PIR CENTER LIBRARY

GLOBAL INTERNET GOVERNANCE AND CYBER SECURITY

AS VIEWED BY RUSSIAN EXPERTS

MOSCOW 2017

GLOBAL INTERNET GOVERNANCE AND CYBER SECURITY: AS VIEWED BY RUSSIAN EXPERTS

Collection of articles

Editors: Albert Zulkharneev, Yuliya Tseshkovskaya

Translation: Ivan Khokhotva

Design: Tatyana Rogovich

Cover illustration created by Starline - Freepik.com

Link to the collection of articles: articles.net.eng.pircenter.org

Publisher: PIR Press LLC, 123242 Moscow, Druzhinnikovskaya str. 30 bld. 1

The translation was done with support of Internet Corporation for Assigned Names and Numbers

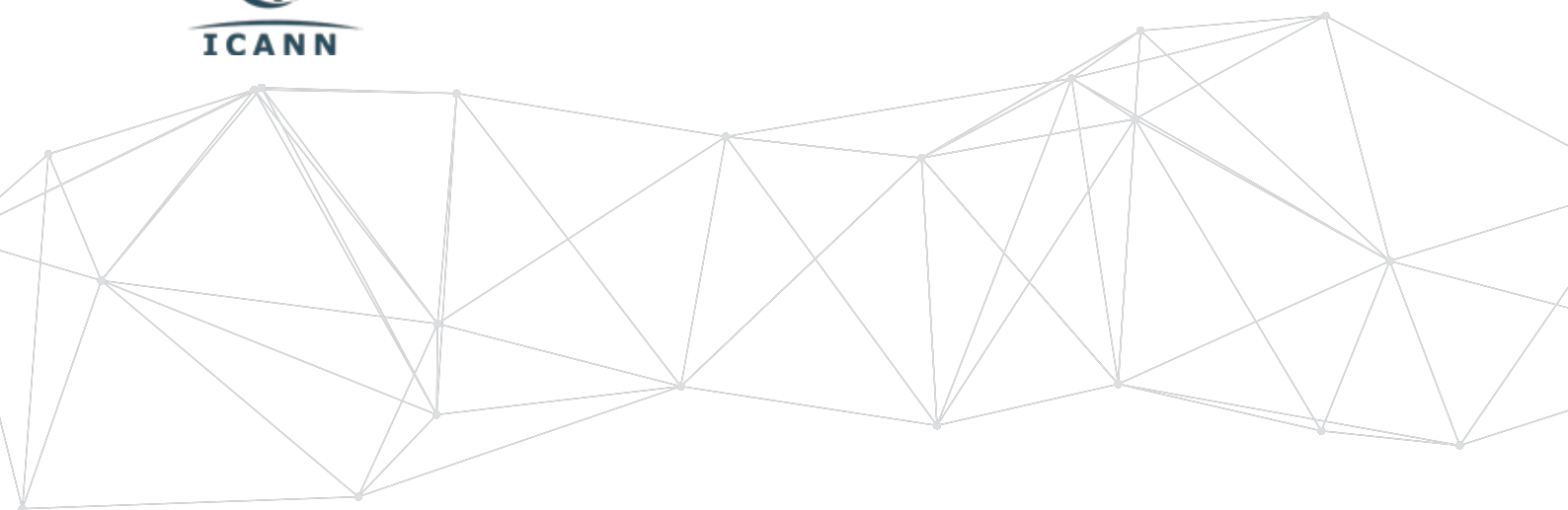


TABLE OF CONTENTS

PREFACE

RUSSIA CONSTITUTES ONE OF THE MOST MASSIVE AND RAPIDLY GROWING SEGMENTS OF THE GLOBAL INTERNET COMMUNITY. It is the 7th country in the world on the number of internet users (more than 104 million users and 7 per cent of Internet penetration). It is in the global Top 5 in terms of the level of connectivity of its national segment of the Internet. The Russian language is the third most popular language on the Internet in terms of the amount of available resources. The .RU zone is the 5th most popular top-level country domain and one of the Top 10 top level domains. Russia is one of only four countries in the world whose market is dominated by home-grown social networks and one of only three countries in the world, along with the United States and China, whose market is dominated by a home-grown search engine. Russia is one of the global leaders in the end-user cybersecurity market. In countries, such as Belarus, Kazakhstan, Kyrgyzstan, Tajikistan and Ukraine 60-86 per cent of all websites are in Russian. The contribution of the Russian Internet economy to the national GDP was 2,4 per cent in 2016.

Digital economy, internet governance and cyber security are at the crossroad of the interests of economic, professional and political groups. Internet of Things, and other major ICT sector growth drivers, also pose challenges to the architecture of the global network, forcing it to expand its size and adapt itself to handling new connected devices. Internet governance and cyber security became a realm of competitive domestic and global politics. One of the key current challenges for all stakeholders is to harmonize the interests of technological progress, economic development and security.

In 2015-2016 Security Index journal, the leading Russian journal on global security, published a series of articles on global Internet governance and cyber security. The articles are done by the most experienced Russian experts, most of them are the members of the PIR Center working group on Global Internet Governance and International Information Security. This collection of the articles includes translation of five of them into English. The translation was done with support of Internet Corporation for Assigned Names and Numbers to acquaint the global Internet community with the views of Russian experts.

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, com-

promising 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 infra-

structure 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/Амака_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)*

VULNERABILITY OF THE INTERNET: FACT AND FICTION

OLGA MAKAROVA,
DIRECTOR OF INTERNET AND CHANNEL RESOURCES DEPARTMENT, MTS

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

Dear Mr. Andropov,

My name is Samantha Smith. I am ten years old. Congratulations on your new job. I have been worrying about Russia and the United States getting into a nuclear war. Are you going to vote to have a war or not? If you aren't please tell me how you are going to help to not have a war. This question you do not have to answer, but I would like to know why you want to conquer the world or at least our country. God made the world for us to live together in peace and not to fight.

Sincerely,

Samantha Smith

The letter above was penned by the American schoolgirl Samantha Smith to Soviet leader Yuri Andropov in November 1982. It was published in the Soviet Union's main broadsheet *Pravda* in 1983.

Ms. Smith was moved to pen the letter by a photo of Yuri Andropov and Ronald Reagan on the cover of Time magazine. The two were named People of the Year – but the accompanying article opined that the new Soviet leader was an extremely dangerous man who posed a real threat to America's national security. It is now perfectly clear that Andropov had no intention of starting a war with the United States – but throughout his rule, the topic was a limitless source of editorial inspiration for Western journalists.

These days, few give any serious thought to the threat of nuclear war. The bugbear of our time and the new source of editorial inspiration is security of the global Internet, and the possibility of its partial or complete shutdown. Tensions are running so high that no-one would be surprised if a new Samantha Smith were to step up to the breach, pleading with the Russian and U.S. presidents to save the Internet in a series of impassioned tweets.

Rumors abound of an impending threat hanging over the World Wide Web. There have been stories about Russian users allegedly being cut off from the World Wide Web. A Russian submarine is supposed to have tried either to cut or blow up intercontinental data cables. All of it sounds suitably dramatic – but it's quite clear to specialists that no individual provider, even a global Tier 1 ISP, can cut off the Internet to an entire country, let alone trigger a planetary outage. Neither is it clear which particular cable the Russian boat is supposed to have assailed, and in what manner: there are dozens of cables crisscrossing the bottom of the oceans, rather than one of two fat data pipes[1,2].

The Internet is an extremely complex structure, and analyzing all possible threats to its proper functioning is well beyond the scope of this study. We are going to focus instead on the vulnerability of the data transmission part of the global Internet infrastructure. We will steer clear of the vulnerabilities in the domain name system (DNS) – that is a massive subject that merits a separate discussion. Let us assume for the purposes of this discussion that the DNS is out of any danger, and that a domain name can reliably be translated into an IP address in every single case.

NATIONAL BACKBONE INFRASTRUCTURE

For the purposes of this article, "national backbone infrastructure" is defined as the infrastructure of cable, satellite, and radio relay data links that connect cities within an individual country. In Russia, the national backbone infrastructure is often referred to as the Russian trunk communication network.

Operators usually build the national backbone/core network infrastructure using fiber-optic cables. Satellite and radio relay systems are employed mostly in remote and inaccessible areas where building and maintaining a fiber network would be uneconomical or technically impossible.

Figures 1, 2 and 3 show the backbone infrastructure of individual U.S. operators that make up the national IP infrastructure, and the national backbone network as a whole.Please note that the U.S. backbone infrastructure has a lot of circular redundancy. The same approach is used by other large network operators in countries throughout the globe.

The Russian national backbone infrastructure consists of the networks of five major operators: Rostelecom, MTS, Megafon, VympelCom, and TransTelecom.

TRANS-BORDER INTERCONNECTS

To connect the individual national backbone networks within the same continent, operators build cross-border interconnections (called "border interconnects" in Russian legislation), mostly using overland fiber optic cables.

Every regional operator aspiring to Tier 1 status must have its own cross-border interconnections in order to connect its own data links to the Global Tier 1 and regional traffic exchange points. The terms *global* and *regional Tier 1* will be explained later on in this article.

At this time, Russia has approximately 89 registered cross-border interconnections.

Building new cross-border interconnections was designated as an important priority by the 2005 World Summit on the International Society meeting in Tunisia as an important factor of eliminating digital inequality.

INTERCONTINENTAL DATA LINKS, UNDERWATER CABLES

Intercontinental data links are usually built and maintained by consortiums that lay submarine data cables.

There are currently seven submarine cable systems between Europe and America: Hibernia Atlantic, TAT-14, Atlantic – Crossing 1, TAT – TNG – Atlantic, Flag Atlantic – 1, Yellow, and Apollo. The Greenland Connect system connects Iceland, Greenland, and North America. Iceland is connected to the European mainland by the FARIG-1, CANTAT-3, and DANICE cable systems. Asia and North America are connected by TATA – TNG – PACIFIC, TRANS-PASIFIC_EXPRESS, CHINA US, JAPAN US, PACIFIC-CROSSING, and UNITY/EAC PACIFIC. The new FAST system is scheduled for completion in 2016, and the NEW CROSS PACIFIC in 2017. Only recently, data traffic between Europe and Asia relied mostly on the SEA-ME-WE-3, FLAG EUROPA-ASISA, and SEA-ME-WE-4 submarine cable systems. Now, however, there is also a growing number of new overland cables routed via Russia, Mongolia, Kazakhstan, Belarus, Ukraine, Poland, Finland, Sweden, and the Baltic states. The complete map of submarine cables is available at the TeleGeography website at http://submarine-cable-map-2015.telegeography.com[9].

There is, therefore, a high degree of redundancy available for routing traffic

FIGURE 1

NATIONAL IP BACKBONE OF COMCAST, WHICH SERVES MORE THAN 15 MILLION U.S. HOUSEHOLDS AND IS PART OF THE U.S. NATIONAL BACKBONE INFRASTRUCTURE[3]

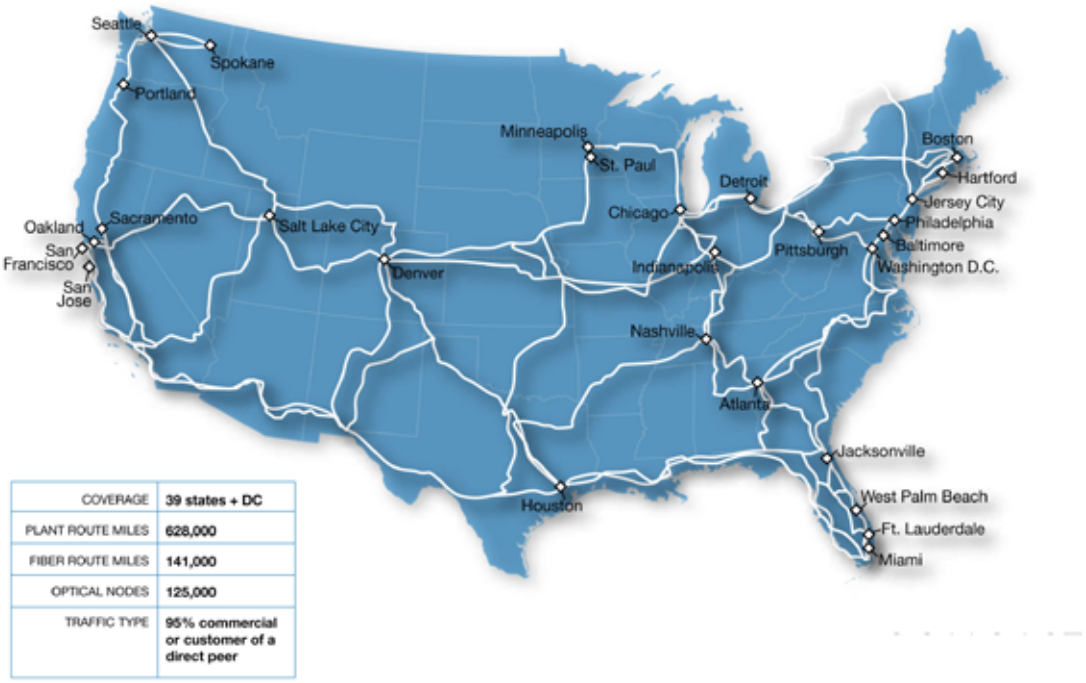


FIGURE 2

NATIONAL IP BACKBONE OF COX COMMUNICATIONS, WHICH IS PART OF THE U.S. NATIONAL BACKBONE INFRASTRUCTURE[4]

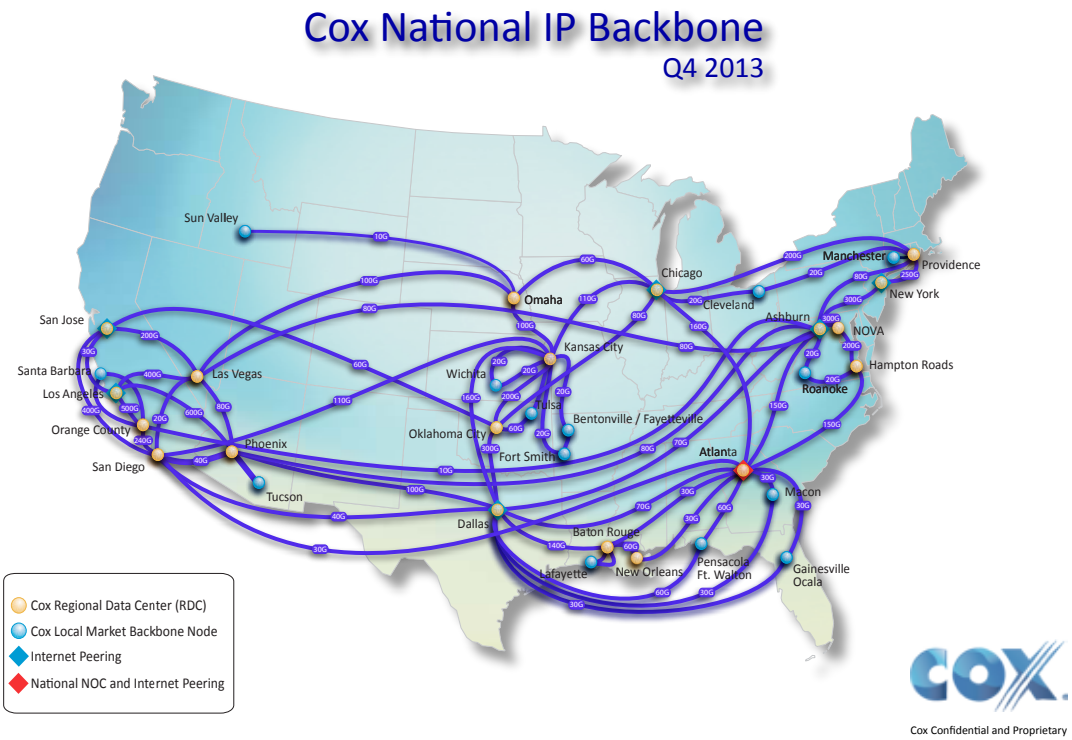


FIGURE 3

U.S. NATIONAL BACKBONE INFRASTRUCTURE[5]

FIGURE 4

BACKBONE NETWORK OF ROSTELECOM, PART OF THE RUSSIAN NATIONAL IP BACKBONE INFRASTRUCTURE[6]

FIGURE 5

BACKBONE NETWORK OF MTS, PART OF THE RUS[7]

FIGURE 6

BACKBONE NETWORK OF MEGAFON, PART OF THE RUSSIAN NATIONAL IP BACKBONE INFRASTRUCTURE[8]

