A RED BUTTON FOR THE INTERNET

ANDREI KOLESNIKOV,
DIRECTOR
AT INTERNET-OF-THINGS
ASSOCIATION, IN 2009-2015 –
DIRECTOR OF THE COORDINATION
CENTER FOR TLD RU.

The original version of the article in Russian is published in Security Index Journal 2015 Winter №4.

“TELECOMMUNICATIONS and the Internet are critical instruments of state governance, the foundation of a strong economy, and an invaluable inter-personal communication tool. The importance of the Internet is hard to overestimate.” This mantra, or something like it, is how Russia’s Internet-related bureaucrats and officials like to open their speeches these days. This article endeavors to provide a simple explanation of complex elements of the Internet’s critical infrastructure, and to describe the technical and organizational measures required to reduce the level of threat facing the underlying infrastructure of the Internet.

THE DAY THE GOVERNMENT NOTICED CRITICAL INTERNET INFRASTRUCTURE

The first serious discussion of critical Internet infrastructure at the level of Russian decision-makers took place in early 2009. It was chaired by Deputy Communications Minister A. Soldatov. Some time earlier, the Russian Security Council also took notice of the growing impact of the Internet on national security. A. Soldatov, A. Platonov[1], the present author (in his capacity as head of the Coordination Center of the Russian National Internet Domain), and several other experts[2] were instructed to compile a list of critical Internet infrastructure elements. Of the many initial candidates, we shortlisted only three: the DNS servers, which receive billions of requests every day; the physical channels; and IP network routing. These are the three pillars of the Internet ecosystem, which is based on trust[3]. The word exercise was also used for the first time in reference to the Internet in 2009.

Back at the time, there was no clear understanding in Russia of how critical Internet infrastructure functions. This is clearly illustrated by the phrasing of various official documents describing various threats to that infrastructure in the 2000s. For example, the 2000 version of the Russian Information Security Doctrine[4] has a single paragraph dealing with the kind of infrastructure that fits the definition of the Internet: “[there are] threats to the security of information and telecommunication instruments and systems, including the existing ones and the ones that are now being built in Russia”. The description of these threats contains a single item that has relevance for proven threats to the security of critical Internet infrastructure: “destruction, damage, or radio-electronic suppression of information processing, telecommunication, and communication instruments and systems”. The list includes several other items, such as “impact on password and key security systems of automated information processing and transmission systems, compromising keys and cryptographic information protection instruments"; "insertion of electronic devices for intercepting information into technical information processing, storage and transmission systems"; "interception of information in data transmission networks and communication channels, decryption of that information, and insertion of false information"; or even "the use of uncertified Russian and foreign information technologies, information protection instruments, and informatization, telecommunication and communication systems in projects to build and improve Russian information infrastructure". None of these threats, however, have ever been confirmed in known cases of disruption affecting the IP address, routing, or physical infrastructure of the Internet in Russia or other countries".

As the same time, some of the definitions contained in the doctrine describe other types of attacks directed against some specific tasks rather than the address infrastructure or routing systems in general. These include, for example, the Man in the Middle (MITM) type of attack[5] , which uses fake security certificates exchanged between the user and the Internet server, making it possible to intercept the information. Replacing a website's genuine security certificate with a fake one is a fairly widespread type of attack in China. Nevertheless, such attacks cannot disrupt the work of the entire network.

Over the past 15 years, the general architecture of the Internet infrastructure has remained unchanged. The same will probably be true a few years down the line – say, in 2020. Nevertheless, the complexity of the Internet and the number of its various branches will continue to grow as the Internet itself plays an increasingly important role in our lives. That is probably why all the official statements begin with the same mantra.

DISCONNECT FROM THE INSIDE OR FROM THE OUTSIDE?

