# Global Internet Come into a New DNS Era

Mou Chengjin
Research Center of International Strategic, China Mobile Communication Federation
Software Evaluation Center of National Information Center
e-mail: Mcjzp139@139.com

***Abstract*—DNS, short for Domain Name System, is an analytic central system, which transfers domain names into IP addresses that can be identified by the Internet. DNS has internal traits within it to conduct commands and regulations in network communication, as well as centralized ones that are inherently political. Unlike other Internet protocols, DNS protocols penetrate the Application Layer, the Internet Layer, the Transport Layer, and provide even more complicated, tailored low-level software that are feasible to the DNS, ranging from authorized Domain Name Servers to Recursive Domain Name Servers, a domain system based Content Distribution Network (DN-CDN), whether private or public, inside or outside the network, it must be dependent on the service provided by Domain Name System (DNS). DNS includes the increase in Client Subnet in DNS Extension Mechanism (EDNS) to conduct more accurate matches to push service.**

***Keyword-DNS; EDNS; SDN; IPv6; TLD***

## I. IMPORTANT LANDMARK EVENTS

### *A. DNS "Execution Day"*

Knowledge of obsolescent, wrong, or inappropriate methods to conduct software work around is required when we need to go on DNS software updating or programming. Some workarounds pertain to DNS software have made it a deeper and refined situation for the US to control and inaugurate Domain Name System, unavoidably there are functional declination and an increase in unpredictable errors and safety risks. Consequently, reinforcement in Domain Name System becomes inevitable.

The Internet Engineering Task Force (IETF) proposed the implementation of DNS Domain Name System Extension Mechanism (EDNS) in 1999. In March 2016, the US Department of Commerce's National Telecommunications and Information Administration (NTIA), Internet Corporation for Assigned Names and Numbers (ICANN) and VeriSign, a company that provides intelligent information infrastructure services which was established in the United States, led to the completion of the domain name root zone key (KSK) replacement plan as domain name root zone managers.

On October 12, 2018, ICANN finished the first global domain name root zone key (KSK) rollover in the history of the Internet and announced there will be rollover every year. Professionals claimed that KSK is a unified "re-keying", followed by "DNS Execution Day" being unified "lock and hinge updating", they interlock with each other, laying codes systematically.

In May 2018, the Internet's worldwide regional regulatory agencies (RIR) announced officially that February 1, 2019would be the "DNS Flag Day". According to the official notifications from regional Internet authorities and the joint alert of the Internet community, non-compliant domain name servers will identified as "Dead" from the "Execution Day" and beyond, which will make inroads on the access of related websites.

Domain name servers are mainly authoritative domain name servers and recursive domain name

DOI: 10.21307/ijanmc-2019-057

servers oriented. Compliance is a "workaround" to dispense with or delete DNS software by updating software version, and to identify or support the Domain Name System Extension Mechanism (EDNS) by Software Defined Interconnection (SDN). EDNS is implemented by the standard RFC 6891 released by the Internet Engineering Task Force (IETF) in 2013.

The application of DNS protocols on the Internet has a history of more than 30 years. It is the first time in the history of the Internet of the "Execution Day" to maintain DNS protocols and update DNS software versions together globally, indicating the DNS into a new beginning, a new phase, and a new generation in control community. The Asia Pacific Network Information Center (APNIC) state: "We hope that all operators of authoritative DNSSEC (DNS Security Extension) servers will be able to successfully update their DNS system software and seamlessly transfer to the next 30 years of DNS era."

The London School of Economics and Political Science (LSE) published an article entitled "China and the Domain Name System" in March 2009stating,"In terms of Information and Communication Technology (ICT), DNS is an 'inherently political' technology. Because of its ability to allocate, store, and resolve Internet addresses, it is undoubtedly an important fountain of political power; and DNS is mainly for the assurance of the latent capacity to conduct successful communication between standardized technologies and system and the avoidance of duplicate allocation of a same network address. 'Inherently political' technologies also characterized by the high concentration of DNS technology itself. Therefore, these who possess the centralized technology of DNS will seize the power and dominance in cyberspace."

*B. To dispense with the "next Internet IPNG"*

The United States has released a series of planned preparations and foreshadows for the implementation of the "next 30-year DNS era", including the deployment of "recognition" for the Internet development.

*1) To Abandon IPv6 as "next generation Internet protocols", this lasts for nearly 20 years*

On July 14, 2017, the US Internet Engineering Task Force (IETF) released Document RFC 8200, announcing the latest official standard for the sixth edition of the Internet Protocol (IPv6) (Code: STD 86).The Document RFC 2460 (the draft IPv6 specification) proposed in December 1998 and the "Next Generation Internet Protocol IPNG" which was originally for the transition to IPv6 abandoned and removed.

The US Internet Regional Working Group pointed out: "In the past few years, the widespread implementation of new data protection regulations around the world is beginning to make inroads on technology companies and consumers worldwide, resulting the change to bad practices of some formerly established best methods required by IETF procedures and regulations." That is to say, the dramatic changes in the global network application environment have caused dramatic changes in the network technology frames and user needs, "which led to the inevitability and necessity of abolishing drafts (protocols) and transitional measures (plans) with IPv6 in the "next generation of Internet ", showing that the Document RFC No. 8200 is based not only on the objective summary and generalization of the history and status of the Internet but the adherence to the principle of "US first" and the maintenance of "the supremacy of US interests", the aim of cyberspace strategy and the security bottom line.

In the United States, the transition to IPv6 proposed with a pretext of the "insufficient number of IPv4 addresses"; the "IPv6 draft specification" and "next generation Internet IPNG" transition plan now abandoned based on the same principles. The reason being not simply in the design of network technology architecture; nor in the strategic error of network

deployment, but a major deployment to deepen and refine the US network hegemony, and a fundamental decision to reaffirm the “inherently political” trait of the Internet.