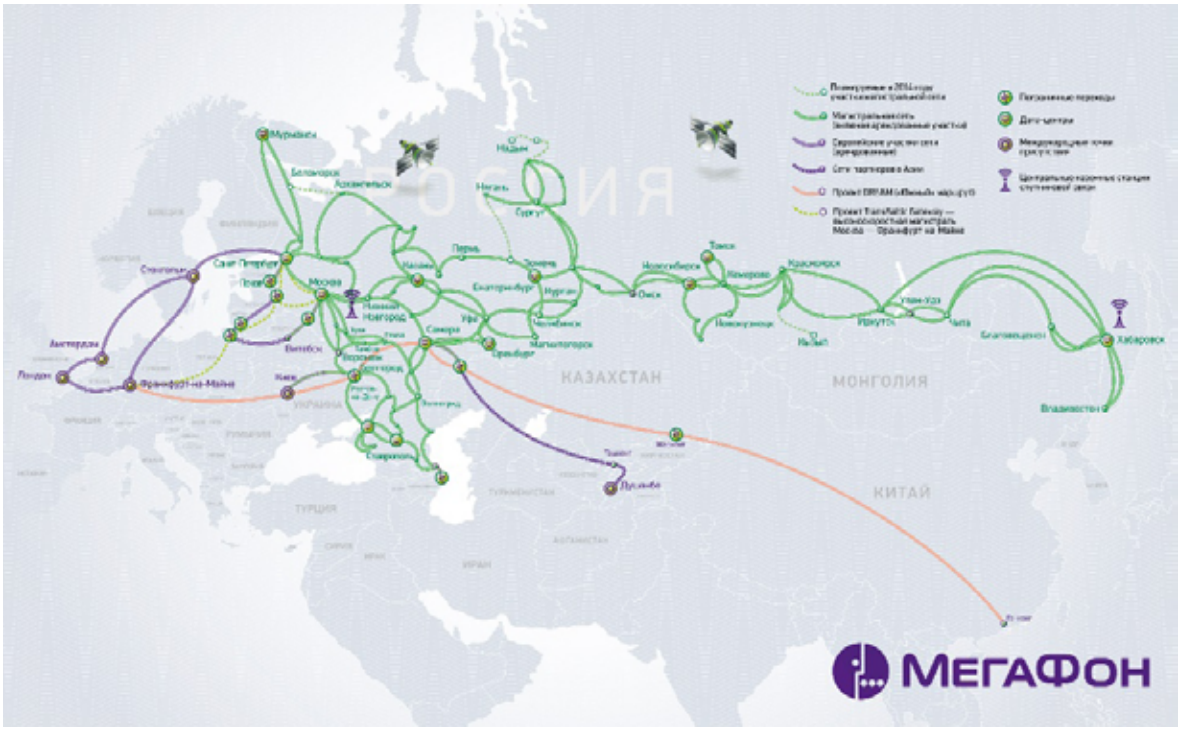
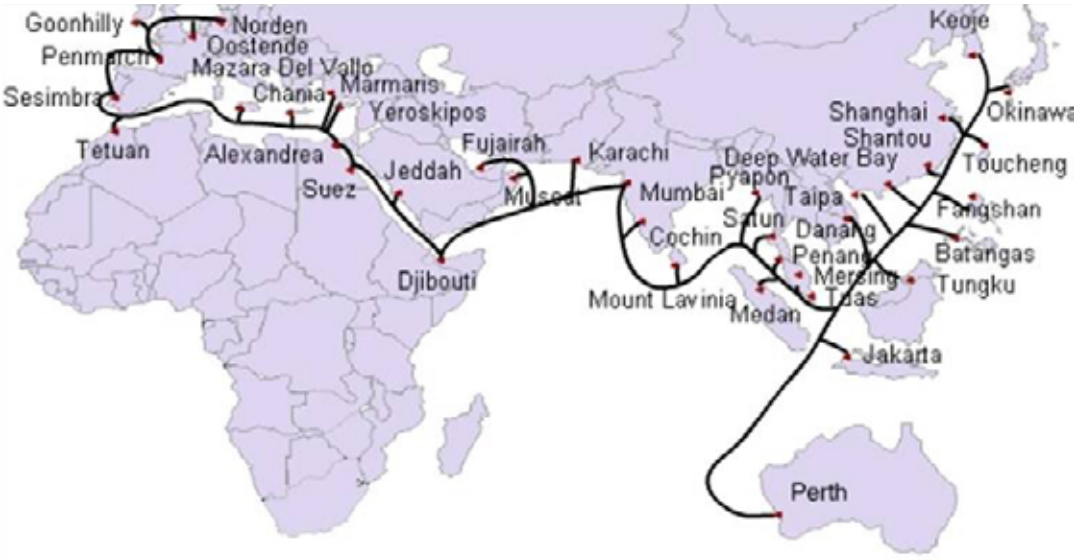


FIGURE 7

SEA-ME-WE-3 SUBMARINE CABLE SYSTEM, WITH THE LOCATION OF THE DAMAGE HIGHLIGHTED IN RED[10,11,12]



between any two continents via various submarine and overland cables. There is also partial redundancy provided by the possibility of routing traffic between two continents via a third – for example, data packets between Asia and America can travel via Europe.

Nevertheless, the global suppliers of Web content and information/communication services (especially American companies, followed closely by the Chinese) aim to have their servers hosted at all the most popular Internet Exchange Points on various continents – the so-called telehouses (data centers for telecoms infrastructure), where large, medium, and small operators can collocate their node infrastructure. In addition to Internet exchange points and telehouses, content and information/telecommunication service providers also have their servers hosted in regional operators' networks. They do not always choose regional Tier 1 operators for such hosting services because in this particular case, the priority is to be as close as possible to the end user. This is one of the most important aspects of the modern landscape of selling content and information/telecommunication services, and one of the ways of maximizing the reach of such services and capturing the target audience, whose value grows in proportion to the growing number of consumers of content and services.

This approach to content and services distribution helps to make savings on buying IP transit from the upstream providers. Using *the any connection, any place, any time principle*, the providers of content and services secure a lot of flexibility in how they reach their users. Such a landscape of content and service distribution essentially takes away market power from the IP transit and upstream providers. They no longer have a say in the content providers' connection decisions or in the distribution of traffic from the content providers' platforms.

Nevertheless, to understand the factors that affect the quality of the service received by the end users, it would be useful to analyze some of the most serious incidents in submarine cable systems.

A submarine cable of the SEA-ME-WE-3 system was damaged in July 2005. Some sources blame the incident on excessive curiosity of the local wildlife. The damage occurred 35 km south of Karachi. The trunk cable itself was left intact; the incident involved only the spur to Pakistan (see Fig. 7). As a result, major problems with connectivity occurred in Pakistan only.

All telecommunications in Pakistan, including Internet access, were badly affected. Back at the time, the country's own Internet resources were still at the nascent stage, and the leading international content/service providers did not have any cache servers in Pakistan itself, so international traffic via that sole submarine cable made up a very large proportion of Pakistani traffic consumption. Incidentally, the situation has not changed much since then.

The same SEA-ME-WE-3 submarine cable system was damaged once again on December 26, 2006 by an earthquake off the coast of Taiwan. The disruption affected Taiwan itself, as well as some users in South Korea and China[13].

On January 30, 2008, a ship anchor damaged the SEA-ME-WE-4 reserve cable system near the Egyptian port of Alexandria. As a result, many users in the United States and Europe were left unable to make international phone calls to countries in the Middle East and South Asia. The outage affected more than 70% of the users in Egypt itself[14].

Like Pakistan, Egypt does not have any significant information resources of its own, so most of the traffic comes from abroad, with few (if any) cache servers in the country itself.

The SEA-ME-WE-4, FLAG FEA, and GO-1 systems suffered another major outage on December 19, 2008. There were also incidents on January 10, 2013, January 30, 2014, and January 8, 2015.

On September 15, 2015, damage to a submarine cable affected Internet users in Singapore and Australia. Users of *Apple* devices were especially hard-hit because the company was rolling out updates to its iOS9 and OSX operating systems at the time[15].

In fact, users in Singapore and Australia were not the only ones who had problems downloading Apple updates during that period. In the summer of 2015, Apple overhauled its entire approach to data distribution. Up until that time, its software updates were available via content delivery networks (CDN) of the global content providers, such as *Akamai, Level 3*, and others. But by September 15, updates were to become available only through direct connections between Apple devices and each telecom operator's servers at the traffic exchange points and telehouses.

Unfortunately, when Apple rolled out the updates, its specialists had not yet managed to properly set up the routing tables, and users of Apple devices received most of those updates via the networks of global Tier 1 operators, causing an overload in many cases due to the unexpected surge in traffic. Apple representatives could not properly explain what happened to their traffic routing.

Other cable systems have been affected by similar incidents from time to time.

It is therefore safe to say that the main causes of the incidents include natural disasters, merchant ships, and (somewhat less often) the marine wildlife.

When such incidents occur, their worst effects are felt in those countries where:

- There are few national information resources;
- There are no major traffic exchange points;
- There is no network of telehouses;
- There are no direct interconnections between the main regional Tier 1 operators (peering connections);
- The regional Tier 1 operators do not yet exist, or cannot compete with the Western providers of IP transit services
- Where the global providers of content and services don't have cache servers because it is technically impossible, because the government would not allow it for political reasons, or because it would be uneconomical.

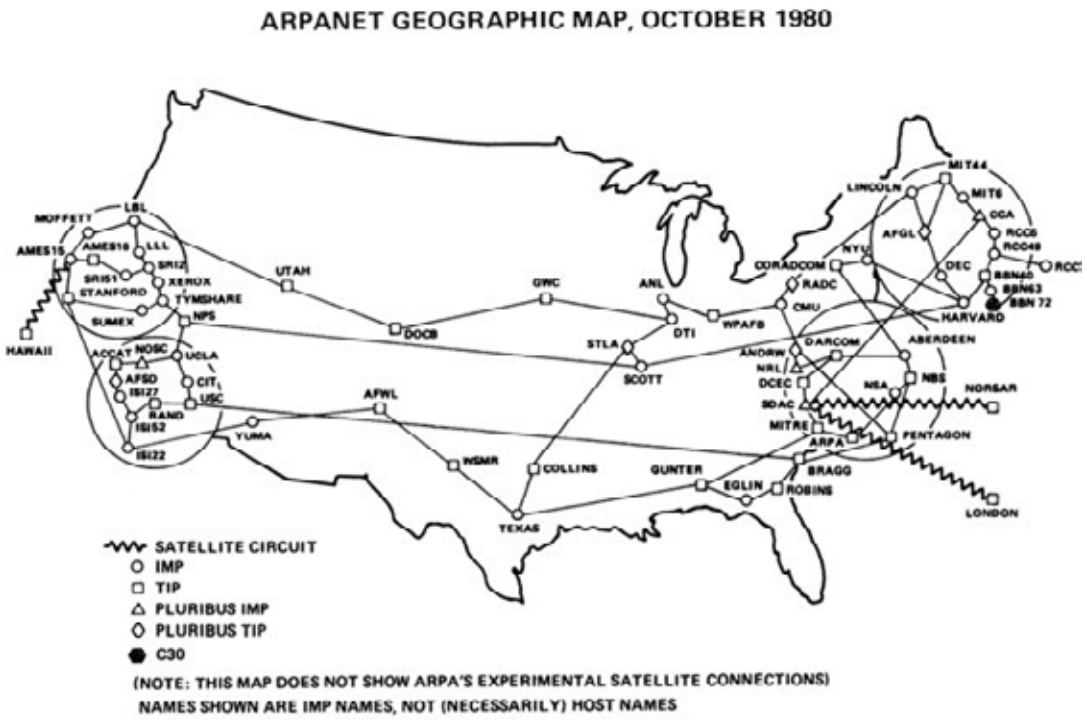
In other words, such outages are especially keenly felt by users in those countries where the national Internet ecosystem is nonexistent. In most cases, however, the Internet has proved fairly resilient to submarine cable outages.

Voice services – especially international telephony – are hit much harder when such incidents occur. Despite the relatively wide spread of Internet technologies, many operators still rely on the SDH (synchronous digital hierarchy) system for long-distance voice traffic. Such traffic is categorized as premium (i.e. top level of service) in telecommunication contracts. Specialized services for corporate clients, including online access to stock exchange trading, have also proved very vulnerable in the event of cable outages.

One of the clear trends in recent years is migration of international voice traffic to IP networks. This is happening very quickly in some countries, but slowly and painfully in others. The difficulty of the transition is mostly explained by the force of habit, as well the (completely unfounded) opinion among some profes-

FIGURE 8

8 INFRASTRUCTURE OF THE INTERNET IN 1980[16]



sional users that IP networks are unreliable. In actual fact, such a transition is entirely justified; numerous examples have shown that submarine cable outages leave the global Internet much less affected than telephony. Thanks to the distributed architecture of the Internet and the local caching of resources in countries around the world, there is much less disruption for Internet users than for SDH-based international telephony subscribers or specialized corporate services.

It will probably take a generational change (and I mean people rather than hardware or software) for international telephony to completely migrate to IP.

INTERNET ECOSYSTEMS: GLOBAL AND REGIONAL

To explain the architecture of the modern Internet and its resilience, let us go back to the time when the Internet itself ceased to be a U.S. Department of Defense project and began its global spread.

At that time, the Internet infrastructure looked roughly as follows in Fig. 8.

As soon as the entire Internet project transitioned to a commercial footing, people had to figure out how to make money on it. That is when the first rules of the game were drawn up.

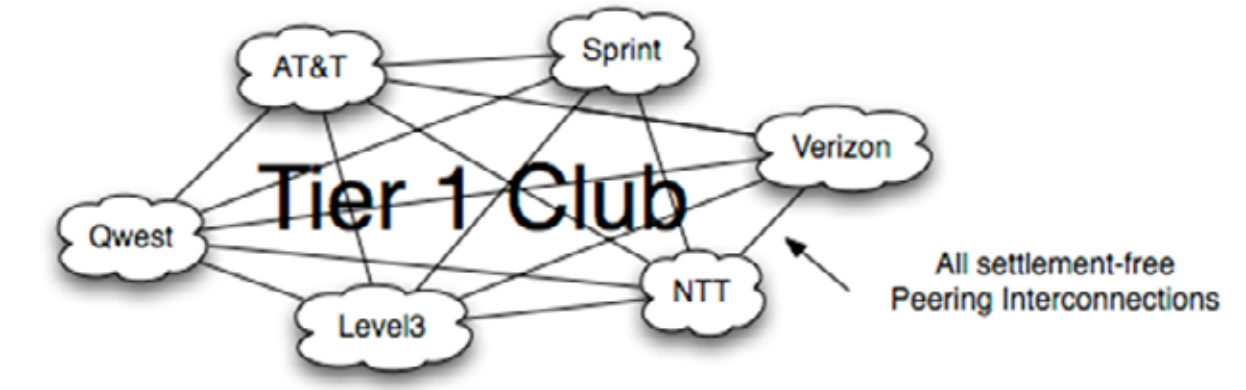
GLOBAL TIER 1 OPERATORS: GLOBAL INTERNET'S FIRST BACKBONE INFRASTRUCTURE

A total of only six companies inherited and/or built the nascent infrastructure of the global Internet. All of them set up peer-to-peer interconnections with each other (see Fig. 8), and their relations came to be known as peering. That was the beginning of the global Tier 1 operators' club; those operators' networks made up the very first global IP backbone.

The six peering partners could exchange traffic generated by their customers and operators, such as ISPs, content service providers, and other companies that had their own autonomous systems. However, none of the peering partners could offer transit between any two of the other peering partners via its own autono-

FIGURE 9

GLOBAL TIER 1 CLUB AFTER THE ACQUISITION OF SOME MEMBERS BY LARGE OPERATORS[17]



mous network.

A FEW WORDS ON AUTONOMOUS SYSTEMS

Current autonomous systems (AS) can use several internal routing protocols, and in some cases there are several sets of metrics within the same AS. Nevertheless, administration of an AS appears to other autonomous systems as a coherent table of internal routing, and shows a coherent picture of resource availability within that system.

Each autonomous system has a unique identifier called Autonomous System Number (ASN). These ASN are used for the exchange of routing data between neighboring autonomous systems, and also as the unique names of the systems themselves. AS usually use one or several internal gateway protocols (AGP) to provide routing data within a system. The currently recommended protocol for external routing is the Border Gateway Protocol (BGP).

MODELS OF CHARGING FOR INTERNET TRAFFIC

All the operators, content service providers, and clients connected to a global Tier 1 had to pay that Tier 1 for their traffic, both inbound and outbound. If an operator, client, or content service provider had a connection to two or more Tier 1s for redundancy purposes, it had to pay each Tier 1 to which it was connected.

Meanwhile, Tier 1s did not have to pay anything to anyone. Breaking up peering agreements and interconnections between members of the Tier 1 club was deemed impossible as it would cause serious damage to the resilience of the global Internet. Later in this article we will describe the grave consequences that have resulted in the past from sporadic attempts by the global Tier 1s to break up a peering interconnection with a peering partner after a commercial dispute went out of control.