The first Russian exercise to simulate infrastructural threats to the normal functioning of the Internet took place in late July 2014 in accordance with an instruction by the Security Council to the Communications Ministry. It triggered angry exchanges in the media and social networks between the users fearing that Russia was trying to disconnect itself from the World Wide Web, and knowledgeable specialists who argued that simulating external or internal threats is normal practice for any responsible government or business[7].

It is hard to argue that proper planning, responsible management of critical infrastructure elements, and detailed procedures for coordinated action by all the relevant parties that will deal with such threats should they materialize are a genuine necessity – regardless of whether the disruption is caused by internal or external factors.

It is not strictly necessary to know what exactly has caused a crisis in order to simulate threats and to develop methods for rapid recovery. Two critical infrastructure elements - the generator of the primary DNS zone file[8] uploaded to DNS root servers and the Internet Routing Registry (IRR) - are physically located in the United States (ICANN) and the Netherlands (RIPE), respectively. This fact leaves some commenters worried about the political risks. But apart from political conflicts, there is also the small but discernable possibility of catastrophic physical damage to the infrastructure resulting from, say, flooding, earthquake, or an asteroid strike.

To build a simulated model of such threats and to develop methods for risk reduction, it would be useful to take a closer look at the critical Internet elements and to create threat reduction models.

DNS ROOT SERVERS[9]

The domain name system is built to a strict hierarchical principle.

Every node on the Internet has its own unique IP address, such as 194.67.1.14. Memorizing these strings of numbers is not easy[10]. That is why network-connected computers, nodes, and Internet resources are assigned names that are easy to

TABLE 1

Host name	IP address	Administered by
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	192.228.79.201, 2001:500:84::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4	US Department of Defense (NIC)
h.root-servers.net	128.63.2.53, 2001:500:1::803f:235	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:3::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

remember. The DNS naming system matches a domain name to an IP address of the required resource, and also performs some other Internet address functions.

A top-level domain, such as Russia's national domain .RU, works under the rules and procedures defined by the Russian national registry called Coordination Center of the National Internet Domain. The .GAME domain belongs to a company called Uniregistry. The .ORG domain is managed by a company called Public Internet Registry, etc. There are more than a thousand top-level domains at this time, including about 250 owned by nation states. The national top-level domains are called ccTLD (country code Top Level Domain). The top-level domains reserved for general use are called gTLD (generic Top Level Domain).

Lower-level domains are managed by their owners. For example, the Russian company Yandex manages the YANDEX.RU domain (second level) and two third-level domains, MAPS.YANDEX.RU and MARKET.YANDEX.RU. The number of levels in such domains is unlimited.

When an Internet resource is requested by its domain name, the connected device sends a query to the DNS system to find out what IP address corresponds to that domain name. DNS is a very dynamic structure. The IP addresses change all the time, but the domain name of a resource stays the same.

DNS servers process billions of requests every day. They are a complex system of servers, routers, and physical channels working under a very high load. To make sure that a request for an IP address is answered as quickly as possible, certain functions of a DNS server a built into smartphones, PCs and other user devices.

In a simplified form, the architecture of the DNS system is as follows:

The top level of the hierarchy is called the root domain. It has no formal name, it is usually denoted by a dot (.) The root domain is managed by ICANN Corporation as part of its IANA function. It contains information about all top-level domains. Information about top-level domains is stored by 13 DNS root servers. This information is constantly updated using the root zone file.

.RU is the Russian top-level domain. The record with information about the Russian DNS servers is stored on the root DNS servers in the root zone file. Changes in that record are entered as part of the IANA function at the request of the Coordination Center of the National Internet Domain.

