), and RMB 45.3 billion (2017). In these three years, the annual compound growth rate of the industry exceeded 20%. It is expected that China will continue to maintain a rapid growth in this industry for the next 10 years and beyond (*see* Exhibit 5.1).

As of December 2017, the number of Internet users in China reached 772 million, ranking first in the world with a penetration rate of 55.8% and exceeding the global average by 4.1 percentage points. China has also become one of the leaders in the global e-commerce market in terms of overall market size and development rigor. According to the survey of e-commerce trading platforms by the National Bureau of Statistics, China's e-commerce transactions totaled RMB 29.2 trillion in 2017, a year-on-year increase of 11.7%, with the volume of B2C sales and the number of online shopping

Exhibit 5.1 Scale and growth rate of China's cybersecurity technology industry from 2012 to 2017



consumers ranking first in the world. China is already a cyber power, and the digital economy has become one of the main drivers of its socioeconomic development.

In contrast, there are many weaknesses in China's cybersecurity technology industry that are not commensurate with the country's status as a cyber power. First, the overall scale of the industry is too small and there are not enough large-scale leading enterprises with core technical capabilities. Second, the relatively weak technological innovation capability and the unfavorable market environment have restricted the development of the industry. Third, the lack of cybersecurity talent, interdisciplinary talent, leading high-end talent, and specialists in core new technology R&D has weakened the development potential of the industry.

Based on historical data, China's cybersecurity investment level has long been lower than the global average, let alone that of the cybersecurity powers, such as the United States and the United Kingdom In 2017, China's investment in cybersecurity accounted for less than 1% of its total investment in informatization, slightly more than one-third of the global average in the same period. In the 2018 federal government budget proposed by the Trump administration, the proportion of cybersecurity investment in total IT investments reached 20%. The difference shows that China owed a huge historical debt to the building of cybersecurity in the rapid development of informatization for the past three decades.

It is safe to say that the relatively weak industrial foundation and overall capacity of the cybersecurity industry do not meet China's urgent needs to maintain cyberspace sovereignty and national security, ensure the healthy development of informatization, or safeguard the digital rights and interests of its people. This is the main contradiction China's cybersecurity technology industry is facing.

China is burdened with historical debts and at the same time faces ever-evolving and increasingly complex cybersecurity threats and challenges. Therefore, it is necessary for the country to be committed to developing and strengthening its cybersecurity technology industry. The Chinese government has promoted the formulation of strategic plans, reinforced the legislation, enhanced security awareness, improved the market environment, and strengthened the building of cybersecurity as a discipline and talent training. All these efforts are paying off. With the annual growth rate exceeding 20% in the past three years, China's cybersecurity technology industry has entered an excellent period of development opportunities. We believe that after a further 10 years of development, China will have a systematic, robust, and prosperous cybersecurity technology industry commensurate with its status as a major cyber power.

5.1.3 Measures to Promote the Development of the Cybersecurity Technology Industry

All the major countries in the world have issued cybersecurity strategies and development plans, and have increased government investments to improve industrial capabilities. In order to accelerate the development of cybersecurity, China has also issued a series of policy documents and regulations since 2016, including the *Outline of National Informatization Development Strategy* (jointly issued by General Office of the Central Committee and General Office of the State Council), the *National Informatization Plan for the 13th Five-Year Period (2016–2020)* (issued by the State Council), the *Cybersecurity Law of the People's Republic of China* (promulgated by the NPC Standing Committee in the form of comprehensive legislation), the *National Cybersecurity Strategy* (issued by the Cyberspace Administration of China under the guidance of the holistic national security concept), and the *International Strategy of Cooperation on Cyberspace* (jointly issued by the Ministry of Foreign Affairs and the Cyberspace Administration of China), demonstrating China's outlook on international cooperation in cybersecurity.

China has established a relatively complete strategic deployment and top-level design, and has elaborated its position on cybersecurity development at the level of policy and legislation. Moreover, by virtue of these policies and regulations, China reiterates its stand on cybersecurity development so as to make the country's cyber governance policies consistent with international cooperation in a comprehensive, open, and independent approach.

In order to promote the sustainable development of the cybersecurity technology industry, the Chinese government adheres to Xi Jinping's Thought on Socialism with Chinese Characteristics for a New Era as the guiding thought, puts into action the strategic deployment to build China into a cyber power, stimulates the demand for cybersecurity, encourages innovation-driven development, optimizes industrial ecology, and consolidates industrial infrastructure (*see* Exhibit 5.2).

In March 2016, the National Development and Reform Commission issued the *National Outline for the 13th Five-Year Plan*. The 28th chapter of the Plan titled "Strengthening Information Security" points out that China must develop a national cybersecurity system to improve its ability in cyberspace governance and safeguard the security of national information.

The *Outline of National Informatization Development Strategy* released in July 2016 also attaches great importance to cybersecurity, regarding it as a key techno-logy and

Exhibit 5.2 The opening ceremony of Digital China Research Institute and the Digital China Core Technology Industry Alliance at the First Digital China Construction Summit in April 2018

Source: CNSphoto

an important field together with mobile communications, Next-generation Internet, Next-generation broadcast and TV network, cloud computing, big data, the Internet of Things, intelligent manufacturing, smart city, and so on.

In September 2016, the *Regulations on the Protection of Minors on the Internet (Draft for Soliciting Opinions)* issued by the Cyberspace Administration of China aims to create a healthy, civilized, and orderly network environment and to safeguard the security of minors, along with their legitimate rights and interests, in cyberspace.