To become a member of the global Tier 1 club, the candidate had to establish peering interconnections with all the existing members. That requirement was entirely justified. In accordance with the agreements, members of the club offered their clients (ISPs or content service providers) traffic not only from their own network, but also from the networks (resources) of other clients (including ISPs and content service providers), as well as all the traffic from their peering partners. Other members of the club did not work with the same customer so as not to undercut their partners and to avoid competition with each other.

Many large operators were forced to acquire an existing member of the Tier 1 club in order to gain membership. For example, Level 3 had to acquire Genuity.

The operators connected to Tier 1s were free to sell traffic to other operators who for various reasons could not get connected to one of the Tier 1s.

In such cases, the operator connected to Tier 1 became a Tier 2, and received the right to sell traffic to and from its own network, the networks of its clients, connected operators, and content service providers, the networks of its own peering partners, and all the traffic received from the global Tier 1.

These traffic selling relationships came to be known as IP transit. The operator or provider selling IP transit services is called upstream, while the operator and provider buying IP transit is called downstream.

The number of tiers in such a system is unlimited.

At about the same time, another very important principle was established: regardless of whether the company is a content service provider (i.e. generates traffic for end users) or a telecommunications operator (i.e. a consumer of traffic on behalf of its users), everyone had to pay their upstream partner. Never and under no circumstances does an upstream partner have to pay anything to the companies that generate traffic – even if that traffic is then consumed by its clients, or the clients of the downstream operators connected to it. The content providers must earn money on advertising, and the operators on the fees paid by their subscribers – but both of them should pay their upstream partners for IP transit.

The American Tier 2s quickly realized that by establishing interconnections with each other, they could make savings on paying for the services of the Tier 1s; the same understanding soon spread further down the tiers.

The question of who can be regarded a peer at the same tier, and who is a customer to whom you can sell traffic, required an individual approach and creative thinking on the part of peering managers.

Interconnections between peers could be established via traffic exchange points or directly. In the United States, where the Internet was born, most of the operators prefer to establish direct interconnections with their peers, bypassing traffic exchange points. In Europe, the situation is somewhat different.

Obviously, during the early days of the global Internet, the European operators who wished to get connected had to pay not only for the IP transit services of the global Tier 1s, but also for the data links via the submarine cables. That is why they had a great vested interest in developing peering interconnections in Europe itself, and in putting content geographically closer to the European consumer.

The global content service providers, for their part, wanted to increase their reach and gain new audiences, so they were prepared to host their servers in Europe in order to reduce transit payments to the global Tier 1, Tier 2, and sometimes even Tier 3 operators.

Establishing a presence in Europe and leasing bandwidth to organize a connection to every local operator was not economical for the global content providers during the early days of the European segment of the Internet. That is why Europe saw a rapid growth of traffic exchange points. W. Norton[18], a researcher of the economics of the Internet, highlights the following reasons for the emergence of traffic exchange points:

The theory of a healthy peering Internet ecosystem:

- Popular traffic exchange points emerge and flourish where there is a large concentration of content users and a large amount of content;
- Where the volume of local (regional) traffic is significant, the international ISPs and CDNs have an interest in creating new traffic exchange points in the region in order to reduce the load on their own international data routes.

The theory of cable exit points:

- The exit points should be topologically close to the places where subma rine cables make landfall, i.e. to seaports.

The theory of geographic proximity:

- London is a convenient place for distributing IP traffic all over Europe
- Frankfurt is a convenient place to collect Middle Eastern and Eastern European traffic
- Australia, on the other hand, lies on *the road to nowhere* in IP transit terms.

The financial center theory (proposed by A. Niper):

- The financial markets are the drivers of the growth of Internet

FIGURE 10

INTERNET TRANSIT PRICE PER UNIT OF TRAFFIC[19]

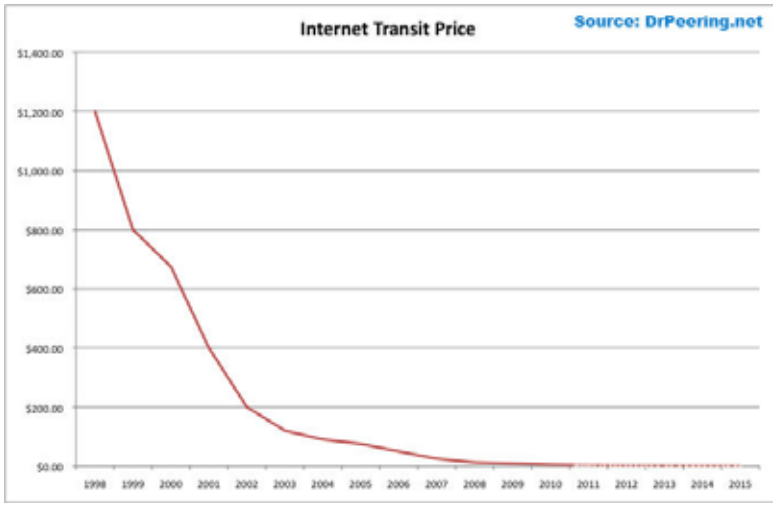
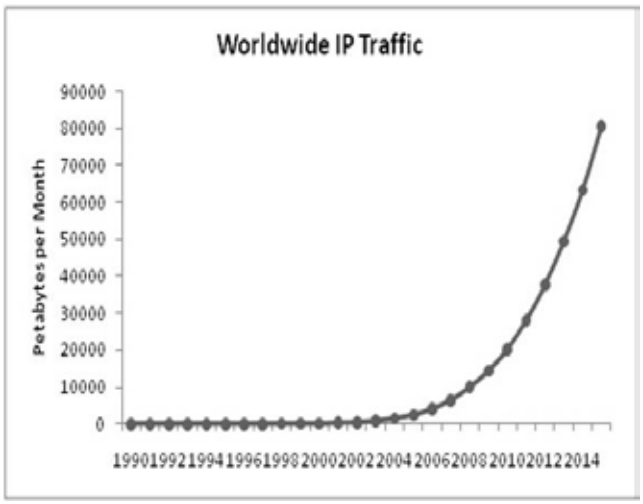


FIGURE 11

GLOBAL IP TRAFFIC GROWTH[20]



exchange points;

- The financial community always wants to cut costs, which encourages the operators to choose locations near the financial centers;
- The largest traffic exchange points are in London, Frankfurt, Amsterdam, New York, Chicago, and Tokyo because that is where the world's largest stock exchanges are. Milan will soon join that list.

The theory of business orientation (proposed by M. Moyle-Croft)

- An unstable legal and regulatory environment undermines any attempt to create regional traffic exchange points and to attract international players;
- Businessmen have no interest in working in a complicated and burden some normative environment set up by national regulators, especially if local regulations are very different from international practices.

The rise of traffic exchange points and the closing of the traffic loop within individual regions led to the emergence of regional Internet ecosystems, with their own regional Tier 1 operators. The development of regional Internet resources, as well as the global content service providers' interest in securing presence at all the large traffic exchange points, led to a significant reduction of the dependence on U.S. providers, and to a greater resilience of the global Internet.

TABLE 1

INTERNET TRANSIT PRICE PER UNIT OF TRAFFIC.

Company	Country	ASN	Number of connected AS
Level 3 Communications (the former Level 3, Global Crossing)	USA	3356 / 3549 / 1	4402
AT&T	USA	7018	2365
XO Communications	USA	2828	2904
Verizon Business (former UUNET)	USA	701, 702	1946
CenturyLink (former Qwest u Savis)	USA	209 / 3561	1367
Sprint	USA	1239	1183
Zayo Group (former AboveNet)	USA	6461	1066
GTT (former Inteliquent)	USA	3257	886
NTT Communications (former Verio)	Japan	2914	718
TeliaSonera International Carrier	Sweden	1299	630
Tata Communications (former Teleglobe)	Canada	6453	569
Deutsche Telekom AG	Germany	3320	535
Telecom Italia Sparkle (Seabone)	Italy	6762	344
Telefonica	Spain	12956	150
OpenTransit (France Telecom)	France	5511	146
*AOL Transit Data Network (ATDN)**	USA	1668	
*Cogent Communications**	USA	174	3537
*Hurricane Electric**	USA	6939	2180

**There is an opinion that these operators pay some of the Tier 1s for peering.*

As a result, IP transit prices have collapsed (Fig. 10, 11).

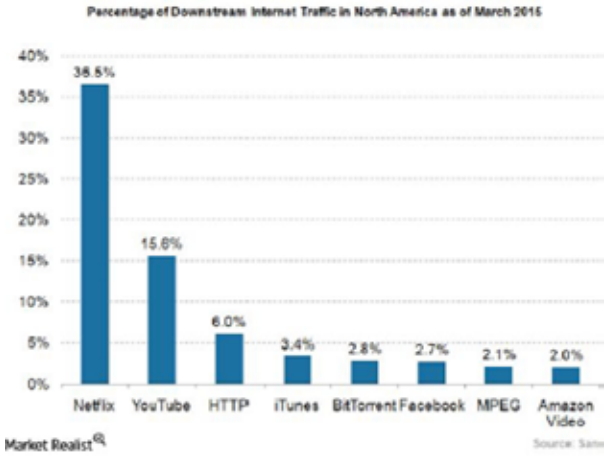
The plummeting IP transit prices forced the global Tier 1s to launch a regional expansion. Their expansion in Europe led to the following trade-off: the global Tier 1s were allowed to do business at the end-user level by granting them access to European infrastructure at the last mile. In exchange, a number of large European provides, including *Deutsche Telekom, Telefonica, France Telecom,* and *Telecom Italia*, have been granted membership of the global Tier 1 club. This did not create more physical infrastructure, but it has increased the resilience of the Internet, and completed the formation of the European regional Internet ecosystem.

At this time, the list of the global Tier 1s is as follows (Table 1)[21].

China and Japan were the key players in the formation of the Asian Internet ecosystem. China has built its Great Firewall to stop the expansion of such global giants as Google in the Chinese market. This opened up the field for domestic information resources such as Baidu, Alibaba, etc. Japan generates large amounts of its own content, some of it using Vocaloid, a speech synthesis software package by *Yamaha Corporation* that relies on stored fragments of natural speech.

FIGURE 12

PERCENTAGE OF DOWNSTREAM INTERNET TRAFFIC IN THE UNITED STATES[22]



That is why 80 per cent of Japanese and Chinese Internet traffic never leaves these countries' own Internet ecosystems, shielding them from the effects of submarine cable outages or disruptions in the global Tier 1 networks. Incidentally, Japan's *NTT Communications* is one of the global Tier 1s.

Hong Kong and Tokyo host some of the world's largest traffic exchange points, where almost every single operator and content service provider of the Pacific and Southeast Asian region has a presence.

According to *The New York Times*, China has recently introduced more stringent requirements for foreign IP messaging services such as WhatsApp, Telegram, and others. The paper has reported that in compliance with a government order, the Chinese police and Internet service providers have begun to disconnect mobile subscribers who use foreign messengers or VPN services.

It has also been reported that China has created and is now testing new technologies for intercepting traffic generated by requests to the Chinese Internet search engine Baidu. If the request meets certain criteria, the system inserts a malicious script in the response traffic, which the Chinese government later uses to initiate DDoS attacks. The technology has been dubbed the Great Cannon. So far, there is very little information about it, and it is hard to say how much of a threat this new technology can pose to the resilience of the global Internet.

It is not just the Japanese and Chinese Internet ecosystems that are largely self-contained; the same is true of the North American ecosystem. The nature of that ecosystem, however, is somewhat different. It centers around paid video on demand, which emerged in the United States and soon became the most popular Internet service in North America. That is why 36% of the Internet traffic consumed by users in the United States originates from Netflix, the largest content service provider that used to make its content available only in North America until quite recently.

This is why Internet users in the United States have little to fear from bogus threats such as a Russian submarine allegedly trying to cut a submarine cable for whatever reason. Far more dangerous is the constant bickering between those who sell their content via other companies' networks, and the companies that build and operate those networks.

PEERING WARS BETWEEN THE GLOBAL TIER 1S: CONTENT VS. NETWORK

The real threats to the resilience of the Internet in North America include the peering wars between the global Tier 1 operators that were waged between the late 1990s and early 2000s.

In his book "The Art of Peeing"[23], W. Norton describes the so-called Chicken tactic, which was first employed in the 1990s. Two companies, *Genuity (BBN Planet)* and *Exodus*, were exchanging large volumes of traffic. At some point

Genuity came to believe that delivering Exodus' traffic all across the country is a valuable service for which Exodus must pay. Exodus countered that Genuity was merely trying to get its content for free. It was confident that Genuity would never de-peer it – but Genuity went ahead and did just that. Exchange of traffic between the two companies resumed only after Exodus set up several traffic exchange points in various parts of the United States. That battle of the giants went almost completely unnoticed by ordinary Internet users or by the regulator[24].

The next such battle took place between AOL and Cogent in 2003, and it proved far more disruptive. AOL decided that there was no longer a parity in its traffic exchange with Cogent; the former took 3 times as much as it gave. Cogent decided that AOL was merely trying to get more money for its content, and countered that AOL does not actually have any nationwide infrastructure of its own, relying instead on Cogent's data pipes. The sum of money at stake was 75,000 dollars a month. The consequences of the tussle were much more visible than in the Genuity vs. Exodus case. The affected users included schools connected to Cogent's networks; they were left with severely restricted access to some of the national resources. There was also an overload of peering interconnections with Level 3. Cogent was forced to buy IP transit from AdobeNet for 35 U.S. dollars per 1 Mbit of bandwidth. Eventually it reached an agreement with AOL, and peering was restored[25,26].

In 2005 Cogent got itself into a war with two operators simultaneously. First, Level 3 decided that Congent was pumping too much traffic via its infrastructure, putting Level 3 at a commercial disadvantage. Cogent argued that Level 3 was trying to force it to raise its own IP transit prices because Cogent's price policy was stealing customers from Level 3. As a result, there was a long period of degraded service quality (including voice services) for both companies' customers[27,28].

In 2005 TeliaSonera decided that it should not be the only one to pay for upgrading the infrastructure that was also used by Cogent. The latter said that forcing it to foot some of the bill was not fair. Both companies' customers were affected by the ensuring disruption. Eventually, a deal was reached, and peering was restored[29].

In 2008 a similar dispute broke out between Cogent and Sprint when the latter decide that there was no traffic parity between them and demanded new peering terms. Cogent accused Spring of breaking their existing agreement. Both companies' customers were affected by the ensuing disruption. In the end, a deal was reached, and peering was restored[30].

In 2008 the largest U.S. operators declared war on Netflix by trying to charge prohibitive prices and degrading the quality of service for customers accessing content distributed via the Netflix platform. The conflict resulted in the adoption of a new package of documents setting out new rules for the Open Internet Order[31]. The 400-page document contains several mentions of Cogent and its previous wars. To avoid such incidents, future regulation (including regulation of peering relationships) would be based on precedent and use a light-touch approach, encouraging market players to settle their disputes and work out the terms of cooperation on their own.

THE FORMATION OF THE RUSSIAN ECOSYSTEM

The growth of the Internet in Russia was very uneven in the late 1990s, with some parts of the country making rapid progress and others lagging behind. The reason for that was the expense of leasing bandwidth to Moscow and St Petersburg, where the international cables usually terminate, and where regional Internet resources were growing very rapidly.

In 1998 Rostelecom launched the first project as part of a larger program of building the Russian national IP backbone. Later on that backbone infrastructure development project was joined by TransTelecom. In 2001, however, Rostelecom's Internet business was transferred to the company's subsidiary RTCom.RU (which currently focuses on satellite communication systems). At about the same time, MTU-Intel launched a large project of offering cheap broadband services to end users in Moscow.

In 2001 Cable&Wireless entered the Russian IP transit market, offering aggressively low prices in the expectation that 75-80% of the traffic it sold would never leave Russia, so the cost of its transit would equal the cost of passing data between two ports of the same router (i.e. zero).

Simultaneously, TransTelecom entered the market with an offer of paying all the information resources for generating traffic consumed by its customers. Peering interconnections between the Russian providers were mostly done via traffic exchange points at the time, with little in the way of rules or terms and conditions.

Had *Cable&Wireless* succeeded in its plans to win a large share of the Russian IP transit market, the Russian Internet ecosystem would have remained in a rudimentary state, and the resilience of the Russian segment of the Internet would have largely depended on the resilience of the European segment.

In the early 2000s, market conditions become ripe for ending free or near-free peering arrangements between Russia's large players and relatively small networks. The large players had come to realize that economically, free peering represented a break in the value chain. They had already begun to invest large amounts of money into their network infrastructure, and free peering was essentially letting all their peering partners use that infrastructure without paying anything for it. As a result, small operators were gaining an unfair competitive advantage by using the inter-regional IP transit infrastructure built by the large players at their own expense.