TABLE 2

Host name	IP address
e.dns.ripn.net	193.232.142.17 2001:678:15:0:193:232:142:17
f.dns.ripn.net	193.232.156.17 2001:678:14:0:193:232:156:17
d.dns.ripn.net	194.190.124.17 2001:678:18:0:194:190:124:17
b.dns.ripn.net	194.85.252.62 2001:678:16:0:194:85:252:62
a.dns.ripn.net	193.232.128.6 2001:678:17:0:193:232:128:6

YANDEX.RU is a second-level domain. The table with information about the Yandex DNS servers is stored on RIPN servers[11]. Changes to the record on the RIPN servers are entered by accredited registrars. The registrars are Russian legal entities that hold accreditation with the Coordination Center for registering domains in the .RU zone and in the Cyrillic Russian .РФ zone. Information about all second-level domains in the .RU domain is stored in the .RU zone file.

The table below lists all 13 DNS root servers that underpin the top level domain name system. These servers respond to queries such as “what is the address of the server that maintains functionality of the .RU domain?” (Table 1).

In addition to these 13 servers, there are more than 200 mirrors of the DNS servers all around the world. They ensure quick response to user DNS requests and resilience of the root server network in various regions. The mirror servers are an exact copy of one of the 13 root servers. Russia hosts seven mirrors that serve users in the Russian segment of the Internet: Copies J, F and L in Moscow, K and I in St Petersburg, L in Yekaterinburg, and K in Novosibirsk. When they receive a request such as “what is the address for information about domains in the .RU zone?”, the root server or one of its mirrors will respond the following (Table 2).

So, once it is known what IP address serves the .RU domain, a client’s request for an IP address of the Yandex.ru server will be resolved by RIPN.NET domain name servers that a physically located at the facilities of the MSK-IX Computer Networks Liaison Center[12]. This is, of course, a very simplified description because the vast majority of DNS requests from clients never go beyond the cache server[13] of the local Internet service provider (ISP).

THREATS TO THE DNS SYSTEM

The root zone file contains information about all the root domains. Let us assume that for some reason, the uploaded file contains an error in the address of the RIPN.NET servers, or has no record at all about the servers of the .RU root domain. Even with a super-resilient DNS infrastructure, we cannot completely rule out an error during the uploading of the unique root zone file to all 13 root servers. The zone file is uploaded automatically, following a pre-defined schedule, or whenever changes are made in the record on top-level domains (.RU, .COM, .NET, etc) by the corresponding registrars[14] after a multi-layer verification by operators of the IANA function[15] at the ICANN Corporation[16].

The correctness of the records in the root zone file is constantly controlled by at least one Russian operator, the already mentioned MSK-IX. The control method is very simple: the operator compares the contents of the new version of the root zone file versus the old version. If unauthorized changes have been made in the record about the .RU and .РФ national domains, then the operator on duty (and they work 24x7, 365 days a year) immediately receives a notification. Additionally, the system monitors the extent of the changes in records about root domains. This is because changes to the root zone file are made infrequently, and above a certain threshold the system automatically generates a notification. A similar method of verifying the validity of the uploaded zone file is also used to monitor the changes made in the records about second-level domains in the two Russian top-level domains. For example, if the extent of the changes made in the .RU zone file received from one of the accredited registrars is above a certain threshold, the zone file is not updated, and the operator on duty receives a notification to that effect.

Hypothetically, if an unauthorized change is made in the record about a top-level domain, this change is promulgated very quickly across all 13 root servers and their mirrors. To reduce that risk, the DNS system uses a fallback method that relies on a duplicate root server containing the correct record about the Russian top-level domains. The effectiveness of that method completely depends on how effectively the key Russian Internet operators can coordinate their action. If the correct record is not quickly restored on the root servers, all the DNS requests of "Where is the information about domains in .RU?" sent by all the users in Russian territory should be routed to the duplicate fallback server. This can be done by analyzing DNS traffic in operators' networks and substituting the IP addresses of the genuine root servers with the IP address of the duplicate server. This should be done as quickly as possible to that the information contained on the cache servers of ISPs can be quickly updated as well.

MSK-IX has been running a duplicate fallback root server for several years. In the event of emergency with a corrupt or missing DNS root zone file, hundreds of such duplicate DNS servers will probably kick in all around the world and serve most of the DNS requests from users in the affected zone.