Correspondingly, the KSK and DNS Domain Name System Extension Mechanism (EDNS), which controls the DNS Domain Name System Security Extension (DNSSEC), are the premise and the foundation for establishing and consolidating the core role and status of DNS in the "next generation Internet ".

*2) The release of three basic principles advocated by IETF intellectual property rights*

In May 2017, the US Internet Engineering Task Force (IETF) issued the official document RFC8179 (BCP79), the “Intellectual Property Rights in IETF Technology”, providing three basic principles in handling Internet intellectual property problems and discarding document RFC3979 and RFC4879. TheRFC8179 document stipulates:

*a) The IETF will make no determination about the validity of any particular IPR claim.*

*b) The IETF, following normal processes, can decide to use technology for which IPR disclosures been made if it decides that such a use is warranted.*

*c) In order for a working group and the rest of the IETF have the information needed to make an informed decision about the use of particular technology*. All those contributing to the working group’s discussions must disclose the existence of any IPR the Contributor or any other IETF Participant believes Covers or may ultimately cover the technology under discussion. This applies to both Contributors and other Participants, and applies whether they contribute in person, via email, or by other means. The requirement applies to all IPR of the Participant, the Participant’s employer, sponsor, or others represented by the Participant that reasonably and personally known to the Participant. No patent search is required.

That is to say, “The Internet is mine, and the rules are made by me.” IETF is legitimate to choose technology that has not intellectual property rights claimed yet, or freely licensed intellectual property technology; IETF can adopt any technology with no promise of any technology license. Indicating that technology adopted by the IETF in Internet engineering applications is free from the restriction of intellectual property rights and ownership owners. It only determined by the IETF whether the technology adopted by the Internet is “compliant”; technology and any application of intellectual property rights are invalid and non-compliant without the consent of the IETF, and the IETF will not admit it. It is commonplace for the IETF to enforce the utterance of security technology in its technical specifications. The release of the three principles of intellectual property rights is only a public announcement of the “removing the burning brands from under the boiling cauldron”, “overweening” and “getting my own way” strategies.

Until November 2018, the US Patent and Trademark Office (USPTO) granted 19,296 patents for IPv6 related technologies, and the European Patent Office (EPO) granted 2,180. The abrogation of IETF for IPv6 as the "Next Generation Internet Protocol" and its decision to implement a global “DNS Execution Day” and the practice of arbitrarily shutting down the best servers of other countries (such as Iraq and Libya, disconnecting the network and services. No matter how powerful the intellectual property rights are, no matter who grants intellectual property rights to them and who's intellectual property rights are, the three principles of intellectual property rights of IETF, the US civil society organization, are placed on the authority of the government to protect intellectual property rights and the authority of the regulatory agencies. They are absolute dominate and the only "compliance" to the Internet.

The principle of “US priority” and “US interest first” and the bottom line always placed beyond

everything else, too is the cyberspace hegemony to maintain the Internet "one network for all" policy.

## II. LEGAL COMPETITION FOR DATA SOVEREIGNTY

The three basic dimensions that make up cyberspace are the infrastructure-centered physical dimension, the data-centric information dimension, and the cognitive dimension centered on human behavior. For more than half a century, irreversible evolution have taken place, from industrialization to socialization, from commercialization to customization, and the quality-quantity evolution from technology-driven to data-driven, especially the dominance and influence of marginal politic power have become increasingly prominent.

The United Nations Internet Governance (IGF) organization has approved the Global Internet and Jurisdiction Policy Network (I&J) as an "open forum" with more than 200 key entities from different stakeholders around the world participated, including governments and networks enterprises, technical groups, civil organizations, academic institutions and international institutions (for some reason, no Chinese organization participated), with the focus of research and discussion being "the jurisdiction of data" for three consecutive I & J annual meetings (including the upcoming annual meeting in June 2019) .

In October 2015, the European Court of Justice (ECJ) made a landmark ruling that overturned the "safe harbor "mechanism proposed by the European Commission at the beginning of this century and has utilized by more than 4,000 companies, including IBM, Google and Ericsson. According to the European Court of Justice, the "safe harbor" mechanism does not provide adequate protection for the personal data of EU citizens, because the United States often violates the privacy protection measures established by the mechanism in the name of national security, public interest and law enforcement needs.

UK is the one with the highest penetration rate of the Internet economy in the G20 countries. The goal of the UK government is to make UK the safest country to conduct online business activities, and the government holds that the level and duration of protection for personal data should be improve simultaneously when the amount of personal data is keeping increased by the development of digital economy. On August 7, 2017, the UK Department of Digital, Cultural Media and Sports issued a report titled "New Data Protection Act: Our Reforms", which passed the new Data Protection Law to update and enforce the personal data protection in the digital economy era and to replace the 1998 Data Protection Act.

The General Data Protection Regulations (GDPR) adopted by the European Parliament came into effect on May 25, 2018. The regulation extends the data protection from subordinates to owners, refines the classification of personal private data, clarifies the "consent" requirements of the data subject, and guarantees the individual's access to the data, the right to restrict processing and the right to refuse data using, and "portable rights" (obtaining a copy of personal data processing), "erasing rights" (also known as the right to be forgotten). Severe high-limit penalties have been imposed for data managers and processors who violate the law to negate data owner rights, to restrict data processing, to interrupt data transmission or to prohibit data access.