At the same time, some of the large players in the Russian market were determined to pursue various ill-considered and populist policies. For example, some of them were lobbying the idea of a new mechanism in Russia that would force Internet network operators to compensate the owners of information resources for the cost of creating and distributing that content over the Internet. The main argument used by these populists was that without content, users would lose interest in the Internet, and since the owners of the information resources have no way of actually earning money on their content, the network operators should share their profits with them.

Compensation for the creation and distribution of content over the Internet was supposed to come in the form of content providers receiving some of the money being paid by ISPs' clients and network operators for Internet access and IP transit. Essentially, they would be paid for the (nonexistent) transit of the traffic generated by information resources. The proposed model was telephony, which has long used the caller pays principle.

In other words, the idea was that content providers would not only use network operators' infrastructure free of charge to bring their content to the audiences, but they would also be paid by the operators for doing so.

Such ideas were very damaging for the growing Russian Internet market. The settlement models used in telephony have never been – and could not be – replicated in any country as a template for settlements between the Internet market participants. Additionally, had these ideas been implemented, they would cause the entire Internet advertising market to stall.

In the early 2000s these ill-considered and populist ideas bandied about by some market participants, in a combination with some other economic factors, prompted the three leading Russian Internet providers of that time – MTU-Intel, RTComm.RU, and Teleross (part of the Golden Telecom group, later acquired by Vympelcom) – to set up a Separate Peering Group that laid the foundation of the regional Tier 1 club in Russia.

The terms of participation in that Separate Peering Group included parity of traffic exchange at the peering interconnections; a certain minimum amount of traffic at the exchanges; and access to interconnections with the global Internet segment in at least two points outside Russia, which required leasing international bandwidth. There was also the usual requirement for any future members of the peering group to establish peering partnerships with every existing member.

Many of the Russian ISPs who were left out of that club because they could not meet membership requirements criticized the move. Nevertheless, its effects have been largely positive:

- The price of leasing international bandwidth has fallen dramatically.
- The new system has encouraged the creation of new cross-border interconnections.
- Almost all intra-Russian traffic never leaves Russia now, whereas previously there were lots of *international loops*.
- Foreign operators no longer have a lot of interest in selling traffic in Russia because sales volumes are low, and such operations are uneconomical.
- Traffic exchange points – especially the MSK-IX point in Moscow – have grown rapidly.
- The Russian market of Internet advertising is experiencing rapid growth thanks to the efforts of Russian providers of content and services.

Over time, membership of the Separate Peering Group has changed. It now includes all the major operators whose networks make up the Russian national IP backbone.

The idea of new regulation that would force network operators to pass on to content producers and distributors some of the money paid for Internet access by their subscribers has not been completely forgotten. It was part of the late 2014 proposals by some intellectual property rights holders on introducing a Global License mechanism. That proposal, however, met with sharp criticism from every Internet market participant without exception[32].

The establishment of the Separate Peering Group enabled the creation of the regional Russian Internet ecosystem, in which 80% of the traffic stays within Russia itself. This has significantly reduced the Russian Internet segment's dependence on the resilience of the global Tier 1 networks.

The vast majority of the Russian regional Tier 2, Tier 3, and other operators have interconnections with at least two Russian Tier 1s. The Russian providers of content and services (Russian legislation refers to them as *organizers of distribution of information over the Internet,* or *as search engine operators*) are usually connected to all the Russian regional Tier 1s, which ensures better access to their resources for the end users.

It is therefore impossible to disconnect all the Russian users from the global segment of the Internet by disrupting the work of any single network operator, even if that operator happens to be a regional Tier 1.

It is therefore safe to say that the reports about some alleged exercises on cutting off all Russian users from the global segment of the Internet are fictitious.

To pull off something like that, all the Russian network operators who have interconnections with the global segment would have to stop letting any traffic through these interconnections. That is impossible for a number of reasons. First, the voice (telephony) traffic uses the same infrastructure as the IP traffic. Therefore, the cut-off would affect not only Internet users but also telephony subscribers and international roaming. Second, all the Russian network operators sell Internet traffic to operators from other countries, including the EU. And third, there is a lot of transit between Europe and Asia via Russian territory.

HOSTING OF FOREIGN CONTENT PROVIDERS' RESOURCES IN RUSSIAN TERRITORY

Due to growing competition and the need to ensure high-quality access to their information resources, many global providers of Internet content and services – such as Google, Akamai, CDN Level 3, etc. – want to host their servers in Russia. That can be done using two main options. Option 1 is for the servers to be hosted at traffic exchange points, or at other independent sites (Data Exchange Center, Telehouse). Access to these servers is offered to all telecommunication operators, as well as to legal entities who are not telecommunication operators under Russian legislation but want to buy Internet access.

Option 2 is to have cache servers hosted directly by individual network operators whose subscribers constitute a potential audience for the content provider.

The hosting of the servers of the global content providers in Russia offers clear benefits to these providers, as well as to the Russian network operators. For the

latter, it translates into savings on international bandwidth and improves the quality of service received by their users. For the former, it offers better access to a potential audience of content consumers.

This approach also improves the resilience of the global Internet for regional users.

CONCLUSION

"The reports of my death have been greatly exaggerated", Mark Twain once informed the Associated Press in a telegram.

The same applies to reports of the alleged fragility of the global Internet infrastructure, the risk of the loss of global connectivity in the event of a single cable being cut, and the possibility of a single network operator leaving all Russian users without access to the Internet. In fact, the exaggeration here is much greater than in the case of Mark Twain.

Upon closer inspection, the global Internet has proved much more resilient to external impact than many other services - especially voice and specialized services provided to corporate customers, including transnational corporations.

The global Internet is one of the greatest human inventions and achievements. It has no traffic control centers and no fail points, because control and decision-making are widely distributed.

The IP protocol will deliver a data packet between any two network-connected devices if even a single route between them remains functional, and there is no total loss of connectivity. The global Internet does not actually have any global elements, with the exception of several unique identifiers: the IP addresses, the AS numbers, and the Domain Name System. That is why the Internet is infinitely scalable and adaptable to changes in the structure or technology of access on the one hand, and technology of the services delivered via the Internet on the other.

That is not to say, however, that the Internet is completely resilient to various misguided experiments, including those initiated by some government ministries and agencies which find it easier to ban every scary new thing than to learn to live in a new reality. Such experiments will not lead to the disintegration or disappearance of the global Internet. But they can catapult the individual nations pursuing such experiments 20 years into the past – and closing such a huge gap in an era of breakneck technological progress will prove impossible. It is safe to say that the Internet is synonymous with innovation. Some experts, such as the renowned economist J. Schumpeter, argued that innovation and economic growth were also synonymous. Schumpeter believed that only the countries where people make discoveries get richer; all other nations cannot escape stagnation. He also believed that the process of innovation can never be peaceful and tranquil because it represents a ruthless cycle of destruction of old industries and creation of new ones – a process as relentless and unstoppable as every other force of nature.

What, then, is the lesson of this story? I think the main lesson is that the Internet is the new reality that is still being shaped, and that we will have to learn to live with, constantly adapting to unstoppable change.

REFERENCES

[1] *Greg's Cable Map http://www.cablemap.info (Last accessed March 16, 2017)*

[2] *Submarine Cable Map 2015, TeleGeography http://submarine-cable-map-2015.telegeography.com (Last accessed March 16, 2017)*

[3] *Our Fiber Optic Network, Comcast Business https://business.comcast.com/about-us/our-network (Last accessed March 16, 2017)*

[4] *Cox National IP Backbone Q4 2013, Cox http://www.cox.com/wcm/en/business/datasheet/national-ip-backbone-map.pdf (Last accessed March 16, 2017)*

[5] *Internet Access to Africa, Hugh and Becky http://www.hughandbecky.org/2013/internet-access-to-africa (Last accessed March 16, 2017)*

[6] *Backbone network of Rostelecom, Rostelecom http://www.rt.ru/data/doc/backbone_map.pdf (Last accessed March 16, 2017)*

[7] *Source: MTS*

[8] *http://lc.megafon.ru/ai/html/4391/files/mgfon-MAP_RU_v45.jpg*

[9] *Greg's Cable Map http://www.cablemap.info (Last accessed March 16, 2017)*

[10] *Hla Oo, Leaking Underground Cable Disrupting Internet in Burma, Hla Oo's Blog, July 29, 2013 http://hlaoo1980.blogspot.ru/2013/07/leaked-underground-cable-disrupting.html (Last accessed March 16, 2017)*

[11] *Communication breakdown in Pakistan, The Sydney Morning Herald, June 29, 2005 http://www.smh.com.au/news/breaking/communication-breakdown-in-pakistan/2005/06/29/1119724673577.html?from=moreStories (Last accessed March 16, 2017)*

[12] *Pakistan cut off from the world, The Times of India, Jun 28, 2005 http://timesofindia.indiatimes.com/world/pakistan/pakistan-cut-off-from-the-world/articleshow/1154683.cms (Last accessed March 16, 2017)*

[13] *Asia phone links start to recover, BBC News, December 28, 2006 http://news.bbc.co.uk/2/hi/asia-pacific/6213501.stm (Last accessed March 16, 2017)*

[14] *https://www.bloomberg.com/apps/news?pid=newsarchive&sid=a3tADKd_tY3g&refer=europe*

[15] *Allie Coyne. Cut submarine cable cripples Apple services for Telstra customers October, IT News, October 2, 2015 https://www.itnews.com.au/news/telstra-iphone-mac-users-report-crippling-speeds-to-apple-services-410006 (Last accessed March 16, 2017)*

[16] *An Atlas Of Cyberspaces, Historical Maps of Computer Networks http://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html (Last accessed March 16, 2017)*

[17] *Tier 1, Internet Peering White Papers, DrPeering International http://drpeering.net/white-papers/Ecosystems/Tier-1-ISP.html (Last accessed March 16, 2017)*

[18] *Tier 2, Internet Peering White Papers, DrPeering International http://drpeering.net/white-papers/Ecosystems/Tier-2-ISP.html (Last accessed March 16, 2017)*

[19] *A Business Case for Peering in 2010, Internet Peering White Papers, DrPeering International http://drpeering.net/white-papers/A-Business-Case-For-Peering.php (Last accessed March 16, 2017)*

[20] *Resources to make strategic peering decisions, Internet Peering White Papers, DrPeering International http://www.drpeering.net (Last accessed March 16, 2017)*

[21] *AS Rank: AS 3320 -- Information for a single AS: AS Relationship Table, CAIDA http://as-rank.caida.org/?mode0=as-info&mode1=as-table&as=3320 (Last accessed March 16, 2017)*

[22] *Puneet Sikka Has YouTube Started to Replace Traditional TV Viewing?, Market Realist, Jul 30, 2015 http://marketrealist.com/2015/07/youtube-started-replace-tv-viewing (Last accessed March 16, 2017)*

[23] *The Art of Peering: The Peering Playbook, Internet Peering White Papers, DrPeering International http://drpeering.net/white-papers/Art-Of-Peering-The-Peering-Playbook.html (Last accessed March 16, 2017)*

[24] *Re: Ratios & peering [was: Level 3 Communications Issues Statement Concerning Comcast's Actions], Nanog mailing list archives, November 30, 2010 http://seclists.org/nanog/2010/Nov/1014 (Last accessed March 16, 2017)*

[25] *AOL, Cogent Peering Spat, DSL Reports, December 31, 2002 http://www.dslreports.com/shownews/24809 (Last accessed March 16, 2017)*

[26] *Find Law. For legal professionals http://legalminds.lp.findlaw.com/list/cyberia-l/msg42080.html*

[27] *Stacy Cowley. Level 3, Cogent resolve peering dispute, renew deal, Computerworld, October 28, 2005 http://www.computerworld.com/article/2559599/networking/level-3--cogent-resolve-peering-dispute--renew-deal.html (Last accessed March 16, 2017)*

[28] *Report and order on remand, declaratory ruling, and order, Federal Communications Commission, March 12, 2015 https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf (Last accessed March 16, 2017)*

[29] *Om Malik. The Telia-Cogent Spat Could Ruin the Web For Many, GIGAOM, March 14, 2008 https://gigaom.com/2008/03/14/the-telia-cogent-spat-could-ruin-web-for-many (Last accessed March 16, 2017)*

[30] *Iljitsch Van Beijnum. Cogent picks peering fight with "zombie" Sprint, Ars Technica October 31,2008 https://arstechnica.com/uncategorized/2008/10/cogent-picks-peering-fight-with-zombie-sprint (Last accessed March 16, 2017)*

[31] *Report and order on remand, declaratory ruling, and order, Federal Communications Commission, March 12, 2015 https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf (Last accessed March 16, 2017)*

[32] *The Global License mechanism was first proposed by William Fisher in the paper "Promises to Keep Technology, Law, and the Future of Entertainment", published in the United States in 2004. The idea was rejected in the USA. In 2008 Fisher's paper was translated into Russian. Attempts at incorporating it into Russian legislation were made in 2014 by the Russian Authors' Society.*

CONTROL IS DEAD, LONG LIVE CONTROL

OLEG DEMIDOV,
CONSULTANT AT PIR CENTER.
IN 2012-2014 OLEG RAN THE PIR CENTER'S PROGRAM "GLOBAL INTERNET GOVERNANCE AND INTERNATIONAL INFORMATION SECURITY".

A KEY COMPONENT OF THE IANA FUNCTIONS in terms of maintaining the security, stability, and resilience of the system of unique Internet identifiers is the business process of managing the DNS root zone. For that reason, its reform (as part of the process of IANA functions stewardship transition) is attracting special attention in the Russian technical community and elsewhere. The key actors in this process are as follows:

- Operator of the IANA (Internet Assigned Numbers Authority) function; this role is currently being fulfilled by the ICANN Corporation. The operator receives, reviews, and processes submissions for entering changes in the DNS root zone file; performs technical validation of the submissions; notifies the operators of the fulfillment of their submissions, and enters changes in the WHOIS root database.
- Administrator of the root zone; this role is currently (until the completion of the IANA functions stewardship transition) being fulfilled by the U.S. National Telecommunication and Information Administration (NTIA). The administrator oversees the processes, procedures and policies that are followed by the operator of the IANA functions; authorizes the root zone maintainer to enter changes in the root zone file upon request from Top Level Domain operators; and authorizes the operator of the IANA function to enter changes in the WHOIS database.
- The maintainer of the root zone; this role is currently being fulfilled by Verisign Corporation. The root zone maintainer enters changes into the root zone file, generates an updated version of the file, and uploads the file to the 13 authoritative root zone DNS servers.

Therefore, while the procedural and bureaucratic part of the process is the responsibility of ICANN and the NTIA, the actual technical work is being done by the maintainer, which is Verisign.

Verisign functions in terms of the business process of DNS root zone maintenance were specified in Cooperative Agreement NCR 92-18742[1] between Verisign and the U.S. government (represented by the NTIA). It was signed on January 1, 1993 by the National Scientific Fund (NSF, whose remit under the contract was later taken over by the NTIA) and Network Solutions, Inc. (NSI, acquired in 2000 by Verisign, which thereby became a party to the Agreement). This is how the business process of DNS root zone maintenance – including operations that are Verisign's responsibility – came into being in 1993-2001. During that period, the DNS root zone file was generated on Root Server A, operated then and now by Verisign.

The original version of the article in Russian is published in the thematic issue of e-journal Cyber Pulse № 3 (21) September 2016

In 2001 the business process underwent significant changes. The DNS root zone master server function was transferred from Root Server A to a new hidden distribution master server, also known as the "hidden master". This server is authoritative for the DNS root zone, and there is no Name Server Record for it. The DNS master servers are usually hidden, so this is by no means unique. Be that as it may, in November 2001, the 13 root servers, including the former Master Server A, became secondary authoritative servers. The new master generates the DNS root zone file, which is then uploaded to the 13 root servers. The upload is done every 12 hours, regardless of whether there have been any submissions (received or processed) for changes in the contents of the file in the intervening period.

The fact that Verisign is a commercial company affects the transparency of the business process of DNS root zone maintenance. In terms of fulfilling these functions, Verisign is accountable only to the U.S. government. Details about the work of the master server operated by Verisign are mostly unavailable to interested parties. Maintaining the hidden master should fall under the scope of the amended Cooperative Agreement between Verisign and the NTIA. But the text of the Agreement does not contain any direct mentions of the hidden master; nor does it explain the need for installing such a server instead of the former primary Server A. Further, Verisign's functions as the DNS root zone maintainer are not included on the agenda of the Root Server System Advisory Committee (RSSAC) under ICANN. Establishment of formal relations between ICANN and the root server operators began with the signing in December 2007 of the Mutual Responsibilities Agreement between ICANN and the Internet Systems Consortium[2]. Another RSSAC document, called "Service Expectations of Root Servers", was published as part of that relationship on December 4, 2015[3]. Verisign's only role in that relationship is to operate Root Server A.