Threat of routing disruption or loss of connectivity

The second threat that is somewhat more difficult to minimize is the disruption of the routing function in the Russian or global segment of the Internet. Let me emphasize the most important aspect from which this particular threat arises. Routing in the Internet is done by the Internet players themselves; there is no equivalent of a central regulator distributing the radio frequency spectrum, for example. Blocks of IP addresses are issued to operators and providers by the regional registrars, of which there are only five:

- *The American Registry for Internet Numbers (ARIN)* – North America
- *RIPE Network Coordination Centre (RIPE NCC)* — Europe, Middle East, and Central Asia
- *Asia-Pacific Network Information Centre (APNIC)* — Asia-Pacific
- *Latin American and Caribbean Internet Addresses Registry (LACNIC)* — Latin America and the Caribbean
- *African Network Information Centre (AfriNIC) — Africa*

The IP address blocks for Russia are issued by RIPE NCC, a not-for-profit organization based in the Netherlands. Providers and operators submit their own requests to RIPE to receive IPv4 and IPv6 address blocks. The registrar has no influence whatsoever on the routing policies of network operators and ISPs. So let me reiterate: network operators and ISPs all over the world make up their routing policies on their own, so, for example, the parameters of the transmission of Internet traffic between Operator A and Operator B are determined by these two operators themselves. Globally, Internet routing is a conglomerate of various policies established by the participants in Internet relations, who merely announce these policies to the outside world as a fait accompli. The situation is compounded by constant changes in the routing landscape, because the routing tables are constantly modified by network operators and providers as they make changes to their networks. These changes are recorded in the Internet Routing Registry (IRR), which is run by RIPE NCC[17]. This is a reference database used by all the operators and providers for drawing up their own routing policies and for other purposes.

There are two routing-related threats. The first is the so-called dynamic routing protocol hack (BGP[18] hijack). A typical example of that hack was the case of Pakistan vs. You Tube[19]. On February 22, 2008, the Pakistani telecommunications regulator ordered 70 ISPs to block access to YouTube in Pakistani territory. The method used to comply with that order was this: Pakistan Telecom, posing as the closest network neighbor[20] of YouTube, announced a new route to the YouTube network to its other network neighbors (that is, to other ISPs). As a result, from the Pakistani ISP's point of view, the entire YouTube network was sent into a black hole[21]. By mistake, Pakistan Telecom also announced that route to nowhere to its external network neighbor PCCW Ltd, a Hong Kong operator. PCCW, being one of the world's largest infrastructure providers, did not verify that announcement and passed it on to its international peers[22]. As a result, two-thirds of the global users (mostly in Asia Pacific) lost access to YouTube. The problem was quickly discovered; the situation was analyzed by Renesys (which has since become Dyn), which monitors Internet routing on a constant and professional basis. Network engineers consider this a rookie error – but it happens from time to time. In most cases there is no malicious intent, but deliberate attempts at traffic intercept cannot be ruled out, either[23]. A BGP hijack can be used to route traffic from the resource being targeted to the attacker's own network and analyze the contents of that traffic. This is serious threat – but it does not actually cause a loss of connectivity in critical Internet infrastructure.

The second threat - deletion of information about routes in the IRR database - is far more dangerous. The deletion does not get promulgated very quickly – but as providers and operators update their routing tables, the network deleted from the IRR database becomes unavailable to other networks. This is a direct threat to the Internet infrastructure.