As mentioned in the previous chapters, the *Cybersecurity Law of the People's Republic of China* was reviewed and approved by the NPC Standing Committee in November 2016 and was officially implemented on June 1, 2017. As the first basic law

in China to comprehensively regulate cybersecurity management, it offers powerful protection for cybersecurity, cyber sovereignty, and national security. It promotes the healthy socioeconomic development in the process of informatization and is a major milestone in establishing the rule of law in China's cyberspace.

On December 15, 2016, the State Council issued the *National Informatization Development Plan for the 13th Five-Year Period (2016–2020)*, which aims to implement the *National Outline of the 13th Five-Year Plan* and the *Outline of National Informatization Development Strategy*. The Development Plan, as an important part of the national planning system for the 13th Five-Year period, serves as a guide to informatization development in all regions and departments in this period.

The Development Plan puts forward six focuses, namely, leading innovation-driven development, facilitating balanced coordination, supporting green and low carbon development, deepening opening-up and cooperation, promoting the principle of joint building and sharing, and defending against security breaches.

It also deploys the work of 10 tasks, including: a modern information technology and industrial ecosystem, an advanced and ubiquitous information infrastructure system, an open and unitary big data system, an integrated and innovative information economy system, a highly efficient national governance system, an inclusive and convenient information system for the people, an Internet information development system for deepening military–civilian integration, a global development service system for network information enterprises, a cyberspace governance system, and a cybersecurity protection system.

From the end of 2016 to mid-2017, following on from the implementation of the *Cybersecurity Law of the People's Republic of China* and with the approval of the Central Cyberspace Affairs Commission, the Cyberspace Administration of China issued the *National Cybersecurity Strategy*. In succession, the National Development and Reform Commission and the Ministry of Industry and Information Technology (MIIT) respectively issued the *Three-Year Action Plan for the Construction of Major Information Infrastructure Projects*, and the *Big Data Industry Development Plan (2016–2020)* to advance the construction of information infrastructure and the development of the big data industry.

In January 2017, in order to further implement the strategic goal of transforming China into a cyber power and forging the healthy and orderly development of China's mobile Internet, the General Office of the CPC Central Committee and the General Office of the State Council jointly issued the *Opinions on Promoting the Healthy and*

Orderly Development of the Mobile Internet. The directives were put forward in several fields, such as the promotion of innovation-driven development and the prevention of security risks of the mobile Internet.

At the same time, the Ministry of Industry and Information Technology formulated and issued the *2016–2020 Plan for the Information and Communication Network and Information Security*, which proposes security and protection measures in six aspects: strengthening organizational structure, enhancing financial support, establishing think tanks, reinforcing the team of talents, highlighting publicity and education, and planning the organization and implementation. In January 2017, the Cyberspace Administration of China issued the *Notice on the National Emergency Plan for Cybersecurity Incidents*, which provides the definition of a cybersecurity incident and classifies it into four grades. The Plan makes provisions for important issues, such as monitoring and early warning, emergency response, investigation and evaluation, preventing cybersecurity incidents, and safeguarding cybersecurity.

In March 2017, the Ministry of Foreign Affairs and the Cyberspace Administration of China jointly issued the *International Strategy of Cooperation on Cyberspace*. It is themed with peaceful development and win-win cooperation and aims to build a community of shared future in cyberspace. As a strategic document guiding China's participation in international exchange and cooperation in cyberspace, it puts forward for the first time China's proposals on promoting cyberspace international exchange and cooperation comprehensively and systematically and offers the China solution for solving the problems in international cyberspace governance. This document aims to aid the international community in building a peaceful, secure, open, cooperative, and orderly cyberspace.

On March 30, 2017, the *Three-Year Action Plan for Cloud Computing Development (2017–2019)* was issued and implemented by the Ministry of Industry and Information Technology. With the goal of promoting the implementation of the strategy of building China into a strong global manufacturing and cyber power, the Plan proposes the guiding ideas, basic principles, development goals, key tasks, and protection measures for the development of cloud computing in China for the next three years.

In April 2017, in order to protect personal information and important data, safeguard cyber sovereignty and national security, and promote the orderly and free flow of network information in accordance with laws, the Cyberspace Administration of China and the relevant departments drafted the *Measures on the Security Assessment of*

the Cross-Border Transfer of Personal Information and Important Data (Draft Measures) in accordance with the *National Security Law of the People's Republic of China*, the *Cybersecurity Law of the People's Republic of China*, and other relevant laws and regulations. It is now soliciting public opinions. In May, the National Information Security Standardization Technical Committee (TC260) issued the *Guidelines for the Security Assessment of Cross-Border Data Transfer (Draft)*, which provides practical and operational guidance to the security assessment systems stipulated in the *Cybersecurity Law of the People's Republic of China*, and the *Measures on the Security Assessment of the Cross-Border Transfer of Personal Information and Important Data*.

In May 2017, the Cyberspace Administration of China issued the *Measures on the Security Review of Network Products and Services (Trial)*, the *Administrative Law Enforcement Procedures for Internet Information Content Management*, and the new *Regulations on Internet News and Information Service Management*. All were implemented from June 1, 2017 onward. The Supreme People's Court and the Supreme People's Procuratorate issued the *Interpretation of Several Issues Concerning the Application of Laws in Handling Criminal Cases of Infringement of Citizens' Personal Information*, which provides the legal basis for punishing criminal acts that infringe citizens' personal information, and for protecting personal information security and the legitimate rights and interests of citizens.

