DNS is the Internet Pivotal Basics and Fundamental

Chengjin Mou
[1.] Senior Researcher of Kunlun Strategy Research Institute and Information Security;
[2.] Director of International Strategic Research Center of CMCA;
[3.] National Conditions Deputy Director of Development Strategic Security Research Center;
[4.] Zhejiang Province Chief Researcher of Beidou Future Networks Space Research Institute
E-mail: mcjzp139@139.com

***Abstract*—DNS provides name resolution services for Internet applications and is an important infrastructure of the Internet. The domain name system is the core infrastructure of the Internet, which is responsible for the composition of irregular digital sequences Internet protocol address (IP) and highly readable domain names are converted to each other, which is an important prerequisite for maintaining the normal operation of the Internet. The domain name system provides domain name to IP address translation. DNS system was designed to run in a trusted environment at the beginning, but now the complex Internet environment makes the vulnerability of DNS protocol appear.**

This paper briefly describes the current situation of the Internet and the domain name system. By analyzing the current situation of the domain name system, the structure of the IPv6 domain name system and the development of DNS related technologies, it concludes that DNS Security issues are not limited to "vulnerability" or "harassment", but have a clear strategic and systematic nature, and have become one of the focuses of unprecedented struggle and competition, that is, "whoever controls DNS will own the Internet". At the same time, this paper also summarizes the latest research achievements in DNS protocol design and system implementation, and prospects the possible hot research directions in the future.

Keyword-DNS; Internet; Domain Name Resolution; IPV6

I. DNS IS THE INTERNET

DNS is the abbreviation of English domain name system which refers to the domain name system of the Internet (the same below) When DNS is referenced in Chinese; it is usually understood directly as "domain name resolution system".

In September, 2021, Geoff Huston, chief scientist of the Asia Pacific Network Information Center (APNIC), pointed out at the Symposium on "DNS openness" held by the European electronic communication regulatory authority (beret), "Every Internet user connected to the Internet must first access DNS without selectivity. In fact, this attribute essentially defines what the Internet is, that is, DNS is the Internet."

In this sense, today's Internet at least includes the DNS system resolved by the bind software of the United States the DNS system[1] resolved by the NSD software independently developed by the Netherlands, and the "Russian sovereign Internet"(RuNet) that independently adjusts the autonomous domain and legislates to regulate DNS resolution.

DOI: 10.2478/ijanmc-2022-0012

While the Russian Ukrainian cyber war, which is called "300000 global hackers" by the US media, is under way, the US internet technology and capital leaders are working together to "sever" Russia, the US will expand its cyber forces, the US has signed the Declaration on the future of the Internet with more than 50 countries and Taiwan, and the US led NATO has accepted South Korea to join the Cyber Defense Center, which has repeatedly stated that, The United States has never given up its hegemonic proposition of "one world, one Internet".

Facts have constantly proved that the view in the Research Report on "China and the domain name system" of the London Institute of economic and Political Sciences (LSE) on March 19, 2009 is groundless, that is, the domain name system DNS is a typical "inherently political" technology; The attempt to change the politicization of DNS lacks binding force; Getting rid of the inherent political nature of DNS technology depends on the change of new standards and architecture.

Facts have further proved that DNS constitutes the key core foundation of the global network addressing mechanism and virtualization services (such as "content push network" CDN) on which the basic functions of the Internet depend. With the rapid development of Internet technology and application, the role of domain name system DNS not only lies in its importance and security, but also highlights the ownership of its command and control.

As of March 23, 2022, the United States has revoked the authorization of "Article 214"[2] of five state-owned telecom operators in China, all of which have taken effect. This means that the Chinese public network, which was fully functional connected to the U.S. Internet in 1994, will be disconnected at any time, regardless of the IPv4 or IPv6 protocol, or other virtual overlay networks attached to the Internet, that is, the most basic DNS link of the Internet will be disconnected, and the addressing mechanism of the Internet root name server system and the basic support for virtualization services will be disconnected.

II. DOMAIN NAME SYSTEM

DNS includes an ecosystem composed of domain name registration, domain name application protocol, domain name resolution hierarchical service, domain name server software, and communication networks, which constitutes an information and communication technology and service (ICTs) supply chain. Therefore, DNS is the "system of systems" of the Internet, and the key foundation and foundation for the "multi stakeholders" of the Internet to attach great importance to (and seize).