Trump is in a tit for tat, and signed the Clarify Lawful Overseas Use of Data (CLOUD) on March 23, 2018; two months in advance of the European Union, requiring the US Federal Bureau of Investigation (FBI) and other law enforcement agencies have the right to get access to Internet data worldwide. The bill holds that timely access to electronic data provided by communication service providers is the key to the US governments for protecting public safety and combating major crimes, including terrorism; the

communication service providers that regulate, control or own such data should subject to the US law. The bill also allows other countries to store personal data of non-US citizens in the United States. According to professionals, the bill gives US law enforcement agencies infinite priority for administrating any data controlled by the service provider, regardless of where the data is stored and where it created.

In other words, the Clarify Lawful Overseas Use of Data holds that the US government, USA companies and institutions are legal and legitimate in accessing any data in the world to be prosecuted and punished against the EU General Data Protection Regulations. .

The year 2018, it called the "first world data protection year".

Undoubtedly, the protection of data sovereignty and security has risen to the battle for national sovereignty and security. What we have seen is still the battle for cyberspace data that dominated by "US priority", "US interest first". "DNS Execution Day" indicates that the cyberspace data battle has penetrated into the control and command system of the Internet in all directions.

Nomine, one of the world's three largest network information centers, is one of the world's first professional CCTLD (Country Code Top Level Domain) operators. The UK's .UK domain name management and registration agency founded in May 1996. Nomine believes that DNS plays a vital role in every network – it sets the technical standard for translating human-readable domain names into machine-aware Internet Protocol (IP) addresses.

In other words, DNS is the underlying backbone platform of network data operations, applications, services, and security. The dispute between data sovereignty and security must first involve the dispute over the control, command, standard, and initiative and discourse power of the DNS.

The "DNS Execution Day" is the inevitable result of data sovereignty competition. The United States yields none in cyberspace data, not only in technology but also in the performance and implementation at the legal level.

## III. China's Network Data Has Major Security Risks

### *A. Servers generally hosted outside the country*

When observing reversely, China is obviously lagging behind in maintaining data sovereignty and security, protecting data, paying attention to and using data. In the form of insufficient emphasis on law, owner management, and governance of data, many institutions and officials who rely on data and contact with data all day are ignorant of the principles, bottom lines, key points, methods, and approaches of data protection. They are politically confused; formality adhered, technically exaggerated, and lazy in management.

According to National Information Center's continuous real-time monitoring based on DNS open source information, there is a top-down tendency in China's party and government organs, state-owned enterprises, well-known websites (service providers) and other servers with their servers indirectly or directly hosted outside the country. In recent years, there is a large number of data leakages in citizens' personal data, corporate data, national data, and other data involving important economic, political, social, cultural, military and other sensitive industries. Some enterprises provide exclusive services of domestic servers hosting to overseas, and Content Delivery Network (CDN) services, without any scruples and hesitation.

In 2017, China ranked first in the top 10 countries of data leaking. The main member including Baidu with 2 billion user phone numbers, names and addresses; Notecase's 1.222 billion email addresses and user passwords sold on the Internet; Shanghai Chonju's 268 million email addresses and phone numbers; Ten cent's 130 million Email address and

user password sold on the network and the like. So far, how do did they reflect and rectify, and how did the government regulatory department investigate and handle with they remain unknown. However, the online articles that disclosed the truth of the leaked data were quickly delete, and the websites that published the articles were under great pressure. Not only are the rights of the individuals and units that have leaked data at least not respected and protected, but the national data security issue is actually “turned to domestic sales” after being discovered and alerted by the outside world. It is really a strange thing.

On October 11, 2018, Wiki Leaks published Amazon’s “highly confidential” internal file "Amazon Atlas." The document lists the address and operational details of more than 100 Amazon data centers in 15 cities across nine countries, among them nine data centers are in China with six in Beijing. In 2013, Amazon signed a contract with the US Central Intelligence Agency (CIA) to build a “cloud” for intelligence agencies to integrate and provide information classified as “top secret”. Amazon also operates a special Gov Cloud area (government cloud) for the US government. Amazon's government cloud center in China is located in Ningxia Province. Many local development zones and high-tech zones have numbly invited Amazon to set up data centers in the region to publicize and provide “business” training for free servers hosting.

On November 20, 2017, Amazon publicly announced that it would provide a "cloud" service to the CIA and its intelligence system (IC) members, known as the "Amazon Secret Service" (AWS Secret Region). Amazon called the service “the first and the only commercial cloud providing the government with a comprehensive data classification service, including non-confidential, sensitive, confidential, top secret data”. Amazon is the only company required to certify confidential data in the "cloud". The Net Ease mail server hosted on Amazon's AWS service platform.

The server is hosted outside the country, on Amazon,, meaning that the path and system relying on the DNS domain name address translation and resolution depend ocean penetrate (leap) China's “firewall”, with no need to go through the “mirror” in China (With no traces left).It avoid the various monitoring and supervision in China, and the big data managed by the host can be selectively filtered and then “pushed” back to the “Cloud” operated b China.

*B. Revolving Doors Abound*

In the early years, some college elites in the United States changed their status and became national politicians. Some senior generals retired as multinational entrepreneurs or scientific research leaders. They considered the "revolving doors" of identity conversion, which provided the possibility for the realization of the American dream.

Over the years, the concept and manipulation of the "revolving door" has applied to the Internet. Based on the situational awareness of DNS real-time monitoring, the “revolving door” problem found in the servers and “cloud” centers of publicly known websites.

The “vest effect” led by the domestic company and jointly produces the data flow to the outside is called the "inner revolving door", otherwise it is called the "outer revolving door". The original source data conducted in China hosted overseas, and the data pushed from overseas is the data being filtered (backup), and cached domestic. Data leakage or malicious utilization are only in the moment of "revolving door", and we are often asking and arguing for whether the data is leaked, how much data leaked, "towing the library" or "collision library".....

Please note that in recent years, the US Department of Justice, the Federal Bureau of Investigation, and other public evidences of criminal prosecution of Chinese citizens (including my national security officials, international students, researchers, entrepreneurs and the like) are mainly obtain through

the "revolving door"-- Open source data, information, and intelligence.