Rookie errors or malicious routing intercepts using BGP hijacks are usually quickly discovered by engineers. For ordinary users, such anomalies can slow down data transfer speeds or, as in the Pakistan vs. YouTube case, make an individual Internet resource unavailable. Detecting incorrect BGP announcements in real time or verifying the correctness of IRR data is not an easy task. First, it requires access to the entire list of all the Autonomous Systems (AS) in the Russian segment. These are thousands of records of telecommunication providers, ISPs, hosting and infrastructure companies, major Internet companies such as Yandex.ru, Mail.ru, and Google, banks, etc. Second, most of the Internet players do not keep a watchful eye on the accuracy of routing information in the IRR database; they have no real need to do so because the correctness of the route is based on a chain of trust between all the participants. Third, to monitor the correctness of routing information, one would need to install test probes (small and cheap software/hardware systems) in all the major networks to conduct regular scheduled routing tests in the network being monitored. These probes must then transmit the information they have gathered to a central server that compares the previous route with the new one and makes conclusions about the correctness of the route. Building a system of route monitoring is a complex task; as of today, it has been accomplished by RIPE NCC and Dyn (the former Renesys). There is also a Russian company called Qrator Labs that monitors routes and network announcements.

To defeat BGP hijacks, operators isolate the network that announces an invalid route. They then get in touch with whoever runs that network and inform them of the problem. There is no centralized mechanism of coordination between all the networks of every operator on the Internet because the Internet itself is completely decentralized.

Deletion of data about network routes from the IRR routing database is a more serious threat. At this time, we are aware only of unintentional incidents of that kind, when network operators accidentally deleted their own routing data. There are no registered cases of malicious action against the IRR public routing database maintained by RIPE NCC.

One of the ways of reducing the threat of the deletion of data from the IRR routing database is to keep an exact copy of that database as a fallback for Russian network and infrastructure operators. This method is similar to the use of duplicate DNS root servers. It has already been partially implemented, but to the best of our knowledge, an integrated system of monitoring routing data in the Russian segment does not exist.

Threats to the Physical Infrastructure

The most effective way of bringing down the Internet is to disconnect the physical data channels used by ISPs. There is no point analyzing the model where an operator's network or a critical node of the Internet has only a single physical channel that connects it with the outside world. Such architecture is completely unacceptable for any critical infrastructure or resource operator.

It is quite easy to establish any individual country's ranking in terms of its resilience to physical loss of connectivity. As a rule of thumb, the more independent channels connect the country to the outside world, the better. Meanwhile, a large and extensive internal network architecture underpins resilience within the country. So, the general principle is, the more operators and the more complex the system of interconnections between them, the better[24]. Of course, a complex architecture is more expensive to operate. But in a model where each Internet player manages its own network, the costs are distributed in proportion to the size of each individual network. Russia is one of the world leaders in terms of the resilience of its Internet infrastructure. There are worries, however, that its traditional approach to security might lead to creating a smaller number of larger players through merger, and to stricter controls. Centralization and stricter controls may actually make matters worse for the Russian segment of the Internet. Logic dictates that a distributed system with an extensive network of interconnections is more difficult to break than a single large operator that channels the entire traffic[25].

The remedy for the threat of a physical loss of connectivity is to have numerous interconnection points and a large choice of routes for the data to travel, careful planning of network architecture, and reliable communication between the operators at times of crisis.

DDoS Attacks

A DDoS attack is the most barbaric method of disrupting the operation of the Internet infrastructure and Internet resources. It can cause serious damage to every website without exception, to financial organizations and government agencies, hosting providers, and cloud services. DDoS attacks can also target DNS servers, which then fail to respond to users' requests. The principle behind the DDoS attack has been described in great detail. Essentially, the perpetrator sends a request to a publicly open Internet service[26] hosted by a powerful platform. The request sent by a computer controlled by the perpetrator to an open DNS server or an NTP time server[27] contains the IP address to which the server should send the response. The size of a DNS or time request in bytes is very small, whereas the size of the response is much greater. This is why if the attacker controls thousands of infected computers that operate as part of a botnet, several open servers can flood with their responses a big chunk of the Internet infrastructure targeted by the attacker. This is the so-called amplification method.