A. Domain name resolution

DNS is actually a distributed database. Its hierarchical structure is similar to the file system structure of UNIX (Figure 1), presenting an inverted "tree" with roots at the top.

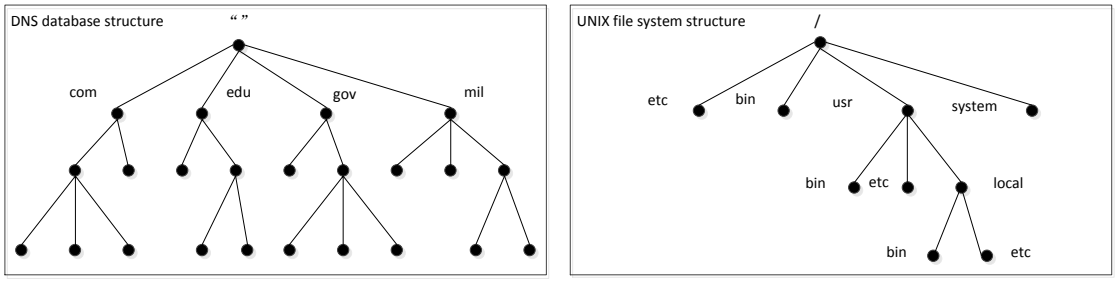

Figure 1. DNS structure of domain name system and UNIX file system structure

The composition and resolution of domain names follow the rule of "right to left" and flow in an orderly manner. They are the root domain name, the top-level (Level 1) domain name, the authoritative (Level 2) domain name, and the sub (Level 3, level 4, etc.) domain name, followed by "." to distinguish. For example, "www.icbc.com.cn" is a three-level domain name. The United States attaches great importance to and closely controls the DNS hierarchical tree system domain name resolution, and never allows any reversible, variable and movable situation to occur.

According to the definition of "DNS terminology" (RFC 84992019-1), DNS "instances" allow multiple DNS servers to have the same IP address in anycast routing, and each server (cluster) is called a "node"; Such DNS domain name server nodes are also called "anycast nodes".

Since 2008, all root domain name servers have applied the "anycast" technology to realize the transformation of the root domain name server into a "system of systems" and provide faster services. Therefore, the global Internet is no longer 13 root domain name servers, but the integration of 13 root domain name server systems [3].

TABLE I. DISTRIBUTION OF NODES OF 13 ROOT DOMAIN NAME SERVERS IN CHINA

Root domain name system(As of November 18, 2021)	**Chinese Mainland (22 nodes)**	**Hong Kong (11 nodes)**	**Taipei (7 nodes)**
A (Verisign)	-	1	-
E (NASA)	-	2	1
F (ISC)	BeiJing:1 HangZhou:1 ChongQing:1 XiNing:1	3	2
H (Army Research Laboratory,ARL)	-	1	-
I (Netnod,Switzerland)	BeiJing:1	1	1
J (Verisign)	BeiJing:1 HangZhou:1	3	-
K (RIPE NCC,Netherlands)	BeiJing:1 GuangZhou:1 GuiYang:1	-	1
L (ICAN N)	BeiJing:1 WuHan:1 ZhengZhou:1 XiNing:1 HaiKou:1 ShangHai:1	-	2

The total number of nodes in the 13 root domain name systems increases or decreases dynamically.

The above Tble1 shows that with the help of anycast technology, the 13 root domain name server systems of the Internet have set up 1469 nodes in the world (configured with established IPv4 and IPv6 addresses).

Please note that any one root domain name server and its corresponding anycast site or node will not be composed of one or two computers or several cabinets, but a server (data cabinet) cluster designed and constructed according to the needs of the service object and scale (target and target group) and sufficient computing support. Among them, the core supporting the computing power of the server cluster is the algorithm.

B. DNS protocol family

In November 1983, the concept, facility, implementation and specification of domain name system DNS (RFC 882, RFC 883) was formally proposed.

The Internet Engineering Task Force (IETF)[4], established on January 14th 1986, is responsible for formulating and promoting the voluntarily adopted Internet standards and specifications, especially the standards constituting the TCP/IP protocol family. At present, RFC involving DNS and related to TCP/IP four-layer architecture and protocols includes 299 protocols (standards) in 7 categories. As shown in Table 2.