In May 2017, the General Office of the State Council issued the *Plan for the Implementation of Integration and Sharing of Government Information System*. Centering on the urgent need for governance and public services, it proposes key tasks and implementation methods for accelerating the integration and sharing of government information systems and fostering the interconnection of information systems of the state and those of local governments. In the same month, the Ministry of Water Resources officially issued the *Top-Level Design of the Cybersecurity of Water Resources*, which aims to standardize the management of cybersecurity in the construction of water conservancy projects, promote cybersecurity water conservancy, strengthen the protection of critical information infrastructure (CII) in water conservancy, and improve the overall ability to guarantee the cybersecurity of water conservancy. The Ministry of Industry and Information Technology issued the *Guidelines for Emergency Management of Information Security Incidents in Industrial Control Systems*, which provides guidelines for the emergency management of information security incidents and information security protection in industrial control systems.

In May 2017, the General Office of the State Council issued the *Guidelines for the Development of Government Websites* to clearly standardize the building and developing of government websites.

In June 2017, the Cyberspace Administration of China, the Ministry of Industry and Information Technology, the Ministry of Public Security, the National Certification and Accreditation Administration, and other relevant authorities jointly formulated and released the *Catalogue of Critical Network Equipment and Cybersecurity Products (First Batch)*. The Ministry of Industry and Information Technology issued the *Cybersecurity Emergency Response Plan for the Public Internet*. The People's Bank of China issued the *13th Five-Year Plan for the Informatization of China's Financial Industry (2016–2020)*, which clearly proposes the guiding ideas, basic principles, development goals, key tasks, and protection measures for information technology in the financial industry during the 13th Five-Year Plan period. On June 27, the Twenty-eighth Meeting of the 12th NPC Standing Committee adopted and promulgated the *National Intelligence Law of the People's Republic of China*, which gives legal provision for protecting national intelligence and for safeguarding national security and interests.

In July 2017, the Cyberspace Administration of China issued the *Regulations on the Security Protection of Critical Information Infrastructures (Exposure Draft)*. It is an important supporting regulation of the *Cybersecurity Law of the People's Republic of China* that ensures the security of CII by regulating the planning, construction, operation, maintenance, use, and security of CII in China. It sets out specific and operative requirements for the CII, the responsibilities of various regulatory authorities, the obligation of the operators, and that of the security testing and assessment system. The Regulations provides important legal support for the security of CII.

In August 2017, the Ministry of Industry and Information Technology issued the *Measures for the Management of the Assessment of Information Security Protection Capability of Industrial Control Systems*, aiming to standardize the assessment of, and improve the capability of security protection of industrial control systems. In the same month, the *Guidelines for the Development of the Comprehensive Standardization System for the Mobile Internet* was released to promote the healthy and orderly development of the mobile Internet industry, and strengthen the role of standards to guide, regulate, lead, and protect industrial development.

In November 2017, the Ministry of Industry and Information Technology issued the *Cybersecurity Emergency Response Plan for Public Internet*, which clarified the

grading, monitoring and early warning, emergency response, prevention and emergency preparedness, and protection measures to forge a comprehensive response capability toward cybersecurity emergencies in the public Internet. This is to ensure timely and effective controls to mitigate and eliminate the harm and loss caused by cybersecurity incidents in public networks, ensure the continuous and stable operation of the public Internet and data security, safeguard the national cybersecurity, and maintain economic operation and social order.

The abovementioned laws, regulations, guidelines, and plans play a fundamental and normative guiding role in building a safe cyberspace, and in promoting the reform of the cyberspace governance system. These successive enactments mark the sustained acceleration of the standardization process and the pace of enhancing cybersecurity. These play an important role in implementing the strategy of building China into a cyber power, promoting the prosperous development of the industry, and strengthening institutional structures, which undoubtedly will ensure the healthy development of China's cybersecurity industry.

In addition, the municipal governments of Beijing, Chengdu, Chongqing, Guiyang, Hangzhou, Shenzhen, and other cities are actively building local cybersecurity-related industrial parks. The Ministry of Industry and Information Technology and the Beijing municipal government are also jointly accelerating the building of the National Cybersecurity Industrial Park in Beijing. In 2016, the construction of the National Cybersecurity Talent and Innovation Base (NCTIB), the first national base featuring a "cybersecurity academy and industry innovation valley," was launched in Wuhan, Hubei Province. For the construction of cybersecurity industrial parks and national bases, a series of targeted guiding policies have been introduced by relevant local governments and national authorities to promote enterprise development and optimize the market environment. These industrial parks and national bases aim to become vital carriers of regional economic development and industrial adjustment and upgrading, bearing important missions such as gathering innovative resources, cultivating emerging industries, and facilitating urbanization.

The experience of current global cyber powers shows that the cybersecurity industry with effective governance structures that conform to the laws of the market economy is one of the most important components of the national cybersecurity capability system. The key to building China into a cyber power lies in expanding and strengthening its cybersecurity industry.