As a result, the global Internet community does not have any open information or a clear idea about the business process of root zone maintenance – unlike, for example, the no less important business process of updating the key signing key (KSK) as part of DNS Security Extensions (DNSSEC) process in the DNS root zone. For the latter process, we have very detailed descriptions of the administrative and technical processes, which give us the full picture of the security and resilience procedures, as well as protocols of the KSK update ceremonies[4].

In that context, the insufficient transparency of the root zone maintenance technical procedures and business processes at Verisign is often criticized by the technical community and other stakeholders. In recent years, these criticisms have increasingly focused on the fact that the status of the root zone maintainer functions remained unclear in the context of the IANA functions stewardship transition. Most of the questions about the Verisign business process, however, remain technical rather than organizational or legal, such as:

- What is the software and hardware used to generate the DNS root zone file?
- How does Verisign ensure the security of the root zone file when it uploads it from the hidden master to the secondary authoritative servers?
- Has there been any standardization in ensuring the security, stability and resilience of the hidden master function and the root zone file upload? Which parts of the technical community were involved in that standardization?
- Is the work of the hidden master subject to independent external audit, and if so, who is the auditor?

Outside parties know only parts of the answers to these questions. It is known, for example, that Verisign uses the Transaction SIGnature (TSIG) protocol to secure the upload of the root zone file. TSIG is a network-level protocol that is mostly used in the DNS, and standardized in RFC 2845[5]. In this protocol, shared secret keys and one-directional hashing are used for cryptographically protected authentication of each connection endpoint. In the DNS root server system, a secret TSIG key is generated thrice a year during informal meetings between root server representatives that take place on the sidelines of the Internet Engineering Task Force (IETF)[6].

It is hard to give a substantive answer to many of the questions without being able to observe the business process itself, or without access to its detailed description. For example, is the use of TSIG enough to eliminate the risk of the root zone file being tampered with during the upload from the hidden master? Is the hidden master itself sufficiently secure, and does it have sufficient redundancy to withstand a major security incident, including a targeted external attack (such as an attempt to replace a root zone file with a doctored version during the upload to the operators of the root zone servers)? Technically, it is clear that the Verisign functions should be more transparent, at least to the technical community.

The debate about managing the unique identifiers system in connection with the IANA functions stewardship transition has drawn additional attention to the status of Verisign. In an NTIA statement of March 14, 2014, which was the starting point for the transfer of the U.S. government's coordinating role, the role of the DNS root zone maintainer in the current architecture of managing the unique identifiers was mentioned among other issues that should be resolved as part of the so-called IANA Transition process. The neutral phrasing of the statement did little to hide the obvious message: if the NTIA is withdrawing from the system of relations connected to the IANA functions, then clearly the U.S. Department of Trade should also withdraw from its direct contractual relationship with Verisign. Otherwise, the entire process would be little more than a half-measure because the U.S. government would retain its de facto control of the technical processes in the DNS root zone.

Even more radical ideas have been voiced on the sidelines of various international meetings and discussions. Verisign does not have any exclusive right to fulfil the function of the root zone maintainer, though it does have a wealth of experience in the matter and a well-established business process. Nevertheless, the process itself is not uniquely challenging or resource-intensive; it does not require the development and maintenance of any complex infrastructure. It is in fact quite simple, and requires only a single site (provided that there is adequate redundancy) to run smoothly. It does not have a complex hierarchy of processes; it has very few participants, and it has a bare minimum of the external perimeter that could potentially be used for an external attack. It is, however, critically important for all Internet users, governments, and businesses because it directly underpins the work of the global DNS (though not the work of the Internet as such) – hence the insistent questions being asked about it. In other words, there are many other entities that could do the job equally well.

Representatives of the Russian Internet community have voiced the following two ideas: 1) Verisign functions should be transferred to IANA itself (or rather, to the PTI), thereby removing the unnecessary third party, and 2) Verisign functions should be transferred to a neutral technical entity that is independent from ICANN (unlike the PTI, which is after all an affiliate of the Internet Corporation). Implementing these ideas would be a major step towards the separation of the IANA functions, which has become one of the key principles in the stewardship transition. Possible candidates for the role of the root zone maintainer include RIPE NCC, one of the most active and advanced regional registries. For both of the aforementioned Russian proposals, however, there is an unfortunate reservation: the United States and Verisign itself would never allow them to be implemented. Verisign would be led by purely commercial considerations; being the root zone maintainer is a major symbolic and reputational asset. The U.S. government, for its part, would not allow Verisign functions to be transferred to a foreign entity because it wants any future DNS root zone maintainer to remain in U.S. jurisdiction. It has no interest in launching a garage sale of its supervisory powers, and the Republicans in Congress would surely go berserk at such a turn of events.

After the launch of the IANA functions stewardship transition process in 2014, the root zone maintainer issue somehow fell off the back of the wagon, and up until the second half of 2015, attempts to restart this public discussion at ICANN conferences went for naught. The question was, however, discussed privately between ICANN, the NTIA, and Verisign itself. The decisive factor was probably the pressure put on ICANN by the ICG, which consistently – and fairly – argued that without the NTIA's withdrawal from the root zone maintenance arrangement,

the entire transition process would be pointless. By October 2015, the decision to exclude the NTIA from root zone maintenance and to draw up a new cooperative agreement between ICANN and Verisign had been taken and formulated in an ICANN/Verisign Joint Proposal on root zone administrator functions[7].

The decision was reflected in March 2016 in the final Proposal submitted for the NTIA's consideration by the Coordinating Group for the IANA Functions Stewardship Transition[8]. The Proposal noted that after the completion of the transition, the anticipated agreement between the PTI and the root zone maintainer would be required once the NTIA has withdrawn from the DNS root zone maintenance process. The Proposal also emphasized that the complete and final transition of stewardship would require a revision of the relationship between the current IANA functions operator (ICANN), the current DNS root zone maintainer (Verisign), and the current root zone administrator (the NTIA). The key point here is that the Proposal, which was quickly accepted by the NTIA, stated that before the completion of the IANA functions stewardship transition, ICANN and Verisign should sign a written agreement without the NTIA, and that the agreement should be made available for public review before it enters into force[9].

The draft agreement on DNS Root Zone Maintainer services between the Internet Corporation and Verisign was released for public review on June 29, 2016. In August, the draft Agreement was approved by the ICANN Board. The document specifies the following list of Verisign functions, which is somewhat different from the previous list in terms of its phrasing[10]:

- Perform technical validation of the data received from ICANN as part of the DNS root zone change submission;
- Notify ICANN of whether the submission meets the necessary requirements;
- Edit, generate, sign (using DNSSEC), and publish the new root zone file;
- Notify DNS root server operators of the availability of the new file;
- Serve as the Zone Signing Key (ZSK) operator for the DNS root zone;
- Perform emergency root zone file generation at ICANN request.

Verisign is expected to perform these functions for eight years, for a symbolic remuneration of 300,000 dollars a year, paid by ICANN. Importantly, there is now a clearly defined algorithm for appointing a new root zone maintainer.

Another aspect of the draft Agreement, which is especially interesting in the context of the discussion on whether the U.S. government is genuinely relinquishing control of the unique identifiers system, is contained in Article 8, Paragraph d) of the Agreement (Suspension of Services). Under the terms of that article, Verisign may suspend any of the Services and/or Additional Services, in whole or in part, and/or suspend access to its Root Zone Maintenance System (RZMS, which includes the root zone file upload server and an FTP file server) to comply with applicable U.S. laws. Verisign's right to suspend includes, in each case, only to the extent necessary to comply with such Law:

1. revoking the right of access (License) to Verisign RZMS (ICANN needs that access to supply Service Data in order to authorize its root zone change submissions); suspending or otherwise restricting ICANN's access to the Verisign RZMS;
2. stopping the acceptance of Service Data from ICANN;
3. delaying, denying, deleting, freezing, or transferring the Root Zone File, and
4. taking such other action, all as required to comply with such Law.

This section of the draft Agreement makes it perfectly clear that the NTIA's withdrawal from root zone maintenance will in no way deprive the U.S. government of the legal instruments to re-exert full control of the process, if need be. DNS root maintenance still resides in U.S. jurisdiction.

There is a proviso that Verisign shall notify ICANN in advance of any actions to suspend and/or restrict the provision of root zone maintenance services – unless of course such notification would break the law – and that it shall in any case immediately notify the Internet Corporation after taking such action. That is a small consolation, but better than nothing.

The Agreement is still at the draft stage, and it is not clear when it might be signed and enter into force. This is unlikely to happen simultaneously with the

expiration of the IANA functions stewardship agreement between ICANN and the NTIA. There is no real need for such synchronicity; it would be sufficient for the community to know that the process is ongoing, and will be completed within a reasonable time frame. In theory, the text of the Agreement might yet change, but the discussion is all but closed. Besides, July 5, 2016 marked the successful completion of a 90-day parallel testing of the new DNS management system directly between ICANN and Verisign[11]. This means that the process is at the final stages, and the global technical community will soon have to live with the new arrangement and with the terms stipulated in the approved draft of the Agreement. Consequently, the debate about the role of the U.S. government in DNS root zone management will continue. The change is not revolutionary, and the DNS root management process fully remains in U.S. jurisdiction.

Does that mean that all attempts at transforming that process over the past two years have failed? Not at all. First, the new configuration of the participants in the process and of the parties to the contract makes it possible to address the technical issues described in this article. Transparency and accountability are the key priorities for ICANN in the long-term process of reforming the governance structure of the Internet Corporation. There is a chance that applying those two principles to the work of the root zone maintainer will make its functions more transparent to the community, and help to build confidence in these functions among the community, including foreign (i.e. non-U.S.) stakeholders. Second, a journey of a thousand miles begins with a single step. It is entirely possible that once the proposed Agreement expires in eight years' time, it will not be automatically extended, and the DNS root zone maintainer functions will be transferred to entities residing in non-U.S. jurisdictions. Or maybe nothing of the kind will happen because everyone will be satisfied with the existing arrangement, and no-one will have any problem with Verisign.

REFERENCES

[1] Verisign Cooperative Agreement and all the amendments, NTIA http://www.ntia.doc.gov/page/VeriSign-cooperative-agreement (Last accessed September 1, 2016).

[2] Mutual Responsibilities Agreement (ICANN and ISC), ICANN http://archive.icann.org/en/froot/ICANN-ISC-MRA-26dec07.pdf (Last accessed March 1, 2016).

[3] RSSAC001 Version 1. Service Expectations of Root Servers. An Advisory from the ICANN Root Server System Advisory Committee (RSSAC), 4 December 2015, ICANN https://www.icann.org/en/system/files/files/rssac-001-root-service-expectations-04dec15-en.pdf (Last accessed September 1, 2016).

[4] Root Zone DNSSEC KSK Ceremonies Guide. Root DNSSEC Design Team J. Schlyter, F. Ljunggren, Kirei R. Lamb, ICANN, May 7, 2010 http://www.root-dnssec.org/wp-content/uploads/2010/05/draft-icann-dnssec-ceremonies-01.txt (Last accessed September 1, 2016).

[5] Root KSK Ceremonies, IANA https://www.iana.org/dnssec/ceremonies (Last accessed September 1, 2016).

[6] Secret Key Transaction Authentication for DNS (TSIG), IETF, May 2000 http://tools.ietf.org/html/rfc2845 (Last accessed September 1, 2016).

[7] Andrei Robachevsky. The Internet from the Inside Out. Ecosystem of the Global Network. Moscow: MSK-IX, 2015. – PP. 108-109.

[8] Verisign/ICANN Proposal in Response to NTIA Request Root Zone Administrator Proposal Related to the IANA Functions Stewardship Transition, NTIA https://www.ntia.doc.gov/files/ntia/publications/root_zone_administrator_proposal-relatedtoiana_functionsste-final.pdf (Last accessed September 1, 2016).

[9] Proposal to Transition the Stewardship of the Internet Assigned Numbers Authority (IANA) Functions from the U.S. Commerce Department's National Telecommunications and Information Administration (NTIA) to the Global Multistakeholder Community. IANA Stewardship Transition Coordination Group (ICG), March 2016, P. 6, &X017 https://www.icann.org/en/system/files/files/iana-stewardship-transition-proposal-10mar16-en.pdf (Last accessed September 1, 2016).

[10] Ibid, p. 7-8.

[11] Root Zone Maintainer Service Agreement, ICANN, June 29, 2016 https://www.icann.org/iana_imp_docs/63-root-zone-maintainer-agreement-v-1-0 (Last accessed September 1, 2016).

INTERNET OF THINGS: VIRTUAL BENEFITS, REAL RISKS

ALEXANDRA KULIKOVA,
GLOBAL STAKEHOLDER ENGAGEMENT MANAGER FOR EASTERN EUROPE AND CENTRAL ASIA AT INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS (ICANN). CONSULTANT AT PIR CENTER.

The original version of the article in Russian is published in Security Index Journal 2015 Fall №3.

"The headline I fear is, 100,000 fridges attack Bank of America."
Vint Cerf[1]

THE OCTOBER 21, 2015 version of the family home of Marty McFly (he of the "Back to the Future" fame) looked impressively futuristic 30-odd years ago, when the movie came out. Now that the real October 2015 has come and gone, our homes look positively backward compared to the 1980s vision. Nevertheless, some elements of the *smart home* already exist. Virtual reality is making breakneck progress; it is changing our day-to-day lives and our ideas of what that life should be, blurring the line between *online* and *offline*.

INTERNET OF WHAT?

According to Recommendation ITU-T Y.2060 (06/2012) by the International Telecommunications Union, the Internet of Things (IoT)[2] is defined as a "global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies (ICT)". The concept of IoT was conceived at the Massachusetts Institute of Technology (MIT), where the Auto-ID Center group, founded in 1999, worked on the radio-frequency identification (RFID) and new sensor technologies. Auto-ID Center included experts from seven research institutions on four different continents. It is they who designed the underlying architecture of the future IoT.

A report by *Cisco Internet Business Solutions Group* (IBSG)[3] suggests that the very concept of the IoT emerged when the number of Internet-connected *things*, or devices, surpassed the number of people on the planet. This happened sometime between 2008 and 2009. In 2003, there were 500 million Internet-connected devices in a world of 6.3bn people (0.08 devices per person). By 2010, explosive growth of mobile technology had produced 12.5bn devices in a population of 6.8bn (1.84 devices per person). Of the total population of our planet, only about 2bn are active Internet users, so there were 6.25 Internet-connected devices per active user. In 2010 Cisco specialists predicted that the number of devices would rise to 25 billion by 2015, and 50 billion by 2020.

Gartner[4] offers a somewhat less ambitious projection of 25bn Internet-connected devices by 2020, but does not dispute the sharply upward trend. There is no longer any doubt that the IoT has arrived. It is already altering our ideas of personal and social relations, of business and economics, and of the risks and threats we all have to face. This is a natural result of the rapid rise and spread of ICT, which will attain a whole new level now that the digital divide is closing and the developing countries are also joining the game.

Meanwhile, the evolution of ICT shows no sign of slowing down. In addition to the old and linear user-device relationship, it has produced a new relationship between two or more Internet-connected devices in which the user is the end beneficiary but not an active participant. In other words, the machine-to-machine (M2M) exchange of information in pursuit of some user-defined task is turning the Internet of Things into the Internet of Everything, or the all-encompassing Internet.

In many ways, that process reflects the general post-industrial trend in which the economy of knowledge and the mediatization of social relations with ubiquitous use of ICT reach a whole new level. The new wave of Internet technologies that enable the generation, perception, collection, analysis, and transmission of what is called big data on a massive scale, is changing the information consumption patterns and daily lifestyles of millions of people. It is also shaping their expectations of the future[5]. Back in the 1970s, the Canadian philosopher Marshall MacLuhan described the electronic media (limited to TV and radio in those days) as *an extension of the human nervous system*. One of his key conclusions was that *the medium is the message*; that is, the medium of communication changes man and society in and of itself. That statement is as relevant as ever now that the ICT has penetrated all aspects of our daily lives in the form of billions of various gadgets. Its true essence, however, is probably best applied to the integration of connected devices into a *Network of Networks*, which radically transforms the scale of its impact on human society.

As a result of the growing digitization of the human environment, we now see the emergence of complex local networks of interconnected devices that form a big part of our lives. For example, IDC defines the IoT as a Network of Networks of uniquely identifiable terminals (i.e. things) that interact without human participation through IP connectivity. That ecosystem currently includes devices (including wearables), IoT platforms, servers, security software, industrial process control software, IT services, etc.

The IoT is making inroads in every imaginable sector, such as consumer appliances, the auto industry, healthcare, fashion, transport, road infrastructure, city infrastructure, payment systems, toys, education technologies, weapons, etc. The IoT showcase is wearables such as fitness trackers, as well as augmented reality devices and technologies[6], in which sensors use data about the user's actions and condition to provide relevant visual information or services.