TABLE II. RFC CATEGORY, QUANTITY AND DNS RELATED QUANTITY

Category of RFC	Number of RFCs	Where the number of RFCs associated with or related to DNS
Standard	122	5
Proposed Standard	3,819	142
Best Current Practice	301	25
Informational	2,791	87
Experimental	522	29
Historic	331	10
Uncategorized	887	1
Total	8,773	299

C. Top level domain name

The service Zone of the root domain name is the top-level domain name. In other words, the root domain name system is available and serviceable only when the top-level domain name is registered and enabled. The authorization and management of the Zone File of the root domain name and the services of the root domain name system are currently only available for 1588 top-level (or first level) domain names. The registration of top-level (or first level) domain names requires the approval and authorization of ICANN [5].

On January 1st, 1985, six top-level domains ".com,.net,.org,.edu,.gov,.mil" were first registered, marking the official operation of the root domain name system. Among them, "com,.net,.org" is called the general top-level domain name, and ".edu,.gov,.mil" is used as the special top-level domain name.

The US national top-level domain name ".us" was registered on February 15th, 1985; The

Chinese national top-level domain name ".cn" was registered on November 28th, 1990.

Currently, top-level domain names are divided into seven types (As shown in Table 3):

TABLE III. TYPE AND QUANTITY OF TOP-LEVEL DOMAIN NAMES

TLD type of top-level domain name	Abbreviation	Current quantity
Common top-level domain name	gTLD	3
New generic top-level domain name	ngTLD	1,240
Country / region code top level domain name	ccTLD	316
Qualified generic top-level domain name	grTLD	3
Infrastructure top level domain name	(arpa)	1
Private top-level domain name	sTLD	14
Test top level domain name	tTLD	11
Total	-	1,588

In practical applications, a large number of registered domain names are secondary (or authoritative) domain names, that is, the names of organizations, enterprises and websites, such as "ccb.com".

VeriSign reported that as of June 2021, 367.3 million secondary domain names had been registered worldwide; among them, 181million are general top-level domain names (GTLD), accounting for 49.3%.

D. Leading DNS software

In 1984, the system software running on the first root domain name server was called "JEEVES", which was designed and developed by Paul Mockapetris. At the same time, the first DNS software version, funded by the Defense Advanced Research Projects Agency (DARPA) of the US Department of defense, developed by Berkeley University (four graduate students) and released in May1984, is called "BIND"[6]. Later, Doug Kingston and Mike Muuss of the U.S. Army ballistic laboratory made major changes to the BIND software code, which was used in the H-Root domain name server of the U.S. Army ballistic laboratory in 1985. Perhaps the H-Root can be considered as the Taproot of DNS domain name resolution.

With the support of the U.S. Department of homeland security, BIND has been completely upgraded and changed from structural design modification to comprehensive code update. In September, 2000, the Internet Software Alliance Corporation (ISC) released the new main version of BIND (BIND 9), which has been used until now: from the release of version 9.0.0 on January 28, 2004 to the release of version 9.17.18 on September 15, 2021, 673 sub versions have been released in 18 years (the life cycle of the sub versions is generally one year), including software upgrade, defect modification and vulnerability patch.

With its first mover advantage and the "promotion" mode of providing free software and open source code, BIND has a market share (allegedly) of more than 90% and is also regarded as a "de facto standard" in the industry. It must be noted that the "free software" of BIND is not equal to "open source code" and should not be confused.

In May, 2002, NLnet Lab in the Netherlands released the DNS software independently

developed, called "NSD", which was enabled in the "K" root domain name server in February 2003, replacing "BIND". At present, four root domain name server systems (D, H, K, L) have adopted "NSD" [7].

In addition, in March 2021, the National Security Agency (NSA) of the United States released the new DNS software developed, called "Protective DNS" (PDNS), which is currently mainly used in military networks and defense infrastructure (DIB) networks. In the sense that "DNS is the Internet", it should also be a system that can be resolved and run independently.

E. DNS supply chain

The simplified relationship of the ICTs supply chain of the root domain name system DNS is shown in the following figure 2:

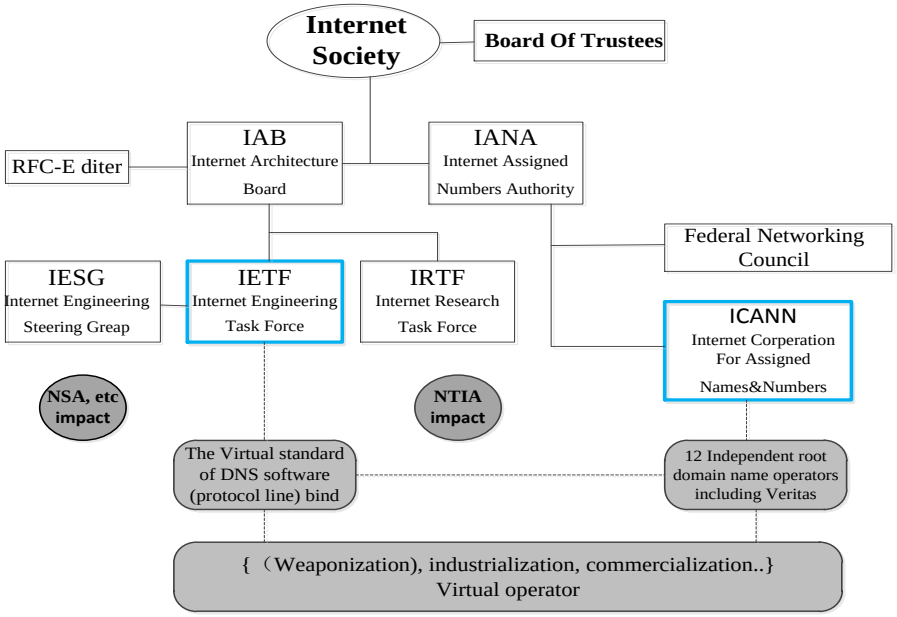

Figure 2. Simplified diagram of ICTs supply chain based on root domain name system DNS

1) ICANN and IETF are parallel, or IETF has no direct relationship between the R & D of technical specifications and the authorization and management of digital resources;

2) 12 root domain name system operating units such as Veritas are not fully subject to ICANN, including the influence exerted by NTIA on behalf of the U.S. government in fact;

3) The DNS standards and specifications of IETF are only the minimum set of codes in DNS software implementation (that is, the codes that implement DNS software protocol stack have enough "discretionary" space, which varies with different software protocol stack developers);

4) All kinds of virtual operators can adapt to the "vest" and change or subvert the application mode and mode of DNS. Such as DNS based content push network (CDN);

5) The National Security Agency[8] (NSA) and the national cyber security and Infrastructure Security Agency (CISA) of the United States have considerable (demand oriented) guidance and (weaponization) influence on the research, development and application of DNS software technology. For example, BIND software has a special and customized version, which is different from the free version open to the public.

In the ecological environment of the root domain name system, if ICANN has the decision-making power over digital resources (domain name, IP address and Asn autonomous system number) and root domain name management, then the domain name execution power in applications and services is another matter.

III. Regulation and governance of DNS

A. Root domain name server

In 1984, the first root domain name server of the Internet was established to serve only the ARPAnet network of the USD Epartment of defense.

In 1985, the number of root domain name servers increased to four, which were hosted by the American Academy of Information Sciences (ISI), Stanford Institute of International Studies (SRI) and the US Army ballistic Laboratory (BRL).

In 1987, the number of root domain name servers was increased to 7, and the services were extended to ARPAnet (Development and Testing network), MILnet (military network), NSFnet (National Science Foundation Network), SURAnet (Southeast University Network), BARRnet [9] (Western Silicon Valley Research Network) and NASA-Science (NASA research network).

In 1995, the year after China's full-featured access to the U.S. Internet, the number of root domain name servers increased to 9, the services were extended to NORDUnet, and the root domain name servers were renamed from "A" to "I".

1997 was an important year for the United States and China to develop the internet almost synchronously. The United States has achieved and improved the Internet in DNS technology, and China has provided a large market for Internet applications:

▲ In January, the United States added four new root domain name servers from "J" to "M". So far, 13 Internet root domain name servers have been built and renumbered from "A" to "M", completing the overall architecture deployment of the Internet domain name system. On January 1st, China's people's network was connected to the Internet.

▲ In May, the "K" root domain name server was transferred from the United States to the Internet Exchange Center (Linx) in London, England, and then to Amsterdam, the Netherlands (autonomous system AS 25152), which was managed and operated by the European Internet Coordination Center (RIPE NCC). On June 3th, China Internet Network Information Center (CNNIC) was established.

▲ In August, the United States transferred the "M" root domain name server to Tokyo, Japan (autonomous system AS 7500). In October, CHINANET was interconnected with CSTNET, CERNET and CHINAGBN.

▲ Please note that since the DNS data message adopts UDP transmission protocol, the data packet length is 512 bytes; The length of IPv4 address is 32 bytes. The IPv4 addresses of 13 root domain names occupy 416 bytes (embedded in DNS message), and only 96 bytes are DNS data and information. Therefore, it is the main reason for limiting the Internet to set up 13 root domain name servers at most.