5.1.4 Adhere to the Principles of Openness and Integration to Promote Industrial Development

China will unswervingly take the path of peaceful development, follow the principle of upholding justice and fairness, and forge a new type of international relations featuring win-win cooperation. China's *International Strategy of Cooperation on Cyberspace*, with peaceful development as its theme and win-win cooperation at its core, advocates the basic principles of peace, sovereignty, shared governance, and shared benefits in international exchange and cooperation in cyberspace. The idea of building a community of shared future in cyberspace initiated by the Chinese government has been recognized and supported by most countries and international organizations.

Guided by the concept of peaceful development, China will firmly follow the path of opening-up and development in its cybersecurity and information technology. As President Xi Jinping said,[1]

> China must not and never will close its door to the outside world. China encourages and supports its IT enterprises to globalize, to strengthen international exchange and cooperation, to actively participate in implementing the Belt and Road Initiative, and to achieve 'where there is the national interest, there is informatization coverage.' All international IT companies are welcome in China as long as they comply with China's laws and regulations . . . Cybersecurity is open and not closed. Only in an open environment and by strengthening international exchange, cooperation, interaction, and gaming, and drawing on advanced technologies can we continue to improve our level of cybersecurity.

Such a statement clearly expresses the willingness of the Chinese government to pursue the open development of cybersecurity. The Chinese government is also actively strengthening international cooperation on the sharing of Internet technologies and promoting technical exchange among countries in the fields of network communications, the mobile Internet, cloud computing, the Internet of Things, and big data, to

1 Quoted from President Xi Jinping's speech at the Symposium of Cybersecurity and Informatization on April 19, 2016.

jointly solve the problems arising from the development of Internet technology, and facilitate the development of new industries and business models.

International corporations, such as Cisco, IBM, Microsoft, Oracle, and Apple hold a large share of the Chinese market and occupy most of the high-end markets in key industries such as finance. International technology companies participating in the informatization of China have achieved excellent financial returns.

There are many successful examples of the industrial cooperation between China and other countries. One of them is the C&M Information Technologies Co., Ltd. (CMIT) jointly established by China Electronics Technology Group Corporation (CETC) and Microsoft Corporation. The company is committed to providing Chinese government agencies and state-owned critical infrastructure enterprises with tailor-made operating systems and services that are safe, controllable, and technologically advanced, and meet the regulatory requirement and user demand. The cooperation between CETC and Microsoft is a major collaboration between China and the United States in the high-tech field, demonstrating the spirit of cooperation from both sides (*see* Exhibit 5.3). With the support of the shareholders from both corporations, CMIT strives to become a leader of technological innovation that will cultivate global high-end technical and management talent, rapidly upgrade domestic technology and upskill the local talent pool, stimulate technological innovation, and help China further develop world-class technologies.

5.2 Cybersecurity Technology

Cyberspace is a unitary system. Its interconnectedness, openness, universality, and other characteristics (such as data and information sharing, and the commonality of communication channels) produce the "wooden bucket effect" and the "chain effect." The vulnerability of any link or aspect in cybersecurity endangers the cybersecurity of individuals, organizations, and even that of the entire country. Therefore, there ought to be systematic ideas and methods for the capacity building of cybersecurity.

5.2.1 Strengthen Capacity Building to Promote Innovation

Since the 18th CPC National Congress, China has formulated a strategic plan for national cybersecurity and promulgated the *Cybersecurity Law of the People's Republic of China*, along with other related laws and regulations. Combining the domestic situation of China and drawing on the experience of international cyber powers, the Chinese government has gradually improved its cybersecurity protection system.

Exhibit 5.3 The signing of the MOU between CETC and Microsoft at the Second World Internet Conference held in Wuzhen, Zhejiang Province, December 17, 2015

Source: Imagine China

Specifically, the related tasks which China has been carrying out include:

- strengthening the implementation of the cybersecurity strategy, detailing the main tasks for cybersecurity, and formulating the development schedule of cybersecurity;
- establishing a cybersecurity organization and management structure with Chinese characteristics and clarified the responsibilities of the various departments;
- advancing the comprehensive construction of a proactive cybersecurity defense system, and accelerating the development of cybersecurity defense strategy research and system;

- building a global cybersecurity platform for strategic early warning and proactive defense so as to achieve an accurate overall awareness of the network; and
- creating a global ecosystem to combine the upstream and downstream activities of the cybersecurity industry in order to improve the structure of the industrial chain, and to achieve the breakthrough and development of core innovative cybersecurity technologies.

In order to advance the development of its core technologies, China is seeking the "breakthrough path" of core technology with overall planning and clear priorities. It is the path that follows the law of technological development, improves the institutional environment to optimize the market environment, achieves breakthroughs in applied technologies driven by basic research, and creates an interdisciplinary, cross-domain, collaborative, and innovative system that connects production, education, research, and application. This path is a strategic breakthrough with self-independent innovation as its core feature (*see* Exhibit 5.4).

On December 3, 2014, the State Council issued the *Notice on the Plan for Deepening the Reform of the Management of Centrally-Financed Science and Technology Projects (Programmes and Funds)*, which consists of five parts:

1. Overall objectives and basic principles,
2. Establishment of an open and unitary national science and technology (S&T) management platform,
3. Optimization of S&T initiatives (Programmes and Funds),
4. Integration of existing S&T initiatives (Programmes and Funds),
5. Implementation progress and work requirements of the Plan.