The CDN Cache Server is an important technical model supporting “revolving doors”. It is the source to provide data (content) to the territory, and also the node that receives data (content) from outside the country. Its open custom port potentially interacts with other countries. Network intrusions and attacks often utilize custom port penetration.

Among Ten cent’s 16 mail servers (IPv4 addresses), 12 of them belong to Los Angeles, with an autonomous system AS 7939, the owner being owner Hurricane Electric (HE, Hurricane Electronics); and the rest 4 in Shenzhen, with an autonomous system AS 132203/132591, with the owner being Ten cent itself. All servers have a "revolving door" function.

Apple has four major domain names in China. The “Guizhou-Cloud Big Data” page is www.colasoft.com.cnicloud.com.cn, and the other three addresses displayed on Apple's official website. The "Canonical Name" of “Guizhou-Cloud Big Data” is www.icloud.com.cn.edgekey.net, the website in China is 47.96.193.19 (www.icloud.com.cn), and the owner is AS37963 (Alibaba Cloud). The IPv4 address 104.100.56.123 mapped to the IPv4 address 23.38.201.117, and the owner is Akamai Corporation of the United States (a service provider with more than one-third of the CDN market in the world). The function of “Guizhou-Cloud Big Data” and the “revolving door” is very obvious and typical, and may involve deeper and broader cyberspace sovereignty and security issues.

The alias of China Railway 12306’s main website is www.12306.cn.lxdns.com, the website in China is 58.216.109.187, the owner is AS4134 (China Telecom), and the five DNSs bound to the alias are all in the United States (AS54994).It is a typical DNS-based content push network (DN-CDN); the domain name of the customer service center dynamic.12306.cn is hosted by the host’s IP address 210.61.207.156 (AS3462), the territory is actually Taiwan (Taipei) and the owner is incredibly the official network operator of Taiwan, Data Communication Business Group.

TABLE I. SOME OF CHINA RAILWAY’S SUB DOMAIN HOSTED IN TAIWAN [210.61.207.156]

| Sub-domain name (alias) | Standardize domain name | IP address visible in the territory (A record) | Business (reference) |
|---|---|---|---|
| dynamic.12306.cn | dynamic.12306.cn.lxdns.com | 110.18.246.12 | customer service |
| ad.12306.cn | ad.12306.cn.wscdns.com | 110.18.246.12 | advertisement |
| travel.12306.cn | travel.12306.cn.wsglb0.com | 110.18.246.12 | go out |
| hotel.12306.cn | hotel.12306.cn.wsglb0.com | 110.18.246.12 | hotel |
| wifi.12306.cn | wifi.12306.cn.wsglb0.com | 110.18.246.12 | Radio communication |
| test.wifi.12306.cn | test.wifi.12306.cn.wscdns.com | 110.18.246.12 | test |
| eximages.12306.cn | eximages.12306.cn.wsglb0.com | 110.18.246.12 | picture |
| epay.12306.cn | epay.12306.cn.lxdns.com | 110.18.246.12 | electronic payment |
| expay.12306.cn | expay.12306.cn.wsglb0.com | 110.18.246.12 | |
| epay-hy.12306.cn | epay-hy.12306.cn.lxdns.com | 110.18.246.12 | |
| exservice.12306.cn | exservice.12306.cn.wsglb0.com | 110.18.246.12 | |
| hyfw.12306.cn | hyfw.12306.cn.lxdns.com | 110.18.246.12 | |

China Railways Member Service's domain name cx.12306.cn managed by the host's IP address 163.171.129.134 (AS 54994), belonging to the United States (California), and the owner is QUANTIL NETWORKS.

TABLE II. SOME OF CHINA RAILWAY'S SUB DOMAIN HOSTED IN TAIWAN [163.171.129.134]

| Sub-domain name (alias) | Standardize domain name | IP address visible in the territory (A record) | Business (reference) |
|---|---|---|---|
| cx.12306.cn | cx.12306.cn.wsglb0.com | 110.18.246.11 | Member Services |
| video.12306.cn | video.12306.cn.lxdns.com | 110.18.246.11 | video |

The above-mentioned hosting servers had opened and used the "Tor the onion router" port 81 defined by the Internet Assigned Numbers Authority (IANA) specification. "Onion routing" is an anonymity-orient, self-contained domain name system and proxy mechanism, mostly used for "dark net" and hackers. Using Tor the onion router to highlight the hosted mainframe will definitely increase risk of severe data leaking. According to the news released by the Ministry of Public Security of China on January 25, there are 406 million passengers during the National Railway Spring Festival in 2019, which far exceeds the US population (326 million). The amount of data and information is considerable, and the value of open source intelligence is difficult to assess. If the United States and Taiwan use this path to launch a network attack or hacker intrusion, it will be able to accurately locate and track any target, and the consequences are unimaginable.

Important note: IANA was formerly managed by the National Telecommunications and Information Administration (NTIA) of the US Department of Commerce. The establishment of ICANN is to fulfill the duties of the IANA. The functions of the two are different and mutually reinforcing, and must be implemented in accordance with the no-cost agreement signed with the Ministry of Commerce and they work well with each other. IANA's functions are developed as part of the ARPANET's deployment of the US department of advanced defense research projects agency, including: 1) coordinating the allocation of Internet Protocol's technical parameters; 2) fulfilling duties related to Internet DNS root zone management; 3) Assign an Internet IP address.

## IV. THE IMPORTANT INSPIRATION PROVIDED BY "DNS IMPLEMENTATION DAY"

### *A. The Bankruptcy of the "Snowman Plan" Lie*

The "Snowman Plan" proposed and announced by ICANN in 2015, its English name is "the Yeti DNS Project", i.e. the "Snowman DNS Plan".