However, this does not mean that if the IPv6 address length is 128 bytes, the root domain name server can be added. In fact, after more than 30 years of transitional tests, IPv6 is still only attached to and subject to the existing 13 root domain name server (system) architecture of IPv4,

and has not established a "pure IPv6" root domain name server (system).

B. Root domain image server

The root domain name mirror server is divided into two types: Global and Local. Two or more servers with identical online content and synchronized updates are all mirror servers except the host server.

Mirror servers are also called "Instances" in the industry. Instances are not interconnected and can be controlled or managed independently based on the Web or the command line.

In the node list of each root domain name server, some instances are marked as "Whole Network", while others are marked as "local". The instance mark indicates the application range of the image server. The application range of the image server is determined and limited by the routing method of the instance (the Border Gateway Routing Protocol BGP of the autonomous system running on TCP).

The whole network instance allows routing announcements to be broadcast on the global Internet, that is, any router on the Internet can know the routing path to (link to) the instance. For a specific source, the established route of the instance may not be the best route, and other instances can be selected as the destination (via). All root domain name server operators must have at least one network wide instance to provide services for the global Internet [10].

For local instances, route advertisements are limited to connected networks. For example, the instance might be visible to only one network operator (ISP) or to an ISP connected at a particular switching point. Other (or remote) domain name resolution requests cannot be viewed and queried. Some root domain name server operators may also choose to deploy local instances according to their own and partner needs.

The mirror server is a server that shares the load of the host. It synchronously maps the data information passing through the host server like a mirror. It can be seen, but it may not be "retained" or complete. Because the mapping of the mirror server is subject to the mirrored host, what the host has can be mirrored, and no change, change or modification is possible or allowed.

It must be noted that the "anycast node" of DNS cannot be considered or used as the "mirror point" of the domain name; hosting an anycast node is conditional, and related parties must sign a confidentiality agreement (NDA).

C. Root domain name server control

The national telecommunications and Information Administration (NTIA), established in 1978 under the Department of Commerce, is an administrative department of the federal government. NTIA's plans and decisions mainly focus on expanding broadband Internet access and adoption in the United States, promoting the use of spectrum for all users, and ensuring that the Internet continues to be an engine of continuous innovation and economic growth.

The "cooperation agreement with Veritas" published on NTIA website states that Veritas manages the authorized root zone documents in accordance with the cooperation agreement No. NCR 92-18742 signed with the U.S. government. Verizon's responsibilities include: editing the root zone file according to the suggested changes, publishing the file, and then distributing the file (through the a root domain name server) to other root domain name server operators. From this point of view, the status and role of root a domain name server [11] in the 13 root domain name

servers is equivalent to the parent root, or the "Female-child root" integrated into one.

Root A has been managed by Verizon for decades under the strong protection of the U.S. government and military. One of the main functions is to distribute and push authoritative updates of top-level domain names to other 12 secondary root domain name server systems every 24 hours to ensure the consistency and uniqueness of the real-time operation of global DNS domain name resolution. Any root set up by countries around the world (including China) according to the Internet layout (including all root domain name mirror servers around the world) must and can only follow root A for real-time synchronous update, coordination and domination, that is, subject to root A. Otherwise, the operation of the whole network (including China's local Internet) may be seriously disrupted, or even a large area of congestion, block and interruption may occur, and the normal service cannot (or cannot) be provided.

Based on the "cooperation agreement" between NTIA and Veritas, from october1, 1998 to october26, 2018, NTIA and Veritas signed 26 public amendment and supplementary agreements. According to the 2015 financial report submitted by Verizon to the Securities and Exchange Commission (SEC), it clearly states:

1) DNS is supervised by the Department of Commerce on behalf of the U.S. government. According to the letter of commitment (AOC) signed by the Ministry of Commerce and ICANN, which took effect on October 1st, 2009, the Ministry of commerce is one of the subjects of continuous review and accountability of ICANN's performance [12].

2) The role of ICANN is to serve as the coordination core among multi stakeholders. The above-mentioned letter of commitment is not binding on ICANN.

3) The role of the U.S. government is to coordinate the management of important aspects of DNS through NTIA, including the functions of the Internet digital distribution authority (IANA) and the DNS Management of the root domain name zone.

