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]

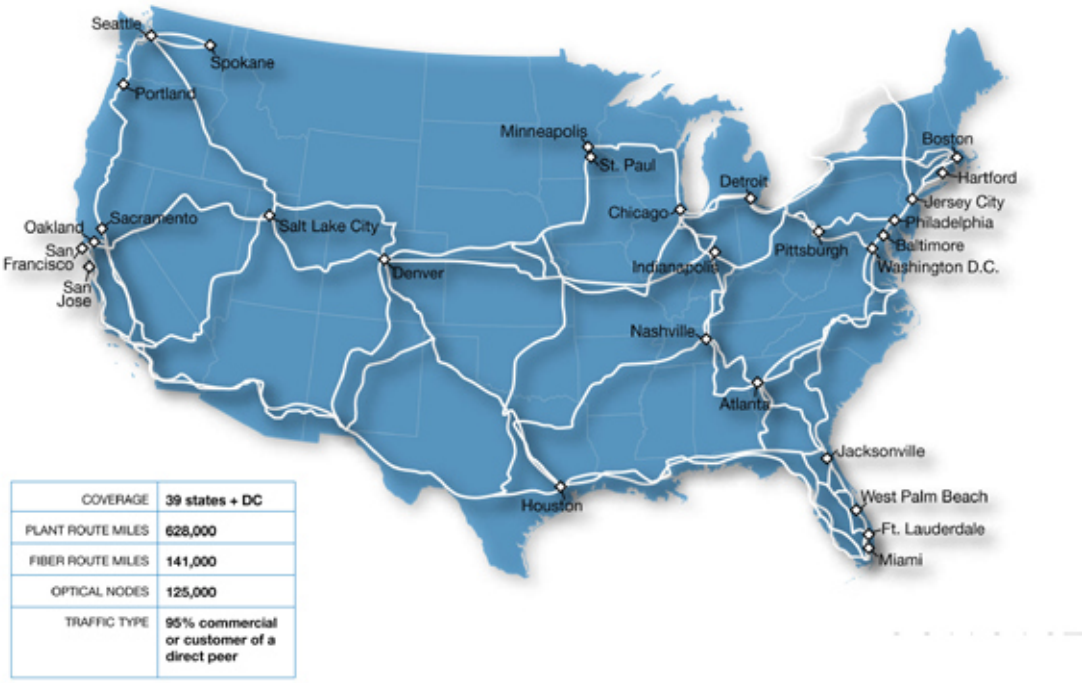


FIGURE 2

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