According to *Gartner*[7], about 38 per cent of U.S. consumers have recently used the *virtual assistant* function built into their gadgets. The expectation is that by the end of 2016, two thirds of consumers in the developed world will use virtual assistants on a daily basis. Technologies for automated prediction of the user's requirements based on his or her behavior and location are making rapid progress, and will become increasingly popular as our lives grow ever more hectic.

The Smart Home concept, in which every smart device has its own IP address – including connected electric appliances, cars, hearing aids, and even items of clothing – is a product of scientific discoveries made in the past two decades. This concept is genuinely changing our lives and turning science fiction into reality. In January 2014, Google acquired *Nest*8, a maker of Internet-connected thermostats, for 3.2bn dollars. Nest thermostats are already very popular in the United States and Canada. They not only automate all the processes required to maintain the optimum indoor temperature, but actually study their owner's habits and change the heating or cooling schedules accordingly. Six months after its acquisition by Google, Nest announced the launch of an applied programming interface that enables the makers of various home appliances and other products to make them compatible and interoperable with Nest devices. Unfortunately, it took hackers no

time at all to find a vulnerability in the Nest software, and the system can now be hacked in a matter of minutes. Still, hundreds of other companies are also working on smart home technologies, and the smart home market undoubtedly holds a lot of promise.

NEW ECONOMIC HORIZONS

According to an *International Data Corporation* (IDC)[9] study, the global IoT market will grow at an annualized rate of 16.9% in the coming years, from 655.8bn dollars in 2014 to 1.7 trillion in 2020. The company believes that devices, connectivity, and IT services will account for the bulk of that market (about two-thirds) by 2020, while devices (modules/sensors) alone will represent 31.8% of the total. Over the next five years, platforms developed specially for IoT, applications, and AAS solutions will also increase their market share.

A study by *RAND Europe*[10] estimates the economic potential of IoT at somewhere between 1.4 trillion dollars a year to 14.4 trillion across all sectors. Sales of connected devices are projected to reach 2.5 trillion dollars in 2020. In other words, the IoT market is still nascent, and is projected to grow at a breakneck pace.

Gartner believes that the IoT will have a major impact on the development of new business models, and that it will help to make electronic businesses more effective. The company's recent study[11] has found that businesses and IT specialists have particularly great expectations of the IoT in the manufacturing and retail trade sectors. Another promising area is the use of the IoT for process optimization at the utilities and services companies, in the industrial sector, auto-making, and consumer goods. A case in point is the energy sector, which increasingly relies on sensors and automatic process control systems built into meters, monitoring devices, energy use management systems, etc.

The new opportunities offered by the IoT can transform the existing industrial processes, companies' relations with their consumers, and in the end, our entire day-to-day lives. For now, there are no comprehensive, all-encompassing IoT solutions; we only have individual examples of IoT-driven transformations in individual sectors (health monitoring, wearables, driverless cars, etc.) There is still a lot of mistrust and lack of understanding in the private sector of how exactly each individual business can benefit from the IoT and recoup the cost of implementing these new technologies. Fundamental systemic transformations will probably have to wait for the arrival of a "killer application" or technology that can transform the market on a global scale. It will serve as the first link between the local networks formed by connected devices to perform some specific task or a set of related tasks.

It is safe to say that in five to seven years' time, the IoT will have reached every single sector of the economy and every market. The low cost of sensor technologies might well make other business solutions uncompetitive. The speed of their development and penetration will kill off all the market players who cannot keep up with the trend and are therefore unable to provide the standards of quality and service customers will have come to expect.

Whole businesses built on data are no longer a theoretical proposition; exponential growth of data about users generated by connected devices will make that data the new gold, the new oil, and the new currency of the 21st century – and these are not just punchy metaphors. Information about users has already become an important driver of growth for private businesses. An increase in the amount of that data and a clearer realization of its value by the users will create a new paradigm of managing that information and of the wider social relations. Effective collection, processing, and analysis of the Big Data will be key to the success of many businesses.

The IoT promises to make various business processes more effective – but it may also give rise to new *grey areas.* The replacement of human decision-makers with machines is still at the very early stage, but it is already raising many ethical and economic questions. It is also presenting new challenges in terms of user and data security. For example, a printer that monitors the level of ink in the

cartridge and orders a new cartridge online can make its user's life much simpler. But it also means that the printer must have access to all the required information to have the cartridge bought, delivered and perhaps even installed – such as the geolocation data, bank details, information about the specific type of the device for which the cartridge is being ordered and, indirectly, about how often the user prints pages. Automating all these processes will require all the related data to be gathered, processed, transferred, and probably stored as well – with all the associated risks.

HURDLES ON THE WAY TO UBIQUITOUS IOT

The speed and success of the deployment of IoT technologies, and the integration of these technologies into the modern social and economic architecture will depend on a number of factors. First, it will require a complete transition to the new IPv6 protocol from the old IPv4, which has all but run out of the available IP address blocks[12]. Technically, this transition is complicated by compatibility problems, and the speed of the transition will determine how many unique connected devices will come online in the coming years. For example, the American Registry for Internet Numbers (ARIN) ran out of primary IPv4 address blocks on September 24, 2015, although blocks are still available for sale on the secondary market. Some parts of the world are switching to IPv6 much faster than others. This will undoubtedly affect the speed of IoT penetration and the uniformity of the IoT standards being drawn up.

Another important requirement for a rapid adoption of IoT technologies is standard protocols that enable devices to talk to each other and to the user. Common standard will be especially important in such areas as data management security, data integrity and privacy, and integrity of the entire IoT architecture. If these requirements are met, IoT technologies will attain a whole new level, ushering in a new paradigm of the development of human society. As already mentioned, IoT technologies are spreading into almost every single sphere all at the same time; as a result, there is still no universal standard of communication between the various connected devices and solutions. A number of organizations (IEEE, IETF, ITU, ISO, and others) are already trying to tackle that problem, focusing among other things on developing proper mechanisms for uninterrupted transmission of IPv6 packets in networks of various configurations, the complexity of which is only going to increase over time. For now, however, they have yet to develop a universal set of specifications that could be applied to all the areas where the IoT is or will be used.

In May 2015, the ITU-T Focus Group on Smart Sustainable Cities (FG-SSC)[13] completed its work by releasing 21 reports on IoT specifications. Its mandate has been taken over by the ITU-T SG20 (Study Group 20)[14], which will continue efforts to develop a universal set of requirements for IoT standards, with a primary focus on *smart cities and communities* (SC&C). That, however, is just one of the fragments of the rapidly growing IoT market. It is also worth noting that the lack of universal standards for interoperability between devices in the entire IoT ecosystem is also slowing efforts to develop mechanisms of protecting these devices from malicious external impact.

Nevertheless, there are individual examples of standards being adopted in some specific areas, such as sensor-mediated authentication. The growing number of online services and connected personal devices makes password-based security systems increasingly cumbersome and outdated. Biometric authentication (based on fingerprints, retina scanning, or voice recognition) is regarded as an extremely reliable method of user authentication. In the spring of 2015, Halifax, a British bank, proposed a new authentication technology for its online banking system that is based on the user's electrocardiogram[15], which has a unique signature for every individual and cannot be forged.

Meanwhile, the FIDO (Fast Identity Online)[16] industry alliance, which was launched in 2012 and now brings together more than 100 major companies (including MasterCard, Visa, Google, PayPal, and Bank of America) as well as the German federal agency for information security (a member since October 2015),

is developing specifications that aim to make online communications more secure using biometric technologies and multi-factor authentication (MFA). For example, Apple has been using fingerprint authentication in its smartphones for several years now; fingerprints can also be used for the Apple Pay service. Microsoft joined FIDO in February 2015, when it announced its intention to use FIDO technologies in its new Windows 10 operating system. So essentially, we have a private-sector alliance developing a universal user authentication standard for electronic devices (Universal Authentication Framework (UAF) и Universal Second Factor (U2F)). Given the size of the companies behind the alliance, there is a good chance of FIDO standards gaining widespread adoption, and perhaps even securing a monopoly in the user authentication technology market.

Finally, providing an uninterrupted energy supply for the huge numbers of various electronic devices is a global challenge. It will require new power generation solutions, powerful servers and energy grids, and technologies of protecting them.

So far, the new technological paradigm is still in the early stages of development and scaling up. The turning point was probably the launch of the first iPhone, which revolutionized the smartphone market. It was a perfect example of destructive innovation (a term proposed by Clayton Christensen)[17] that has taken an entire industry to a whole new level while also delivering a devastating blow to some of the successful long-established businesses. The new priority of user-friendliness proved a winning formula at that stage in IT progress. Meanwhile, the growing ubiquity of the Internet has enabled a rapid expansion of the ecosystem of connected devices. The next leap of destructive innovation will probably center on universal standards, enabling all the connected devices that make the Internet of Things to speak the same language, thereby achieving new synergies. This is what the world is gradually moving towards, and this new scale of the IoT promises both a new quality of life and a whole host of new security threats.

WHAT ARE THE RISKS?

The unbelievable new opportunities opened up by the ecosystem of connected devices acting as part of a single network go hand in hand with new risks. Those risks can seriously undermine social and economic progress. What exactly are the risks, and how real are they?

CYBERSECURITY OF EVERYTHING?

As the number of Internet-connected things grows, so does the number of potentially hackable devices. This a natural and inevitable downside of the development of digital society; security measures often struggle to keep up with technological innovation. So, to borrow a phrase coined by Kaspersky Lab, IoT can stand not only for the Internet of Things, but also for the Internet of Threats. The scale of those threats is directly proportionate to the scale of digital progress. According to the insurance giant Lloyds, cyberattacks cost companies around the world 400 billion dollars a year. That figure includes the damage itself and the cost of disruption caused by these attacks. Interestingly, about 90% of cyber insurance is being purchased by U.S. firms[18].

The growing number of connected devices makes it increasingly more difficult to attribute cyberattacks because there is a growing number of hubs through which these attacks (such as anonymized DDoS attacks) can be routed. In other words, it is becoming ever more likely that one of your devices may at some point become an accomplice in a cyberattack, completely unbeknownst to you.

In July 2015, the *Wired* magazine reported[19] that two hackers had demonstrated the possibility of using a software vulnerability called *Zero-day exploit* to take remote control of a Jeep Cherokee after hacking its Internet-connected multimedia system. As the journalist who did the experiment traveled in the hacked car at 70 miles per hour, he watched the hackers remotely change settings on his climate control and radio, turn on windshield wipers, and then cut the transmission. All he could do was hope for the best, unable to control his own vehicle.

That was the first such demonstration. In addition to being great PR for the hackers involved, and an important lesson for Chrysler, it threw into stark relief the *other side* of digital technologies penetrating all spheres of our daily lives – especially in situations where keeping a connected device from running amok can be a matter of life and death. The digital interface of many systems and devices makes them that much easier for the user to operate, but it also makes them vulnerable to cyber-intrusions. The dangers include unauthorized access to user data, corruption of that data, personal data theft, financial theft, acts of sabotage against industrial infrastructure, etc. Finally, enormous opportunities are opening up for cyber-espionage. The amount, topology, and granularity of the data available online hold a great promise of convenience for the end user, but they also raise the prospect of major damage caused by that data falling into the wrong hands.

The deeper IoT technologies penetrate our social and economic systems, bringing together a growing number of key network elements, the more serious the potential consequences of a hacker attack. Hackers breaking into IoT devices that make up an interconnected digital society infrastructure can cause the same kind of trouble as old-school hacking on individual standalone devices – but on a much grander scale. For example, a city running a *smart energy grid* can make huge savings by optimizing energy flows, but it also becomes a vulnerable target for hackers, and a single hacking incident can have catastrophic consequences for the entire grid.

A case in point is the massive blackout in the northeastern United States and Canada[20] in 2003, which left 40 million Americans and 10 million Canadians without electricity, and forced closures of several international airports in both countries. It turned out that the blackout was caused by an error in the software operated by the energy utility FirstEnergy in the state of Ohio. As a result of that error, grid controllers did not react in a timely manner to a short circuit caused by overheated street wires sagging and touching a tree. Had that single short circuit been quickly isolated, the problem would not have cascaded to affect tens of millions of people. It is easy to imagine similar scenarios caused by a malicious act rather than an error – targeting, for example, the monitoring systems of other elements of a smart grid. Incidentally, dangers such as this one are precisely the reason why the control systems at some critical infrastructure facilities (such as nuclear power plants) are deliberately being left stuck in the analogue age instead of upgrading them to new IT technology.

The interdependence of various systems can cause a domino effect, leading to grave consequences, including human casualties. In April 2015, the U.S. Government Accountability Office released a report[21] warning that modern airplanes' connection to the Internet and their growing cyber-reliance on ground systems "can potentially provide unauthorized remote access to aircraft avionics systems". These new interconnected systems installed on the latest planes now require a separate certification process with the Federal Aviation Administration; there are also plans for a complete review of cybersecurity requirements for all avionics systems.

Meanwhile, auto makers are also trying to produce universal standards[22] using the *safety by design* principle, meaning that measures to minimize cyber risks are taken early on during product R&D.

It is safe to say that any projections for the growth of the IoT market must take into account the inevitable cybersecurity incidents that will cost billions. Such incidents are bound to happen because connected products' defenses against cyber-intrusion are often developed after these products hit the shelves. Since the IoT market is still far from maturity, players are trying to seize a share of that market as early as possible. As a result, they tend to shunt aside any concerns that could potentially delay product launch – including cybersecurity concerns. In the future, once the problem of protecting users and their data in the IoT context becomes even more obvious, the market for IoT cybersecurity products will become another major growth driver, spurring fierce competition among the developers of such products.

THE ETHICAL SIDE OF THE COIN: PRIVACY

As we discuss the future of the IoT on the global and local scale – especially in the context of security – let us not forget that the IoT is also increasingly transforming the approaches to online privacy. Debates about the right to privacy (enshrined in such international documents as Article 12 of the UN Universal Declaration of Human Rights[23], Article 8 of the European Convention on Human Rights[24], and Article 17 of the International Covenant on Civil and Political Rights[25]) have become especially relevant after the revelation in the summer of 2013 of mass electronic surveillance by the U.S. National Security Agency (NSA). New opportunities for mass snooping are also being opened by the technology companies that build their business on targeted advertising that is based on information about individual users' activities and preferences. In addition to the personal and communication data that have long been available, companies are now also gaining access to geolocation, biometric, and other information that enables them to build an increasingly accurate portrait of each individual user and his or her daily activities. This opens breathtaking vistas for advertisers and other actors who want to know as much as possible about every specific individual or groups of people, for legitimate or nefarious purposes.

The rise of the IoT takes the privacy problem to a radically new level; attitudes to that problem and approaches to resolving it will vary depending on how well each individual community tolerates mass data gathering. We can assume that the development of IoT technologies will be more rapid in the United States, for reasons of America's historically more liberal attitude to personal data gathering and its lack of a single regulatory instrument in this sphere. Witness, for example, the latest instalment in the old saga of America and the EU trying to harmonize their trade relations and resolve the related issue of personal data transfers across the national borders[26]. Furthermore, the boundary between the public and the private in cyberspace is becoming increasingly blurred as the amount of user data generated, processed, and transmitted online continues to grow; the existing instruments do not fully take this particular circumstance into account.

Nevertheless, even those societies that don't have much of a problem with public availability of online user data will inevitably realize that the user agreement is not entirely fair. How adequate is the price users pay for *free* services such as web search, email boxes, or IoT technologies by surrendering their personal data, which are then used for commercial purposes?

As already mentioned, the scale of this symbiosis will continue to grow, as will the risks related to the leakage or corruption of user data. Meanwhile, the business model itself will continue to develop as more IoT-connected devices become platforms for user data generation. For now, we are talking about anonymized and aggregated data – but personal attribution of such data can easily be restored by comparing various data categories. Besides, as IoT technologies become an ever more ubiquitous part of the basic infrastructure of our daily lives (utilities, healthcare, transport, etc.) it will become increasingly difficult to forego their use. The user still has the right to adjust their privacy settings to their individual liking – but at the cost of losing some of the services. Another alternative is just to decline the user agreement completely.

One of the best examples of this trend is the growing popularity of virtual assistants[27]. Apple launched its Siri assistant back in 2010, complete with such functionality as searching for information, sending text messages, making phone calls, scheduling appointments, and placing online shopping orders by giving voice commands. Siri has since been followed by Google Now, Microsoft's Cortana, Facebook M, and even Duer, developed by China's Baidu. Over time, the convergence of various mobile services will expand the functionality of virtual assistants, and data searches will be performed taking into account everything the virtual assistant already "knows" about its owner.