ICANN's best-known responsibilities and missions are to coordinate the global Internet's unique identifier system as a technical coordinator for the Internet Domain Name System (DNS) to ensure the stable and secure operation of the unique identifier system.

The "Snowman DNS Program" website hosted by ICANN clearly states that the "Snowman DNS" system is a test platform for root domain name services and some experiments and will do not add/delete delegates in the IANA root zone, and all resource records (Resets) are identified by the "Yeti" security extensions (DNSSEC) key, no alternate domain space is provided.

Paul Dixie, proclaimed himself as the "father of domain names", one of the founders of the Snowman DNS Program, stressed and warned in 2016 that if the "Snowman Plan" is considered to be a domain name expansion, anyone in addition to IANA will be able to effectively edit the top-level domain space, such as adding a new top-level domain (TLD) or changing the ownership of an existing top-level domain (TLD). The

answer is definitely not; if you touch it (to instead the root domain name service), you will die; and if a certain country wants to create its own Internet DNS system, independence will be unhealthy, vulgar and short-lived.

Paul's "Snowman DNS" working mode:

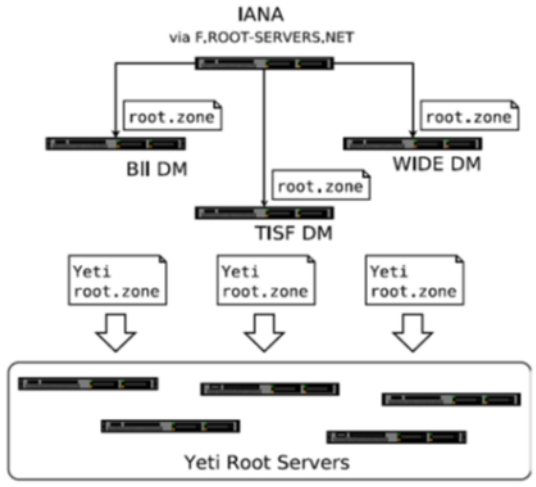


Figure 1. Snowman DNS working mode

For a long time some professionals and government officials in China spare no effort to advocate that the "Snowman Plan" is led by Chin, represented by Beijing Tinder Interconnect Information Technology Co. Ltd. (BII Group), and claimed that China had "Built a global IPv6 root server network and demonstrating a new IPv6 root server capabilities", "China deployed four IPv6-based root servers, breaking the predicament of China with no root servers in the past." and the like.

Ruthlessly, the "DNS Execution Day" returned the "Snowman Plan" back to reality. The result of DNS's compliance announced the impeachment of the "Snowman Plan" in the beginning of the Internet's "the next 30 years of the DNS era"; or it was a "slapstick" exploited by someone. The practice makes "alternative routes for the domain name" unsustainable, as well as the melting of invest and foundation of the "snowman" (deceitful publicity and fake amounts) which lasts for more than three years.

Beijing Tandy Interconnect Information Technology Co. Ltd. (BII Group)'s IPV6 domain name server compliance testing result

IPv6 address: 240c:f:6644:2:0:276a:c70

Test result: Fatal error detected

dns=timeout
edns=timeout
edns1=timeout
edns@512=timeout
ednsopt=timeout
edns1opt=timeout
do=timeout
ednsflags=timeout
docookie=timeout
edns512tcp=timeout
Optlist=timeout

All 11 tests are out of order

Figure 2. Result of IPV6 DNS Compliance Testing

It is worth pondering that the DNS Extension Mechanism (EDNS) was proposed by Paul in 1999 (RFC 2671) and became a standard in 2013 (RFC 6891). However, Paul turned a blind eye to "snowman" deceitful technology, its non-compliant application and self-deprecating in the Internet community (that is, the flexible workaround of the claimed "one world, one Internet, one domain name system"). So where does the reason lie? Is Paul fooling the experts of the BII Group or vice versa? Or is there a tacit agreement between the two?

The above facts also clearly reveal that the Internet vitality based on IPv4 technology is still vigorous. For the United States, the "DNS era of the next 30 years" is still the IPV4 era.

According to the "USG v6 status statistics" collected by the National Institute of Standards and Technology (NIST) until December 22, 2018, only 2% of the US-supported IPv6 industries are still in operation in spite of the US government's nearly 20-year IPv6 transition plan,98% of them have transitions or no progress; only 3% of US universities use IPv6 domain name operations, 97% of them have

transitions or no progress, which is an abnormal dynamic that cannot be ignored. According to the APNIC statistics, until October 31, 2018, the rate of US IPv6 users has dropped from the first to the third worldwide, and China ranked 71st. According to Google's monitoring, the adoption rate of IPv6 in the United States is actually a mere 36.31%.

The Asia Pacific Network Information Center (APNIC) report pointed out that from the second half of 2017 to August 2018, the IPv6 deployment status had declined. Operators who are under higher pressure of an IPv4 addresses shortage have a low IPv6 deployment rate, which does mean that there is no urgency to deploy IPv6 in a client/server (C/S) environment in many areas of the Internet. In other words, the pressure of address shortage is not a sufficient and necessary prerequisite for deploying IPv6 on a large scale.

Entrusted by the Office of the Chief Technology Officer (OCTO) of the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Governance Projects Group (IGP) of the Institute of Public Policy at the Georgia Institute of Technology published a survey report entitled “latent standard war” in February 2019, the research analysis found that it’s not a “transition” issue that makes sense between IPv4 and IPv6, but economic disputes between the two routes in technological evolution; and the current lopsided IPv6 deployment rate and the relevant data violates a simple or predictable pattern.