The key point is that all the above root domain names (regardless of the parent root, Taproot and secondary root), root domain name system (host and image distribution, establishment and operation control system), IPv4 and IPv6 protocols are the network terms, proprietary functions and specific elements of the Internet developed by the United States. The Network sovereignty of the Internet, including naming right, jurisdiction, design and planning right, rule determination right, operation dominant right, routing dominant right, data control right, as well as the distribution and lease right of domain name address, the distribution and coordination right of root domain name mirror server node, etc., can only be decided by the United States. Any country (including China, Japan, European countries, etc.) and organization (including the United Nations, ISO/IEC, ITU, etc.) outside the United States does not count.

Female root refers to the source root of the whole Internet. The U.S. military network evolved and reconstructed from ARPANET is the core network, origin network, network in network and leading network (main network) of the Internet. The "Female root" should be hidden in the "main network" that the U.S. military absolutely controls and provides a high degree of security.

Taproot is the direct root and the direct root of the Internet. Root A is considered to be the Taproot among the 13 Internet roots, and the Female 12 roots are Auxiliary roots. For example, root M in Japan is the Auxiliary root.

The U.S. government has carefully planned and constructed the jurisdiction (legal system) and control (governance mechanism) over the Female root, Taproot and the Auxiliary root of the root domain name, which can not be disobeyed and changed by any other countries, organizations and individuals.

IV. WHERE IS DNS GOING

A. DNS Security Extension

With the increasingly prominent security problems and risks of domain name resolution system DNS, IETF has continuously issued a set of standards and specifications "Domain Name System DNS Security Extension" (DNSSEC) since 2005.

At 0:00 on October 12th, 2018 (Beijing time), ICANN implemented the domain name root zone key reversal (KSK, key signing key) on the global Internet, replacing the single trust root used to verify the consistency of DNSSEC response, which is the first time in the history of the Internet.

But so far, the application of DNSSEC is far lower than expected. Among them, the technical reasons include: the digital signature of DNSSEC increases the number of bytes of DNS resolution response packets, making most DNS resolution response packets remain under the UDP transmission limit of 512 bytes, which is becoming more and more challenging. At the same time, in order to keep the DNS specification unchanged, packets with more than 512 bytes can be truncated and switched to TCP to obtain domain name resolution responses with more than 512 bytes, potentially reducing the efficiency of DNS (and increasing the delay and fragmentation of packets).

Therefore, in reality, the deployment and application of DNSSEC are "layered and segmented". For example, DNSSEC is adopted for the domain name resolution service of root domain name and top-level domain name, while DNSSEC is basically not adopted for the domain name resolution service of authoritative domain name, recursive domain name server and user terminal.

Geoff Huston, chief scientist of APNIC [13], believes that the current status shows that DNSSEC is one of the typical cases of application failure.

According to the measurement statistics of APNIC, as of May 6th, 2022, the average verification rate of DNSSEC in the world is 29.91%, of which (As shown in Table 4):

TABLE IV. AVERAGE VALIDATION RATE OF DNSSEC IN THE WORLD

Country(and Region)	DNSSEC Average validation rate
India	59.60%
Russia	52.23%
America	38.78%
China(mainland)	0.93%
(Hong Kong)	57.25%
(Taiwan)	6.41%
(Macao)	5.23%

The interoperability of IPv6 and IPv4 technologies ("mutual incompatibility") is one of the key foundations and fundamental cruxes of Internet security issues. Although both belong to the Internet Protocol (different versions) and are controlled and operated by 13 root domain name server systems that also use and rely on the Internet, there are still a large number of potential instability factors and unknown security risks that cannot be predicted and prevented, Necessary and necessary practical (parallel) operation experiments and verifications must be carried out to explore possible solutions, which requires incalculable economic costs and security costs, or the gains outweigh the losses.

B. Yeti DNS Project

In June 2015, ICANN launched the "Yeti DNS Project" proposed by American expert Paul Vixie and the Japan WIDE organization (Japanese translation “雪だるまプラン”,Translated into English as "Yeti DNS project")

The "Yeti DNS Project" is an experimental project for parallel testing of IPv4 and IPv6 domain names. ICANN uses the "Yeti DNS" DNSSEC key to test all restart and Reset settings in the M root domain. It does not provide a substitute domain name space, but only changes (adds) the delegation information of the M root domain name system resolution.

American professionals acknowledge that this preliminary technical test project, which is temporary and allowed to fail in the test environment, is neither the experiment of "technical prototype", nor the deployment of root domain name server system in the production environment, nor the "new pattern of IPv6 root domain name server hypothesis", and has been completed at the end of December 2017.

