Review of Network Technology System from the Past, Present to the Future

Mou Chengjin
China International Strategic Research Center of Mobile Communications Joint Association
Beijing, 100029, China,
E-mail: mcjzp139@139.com

Guo Xiaohui
Henan Vocational College of Agriculture
Zhengzhou, 451450, China,
E-mail: mcjzp139@139.com

***Abstract*—Since China's public network got access to the Internet in 1994, the study, research and understanding of the Internet have been blindly superstitious to the United States for a long time, copying the rules and regulations of the United States, and the textbooks in the field of Internet and information are almost completely Americanized. For more than 20 years, we have not formed our own systematic and profound research and practical views on the Internet, most of which are based on the half understood, ignorant, and parrot-like knowledge and cognition instilled from the United States.**

Being controlled by others in ideology is even worse than in technology. At present, China's understanding of the Internet is very superficial from the superior to inferior. We failed to firmly grasp the technology controlled by others and legal key points. We didn't adhere to independent innovation, which resulted in that we were repeatedly passive or even long-term passiveness in cyberspace strategies and tactics.

This paper will start from the history and technical characteristics of the emergence of the Internet, comprehensively discuss the problems that have existed since the emergence of the Internet more than 20 years ago, and reflect on the future development of the international network, making the Internet a truly open and shared international network.

Keywords-Network; Internet; Future Network

I. INTRODUCTION

The computer network refers to the computer system which can provide transmission, storage, analysis and sharing of data for the purpose of acquiring and mastering data. It serves for the needs of communication with others. Two or more computer networks with communication protocol, transmission channel and infrastructure interoperability constitute a computer network interconnection and interworking system that connects and shares data. Strictly speaking, it can be called interconnected network.

Future Network or an international network system consists of all ubiquitous networks connected, interacting and sharing different carriers, sources, function-matching and operating purposes, whether wired or wireless, ground or space. The current Internet is just a computer network using a single TCP/IP communication protocol, not two or more interconnected networks. It is not the interconnection or internet by the exact definition, so it can't be called an interconnected net, or rather it may be called a computer connected system.

If the origin is wrong, everything is wrong. This is especially true of our understanding of interconnected Networks.

What is the Network? What is the interconnected Network? What is the Future Network? What is the different or relationship between IPv4, IPv6 or even IPv9? What are the fundamental drawbacks of Internet architecture and principles? Do we have safe, credible and effective response plans and coordination measures for the newly-emerging problems, new things, new technologies and new spaces in the process of intelligent network development? We all need to advance with the times to re-understand, redefine, re-explore and re-study it. We need to take the opportunity to seriously correct the deviation and mistakes in cognition and knowledge, and let the network users, the people across the country and our future generations know the facts in a practical way.

II. ARCHITECTURE OF THE INTERNET

It is generally believed that the American Internet, which adopts IPv4 technical protocol, has entered the post IPv4 era due to the lack of address design. At present, renting IPv4 address and adopting IPv4 technical protocol constitute the Internet of various

DOI: 10.21307/ijanmc-2020-009

countries, which is still the mainstream of computer network.

The U.S. military says its IPv4 address can be used until the end of 2029. In recent years, the United States has continued to assign IPv4 addresses to the United States and other countries around the world, excluding China.

IPv6 protocol is designed to solve the problem of IPv4 address shortage. It can provide 2 ^{128} address scale, and that's all. The application and resolution of IPv6 address is still based on the network architecture of IPv4, that is, the original, traditional and irreversible design architecture of the Internet and the tree network architecture (IPv4) continuously improved, strengthened and tightly controlled by the U.S. government and military.

It is inevitable that IPv6 can't interoperate with IPv4 in technology, which is bound to lead to the confusion of network architecture and operation. Therefore, IPv6 special network architecture has to be rebuilt to replace IPv4 network architecture (involving almost all the network software and hardware of infrastructure), which constitutes a "subversion" of the Internet based on IPv4 in fact.

After more than ten years of transitional practice, the United States has found that the cost of rebuilding IPv6 network is too large, there are too many security traps, and the technical agreement is not mature. Besides, "subverting" IPv4 has brought about a series of extremely serious problems in economy, society and military. In fact, the U.S. military and government have abandoned IPv6 transition plans since 2011. In 2017, the adoption rate of IPv6 in the United States dropped from the first in the world to the third.

On July 14, 2017, the Internet Engineering Task Force (IETF) of the United States issued RFC 8200, which announced the latest standard (STD 86) of the sixth edition of Internet Protocol (IPv6). At the same time, it abandoned the RFC 2460 (IPv6 draft) proposed in December 1998, and deleted the "next generation Internet Protocol IPng" which was in transition to IPv6.

Over the past few years, the widespread introduction of new data protection regulations around the world is having a dramatic impact on technology companies and consumers around the world, resulting in some previously established best practices in IETF procedures and regulatory requirements becoming undesirable, the U.S. Internet regional working group (IntArea) said.