The objectives of the reform are to strengthen top-level design, break the barriers between higher and lower levels or between different departments and regions, and reform the management system. It aims to coordinate the scientific and technological resources, strengthen the functional divisions of each department, establish an open and unified national S&T management platform, and build a scientific and technological planning system that has a reasonable overall layout and a clear functional orientation with Chinese characteristics. Further, it aims to establish a performance-oriented management system with clear objectives, and to form a platform and build an organization and management mechanism that is standardized, efficient, open, and transparent.

Exhibit 5.4 A staff member showing cybersecurity-related high-tech products to visitors at the 2018 International Social Public Security Products and Technology Exhibition held in Chengdu, Sichuan Province, May 10, 2018

Source: CNSphoto

The Plan is focused on national goals, which are to accelerate S&T innovation, promote the efficient allocation of scientific and technological resources, and enhance the intensive integration of science and technology with the economy. It aims to greatly motivate researchers to innovate, and give full play to the strategic role of S&T initiatives (Programmes and Funds) for improving social productivity, thus enhancing overall national strength and international competitiveness, and safeguarding national security.

The Plan clarifies that the original, with more than 100 science and technology plans and initiatives, will be adjusted, optimized, and integrated into five major categories: the National Natural Science Foundation, the National Science and Technology Major Projects, the National Key Research and Development Programs, the Technology Innovation Guidance Projects, the Base, and the Talent Projects.

China has planned and carried out the National Key R&D Program for Cybersecurity. The Program integrates the original National High-tech R&D Program (known as the 863 Program), the 973 Program, the National Science and Technology Support Program, the International Science and Technology Cooperation Program, as well as the different industrial technology R&D funds managed by the National Development and Reform Commission, the Ministry of Industry and Information Technology, and the scientific research projects of the public welfare industry managed by the relevant authorities. According to application guidelines, the goal of the National Key R&D Programs for Cybersecurity is to gradually promote the establishment of an independent technology system for cybersecurity protection, governance, assessment, and analysis that keeps pace with international standards adapted to China's cyberspace. The Industrial Development Promotion Center of the Ministry of Industry and Information Technology is responsible for the management of this special project. There are five innovation chains in the National Key R&D Programs for Cybersecurity. The first batch of eight sub-programs will be launched in five technological directions, including innovative defense technology mechanisms and space-ground integration information security protection technology.

As the world's largest developing country and the second largest economy, China is also a major contributor to global economic growth. China has always advocated the concept of peaceful development and is an important force for maintaining global peace. The country's stable development not only benefits the 1.42 billion Chinese people, but also advances the social development of mankind. Without cybersecurity, there will be no national security. China is steadfastly committed to enhacing capacity building and technological innovation for cybersecurity, making cyberspace a beautiful spiritual home shared by hundreds of millions of people, keeping the cyberspace healthy and ecologically principled, and bringing the benefits brought by the development of information technology to all the people of the world.

5.2.2 Enhance the Autonomy and Controllability in Core Technologies

Since the cybersecurity protection capability is highly dependent on network information technology, countries have attached great importance to technology R&D and application, and have taken strategic measures to enhance their autonomy in technologies.

The Chinese national leaders have clearly demanded that China must be determined and persistent to achieve breakthroughs in its core information technologies.

China is striving to master core technologies to achieve autonomy and controllability in the key fields of information technology—the only way to realize the goal of building China into a cyber power, safeguarding the sustainable development of an information society, and maintaining national security. On the one hand, core technologies are the important treasure of the country, among which the most critical ones ought to be acquired by independent innovation and self-reliance. Such technologies can neither be transacted in the market nor bought with money. Rather, they can only be developed through independent R&D. On the other hand, we must persist in opening-up and innovation. Emphasizing independent innovation does not mean engaging in R&D behind closed doors. Only by strengthening international exchange, cooperation, and competition, and drawing on advanced technologies in an open environment can we be improving our level of cybersecurity.

Autonomy and controllability do not mean a complete replacement of foreign products with domestic products or reinventing the wheel in cybersecurity technology. Rather, we ought to aim for breakthroughs in our core technologies. The information technology industry is an open, collaborative and global supply chain ecosystem. In the development of independent and controllable core technologies, we ought to pay attention to the key links in the industrial technology chain and strengthen the supply chain linkages. There is a basic standard to ascertain whether we have true autonomy and controllability, and that is when our industrial development and cybersecurity are not subject to the control of others.

China will not yield to the threat of or blackmail by any country with advantages in core technologies, and resolutely opposes any form of "technical hegemony." China will also not seek illegitimate interests by violating market mechanism and international trade rules or beyond, after achieving breakthroughs in its core technologies.

Core technology is the key to the development of China's cybersecurity technology industry. We must take the cybersecurity needs of the whole society as the main driving force, fight hard to achieve technological breakthroughs in cybersecurity, and support enterprises, universities, scientific research institutions, and other bodies so as to make a quantum leap forward in our core technologies. Meanwhile, we ought to strengthen the research in cybersecurity technologies and the application of new technologies, such as the industrial Internet, artificial intelligence, big data, among others.

With demand as the driving force, we must accelerate translating the cybersecurity technology achievements, so as to cultivate and expand the market for cybersecurity products and services. We should guide key industries such as communications, energy,

Exhibit 5.5 Product Demonstration of the Arm Platform Security Architecture at the Fourth World Internet Conference in Zhejiang Province, December 3, 2017

Source: CNSphoto

finance, and transportation to increase the investment in the cybersecurity of critical infrastructure, promote the diffusion and application of cybersecurity products and services, incubate new technologies and applications, and accelerate iterative upgrades and innovations in cybersecurity products and services (*see* Exhibit 5.5).