A powerful attack by a large botnet immediately becomes visible to many other parties. The attack disrupts the work of the resource being targeted. It also disrupts the work of the backbone channels and traffic exchange points. As a first response, an operator can suspend routing from the direction of the attack. Then comes the time to analyze the situation and identify the source of the attack. This requires close coordination with the network neighbors. Currently, all the major Russian operators have mechanisms to control DDoS traffic. Many of them use traffic scrubbing, and there are now high-quality anti-DDoS products and services available on the market[28].

Table 3 summarizes the information about the three main threats to Russia's critical Internet infrastructure.

As more instruments become available to monitor critical elements of the Internet infrastructure, operators gradually install systems to monitor their own

TABLE 3

Threat	Potential for disruption	Remedy	Coordination required
Deletion of the .RU domain record from the DNS root servers or isolation of root servers for Russian networks	Very high. With websites and infrastructure elements in the .RU domain becoming unreachable	Cloud infrastructure with duplicate root servers controlled by a Russian company	As close as possible, between all Internet players and the relevant government agencies. The addresses of the DNS root servers should be substituted with the address of the duplicate server hosted by national-level operators.
Disruption of routing of loss of connectivity – *BGP hijack*, routing hack	Low. Possibility of traffic analysis by the interloper.	Widespread use of systems to monitor routing in the Russian networks and constant monitoring by the operators to ensure that the routing tables are correct.	Minimal. Problem can be resolved by the operator of the hacked route.
Routing disruption or loss of connectivity – deletion of network record in the IRR routing database	High. The disruption occurs slowly but surely. Loss of access to networks, including Internet resources.	Monitoring of the routing records for Russian operators. Availability of a backup copy of the IRR database managed by a Russian operator.	As close as possible, between all Internet players and the relevant government agencies. If routing anomalies are detected, the backup Russian copy of the IRR database should kick in.
Threat to physical infrastructure	High. Instant loss of Internet connectivity for entire regions. For incidents inside the country, loss of connectivity for individual networks.	The more routes and channels, the better. Preplanned routing policies between the leading Russian operators.	As close as possible, between a significant number of players and the relevant agencies. Backup channels should kick in during incidents affecting physical infrastructure.
DDoS attack	Low to high	Deflecting the attack at the border routers[29]. Traffic scrubbing.	Medium. Close coordination with network neighbors through which DDoS traffic is flooding in.

critical components. At the same time, preparedness for major crises also requires careful planning of response scenarios and regular training events to put those plans into practice. These efforts should involve numerous Internet players that underpin the functioning of critical infrastructure, especially telecommunication operators and providers of the address and information infrastructure. The two most important elements of recovery from global incidents affecting the Internet infrastructure are careful planning of crisis scenarios and close coordination.

COORDINATION AS THE MAIN ELEMENT OF PROTECTING THE INFRASTRUCTURE

There are two coordination methods available. The first method is decentralized; it works as part of the informal communication between the personnel of telecommunication companies, providers, and Internet infrastructure operators. In the absence of any catastrophic incidents or malicious disconnections, this mechanism is fully up and running in Russia and other countries.

The second coordination method is required at times of crisis; it should be implemented at the national level because disruption of the national Internet infrastructure may be caused by some very serious problems that require government intervention. It is an obvious conclusion that coordination is the key element of protecting critical Internet infrastructure from various threats. Let us see what action the government is going to take in the coming months and years.

Several Russian crisis response centers are already up and running. One of them is RU-CERT, the oldest group of experts that coordinates responses to network threats in Russia and abroad. Another is the state-run GOV-CERT, which works as part of the FSB to protect government websites and other resources. There is also the GIB-CERT, run by GROUP-IP; it analyzes network incidents, hacks and other malicious acts on a professional basis. There is an incident response center at the telecoms regulator Roskomnadzor. All these centers maintain informal contacts with network operators, providers, hosting companies, and information resources. There are currently no laws or regulations on the methods of coordination between the various Internet actors during critical incidents. Neither is there any information about the procedures of such coordination. Nevertheless, the Russian Security Council has already ordered such procedures and regulations to be drawn up; this is the first and necessary step the government should take.