According to “Supporting China's IPv6 Scale Deployment - China's IPv6 Service End-to-End User Experience Monitoring Report” released by China's “National Next Generation Internet Industry Technology Innovation Strategic Alliance” on November 1, 2018, there are 7.18 million IPv6 Active Users (IPv6 Allocated and with IPv6 Internet history records within one year) with mobile broadband and 2.33 million with fixed broadband, 9.51 million in total. According to the “promoting the scale of IPv6deployment” requirements to reach a 200 million at the end of 2018, the current number is still far behind.

IPv6 subverts the situation of IPv4 network application architecture, and it is difficult to solve a large number of known and unknown security traps and security barriers.: huge investment and operation and maintenance costs, and the economic benefit in the future is distant no matter whether it is market economy or planned economy; the balance of trade-offs. It is imperative to re-adjust the strategy of deploying IPv6 in a realistic manner. Our country must make an early decision.

In the face of well-known and irrefutable facts, what will the Beijing Tandy Interconnect Information Technology Co. Ltd. (BII Group)’s experts say? Self-defense or explanation? Should the administrative, law enforcement, auditing, and supervision departments of the state and governments at all levels seriously perform their duties?

*B. BIND is the Key and Crucial Part*

The US Defense Advanced Research Projects Agency (DARPA) funded the development of BIND in 1980 and BIND, which was taken over by the US Internet Systems Alliance (ISC) after 1984, is the most important core step and strategic deployment of the Internet. It is for not only the "kidnapping" of the DNS hub platform, but also for the close integration in the "soft and hard" aspects, firmly grasping and controlling the ownership, command, control and decision-making power of the DNS. BIND has embedded in the DNS and has become the “de facto standard” for DNS bundled applications. The global software market, which dominates DNS applications, is not only a “traffic light” rule that guides the flow of Internet data, but also a baton that conducts compulsory obedience if you have “bad Behavior”; you will be in violation of the law, get lost, embarrassed, and chaotic or hit the wall.

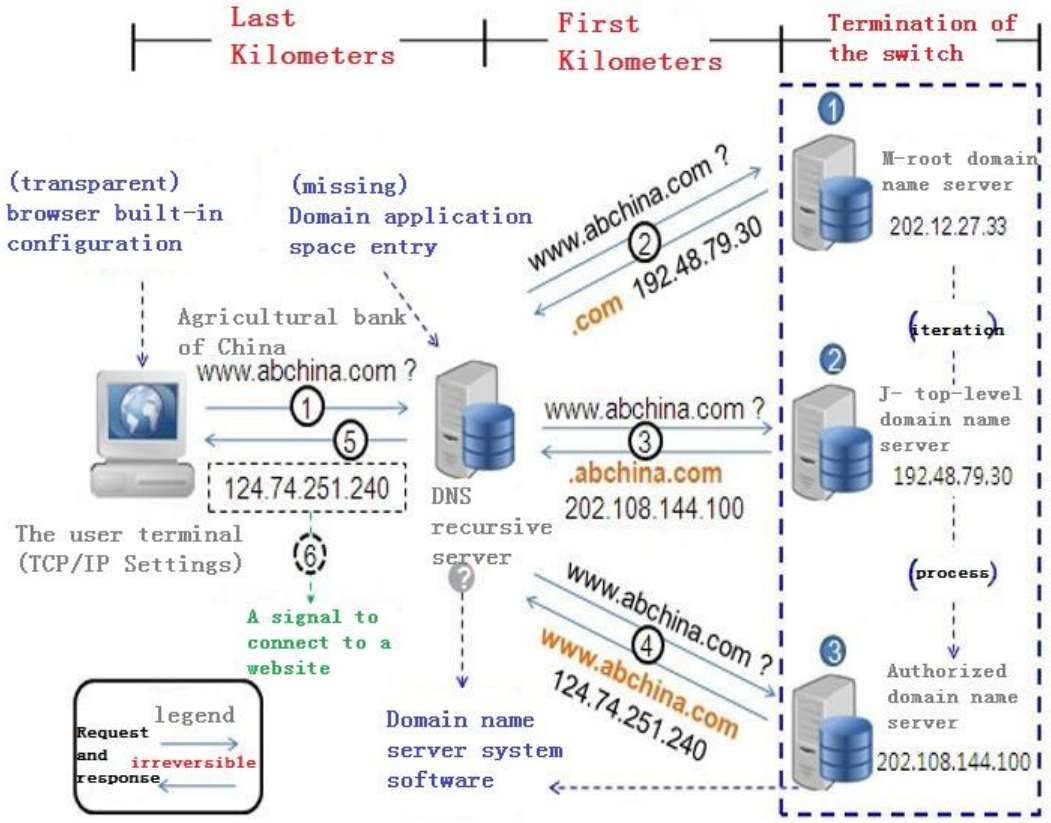


Figure 3. Structure of BIND

The picture above shows that under the role of BIND (control command guiding software interconnection and interoperability), the DNS application drives the recursive server, the recursive domain name server and the domain name resolution system perform conduct three irreversible domain name resolution iterations by "right to left" interaction process. However, any of these links may be eavesdropped, stolen, tampered with or transferred. It may also be a "safe information exchange" after being "legally mirrored" by the hierarchical service providers. It is “sifter-type” vulnerability that professionals must have knowledge of it.

The US Department of Defense uses the domain name system to set the Internet logical boundary, and the US Department of Defense Network Information Center (DOD Network Information Center) operates and manages the military-specific network NIPR net. BIND (developed by the US Department of Defense), which is solidified in DNS, was targeted to the data flow to the US Department of Defense Network Information Center firstly and then to other network information center nodes such as intelligence departments.

We must pay attention that the process DNS request data (and information) is identical during the parsing interaction. Some experts explained that: “The content stored in the root server is very few. Usually, ordinary users will not access the root server when they surf the internet.” If it is not an ignorant mistake, it must be intentionally misleading.