5.3 Cybersecurity Talent

As a Chinese saying goes, "To run a country, the possession of great talent is a top priority." At all times, and in all countries, the quality and quantity of talent determine the rise and fall of an industry, a nation, or a country. The rapid development

of globalization and informatization has brought unprecedented opportunities and challenges to the discovery, cultivation, and reservoir of cybersecurity talents in China. The Chinese government has proposed the ambitious goal of building China into an innovation-driven country and a cyber power, and has also set new requirements for cybersecurity talent development.

5.3.1 Develop the Discipline of Cybersecurity

There is still a huge gap in the cultivation of cybersecurity talents in China. According to the *Internet Development Security Report for the First Half of 2017* released by Tencent Security, the total industry demand for cybersecurity talent exceeded 700,000. It is estimated that the number of cybersecurity practitioners will reach 1.12 million by 2020, 3.36 million by 2027, and 10.9 million by 2035. At present, the number of students with the relevant degrees has failed to meet the demands of the cybersecurity industry.

In February 2014, the General Office of the Ministry of Education and the General Office of the Ministry of Industry and Information Technology jointly issued the *Notice on Conducting the Survey on the Cultivation of Information Security Talent ([2014] No. 4)*. According to this survey, the average annual number of university graduates with a degree in information security was 11,000 from 2012 to 2014. Among these, university undergraduates, postgraduates, vocational school graduates, and adult education graduates accounted for 49%, 29%, 19%, and 3%, respectively. The average annual employment rate of undergraduates, postgraduates, and vocational school graduates with a degree in information security was 96%, 97%, and 96.3%, respectively. Most of these were employed in enterprises, government agencies, and institutions. More than 25% of undergraduates were employed in private enterprises; more than 25% of postgraduates were employed in state-owned enterprises; and another 20–25% in private enterprises. Enterprises are the main employers of these university graduates.

By 2014, 103 information security-related undergraduate programs had been established in 81 colleges and universities in China. However, there was no discipline of information security in the *Catalogue of Postgraduate Programs of China* at that time. In order to promote the postgraduate study of information security, 74 universities started to offer postgraduate programs in the subject under 14 related first-level disciplines, and some schools have set up information security programs as an independent

second-level discipline.[2] However, a number of issues restricting the development of cybersecurity-related disciplines can still be observed.

Differing foundations or entry points, an inconsistent academic orientation, confusing teaching content, and mutual constraints have seriously affected the systematic education of cybersecurity talents. Consequently, the total number and structure of cybersecurity talents are far from meeting industry demands, and a serious shortage of interdisciplinary talents and professionals exists. The survey shows the following challenges and deficiencies in the education of cybersecurity professionals:

1. Inadequate teaching staff. According to data in 2014, the proportion of teachers with a doctoral degree in the discipline of cybersecurity was less than 60%, the high-level professional teachers only accounted for 7% of the teaching staff, and leading experts with significant international and domestic influence and reputation were scarce.
2. Incomplete system of teaching materials. The quality of teaching materials is uneven and high-quality professional teaching materials are urgently needed to improve the structure of teaching materials.
3. Unsystematic practical education. Theoretical teaching is divorced from reality. Students have few opportunities to conduct practical experiments and rarely handle real-life cybersecurity issues. Hence, they have little knowledge of mainstream cybersecurity technology products.
4. Insufficient funds. Because of the setting, management, and prioritization of cybersecurity-related courses and disciplines, the fund for strengthening the teaching structure is limited and fails to cultivate the talent as is required by the industry.

In response to the abovementioned challenges, the Chinese government has stepped up its efforts in building cybersecurity-related disciplines. On June 11, 2015, the Academic Degrees Committee of the State Council and the Ministry of Education jointly issued the *Notice on Adding Cybersecurity to the First-Level Disciplines ([2015] No. 11)*, setting cybersecurity as a first-level discipline (code number 0839) and

2 Editorial Note: In Chinese higher education system, first-level disciplines refer to major academic disciplines such as philosophy, law, and sociology. The second-level disciplines are the branches of the major disciplines, such as Chinese philosophy, history of law, and demography.

awarding graduates with an engineering degree. This marks a crucial step in accelerating the cultivation of high-level talent in the field of cybersecurity. By doing this, universities are allowed to award graduates with bachelor's, master's, and doctoral degrees and can systematically train interdisciplinary and innovative talent to meet the urgent needs of the country.

On June 6, 2016, with the approval of the Central Cyberspace Affairs Commission, the Office of the Central Cyberspace Affairs Commission, the National Development and Reform Commission, the Ministry of Education, the Ministry of Science and Technology, the Ministry of Industry and Information Technology, the Ministry of Human Resources and Social Security, and other relevant authorities jointly issued the *Opinions on Strengthening the Building of Cybersecurity Discipline and Talent Cultivation*, in order to improve the building of cybersecurity as a discipline and cultivate young talent.

This document offers the following proposals: accelerating the development of the discipline faculties, and schools of cybersecurity, innovating cybersecurity talent cultivation mechanisms, strengthening the compilation of cybersecurity teaching materials, and reinforcing teaching staff. Other proposals in the Opinions also include promoting collaborative innovation and cooperation between higher education institutions and enterprises, enhancing on-the-job training for cybersecurity practitioners, increasing the awareness of cybersecurity, providing skills training for all, and improving supporting measures for the education of cybersecurity professionals (*see* Exhibit 5.6).