According to Gartner, 38% of U.S. gadget owners have recently used the virtual assistant function built into these gadgets. The current projection is that by late 2016, about two thirds of users in the developed markets will do so on a daily basis. As big data analysis, voice recognition, and artificial intelligence technologies continue to improve, so will the usefulness of virtual assistants. Also,

as the amount of the information being processed increases, users will be ever more inclined to offload part of their work on a capable electronic assistant. It is, however, important to remember that virtual assistants' independence in decision making, combined with access to user data granted to various applications installed on the user's smartphone, creates a potentially problematic situation with centralizing control over all that data. Centralization always increases a system's vulnerability. For example, a debate is now under way[28] about the Windows 10 operating system's aggressive policies on collecting user data, including data collection by Cortana. According to some reports about the Cortana algorithms, that virtual assistant sends some user data to Microsoft servers even if the user has opted out of using Cortana.

Some of the smart TVs made by Samsung also have built-in voice recognition. The microphone can of course be switched off – but the possibility of it being switched back on again remotely, unbeknownst to the TV's owner, undermines the owner's confidence that they control privacy in their own home.

In this context, the user would be entirely within their right to demand a revision of the whole deal, and a new, more transparent report by communications companies on making user data available to third parties, i.e. their commercial partners, which are usually referred to in user agreements as "trusted third parties". This also has implications for fair competition and equal access to the services of various third parties. Of course, virtual assistants will have an option to default to a specific trusted third party for various user-requested services, unless the user specifies which particular party he wants. For example, if a user asks his or her virtual assistant to call a taxi, it can default to Uber rather than, say, Gett. The user will still be able to make the final decision and choose his or her preferred service provider. Nevertheless, as our lives become more hectic, there will be a growing scope for virtual assistants to make these day-to-day decisions completely on their own.

It is important to understand that we are not just talking about the philosophical issue of finding the right balance between privacy and convenience. This is also about how comfortable users will be with disclosing information about themselves to the outside world without being in full control of where that information ends up, who has access to it, and how it can be used today, tomorrow, or the day after. Unauthorized or uncontrolled access to an individual's medical data gathered by wearables, sensors built into closing, fitness gadgets, etc. – let alone the data and conversations stored on PCs or smartphones – can be misused and abused by insurance companies, employers, business partners, etc. Last year, there was a discussion in the UK about legalizing the sale of patient databases maintained by the NHS (the National Health Service) to pharmaceutical and insurance companies[29] - including such data as ID numbers, birth dates, gender, ethnicity, and postcode – *in order to improve the quality of service*. The measure has not been implemented, but breaches of such data are already a regular occurrence. Meanwhile, the growing number of various user applications that make use of those data increase their vulnerability even further. Intrusions and theft by hackers are also all but inevitable[30].

In a situation where user data is increasingly being seen as the *oil of the 21 century*, or as *new currency*, it becomes blindingly obvious that if you are a being offered a free product, you can be certain that the real product is you. That is why the growing number of *smart device* makers that join the IoT ecosystem will have to build a relationship of trust with their users, with total transparency and detailed reporting about how user data are being used by the company itself and by its partners. Responsibility and diligence in this area will become part of the corporate brand, and data security measures a new way of gaining competitive advantage over rivals. It is quite possible that at some point in the future, industries will develop new best practices by means of self-regulation, in addition to rules introduced in national legislation and regional bylaws.

For example, a growing number of technology companies regularly publish transparency reports[31]. The practice was initiated by Google in 2010: after it withdrew from the Chinese market, it began to publish statistics on national governments' requests for disclosure of user data or for the blocking of various

content. In 2013, Edward Snowden's revelations about the use of IT companies by the secret services for electronic snooping gave a fresh impetus to the practice of transparency reporting; by that time, such reports were being published on a regular basis by at least 10 major IT companies. In an effort to reassure their users, a growing number of companies are now following the example set by Google. In the future, law-enforcement and security agencies will undoubtedly send their user data requests to more companies; there will also be more of the various data to request. As for the transparency reports, they should also include information about the nature of the relationship with *trusted third parties* – that is, commercial partners. At this time, transparency reports do not normally specify the precise information that has been requested by governments. But as the amount and the granularity of the data increases, companies will inevitably have to think about improving the procedures of reporting both to the governments and to their own users.

Another promising area is the use of open data, platforms, and standards, which would make less relevant the problem of finding the right balance between profit and privacy.

WHO IS TO BLAME?

Another important question without an obvious answer is who (or what) is responsible for any incidents involving smart devices, and for the resulting damage. If a device has elements of artificial intelligence and makes independent decisions, should it also be held responsible for the consequences? Operator-independent M2M communications, in which decision-making is delegated to machines, blur the boundary between the *actor* and its *instrument*[32]. Who or what exactly is the actor, and who has agency: the human operator that delegates decisions on replacing a spare part to the machine, or the machine itself, which supplies the human operator's bank details to an unreliable online shop that sells the spare part? Insurance companies will have a particular interest in finding the right answer to that question.

Furthermore, the aforementioned problem of user data being generated and transferred by smart devices to third parties will become especially pressing as devices become increasingly interconnected, with instantaneous data processing and exchange. Which particular device (or devices) has "ownership" of the data, and which device is responsible for the security and integrity of that data?

RULES OF THE GAME

There are now many more questions than answers because the body of regulations for managing and minimizing all the existing risks has yet to be put in place. Some countries, such as the United States and South Korea, deliberately pursue a policy of regulatory nonintervention while the companies are fighting to secure a share of the IoT market, and while the direction of the IoT industry's technological and economic development remains unclear. This is recognized in a June 2015 ITU report[33] in IoT regulation. There are many uncoordinated studies and regional attempts at channeling the development of the IoT, or at least getting a clearer idea of the potential challenges. The problem is that, as in the rest of the IT industry, regulatory efforts often fall well behind the already available technology and products. Also, the steps being taken are sometimes mutually contradictory. For example, at a conference held in March 2015 in Brussels by the European Commission, technological companies discussed the need for lifting the obstacles to the development of the IoT in Europe, especially in view of the fierce competition from U.S. and Chinese rivals. Europe's high Internet penetration rates and the EU's Digital Single Market program can stimulate the development of IoT technologies. But at the same time, Europe has such clear obstacles as the already mentioned differences over the protection of personal data when it crosses the national borders.

The United States is investing huge resources into the IoT – but these efforts are being held back by the poor penetration rates, low speeds, and high cost of broad-

band Internet access in the country. The Federal Trade Commission has recommended that the government desist from any direct IoT regulation – probably in the hope of facilitating rapid technological progress without any restrictions. Nevertheless, various government agencies are well aware of the existing and potential risks. For example, the FBI has issued guidelines on managing new cybercrime risks arising from the spread of IoT technologies[34]. As already mentioned, the lack of universal and global IoT standards is holding back the entire industry. Still, the private sector is pinning great hopes on the IoT. For example, in the spring of 2015, IBM announced an investment of 3bn dollars into its new IoT division. Awareness of the standardization problem is also encouraging private companies to seek cooperation and coordination in order to optimize their business processes.

In 2014, the Internet and technology giants IBM, Cisco, General Electric, Intel, and AT&T formed the Industrial Internet Consortium[35] to facilitate the development of engineering standards for industrial IoT devices, share best practice, test new products, and coordinate research in the area of safety and security of new technologies. The consortium has since been joined by numerous large and small companies, research centers and universities, and government organizations. The IIC includes a separate Security Working Group[36].

China is one of the leading players in the IoT field. In fact, it invests more into this sector than either Europe or the United States. According to RAND Europe, in 2012 the Chinese spent 625m dollars on developing IoT technologies. The Chinese Ministry of Information and Technologies has also set up a 775m-dollar fund to create techno parks all over the county over a five-year period. In 2013, the Chinese government established an inter-agency council for coordinating government policy and initiatives on the IoT[37]. In 2013 the council contributed to a new government directive and working plan for IoT development, with specific goals for the development, standardization, application, and rollout of products, business modeling, regulation, and training.

For the time being, however, the size of the Chinese market is way ahead of its consumer maturity. There is also a huge potential in the entire Asia Pacific Region, where the most mature markets in terms of the per capita numbers of connected devices are Australia, New Zealand, and South Korea. According to the research company IDC[38], the IoT market in the AsPac region (excluding Japan) will grow from 250bn dollars in 2013 to 583bn in 2020. The number of connected devices in the entire region is projected to rise from 2.59bn in 2013 to 8.98bn in 2020. Nevertheless, this market is still in the early stages of its development, and the makers of smart devices are not focusing on the existing and future security threats because such a focus would inevitably increase their development, manufacturing, and distribution costs. Still, many large companies with a strong presence in the region[39] – such as Cisco Systems, Fortinet, and Check Point – are already well aware that the issue must be addressed without delay, so that the development of their future products could take into account certification requirements and other regulatory compliance issues. So far, there is no clear set of rules or procedures in this area.

In Russia, the consumer IoT market is being formed predominantly by foreign gadget makers, but in view of the recent import substitution trend, there is now more emphasis on domestic R&D. The broadband penetration rates in Russia are fairly high, so the outlook for the IoT market is positive. Unsurprisingly, Rostelecom[40], the country's largest telecommunications operator, is one of Russia's IoT pioneers. It plans to make a major contribution to structuring the national market for the industrial IoT. To that end, it wants to borrow the experience of the aforementioned Industrial Internet Consortium, which it has joined in order to gain access to case studies, research, and emerging standards. There are now plans for setting up a Russian equivalent of the IIC, called Association for Facilitating the Development of the Industrial Internet in Russia. The body should be up and running by the end of 2016. Growth opportunities in the various Russian industries and the potential for their integration on the huge Russian market promise great economies of scale. Rostelecom expects that industrial companies will be the first to join the new Association, followed by the suppliers of technological solutions and expert groups. For example, a preliminary agreement has already been

reached with the Russian Space Systems (RKS) on the use of industrial Internet technologies in the space industry.

These efforts undertaken by a single Russian company are clearly inadequate in view of the size of the Russian market; nevertheless, they are timely and very important. The Internet of Things, including the Industrial Internet, is one of those areas of global development where the rules of the game are being written and the roles are being distributed right at this moment. Russia has a great opportunity not to miss out on this latest spurt of technological progress, and to become an important player at least in some of the most promising markets, both local and perhaps even global, before foreign companies irreversibly seize the initiative. These markets include the defense industry, the financial sector, transport, etc. The ongoing crisis in the global economy and the local Russian trend towards import substitution create a favorable climate for achieving such a goal. For now, Russia does not have an extensive toolkit of regulatory instruments for the IoT industry – but its government is making a strong emphasis on protecting personal data of Russian citizens (a case in point is Law 242-FZ, under which all personal data of Russian citizens must be stored on servers in Russian territory from September 1, 2015). That emphasis will make a strong contribution to the development of the IoT ecosystem, especially in terms of security.

The security aspects of the development of the industrial IoT will inevitably be discussed in the context of international cooperation on responsible conduct in cyberspace. The voluntary code of conduct agreed by the UN Group of Governmental Experts in the summer of 2015 includes not attacking critical infrastructure facilities and not implanting malicious software functionality into IT products. There is also a whole range of confidence-building measures such as exchange of information about the existing vulnerabilities and risks, providing assistance to CERT/CSIRT rapid response groups, etc. If these agreed measures were to be fully implemented, the development of the industrial IoT in countries around the world could be underpinned by reliable cybersecurity arrangements agreed at the highest level. But despite that trend towards internationally agreed rules of the game in terms of nation-states' conduct in cyberspace, the degree of mutual confidence on the global arena is still insufficient for these rules to be always observed.

On the lower level of user devices, one of the major risks is the ongoing debate about the need to weaken end-to-end data encryption in communication products in order to facilitate the work of law-enforcement and security agencies' investigators. Such a possibility is already being discussed in the United States and the United Kingdom. If these two countries implement such proposals, other governments will follow suit. Experts believe, however, that effective data encryption can either be secure for all – including criminal actors – or insecure for all. The public debate is still ongoing, and its outcome will largely determine the level of user confidence in new IoT products. Still, in countries where the public has a fairly high level of confidence in their government as the guarantor of national, public, and individual security, this problem may never fully arise.

CONCLUSION

The Internet of Things is at a very interesting phase in its development. Its social and economic potential to change people's lives in many different areas has already been realized (though perhaps not fully). Countries and companies around the world have also become aware of the need to seize a dominant position in the process of IoT development and thus secure a head start for themselves before the competition begins in earnest. Finally, the regulatory framework is only just taking shape and remains quite flexible, leaving a lot of room for innovation and competitive struggle.

It is also clear that the security risks that have already come to the fore are holding back the development of the IoT market; on the other hand, they also open up a competitive niche. The leaders of that market realize the need to take

security into account at the very early stages of R&D, even universal standards of device interaction or device/user security become available.

We can expect continued efforts at establishing common sets of rules and procedures for the IoT both by the industry itself and by government regulators – though the latter will probably tend to lag behind industry development. Success in finding the right balance between being the first to market and ensuring proper security measures will mostly depend on the expected social and economic benefit of IoT technologies in each individual society and market, and on the public's expectations in terms of security provisions. It will also depend on the willingness and readiness of specialists in different industries, business leaders, and IT developers on the one hand, and cybersecurity / information security specialists on the other, to arrive at joint technological solutions. Any regulatory decisions must facilitate that dialogue. The result of it will determine whether the IoT will come to be the Internet of Things, or the Internet of Threats.

REFERENCES

[1] *Vice President of Goggle and one of the Internet pioneers.*

[2] *ITU-T Recommendation Y.2060 http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060 (Last accessed October 11, 2015)*

[3] *Cisco Systems report "How the Next Evolution of the Internet Is Changing Everything" http://postscapes.com/cisco-internet-of-things-white-paper-how-the-next-evolution-of-the-internet-is-changing-everything%20 (Last accessed October 11, 2015)*

[4] *The Internet of Things Is a Revolution Waiting to Happen, interview with Jim Tully, Vice President of Gartner http://www.gartner.com/smarterwithgartner/the-internet-of-things-is-a-revolution-waiting-to-happen/?cm_mmc=social-_-rm-_-gart-_-swg (Last accessed October 11, 2015)*

[5] *Lecture by Marshall MacLuhan, "Medium in the message", June 27, 1977, given in Australia. http://www.youtube.com/watch?v=ImaH51F4HBw (Last accessed October 11, 2015)*

[6] *Augmented reality: a space between reality and virtual space*

[7] *The software secretaries, The Economist, September 12, 2015 http://www.economist.com/news/business-and-finance/21664071-technology-firms-are-competing-become-consumers-personal-secretaries-big-implications (Last accessed October 11, 2015)*

[8] *Google Nest, https://nest.com (Last accessed October 11, 2015)*

[9] *Explosive Internet of Things Spending to Reach $1.7 Trillion in 2020, IDC http://www.idc.com/getdoc.jsp?containerId=prUS25658015 (Last accessed October 11, 2015)*

[10] *Europe's Policy Options for a Dynamic and Trustworthy Development of the Internet of things, RAND Corporation http://www.rand.org/pubs/research_reports/RR356.html (Last accessed October 11, 2015)*

[11] *The Internet of things is a Revolution Waiting to Happen, Gartner http://www.gartner.com/smarterwithgartner/the-internet-of-things-is-a-revolution-waiting-to-happen/?cm_mmc=social-_-rm-_-gart-_-swg (Last accessed October 11, 2015)*

[12] *North America is out of IPv4 addresses—for really real this time, Ars Technica http://arstechnica.com/business/2015/09/north-america-is-out-of-ipv4-addresses-for-really-real-this-time (Last accessed October 11, 2015)*

[13] *Internet of Things Global Standards Initiative http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx (Last accessed October 11, 2015)*

[14] *(SC&C) ITU-T Study Group 20 http://www.itu.int/en/ITU-T/about/groups/Pages/sg20.aspx (Last accessed October 11, 2015)*

[15] *Halifax trials heartbeat ID technology for online banking, Guardian, March 13, 2015 http://www.theguardian.com/technology/2015/mar/13/halifax-trials-heartbeat-id-technology-for-online-banking (Last accessed October 11, 2015)*

[16] *FIDO Alliance, https://fidoalliance.org (Last accessed October 11, 2015)*

[17] *Clayton Christensen, professor at Harvard, http://www.claytonchristensen.com/key-concepts (Last accessed October 11, 2015)*

[18] *Stephen Gandel. Lloyd's CEO: Cyber attacks cost companies $400 billion every year, Fortune, January 23, 2015 http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds (Last accessed October 11, 2015)*

[19] *Andy Greenberg. Hackers Remotely Kill a Jeep on the Highway - With Me In It, Wired, July 21, 2015 http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway (Last accessed October 11, 2015)*

[20] *Blackout hits New York City and the Northeast in 2003, New York Daily News, August 13, 2015 http://www.nydailynews.com/news/national/blackout-hits-northeast-united-states-2003-article-1.2322074 (Last ac-*

cessed October 11, 2015)

[21] FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen, Report by the U.S. Government Accountability Office. April 14, 2015 http://www.gao.gov/products/GAO-15-370 (Last accessed October 11, 2015)

[22] Five Star Automotive Cyber Safety Program, Cavalry https://www.iamthecavalry.org/domains/automotive/5star (Last accessed October 11, 2015)

[23] UN Universal Declaration of Human Rights http://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml (Last accessed October 11, 2015)

[24] European Convention on Human Rights http://www.echr.coe.int/Documents/Convention_RUS.pdf (Last accessed October 11, 2015)

[25] International Covenant on Civil and Political Rights http://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml (Last accessed October 11, 2015)

[26] Article 25 (1) of Directive 95/46/EC stipulates that the Member States shall provide that the transfer to a third country of personal data is allowed only if the third country in question ensures an adequate level of protection. In terms of the European legislation, the United States is not considered to be a country where adequate level of protection is ensured. For the purposes of harmonization, the EU has created a mechanism of approval by international corporations of special universal corporate rules for data processing (Binding Corporate Rules, Article 26 (2) of Directive 95/46/EC), and agreed special principles that enable data transfer for individual companies (more than 4,000 of them) (Safe Harbor – EU Commission Decision No 2000/520/E of July 26, 2000). Edward Snowden's disclosures have shown that this mechanism does not ensure adequate data protection. Work is currently under way on new EU personal data protection regulations, which should include a general principle whereby the provisions on the transfer of data to third countries or international organizations should also be applied to any subsequent transfers of personal data from such third parties to other entities (Article 40 of the draft regulation). There are also plans for the abolition or revision of the Safe Harbor mechanism. On October 6, 2015, the European Court ruled that Safe Harbor is illegal and should not prevent EU member states from protecting their citizens' right to privacy, and that EU members should have the power to block the transfer of their citizens' personal data to third countries where necessary.