Given the information on May 12, 2017, when the “WandaCry” ransom ware incident spread rapidly in

more than 150 countries and regions around the world. A British engineer stumbled upon the "want to cry" virus through domain name to conduct command and control (C&C), and used the "Kill Switch" method to effectively curb the “WandaCry” virus, which was praised by the industry and the media as an “Accidental Hero”. At the same time, the world has realized the BIND solidified” end switch” function of the DNS.

“Termination switch” is a new Internet term or a network hot word involving data sovereignty, network security, and Internet governance. The exact definition of Internet Kills which is: a control mechanism designed to be activated as a countermeasure to shut down all or part of the Internet traffic.

US Senator Joe Lieberman and other people submitted a legislative proposal “Protecting Cyberspace as a Nationalization Act Asset Act of 2010)” (S. 3480) at the 111th Congress on June 19, 2010, was called by the media as the Internet Termination Switch Act.

The Electronic Privacy Information Center (EPIC) of the American Civil Human Rights Organization began to track the US government's Standard Operating Procedure 303 secret plan document in 2011. The 30-page “Emergency Radio Protocols” drafted by the National Telecommunications Coordination Center (NCC) and approved by the National Communications System (NCS), proposes the process to “close and restore commercial and private wireless network when the country is in crisis.” It represents the policy of the US government and is also called the "Internet Kill Switch" by the industry and the media.

ICANN's official website published a passage entitled “What is the Internet termination switch? Who has the key?”On July 22, 2016, clarifying that the Internet "termination switch" is in the domain name root zone and ICANN holds the key. Russian experts call it the “red button of the Internet.”

Europe, Russia and other countries have been highly vigilant against the US control and command to solidify BIND's DNS. The NSD developed by NLnet Lab in the Netherlands based on BIND standards. Although the technology research and the support are relatively independent, it has not yet to form a mainstream. But at least, from the perspective of DNS application, it is possible to avoid “all eggs in one basket” and reduce risks; and from the perspective of open cooperation, research and development of controllable technologies and products can lead to the balance of different companies and seek a balances; in the long run, it is beneficial to the Internet domain “building” to balance of DNS control. Russia recently announced that it will take the test out of the global Internet in the near future (April 1). The focus and purpose is to check the content blocked by the traffic, to ensure that the traffic between Russian users (more than 90%) remains in the country, and it can only be the necessary countermeasures about research and development to control parallel DNS.

Our country should catch up. While drawing on and utilizing BIND in the United States and NSD in Europe, we can encourage the reference to the boundary and frontier security defense measures of the "Einstein 3" plan, and cut into the situational awareness based on real-time monitoring of DNS open source data information to accumulate experience, and re-recognize and explore the source of governance and control of the Internet, strive to develop the DNS system software that is self-controllable and compatible (check and balance) for both BIND and NSD.

### *C. Data Sovereignty and Security are the Key Point*

In summary, Data Sovereignty has become the consensus and action of the United States, the European Union, and many countries (including the legislation and governance), especially after the “Prism Gate”, it becomes the important “topflight” Without the principle of data sovereignty, not only is data

security and privacy at risk, but national data assets are inevitably threatened. In particular, it should be pointed out that the "interconnection" of the Internet today is conditional and bordered! For example, China's IP address is used as a "blacklist" by some professional websites outside the country, and the access to it is prohibited (404, no access authorization).

The general identification of data sovereignty is: the government's control over the collection of data in the country, including data residency (the location where data is forced to store), data retention (the compulsory reservation of data trade records).

The United States is the initiator of the Internet. At first, it was introduced from the military APA network to the European Internet in order to transmit open source data (information, intelligence). For more than half a century, the United States has built and developed the Internet; the technological innovation is always about data sovereignty, data security and data utilization (acquiring intelligence)--all for data. Even from this perspective, we must re-recognize and deepen our understanding of the relationship between United States and the Internet, the world and the Internet, China and the Internet in all ways. We are obviously seriously lagging behind when we continue to follow the understanding, and thinking of the Internet 20 or 30 years ago in the United States and the situation even becomes more and more serious, ruthlessly ignoring our innovation and entrepreneurship in cyberspace, making us just wait and see again and again. Being completely marginalized, the scientific advancement of the future network is gradually drifting away.

Today, any network technology carries data. Network applications generate data; interconnections exchange data; network services face data; network innovation development (such as artificial intelligence) relies on data; network security (national security) protects data, Data has been integrated into the driving force of human social development, building the collective assets, culture and language of the community. Data, whether territorial or affiliated, has been transformed and applied in different degrees and at different levels "genetically modified". The "face-changing" of data has become the norm and has become a subversive factor for maintaining or shaking the fundamentals of cyberspace sovereignty and security.

Most Chinese citizens and officials are not sensitive enough to network data. They know nothing about cloud computing, big data, small probability events, open source information, and always think that there is no bearing between themselves and the unit, not to mention the full use of data, the urgent need to build and develop data centers, and the great importance of it. The DBS Group study believes that the overall utilization rate of China's data centers is less than 50%, and the utilization rate of data centers in the lower cities is only a 20%. In the next 3-5 years, the demand for data centers will not be transferred to the data centers of the lower rate cities on a large scale. Because of this, Amazon, Apple, Microsoft, IBM, etc. have come to China to build data centers in the past few years, called China services, which are actually American services. Ten cent, Net Ease, Baidu, 360, Railway 12306 and even party and government agencies have also been "managed" to overseas hosting servers in exchange for "free" advanced technology services and individual business interests in China. DNS-based CDN (and SDN) technology has formed the mainstream and technology trends of the Internet for years to come.