American professionals clearly pointed out that the tests and experiments of the "Yeti DNS Project" have proved that:

1) The "Taproot root server" of IPv6 is not a truly independent Taproot server, but a testing server under the Taproot root server of IPv4. Technically, the status of the 25 new IPv6 root servers in the "Yeti DNS Project" is actually lower than that of the 13 IPv4 root servers.

2) The so-called IPv6 "Taproot root server" in China is controlled and monitored by the IPv4 Taproot root server and f root server in the United States. "The root server of IPv4 still has the right to interpret the root server of IPv6." "Even if China has a root server for IPv6 in the future, it does not mean that China can play a leading role."

3) The security performance of IPv6 is inferior to that of IPv4. IPv4 addresses can be dynamically allocated, and each IPv6 website has only a certain static address, which is easy to be accurately located and attacked. Therefore, the U.S. government and the U.S. military do not use IPv6, and deliberately push China to spend a lot of human, material and financial resources to build a pilot IPv6 system.

4) The "Yeti DNS Project" does not attempt to "bifurcate the domain name space". All tests are based on the expansion under the IPv4 architecture, rather than "starting a new business" to re-establish a new domain name management system and root domain name server. In other words, whether IPv4 or IPv6, the global Internet's total hub, data exchange center, backbone network, Taproot root server and Web master station are still in the United States, which are built, controlled and managed by American enterprises. IPv6 and the "Yeti DNS Project" have not solved China's Internet security problems at all.

In short, the United States has full sovereignty over both IPv4 and IPv6 domain name space. The US government, US politicians and US politics do not allow any country, any organization or any individual to change or shake the US "one net dominating the world", which has become a well-known Internet common sense, scientific common sense and political common sense all over the world.

C. Development of DNS related technologies

1) Since January this year, ICANN has widely publicized a revised action measure: "Knowledge-Sharing and Instantiating Norms for DNS and Naming Security", referred to as "KINDNS".

On March 10th, at the 73rd annual video conference of ICANN (ICANN 73) [14], the Middle East representative of AFRINIC, the management organization of Africa, issued a "statement" on "digital signature and verification of DNSSEC":

It is emphasized that DNS is crucial to ensure the continuity of network services. Defective or invalid DNS services will have a negative impact on the experience of any institution and organization (including customers, partners or employees), affect e-commerce applications, cause loss of revenue and damage the brand image. It is disclosed that 63% of institutions and organizations will be offline and out of service due to DNS attacks in 2021; It is recommended to clarify the "return on investment" (ROI) in DNSSEC deployment and application and the "risk loss rate" (ROR) for delayed deployment and application of DNSSEC.

On May 19th, ICANN made an official reply, acknowledging that the importance of DNS Security operation to the overall stability and flexibility of the Internet was recognized, which is the core of ICANN's mission; Indicates that the series of recommendations put forward in the statement are consistent with ICANN's "five year strategic plan" and "five year plan for the Middle East and surrounding countries and regions", that is, they are related to ICANN's regional objectives; Define the regional objectives of ICANN, including:

—Through cooperation and support with multi stakeholders, to develop technical capacity and establish a regional network of technical experts;

—Identify and mitigate the security threats DNS faces by participating in the work of multiple stakeholders.

"Multi stakeholder", in fact, is to build a new "threshold" of exclusive competition through the cooperation between the government and private enterprises, and take their own interests or vested interests. One of the "principles" put forward in the "Declaration on the future of the Internet" signed and issued by the United States with the EU, more than 50 countries and Taiwan on April 28, namely "protecting and strengthening multi stakeholder governance methods".

2) The technology and services of DNS are undergoing fundamental changes, not only in the underlying protocols (and key technologies), but also in the alliance of governance models and the strengthening of management means.

The "QUIC" protocol [15], a new generation of network data transmission protocol based on the "UDP" protocol, is known as a subversive innovation comparable to the "TCP" protocol.

On May 11, IETF released the updated version RFC 9250 in the standardization process of "DNS based on private QUIC connection"; On May 20, IETF updated the second version of the standardization process based on the "UDP" protocol.

D. Attention tips

1) The global Internet digital resources allocated and managed by ICANN mainly include: top-level domain name, IP address and ASN autonomous system number. Although the average verification rate of global DNSSEC (29.91%) is close to the average application rate of IPv6 (31.22%), ICANN builds and promotes "DNS" (KINDNS framework) and does not try to build a global IPv6 application ecosystem. Is it consciously "favoring one over the other"?!