COVERT THREATS

Let us also review other threats to the Internet infrastructure that are often discussed, but have not actually been seen in real life for the time being.

Routing intercept and a complete shutdown of connectivity between networks. In theory, this can be achieved with the help of putative undocumented functions (back doors) in the backbone routers. If an attacker gains access to such back doors, it will be able to remotely shut down the Internet in an individual country. There are rumors (not backed by any facts) that such a shutdown has happened in Syria.

Back door in the RSA encryption algorithm. The RSA encryption standard is used in 99% of all the Internet-connected devices. Since the standard was developed in the United States, there are rumors that there is a back door in this algorithm that makes it possible to intercept and decrypt RSA-protected information. These rumors are persistent but not consistent with facts; there can be no back doors in the algorithm itself because it can be easily reproduced and verified. But there can be back doors in the software and hardware that relies on the RSA algorithm.

Submarines cutting off intercontinental fiber optic cables[30]. The article in The New York Times claiming that such an attempt has been undertaken was widely ridiculed because there are dozens and hundreds of cables crisscrossing the oceans, so damaging one of them cannot cause any major disruption even in individual countries, let alone globally.

Despite the variety of Internet traffic, the availability of numerous alternative routes, and dynamic routing, we must take into account threats to the basic IP and routing infrastructure, as well as the risk of physical disconnection, when building models of countering threats. The exact reasons that can cause a deep Internet crisis in an individual country are not particularly important for the specialists whose job it is to ensure a rapid and smooth recovery. Even a complete transfer of the IANA function from the U.S. jurisdiction to the global Internet community or to individual national governments will not guarantee a complete protection from an error in the DNS root zone file. Neither will new regulatory requirements aimed at improving the situation by leveraging the capacity of the autonomous systems of Russian operators and large Internet platforms provide a complete protection from deletions of network blocks from the IRR database. That database relies on voluntary reporting by Internet players about their routing arrangements. Protection of the infrastructure must be based on a deep understanding of the architecture and vulnerabilities, as well as detailed scenarios and well-practiced actions by the main Internet players in Russia.

What can be done if the Internet goes down in an entire town, province, or country? It is likely that mobile networks will have gone down as well by that point, and some of the landlines. Such a scenario would inevitably cause major disruption because various critical services (utilities, ambulance, etc) rely on mobile communications.

Ordinary users will simply have to wait for engineers to fix the problem. Meanwhile, engineers maintaining the physical channel infrastructure and routing specialists will certainly get in touch and work together to restore the affected infrastructure.

It is unfortunate that at the moment, there is no single telephone number one could call in the event of any threats to the Internet infrastructure. Of course, engineers will do whatever they can to restore the work of the Russian segment of the Internet. It appears that the need for setting up a single coordination center should be the main conclusion the Russian Security Council should reach after analyzing the results of the exercises held in 2014. Further crisis response scenarios should be developed on the premise that such a center will be set up.

REFERENCES

[1] A. Platonov, CEO of AO Internet Technical Center. Previously served as head of RIPN, which controlled the .RU domain servers – RIPN.NET

[2] M. Yakushev (ICANN) and D. Burkov (RU-CENTER, RIPE) also worked on this issue at various points. Valuable contributions to the work of the group were made by the Communication Ministry's I. Khimchenko and O. Chutov.

[3] Internet providers and operators who are not bound by contractual obligations allow traffic between third countries' users and resources to flow through their networks. This is a key rule that enables the Internet to function as a global system. The trust is based on Internet protocols.