Since the 18th CPC National Congress, important progress has been made in professionalizing cybersecurity talent with the establishment of the first-level discipline of cybersecurity and the introduction of a series of incentives for talent cultivation.

By the end of 2017, more than 35 universities have been approved by the Academic Degrees Committee of the State Council to offer doctoral programs in cybersecurity. As of the end of April 2018, nearly 200 universities have set up cybersecurity-related programs. At present, 35 universities have established cybersecurity schools. In 2019, according to a preliminary estimate, some 20,000 students with a degree in cybersecurity will graduate from universities in China (*see* Exhibit 5.7).

5.3.2 Innovate Talent Cultivation Mechanisms

The rivalry in global cyberspace has increasingly become a competitive spur for talent. In the cybersecurity strategies of many countries, strategic deployment has been made

Exhibit 5.6 List of Universities with a Cybersecurity School[3]

University of Science and Technology of China ★	Wuhan University ★
Xi'an University of Electronic Science and Technology ★	Huazhong University of Science and Technology
Beijing University of Posts and Telecommunications	Beijing University of Aeronautics and Astronautics ★
Shanghai Jiaotong University	Peking University
Sichuan University ★	Tsinghua university
Harbin Institute of Technology	Southeast University ★
University of Electronic Science and Technology	Chengdu University of Information Engineering
Nanjing University of Posts and Telecommunications	Hangzhou University of Electronic Science and Technology
Jinan University	Criminal Investigation Police University of China
Information Engineering University of the PLA Strategy Support Force ★	People's Public Security University of China
University of Chinese Academy of Sciences	Gansu Institute of Political Science and Law
Northwestern Polytechnical University	Chengdu University of Technology
Nankai University	Hebei University
Nanchang University	Guangdong University of Foreign Studies
Xinjiang University	Tianjin University
Guilin University of Electronic Science and Technology	Beijing Institute of Electronic Science and Technology

3 Editorial Note: The seven universities marked with ★ in the table were selected as the first batch of participants in the pilot project of building first-class cybersecurity schools.

Exhibit 5.7 The Cybersecurity Talents Cultivation, Innovation, and Entrepreneurship Forum in Wuhan, Hubei Province, September 20, 2016

Source: Imagine China

to cultivate cybersecurity talent and strengthen cybersecurity talent pools through professional training, entrusting educational institutions to train, and selecting from hacker contests.

At present, more than 50 countries and regions including the United States, the European Union, Russia, and Japan have introduced national cybersecurity strategies and formulated cybersecurity talent training programs. As early as 2003, the United States wrote the cybersecurity education plan into the *National Strategy to Secure Cyberspace*. In 2012, the United States released the *National Initiative for Cybersecurity Education Strategic Plan*, which explicitly proposed to expand the cybersecurity talent pool and cultivate a team of cybersecurity professionals. The United Kingdom also clearly stated in the *National Cyber Security Strategy* published in 2009 that it is necessary to encourage the establishment of a team of cybersecurity professionals. In 2016, in order to build a reservoir of professional cybersecurity talent, the British

government invested £20 million to launch a new "campus network program" to provide cybersecurity training for youths.

On April 19, 2016, President Xi made the following statement at the Symposium on Cybersecurity and Informatization:

> The Internet is mainly the enterprise of the young. It is necessary to cultivate talent without any restrictions. We must emancipate the mind to recognize and make good use of talent. We ought to spare no effort in cultivating Internet and IT talent. We also ought to employ the best teachers, compile the best textbooks, enroll the best students, and build first-class colleges of cybersecurity.

On August 8, 2017, the Secretariat of the Cyberspace Administration of China and the General Office of the Ministry of Education jointly issued the *Measures for the Management of the Pilot Project of Building First-Class Cybersecurity Schools*. The document clarified that the Cyberspace Administration of China and the Ministry of Education decided to implement a pilot project to build four to six world-class cybersecurity schools from 2017 to 2027. Experts and representatives from various fields were invited to evaluate and score the applications submitted by the universities. In strict accordance with the results of evaluation, seven universities were selected as the first batch to carry out the pilot project of building first-class cybersecurity schools.

The first batch of universities are Xidian University Southeast University, Wuhan University, Beijing University of Aeronautics and Astronautics, Sichuan University, the University of Science and Technology of China, and Information Engineering University of the PLA Strategy Support Force, which was established by the merger of the former PLA Foreign Languages Institute and the PLA Information Engineering University.

In recent years, under the joint guidance of the Cyberspace Administration of China, the National Development and Reform Commission, and the Ministry of Education, the National Cybersecurity Talent and Innovation Base has created a first-class mechanism in strengthening the leadership of the government, conducting high-level planning, and exploring its development model. It has built a new pattern featuring government guidance, university–enterprise cooperation, and the participation of non-governmental organizations to intensify and speed up the construction of the Base.

In addition, to accelerate the development of the cybersecurity industry, the National Cybersecurity Talent and Innovation Base has introduced a series of preferential policies to create a good ecological environment, attract investment, and promote the signing and implementation of various projects while at the same time building first-class industrial parks with facilities to accommodate enterprises. It is impossible to seek sustained industrial development if core technologies and critical infrastructure are restricted and controlled by others. Therefore, the Base is striving to solve this dilemma through innovation, combining regional science and technology innovation resources, creating an open environment for mutual learning and exchange, and drawing on advanced technology so as to continuously improve the overall level of cybersecurity technology in China.