Please note that the U.S. Internet Engineering Task Force issued the official document RFC 8179 (BCP 79) in May 2017, namely, "intellectual property issues in IETF technology", which provide three basic principles for IETF to deal with Internet intellectual property claims (discarding RFC 3979 and RFC 4879 simultaneously):

1) The IETF will not determine the validity of any specific intellectual property claim.

2) In following the normal practice? The IETF can decide to use technology that has been exposed as intellectual property if necessary.

3) All participants in the IETF working group discussions must disclose known intellectual property rights or any intellectual property rights covered and likely to be covered under discussion and their recommenders. This requirement applies to all IP claimants, their employers, sponsors, or agents of IP claimants, without the need for patent searches.

In this way, IETF tends to choose technologies with undeclared intellectual property rights, or technologies with free intellectual property rights; IETF may adopt technologies at its discretion, or not commit to licensing; and IETF specifications do not stipulate mandatory security technologies. Therefore, IETF does not define the internal or external problems of the main patent technologies for IPv6.

So what's the practical significance of saying that China has more than 100 IPv6 intellectual property rights? After all we are still subject to the United States and IETF!

III. THE PROBLEM OF IPV6

Practice has proved that many IPv6 Security traps occur and appear when IPv6 cannot interoperate with IPv4, or when IPv6 is trying to run with the network architecture of IPv4 technical protocol. Once they happen, they will not go away, just like opening Pandora's box (security trap or temptation) of network security. For example:

The design of interface ID in IPv6 address will lead to the mandatory real name system for ordinary users in disguise. Because IPv6 also stipulates that interface ID can be allocated in other ways, even random number and manual way, the experts of IPv6 like hackers can easily hide their physical address. This state is no more insecure than IPv4, but an astonishing security scandal once it is widely known, easily operated and arbitrarily adopted by ordinary users who have no knowledge of IPv6. The gateway tunneling may also help hackers or spies of hostile camps hide their whereabouts, making hackers more difficult to find, or causing greater national strategic security problems.

Network address and addressing mode of IPv6, data routing and exchange are real end-to-end, and there is no need for network address translation (NAT). At the same time, the network identification of user equipment is directly exposed, which can be easily collected and used. Through the cross aggregation and correlation analysis of multi-source and multi-element identification data, it is easy for humans and machines to be bound permanently, and thus beyond the current "precise push" (advertising) ability, deriving "precise tracking", "precise positioning", "precise strike", etc., with great potential security risks. IPv6 is applied to smart home, smart community, big data, cloud computing, etc. It may be "accurate" to the details of a family, a family member or the staff in the same office, etc., which is extremely dangerous.

On the one hand, almost all servers of well-known websites are hosted abroad. For example, Netease e-mail server is hosted on Amazon's cloud service platform (AWS). At least the IP address belongs to Amazon. The risk and consequences of domain name and address being controlled are obvious. It is simply to hand over hundreds of millions of Netease users to the U.S. Central Intelligence Agency and its intelligence system (IC) members for all-round, all-view and all-time monitoring and supervision.

Amazon has publicly announced the provision of cloud services to the CIA and its members of the intelligence system (IC), which is known as the "Amazon cloud service platform secret zone" (AWS, Amazon Web services). Amazon called the service "the first and only commercial cloud provider to provide comprehensive data classification services to the government, including non-secret, sensitive, classified and top secret data."

On the other hand, BIND, the system software of DNS server, has become the standard of implicit monopoly. Almost all users in the world do not know the truth (the relevant national authorities and scientific research institutions have never issued a warning, nor have guided users taken any preventive and governance measures), that is, the United States has long been on all DNS servers (IPv4 and IPv6) on the Internet, solidified the necessary route to the network information center of the United States Department of defense first. No matter what users are who, whether like it or not, all data and information exchanges must unconditionally comply with the security principles and measures of "American interests first".

The Great Wall firewall is invalid for IPv6. At present, IPv6 network in Colleges and Universities can easily log in the "forbidden network" of foreign countries (websites of religion, terror, anti-propaganda, etc.). Another reason why IPv6 is not suitable to replace IPv4 is the conflict about IPv6 on the Internet backbone network, which leads to the congestion of network flow. At present, there is no reliable technical solution.

The overall comparison of IPv4 and IPv6 in the case of a single failure shows that in 86% countries, IPv4 connection is more reliable. An important discovery in IPv6 field is that many ISPs do not have correct network connection under normal operation conditions. For example, in the United States, only about 10% of autonomous systems (AS) support IPv6, while in China, China Telecom (AS 4134) only gets global connectivity through one service provider, hurricane electric (HE), which is in worse condition.

Technically speaking, China's public network has fallen into the hands of others, the above-mentioned major IPv6 Security Risks (pitfalls, temptations and solidified routes, etc.) are not completely solved, and state organs and special departments, as well as important sensitive industries involving the national economy and people's livelihood, dare not use them. If it is used, the consequences will be unpredictable.