[4] Russian Information Security Doctrine, September 9, 2000 http://www.scrf.gov.ru/security/information/document5 (Last accessed March 16, 2017)

[5] Main-in-the-Middle attack, Wikipedia https://ru.wikipedia.org/wiki/Атака_посредника (Last accessed March 16, 2017)

[6] Anastasiya Golitsina. Security Council to discuss Russia's disconnection from the global Internet, Vedomosti, September 19, 2014 http://www.vedomosti.ru/politics/articles/2014/09/19/suverennyj-internet (Last accessed March 16, 2017)

[7] Security Council to discuss Russia's disconnection from the global Internet, Kommersant, September 19, 2014 http://kommersant.ru/doc/2570278 (Last accessed March 16, 2017)

[8] DNS servers, Wikipedia https://ru.wikipedia.org/wiki/DNS-сервер (Last accessed March 16, 2017)

[9] Internet root serves http://www.root-servers.org (Last accessed March 16, 2017)

[10] Domain names currently also serve a marketing function. Attractive domain names are more valuable as part of the corporate brand.

[11] RIPN: English name of ROSNIIROS, Russian Institute of Public Networks

[12] In fact, RIPN.NET is not a separate physical server but a cloud that relies on the anycast protocol to ensure extremely rapid response from the nearest point of network presence. The same principle is used for root servers and national domain servers (.RU, .RS, .AZ and others), as well as domains for general use (.COM, .ORG, .MUSIC and others). The service availability indicator for RIPN.NET is 100%; there have been no interruptions of service in over 20 years.

[13] DNS cache server channels through itself all DNS requests from ISP clients. It contains an up-to-date table of correspondence between domain names and IP addresses in all domain zones, thereby ensuring a very quick response to user requests from the ISP's network.

[14] The administrator (registrar) of the .RU and .РФ national domains is ANO Coordination Center of the National Internet Domain.

[15] Internet assigned numbers authority https://www.iana.org/about (Last accessed March 16, 2017)

[16] Entering changes into records about root domains is part of the IANA function discharged by an ICANN division.

[17] FAQ: RIPE Database, RIPE NCC https://www.ripe.net/manage-ips-and-asns/db/faq (Last accessed March 16, 2017)

[18] Border Gateway Protocol, Wikipedia https://ru.wikipedia.org/wiki/Border_Gateway_Protocol (Last accessed March 16, 2017)

[19] *Peter Svensson, Pakistan causes YouTube outage for two-thirds of world, ABC news*

[20] *http://abcnews.go.com/Technology/story?id=4344105&page=1 (Last accessed March 16, 2017)*

[21] *Network neighbor: operator or provider with whom there is connection and traffic routing arrangement.*

[22] *In this context, a black hole is a widespread (and barbaric) method of IP address filtering.*

[23] *A peer is more or less the same thing as a network neighbor.*

[24] *Kim Zetter. Someone's Been Siphoning Data Through a Huge Security Hole in the Internet, Wired, May 12, 2013, http://www.wired.com/2013/12/bgp-hijacking-belarus-iceland (Last accessed March 16, 2017)*

[25] *Syria, Venezuela, Ukraine: Internet Under Fire, Dyn Guest Blog, February 26, 2014 http://research.dyn.com/2014/02/internetunderfire (Last accessed March 16, 2017)*

[26] *Maxim Tsurkov. Communication Ministry pledges not to allow another massive Internet disruption in Azerbaijan, Trend, November 20, 2015 http://www.trend.az/business/it/2459139.html (Last accessed March 16, 2017)*

[27] *DDoS attacks use open DNS servers or time servers.*

[28] *Network Time Protocol, Wikipedia https://ru.wikipedia.org/wiki/NTP (Last accessed March 16, 2017)*

[29] *For example, Qrator Labs http://qrator.net/ru. (Last accessed March 16, 2017) Rostelecom network uses the Arbor system and traffic scrubbing to protect its users.*

[30] *Border routers are installed on the border of an operator's or provider's network and connected either to an international provider or to a traffic exchange point.*

[31] *David E. Sanger, Eric Schmitt. Russian Ships Near Data Cables Are Too Close for U.S. Comfort, The New York Times, October 25, 2015 http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?_r=1 (Last accessed March 16, 2017)*