2) The non mandatory technical standards for DNS are formulated by IETF, but the digital resources of DNS (such as top-level domain name

authorization and port allocation) are managed by ICANN (and IANA). ICANN has built a "KINDNS framework" for the research and development of IETF standards and related technologies, building (seizing) a "first mover advantage" platform for the global Internet.

3) Although ICANN is still maintaining DNSSEC, when QUIC based DNS (DOQ) becomes the standard, it may replace DNSSEC. In other words, DNSSEC is only a transitional or "dead meat meal".

Combing the domain name system DNS, an intuitive and simple evolution is that DNS has already become the "hub" (command and control system) and "commanding point" (navigation system for positioning and redirection) of the Internet from its initial idea as the Internet "phone book" (file system).

E. Epilogue

DNS Security is not limited to "vulnerability" or "harassment", but has a clear strategic and systematic nature, and has become one of the focuses of unprecedented struggle and competition, that is, "whoever controls DNS will own the Internet" [16].

The Internet is man-made. It is the creative result of human collective wisdom. It is a systematic innovation that carries forward the past and advances with the times with the continuous sublimation of human knowledge, culture, science and technology. Especially in the evolution and development of DNS domain name system and its security technology, there is no shortcut, no "one move to beat the world" and no "eternal" technical know-how once and for all.

DNS is the key foundation and foundation of the Internet. The innovation of DNS domain name system is not only a technical programming based on experience, but also an ecosystem project, including dynamic supply chain and potential political, economic, diplomatic and military strategies and strategies.

Complete the manuscript May 24, 2022.

REFERENCES

[1] Huning. dengwenping. Yaosu Research status and challenges of Internet DNS Security [J] Journal of network and information security, 2017, 3 (03): 13-21.

[2] Miaochen. Analysis and Research on Internet DNS traffic [D] Beijing University of Posts and telecommunications, 2013.

[3] Salnikov, Andrii, Kónya, Balázs. DNS-embedded service endpoint registry for distributed e-Infrastructures [J]. Cluster Computing, 2021 (prepublish).

[4] Xie Chongfeng. Viewing the development trend of IPv6 from IETF dynamics [J] ICT and policy, 2020, (08): 12-17.

[5] Kouwenjun. Research on IPv6 domain name system [J] Scientific consulting (Science and technology. Management), 2016 (03): 42-44.

[6] Liuqing. Security issues of Internet domain name system in China [J] Modern telecommunication technology, 2010, 40 (04): 9-11+17.

[7] Liyanxing. Research on DNS Security Extension and scalable distributed DNS [D] University of Electronic Science and technology, 2021,Doi:10.27005/d.cnki gdzku 2021. 002068.

[8] Zhangwenjia. Research on Key Technologies of DNS root zone resolution self verification [D] Harbin Institute of technology, 2019, Doi:10.27061/d.cnki ghgdu 2019.000952.

[9] Chenghongbo. Research and deployment of DNSSEC security mechanism [D] Shanghai Jiaotong University, 2006.

[10] Luodexiang. Research on attack and defense technology of some Internet security protocols [D] Shanghai Jiaotong University, 2007.

[11] Lei He, Quan Ren, Bolin Ma, Weili Zhang,Jiangxing Wu.Anti-Attacking Modeling and Analysis of Cyberspace Mimic DNS [J]. China Communications, 2022, 19(05):218-230.

[12] Dengchengjun, LiuYing. Implementation of DNS service in next generation Internet [J] Journal of Chongqing Electric Power College, 2021, 26 (02): 35-37+48.

[13] Jiazhuosheng. Research on active defense architecture and key technologies based on domain name service log analysis [D] Beijing Jiaotong University, 2021, Doi:10.26944/d.cnki.gbfju.2021.000328.

[14] Chang Deliang, Hao Shanshan, Li Zhou, Liu Baojun, Li Xing. DNSWeight: Quantifying Country-Wise Importance of Domain Name System [J]. IEEE ACCESS, 2021, 9.

[15] ChenBo. Analysis on security protection technology of DNS [J] Electronic technology, 2020,49 (06): 80-81.

[16] Zhangjichuan. Research on enterprise DNS Security Scheme Based on blockchain technology [D] Harbin Institute of technology, 2020,Doi:10.27061/d.cnki ghgdu 2020.002902.