In order to speed up the cultivation of cybersecurity talent and the building of cybersecurity as a discipline in China under the guidance of the Cyberspace Administration of China, the Cybersecurity Special Fund of China Internet Development Foundation initiated and launched the Award for Cybersecurity Talent, the Award for Excellent Teachers of Cybersecurity, the Award for Excellent Cybersecurity Textbook, and the Cybersecurity Scholarship.

According to the evaluation criteria of those awards, the Fund plans to award annually one outstanding talent, 10 excellent talents, and 10 excellent teachers, and offer scholarships for 100 undergraduate and 100 postgraduate students of cybersecurity. The prize for the outstanding talent is RMB 1,000,000, the prize for each excellent talent is RMB 500,000, the prize for each excellent teacher is RMB 200,000, the prize for each excellent textbook is RMB 100,000, and the scholarships for each excellent undergraduate and postgraduate student are RMB 30,000 and RMB 50,000, respectively. These awards play an important role in cultivating cybersecurity talent in China. The Cybersecurity Special Fund of the China Internet Development Foundation was established with donations (*see* Exhibit 5.8).

In cyber conflicts, it is crucial to understand the cyberattacker's thinking in order to develop the means for effective defense, an advantage that cybersecurity competitions have over traditional education. DEFCON and PWN2OWN are internationally renowned cybersecurity competitions. In China, similar contests are also organized, such as Capture the Flag (CTF), Data Analysis Competition, Robotic Offensive and Defensive Games, Actual Combat Range Competition, and other types of cybersecurity competitions. The most influential ones are the National University Information Security Competition which has been held for twelve years,

Exhibit 5.8 The 2018 Cybersecurity Talent and Outstanding Teacher prize awards ceremony held in Chengdu, Sichuan Province, September 19, 2018

Source: Visual China

the XCTF International League, the Information Security Triathlon, the China Cybersecurity Technology Contest, RHG, among others. Cybersecurity competitions provide more and more people with opportunities to understand the application scenarios of cybersecurity in real life and to learn the various divisions of labor in career development. As an important means to discover, cultivate, and select cybersecurity talent, competition is a key part of the cybersecurity education and training system. Nowadays, the development of such cybersecurity-related events is in the ascendant in China (*see* Exhibit 5.9).

In 2014, the Ministry of Education launched the project "Collaborative Education through Industry–Academy Cooperation." Since then, the number of enterprises and universities participating in the project, the number of projects solicited, and the

Exhibit 5.9 The Cybersecurity Skills Challenge as part of the 2018 National Cybersecurity Promotion Week, Chengdu, Sichuan Province in September 2018

Source: Visual China

funding allocated for the project have achieved annual large-scale growth. In May 2018, the Higher Education Department of the Ministry of Education announced the guidelines for the application of the first batch of projects of 2018. Altogether, 346 companies supported 14,576 projects with funds, software, and hardware worth RMB 3.515 billion. Cybersecurity is one of the key areas supported by the project. Internet giants and cybersecurity enterprises in China including Tencent, TOPSEC, and Qihoo 360 actively participate in the project.

In order to improve the competence of teachers in the discipline of cybersecurity, the Cyberspace Administration of China organizes some 20 teachers to go abroad for centralized training every year. At present, two terms of training have been completed in the United States and Israel and the third term was held in the United Kingdom in 2018. Each training session includes lectures by internationally renowned experts, in-depth exchanges with foreign education peers, and field visits

to observe the development of cybersecurity education and technology industry, in whichever country the training is held.

We will adhere to the concept of exploring talents in various ways, evaluating talents in a dynamic and scientific approach, and cultivating talents in the whole life cycle. In the building of the first-level discipline of cybersecurity, we will integrate the disciplines of natural science, engineering science, and social science, so as to lay a solid foundation for the development of a multilevel cybersecurity talent system. We will deepen the collaborative talent cultivation model that integrates government administration, enterprises, universities and research institutes, and users. We will also uphold the concept of "going out and inviting in" to improve the practical and innovative abilities of talent, and take advantage of the diversified global forces to promote and standardize the cultivation of talent and to create an innovative talent cultivation mechanism of international standing and influence. Innovative enterprises require high-caliber talent. We ought to discover talents during our innovative work, cultivate talents in innovative activities, and pool all talents to build a large well-structured team of high-quality cybersecurity experts.[4]

The training, reservoir, and use of cybersecurity talents ought to be based on the principle of paying equal attention to nurturing domestic talent and attracting international talent. Given the urgent demand for leading talent in network technology, it is necessary for China to increase its efforts to attract high-end talent. These cybersecurity personnel must not only have the requisite skills, but also demonstrate patriotism and have an excellent sense of public duty. To optimize our cultivation of cybersecurity talent, we must prioritize the synergies among universities, research institutions, and IT enterprises. Meanwhile, we ought to strengthen international talent exchanges and take advantage of multiple resources to cultivate innovation-driven cybersecurity talent.

At the same time, China will aid and offer sustained support to developing countries engaged in capacity building, by way of technology transfer, construction of critical information infrastructure, and personnel training. We will work hard to close the digital gap between developing and developed countries and share the development opportunities brought by the Internet with more developing countries and their peoples.

---

4 Quoted from President Xi Jinping's speech at the Symposium of Cybersecurity and Informatization on April 19, 2016.