The principles, systems, and strategies that US internet is dominated and controlled by the US military remain unchanged. The U.S. military has established and improved a network operation system with strict command and coordination from the top down, especially in the field of cyberspace, which is strictly regulated by the U.S. military.

However, it is difficult for China to make a firm response to network operations in the first time, and to organize a high-speed, high-efficiency and high-intensity anti reaction capability of the military civilian joint network operation system in the first time. The current supervision, command and coordination system and framework of cyberspace in China are neither suitable for the perception situation of the Internet in the United States, which has completed and improved the preparations for launching cyber war at any time in terms of technology and law, nor for the needs of accelerating the construction of cyber power and effectively responding to the United States' overall containment of China in cyberspace.

IV. "TWO CHINA" ON THE INTERNET

ICANN is suspected of deliberately manufacturing "two Chinas" on the Internet for a long time, deliberately setting the technical conditions and basis of "two Chinas" that can cause network information confusion, and deliberately restraining, containing and interfering with China's autonomous and controllable development of sovereign and secure networks.

According to the regulations of internet name and digital address distribution agency in the United States, some IP addresses are assigned to the five regional Internet registries (RIR) in the world, and then the five regional Internet registries are respectively responsible for the registration services in the region. IP address and AS number assignment for Asia Pacific countries are managed by the Asia Pacific Network Information Center (APNIC), which is established in Australia. Under the five regional Internet registries, RIR is divided into national registration agency NIR and regional registration agency LIR. The U.S. Internet name and digital address distribution agency divides the Asia Pacific region into 56 economies (countries and regions).

The Asia Pacific Network Information Center has seven core members (national registration agencies) who can enjoy special preferential conditions, including China, Japan, South Korea, Vietnam, India, Indonesia, and even Taiwan.

According to the official website of Taiwan Internet Information Center (TWNIC), founded in December 1999, its original competent department was the Ministry of Transport of Taiwan Authorities. In December 2017, it was changed into the National Communication and Broadcast Commission and became the national network information center.

In December 1999, it was at a time when Lee Teng Hui publicly supported Chen Shui Bian's campaign for "President" and Taiwan's independence was more active. On May 20, 2000, a gun shot put Chen Shui Bian on the throne of "President". Since then, in the "Internet" activities held around the world, Taiwan's "national flag of the Republic of China" has been put in the venue; Taiwan's representatives of TWNIC, the "national registration agency", enjoy the same treatment as those of CNNIC (China Internet Network Information Center) of the People’s Republic of China.

China has clearly declared the principle of "one China" sovereignty in international organizations, but why is the Internet an exception? Why should we tolerate the emergence of "two Chinas" on the Internet many years after China's full-featured access to the Internet in 1994? It concerns the geopolitical issues of Internet governance, the logical, physical and perceptual boundaries of Internet monitoring, and the fact that Taiwan can easily control China's data sovereignty and open-source information by using domain name rotation, data "transgenic" technology and other technologies. It concerns the sovereignty principle and security bottom line of China's cyberspace. This is not a simple technical issue, but a general political issue.

China's “Anti-Segregation Law”, issued in 2005, clearly declared that there is only one China in the world, the mainland and Taiwan belong to one China, and China's sovereignty and territorial integrity are inseparable. The state will never allow the "Taiwan independence" secessionist forces to separate Taiwan from China in any name or in any way. The fact that the "Taiwan independence" secessionist forces split China in any name or in any way, the state may take non peaceful means and other necessary measures to safeguard its sovereignty and territorial integrity.

Any negligence on the sovereignty and security of cyberspace data (no matter professional or amateur) may lead to irreparable loss or disaster of cyberspace sovereignty and security (national sovereignty and security) at any time. How can one tolerate others encroaching on one's preserve?

V. SUGGESTION

Firstly, re-understand the Internet and deepen the governance of the Interconnected Network. Based on a wide range of opinions, we should open up and conduct large-scale discussions on the deployment of IPv6, practically adjust our strategies and tactics in the field of cyberspace information, correctly guide and promote the construction and development of China’s sovereign network, future network, and the global community of destiny in cyberspace.

Secondly, re-consider the e-government extranet, comprehensive website and network infrastructure security, design and implement China's autonomous and controllable cyberspace security monitoring system.

Thirdly, thoroughly eliminate and eradicate the adverse effects, political weaknesses and technological constraints of "two Chinas" on the Internet.

About the authors

Mou Chengjin, the director of the international strategy research center of China Mobile Communications Federation. The paper version was

firstly published in Chinese on December 12, 2018, revised in January 2020. If the Chinese version was needed, please contact the author. Email: mcjzp139@139.com .

Guo Xiaohui, associate professor of Henan Vocational College of Agriculture. Email: guoxiaohui@hnca.edu.cn