In most network environments of national key information infrastructure, gatekeepers, firewalls, intrusion detection systems, anti-virus software are usually configured to control the data traffic of TCP/IP and other network protocols, and to implement the physical isolation (PNI) between internal networks (private networks) and public Internet.

However, the rather universal stipulation and phenomenon deviate from the facts. Cyber security threat exploits this cognitive misunderstanding and the blind spot of supervision, DNS is used as a carrier to bypass the network security protection mechanism and transmit sensitive data from inside the enterprise to the outside of the enterprise. Even the ""physically isolated" private network still relies on DNS requests and responses to form an interaction between internal and external network (connection de facto). Usually it is "unblocked" (such as firewall port 53) and the commonly-held blind area (such as DNS abuse, misuse), so that the abnormal behavior of intranet DNS applications and information leakage through DNS is basically out of control.

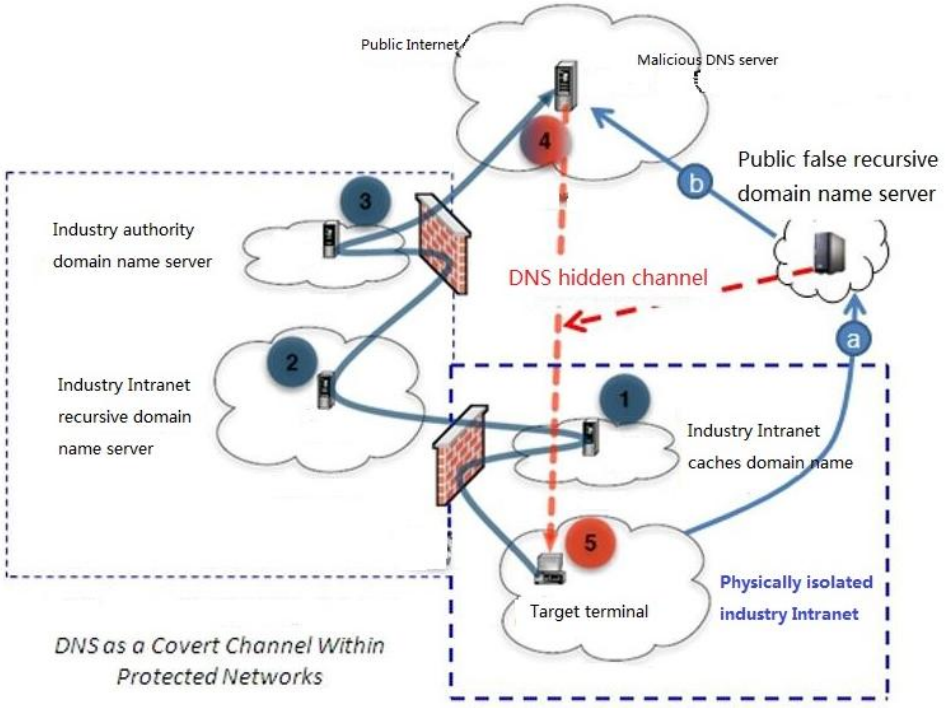


Figure 4. DNS as a Covert Channel Within Protected Networks

In the diagram above of the US Department of Energy (DOE), the "channels" of (1)-(2)-(3) are inherent to the industry intranet and industry extranets, that is, part of the network system; (a)-(b) "channel" is caused by DNS abuse or the existence of a loophole in the target terminal, that is, the application of chaos out of control (such as random use of Google public DNS service, 8.8.8.8, etc.); (4)-(5) forms the hidden channel of DNS that can be used not only as a transmission carrier for leaking data, but also as a means of command and control (C2) (such as APT).

Johnson from US Secretary of Homeland Security reported in January 2016 that the Einstein Plan for the National Cyber Security System (NCPS) began in 2010 and entered the third phase (called E3A) in April 2013. It not only monitors cyber attacks, but also has the ability to intercept and handle the confidential information; it can also effectively protect the government network's security and respond to the most advanced network attack opponents. Simultaneously E3A provides a platform for new technology research and development, and cooperates with advanced technology and expertise of government departments and private industries to discover unknown network attacks. The US Congress has mandated that all federal

administrations join the E3A program by the end of 2016.

"Einstein-3" (E3A) provides four main functions: 1) defense: real-time mitigation of already known or suspected cyber security threats; 2) screening: identification of invaded information systems, system components or host terminals, as an immediate response to security incidents; 3) perception: customized development, maintenance, and service for the network security status of the federal government information system, based on "Security is Normal Monitoring". 4) Discovery: monitoring and identifying new or emerging cyber security threats targeting federal government information systems to enhance cyber security defenses.

It is recommended that the state should formulate and launch China's network sovereignty and security strategic plan based on "Einstein-3" (E3A), using the existing network infrastructure to build an autonomous and controllable DNS situational awareness system, and build China's data sovereignty, data security, and data utilized for the new cyberspace Great Wall.

## V. CONCLUSION

Today's Internet is facing a number of major changes. All countries are trying to grasp the latest technology for this revolution. As the United States announces the abandonment of the "next-generation Internet IPNG", it marks the entrance to a new era for the Internet. Based on the current status of worldwide Internet domain name system research, this paper analyzes the international research level of this technology, discusses Internet security and data security problems we are now facing, and puts forward the importance of independent research and development of Internet domain name system. At present, most of the servers in China are still hosted in foreign countries, which pose considerable, latent danger to data security. Under the current environment of Internet innovation, it is necessary to grasp the immediate opportunities and conduct research and development of the Internet domain name system to ensure China's data sovereignty and information security, and keep pace with the Internet development era.

## VI. ACKNOWLEDGEMENT

This passage is written by the Director of International Strategic Research Center of China Mobile Communication Federation; the Chairman of Nanjing Huadao Network Technology Co. Ltd.