[27] The software secretaries, The Economist, September 12, 2015 http://www.economist.com/news/business-and-finance/21664071-technology-firms-are-competing-become-consumers-personal-secretaries-big-implications (Last accessed October 11, 2015)

[28] Alexandra Kulikova. Windows 10: Farewell to Privacy, Forbes (Russian edition), August 26, 2015 http://www.forbes.ru/mneniya-column/idei/297823-windows-10-proshchanie-s-privatnostyu (Last accessed October 11, 2015)

[29] Randeep Ramesh. NHS patient data to be made available for sale to drug and insurance firms, The Guardian, January 19, 2014 http://www.theguardian.com/society/2014/jan/19/nhs-patient-data-available-companies-buy (Last accessed October 11, 2015)

[30] Kris Simmons. NHS-accredited health apps vulnerable to hacking, CelebCafe, September 25, 2015 http://celebcafe.org/nhs-accredited-health-apps-vulnerable-to-hacking-2120 (Last accessed October 11, 2015)

[31] Alexandra Kulikova. Transparency reporting and confidentiality policies of ICT corporations before and after Snowden, Puls Kibermira electronic journal by PIR Center, No 1 (108), 2014

[32] Agency in the Internet of Things, European Commission report, 2013 https://ec.europa.eu/jrc/sites/default/files/lbna26459enn.pdf (Last accessed October 11, 2015)

[33] Regulation and the Internet of Things, GSR discussion paper https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/GSR_DiscussionPaper_IoT.pdf (Last accessed 11.10.2015)

[34] Internet of things poses opportunities for cybercrime, Federal Bureau of Investigations, September 10, 2015 https://www.ic3.gov/media/2015/150910.aspx (Last accessed October 11, 2015)

[35] Industrial Internet Consortium, http://www.industrialinternetconsortium.org (Last accessed October 11, 2015)

[36] Security Working Group, Industrial Internet Consortium, http://www.industrialinternetconsortium.org/wc-security.htm (Last accessed October 11, 2015)

[37] How China is Scaling the Internet of Things, GSMA report, July 2015 http://www.gsma.com/newsroom/wp-content/uploads/16531-china-iot-report-lr.pdf (Last accessed October 11, 2015)

[38] Asia/Pacific Becomes the Frontline for IoT, with Industry to Connect 8.6 Billion Things and Create an USD583 Billion Market Opportunity by 2020, IDC, press release of April 9, 2015 http://www.idc.com/getdoc.jsp?containerId=prHK25553415 (Last accessed October 11, 2015)

[39] Eileen Yu. Certification, regulation needed to secure IoT devices, ZD-Net, May 21, 2015 http://www.zdnet.com/article/certification-regulations-needed-to-secure-iot-devices (Last accessed October 11, 2015)

[40] Marina Chernetsova. "In another year's time, it will be too late to build the Russian Industrial Internet", interview with B. Glazkov, Rostelecom, TheRuNet, October 9, 2015 http://www.therunet.com/interviews/4945-cherez-god-stroit-rossiyskiy-promyshlennyy-internet-budet-uzhe-pozdno (Last accessed October 11, 2015)

ACCUSATIONS OF CYBERATTACKS: THE FACTS TO KEEP IN MIND

ANALYSIS OF THE JOINT STATEMENT BY THE U.S. DEPARTMENT OF HOMELAND SECURITY AND THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE ACCUSING THE RUSSIAN GOVERNMENT OF DIRECTING CYBERATTACKS AGAINST U.S. POLITICAL ENTITIES

ALEXEY LUKATSKY,
BUSINESS CONSULTANT ON INFORMATION SECURITY AT CISCO SYSTEMS, MEMBER OF THE PIR CENTER ADVISORY BOARD AND WORKING GROUP ON INTERNATIONAL INFORMATION SECURITY AND GLOBAL INTERNET GOVERNANCE

The original Russian-language version of the article is published the Russian Confidential monthly bulletin Issue № 7 (235), vol.15. 2016

OVER THE PAST FEW MONTHS RUSSIA HAS SEEN A GROWING TIDE OF ACCUSATIONS OF MOUNTING CYBERATTACKS against other countries. According to some U.S. politicians and media outlets, pro-Kremlin hackers are behind some of the most high-profile attacks, including the ones that targeted the Democratic Party, the WADA anti-doping agency, the U.S. national media, and election websites of several U.S. states. Even the recent leak of the NSA cyber weapons archive has been ascribed to Russian cyber criminals allegedly directed by the Kremlin. The U.S. Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (USIC) have felt compelled to make a statement officially accusing the Russian government of directing cyberattacks against U.S. political entities[1]. Up until that moment, only China and North Korea had been "honored" in such a way. Let us therefore look at whether the statement by the U.S. secret services is grounded in facts, or whether it merely reflects a political and geopolitical struggle in the United States itself and in the global arena.

According to the U.S. statement, there were two parties to the hacking incidents: the United States was the victim, and Russia was the aggressor. How accurate is such a description? When talking about weapons in the material world – i.e. nuclear warheads in their silos, military units at their bases, plane squadrons or naval fleets – it is quite clear who controls them. A naval fleet cannot be assembled by some oligarch, and no amateur can build a nuclear missile silo. The situation becomes very different, however, when talking of cyber threats. Technically speaking, the cyberattacks against the United States could have been launched

from Russia, from the United States itself, or from any other country that wanted to frame Russia and to see it accused of unfriendly actions against America. All that was needed for such a frame was to lease a server at any of the numerous Russian data processing centers. Or, even simpler, the malefactor could have just hacked a computer at any of the Russian government agencies in order to make them appear the source of the attack.

To speak with certainty about who was behind the cyberattacks against the U.S. governmental and private entities, one needs to look at such attributes of the attacks as their source, their timing, and – most importantly - the attacker's motivation. To ascertain these facts, one needs to collect concrete pieces of evidence – also referred to as indicators – that will point to the perpetrator. These attribution indicators include:

- Registration of the IP address and of the domains either involved in the attack or providing the infrastructure required for the attack. These include not just the country of registration but such information as the owner of the domain or the IP address, and the owner's contact details.
- Tracing of the attack to its source, or at least to the general location of the source. Many of the network devices that underpin the Internet infrastructure have the functionality required for such tracing.
- Timing. Investigators often look at the time and date of the writing of the malicious code, as well as the time when the attack was launched, or when it was at its most active. With some reservations, such information can be used for further analysis. In and of itself, it cannot positively identify the perpetrator, but it can narrow down the list of countries that may have been involved in the attack.
- Analysis of the malicious code itself. The code may contain comments, notes, links to websites, domain names, and IP addresses involved in the attack, as well as information about the operating system in which the code was written, the language of the code, and other regional settings.
- Apart from studying fragments of the code, some researchers also try to identify the "signature" of the code-writers and determine which school of programming they come from, i.e. American, Russian, Chinese, etc.
- Signature analysis is closely linked to the linguistics – or, more precisely, to the stylistic analysis of the text contained in notes, comments, references, etc. It is well-known that depending on the person's national, cultural, and linguistic background he or she will have a different style of writing, which can be identified and pinned down to a certain geographic location.
- The so-called honeypots: this is a once-popular instrument that is now making a comeback. It boils down to creating a fake website specifically designed to attract a cyberattack, whereupon experts study the traces left by the perpetrators.
- Another instrument is classical investigation techniques of the kind we have all read about in crime fiction. These involve undercover agents, infiltrators, supergrasses, and other sources of information that can at the very least narrow down the circle of the potential suspects.
- Analysis of activity on message boards and in social networks.

In some cases the perpetrator can be identified on the basis of the steps he or she takes after the attack – this is the so-called post-factum analysis. Sometimes the hackers boast about the attack or accidentally spill the beans on their social network pages. Sometimes – for example, when the target is a bank – the perpetrators can be traced by following the money. Stolen information often surfaces in the open or invitation-only online auctions and exchanges. Investigators posing as potential buyers can haggle with the seller and use the process to obtain valuable information that can help them to attribute the attack.

The joint statement by the DHS and USIC does not offer any solid proof. It contains only general phrases claiming that the methods and the motivation of the attacks point to Russia, and that the servers used in the attacks belong to a Russian company. Unfortunately, in and of itself, the address used in the attack cannot be regarded as a solid piece of evidence; it does not mean that the owner of the address was the actual perpetrator. The server may have been merely one of the numerous

links in a long chain. It may have been hacked, unbeknownst to its owner. Nevertheless, the various companies that investigated the hacking of the Democratic Party's servers (ThreatConnect, CrowdStrike, Fidelis, Mandiant, and others), build their case against Russia on the one attribute – the ownership of the address used in the attack – that is the easiest to fake. In some cases they even mention the Moscow time zone as evidence of the alleged "Russian trace", forgetting that Russia is spread across nine different time zones, and that (depending on summer or winter time) Moscow itself can be in the same time zone as Turkey, Iraq, and Syria. All three countries have the potential motivation to mount a cyberattack against the United States.

The alleged evidence of the Russian government's complicity in the attacks also leaves much to be desired. For example, this is how the case against the Kremlin was put by The Independent: "*And who was responsible for the leak? Almost certainly, experts say, the Russians, directly or indirectly. For one thing, the Kremlin has a long record in doing this sort of thing, meddling in internal politics across Europe. Back when the DNC hack became public, in mid-June, Russian agents were identified as prime suspects*". And this is what CrowdStrike had to say on the matter: "*Extensive targeting of defense ministries and other military victims has been observed, the profile of which closely mirrors the strategic interests of the Russian government, and may indicate affiliation with the Main Intelligence Department, or GRU, Russia's premier military intelligence service.*" To summarize, Russia's accusers insist that only the Russian secret services, and no-one else, would have an interest in attacking U.S. political and military targets in cyberspace. Unfortunately, neither the IP address tracing, nor linguistic analysis, nor any other technical attributes answer the question of why the attack was launched; all they can do is try to determine the source of the attack. The only instruments that can potentially answer the question "Why?" are analysis of social network activity, post-factum analysis, and the work of agents in the field – all of which take time.

A definitive answer to the question "Why?" may be simply impossible to obtain. There are many reasons for that, including:

- Geopolitics. When somebody wants to portray as certain country as enemy and construct a link between an attack and a certain government, reason and logic are often left by the wayside. Besides, identifying the real source of a complex attack routed via several countries and even several continents requires active cooperation between specialists from different jurisdictions, and from countries that may be at odds with each other.
- Legal framework. Cyberspace is the only one of all the spaces (land, sea, air, and outer space) that is not regulated by any international law. All attempts at cyberspace regulation, as well as efforts to agree at least some kind of voluntary code of conduct, have failed. Another complication is that cyberspace is independent of geography. And unlike the traditional spaces in which warfare is waged, nation-states are not the only recognized actors in cyberspace. There are numerous other actors, such as armed rebels, terrorist groups, and cyber-anarchists. In essence, we are at the threshold of a new technological order, with the entire system of international law undergoing major transformations triggered by the rise of IT.
- Technology. When the protocols that underpin the Internet were being designed back in the 1960s and 1970s, few must have worried about the need for positive identification of every link in the chain that takes a data packet from Point A to Point B. In fact, the entire Internet technology is based on decentralization and distributed architecture. The situation is further compounded by the lack of clear definitions; the absence of generally accepted rules or standards regarding traffic monitoring, accounting and exchange; vast volumes of traffic (resulting in short storage time for digital evidence); and the use of intermediate proxy servers.
- Economic considerations. Neither the telecoms companies, nor the hosting providers or other commercial actors involved in the workings of the Internet are interested in long-term storage of digital evidence, or in conducting proper investigations of cyberattacks that would result in a clear attribution. Their priority is uninterrupted work of all their services, which requires rapid recovery and restoration of their systems to a pre-attack state, usually resulting in the destruction of evidence.

What, then, has been Russia's response to all these charges by the U.S. media and politicians? Russia has chosen an entirely understandable tactic: don't try to explain itself, because that will be just taken as an admission of guilt. There are plenty of specialists in Russia who could conduct the attribution process and form their own opinion as to who was really behind the attacks. Unfortunately, according to Russian Foreign Minister Sergey Lavrov, when Russia asked Washington to exchange relevant information and to let its experts have a look at the evidence allegedly proving its complicity, the United States refused. This may have been because there is no evidence – or perhaps because what evidence there is actually disproves the Americans' version that Russia was the perpetrator. Be that as it may, Russia is currently unable to formulate its own version of what really happened. Unlike the case of the Malaysia Airlines flight shot down over eastern Ukraine (where Russia could present evidence gathered by its own monitoring systems, as well as the results of live experiments) in the case of the cyberattacks Russia simply does not have any such evidence. Given all the aforementioned difficulties of attribution - especially if Russia is telling the truth and the attacks were staged by someone else - such evidence may be available only to the United States.

As we have demonstrated, correctly attributing a cyberattack is a difficult challenge. Also, it is perfectly clear that in the current geopolitical circumstances, certain nations can benefit from accusing other nations of staging attacks, even if those charges are not backed by any solid evidence. There are various instruments that can potentially be used to determine the source of the cyber threats, at least at the country level; these instruments aren't always used, but they are there. Unfortunately, however, we lack the means (excepting perhaps the work of agents in the field) to differentiate between an attack initiated by a state, and an attack perpetrated by a non-state actor.

To conclude, it is worth emphasizing that correct attribution of cyber threats is a very complex challenge. Unlike the traditional threats, in the case of cyber threats we cannot identify the perpetrator or establish the motives for the attack using technical means alone. Also, special operations in cyberspace are often conducted across several jurisdictions, and their investigation requires international cooperation. That cooperation is not always possible in view of the current geopolitical climate, where some nations mistrust each other and resort to trading all kinds of wild accusations.

REFERENCES

[1] *Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security, Department of Homeland Security, October 7, 2016* https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national *(Last accessed March 16, 2017)*

PIR CENTER'S PROGRAM

GLOBAL INTERNET GOVERNANCE AND INTERNATIONAL INFORMATION SECURITY

PIR CENTER IS A PARTNER ORGANIZATION of PIR Press and a leading Russian independent think tank conducting research in the field of global security including the issues of WMD nonproliferation and disarmament, arms control, cyber security, impact of emerging technologies on global security and regional security. PIR Center was established in 1994.

PIR Center launched research in the field of information security and global internet governance in the end of 1990s when these issues just started to evolve in Russia's security agenda. Thus PIR Center became a pioneer in this field; in 2001 a collective monography "Information Challenges to National and International Security" (in Russian) was published, presenting a comprehensive scientific and analytical review of the issues of information security for the first time in Russia. In 2011, PIR Center launched the Program "Global Internet Governance and International Information Security". Within the framework of the Program, the PIR Center regularly organizes expert workshops, roundtables and trainings, publishes research papers and reports as well as e-journal *The Cyber Pulse*. As the Program evolved, the PIR Center has established itself as a leading Russian non-governmental think tank conducting research on ICTs in global security context. The PIR Center has been collaborating with technical actors in Russia and abroad, private companies, think tanks, universities, international nonprofit organizations (ICANN, ICRC) and intergovernmental organizations including the UN bodies (UNIDIR, ITU, ECOSOC). From 1194 the PIR Center (from 2014 its partner PIR Press) publishes Security Index Journal, the Russian journal on international security.

Trialogue Club International, PIR Center's partner from 1994, is a meeting place for diplomats, experts, businessmen, journalists and the source of exclusive information on Russian foreign policy and global security.