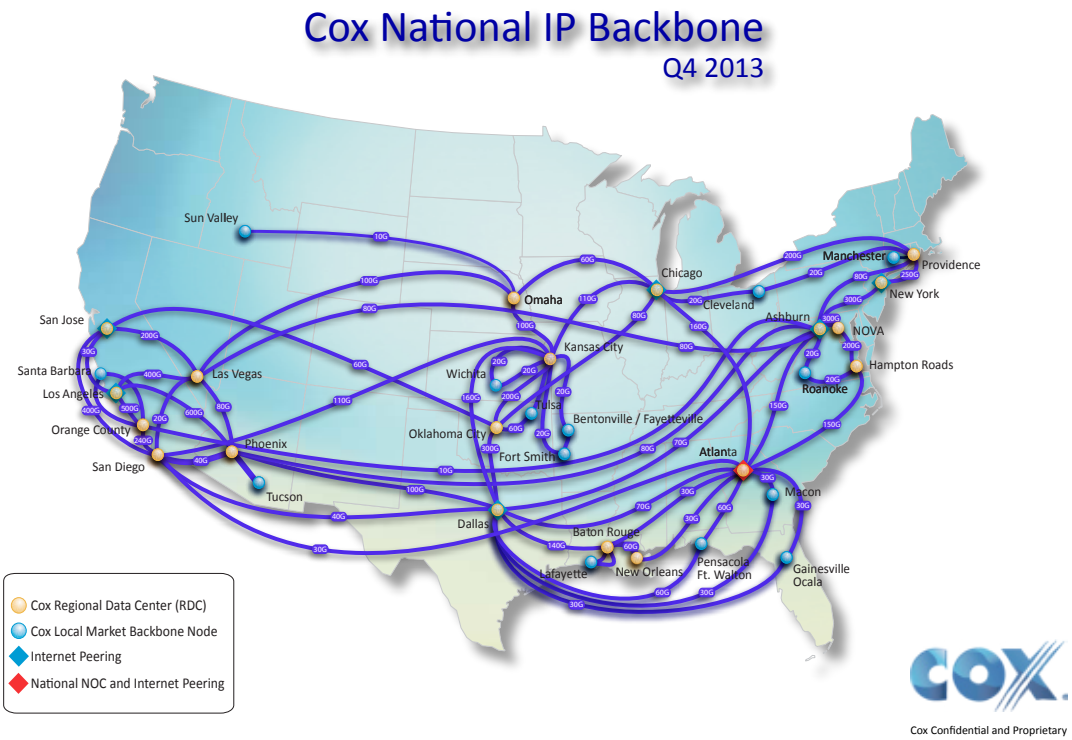


FIGURE 3

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]

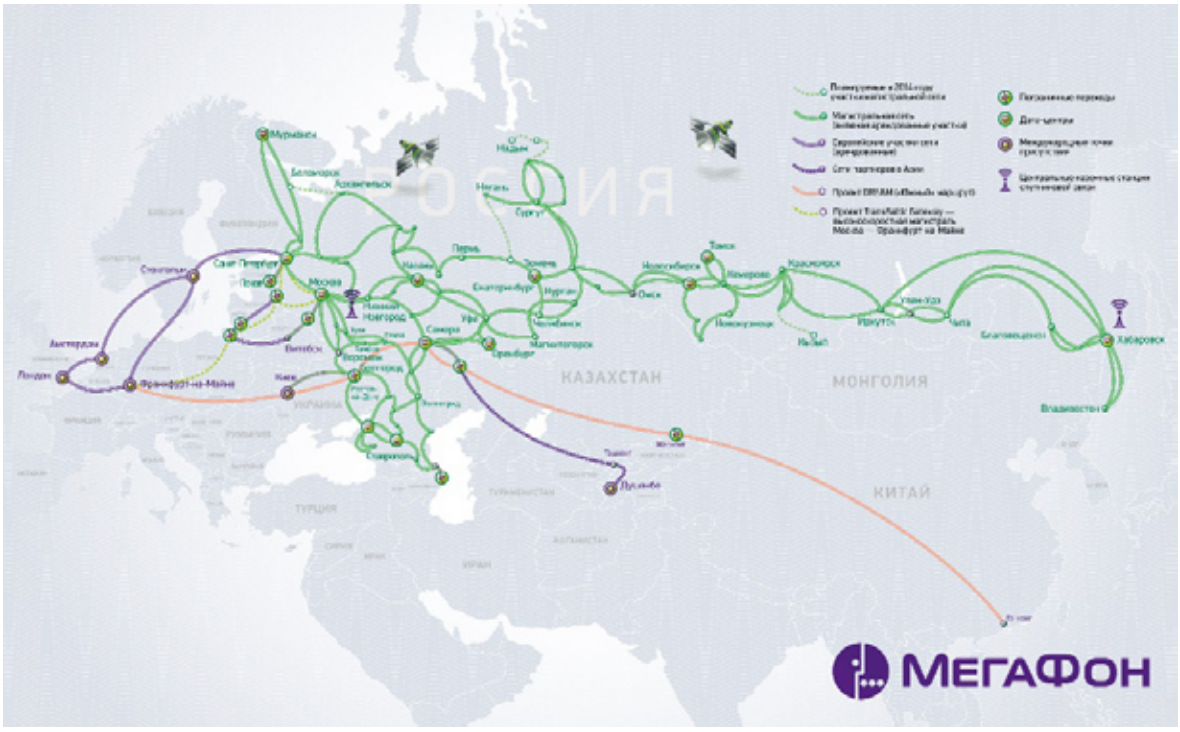
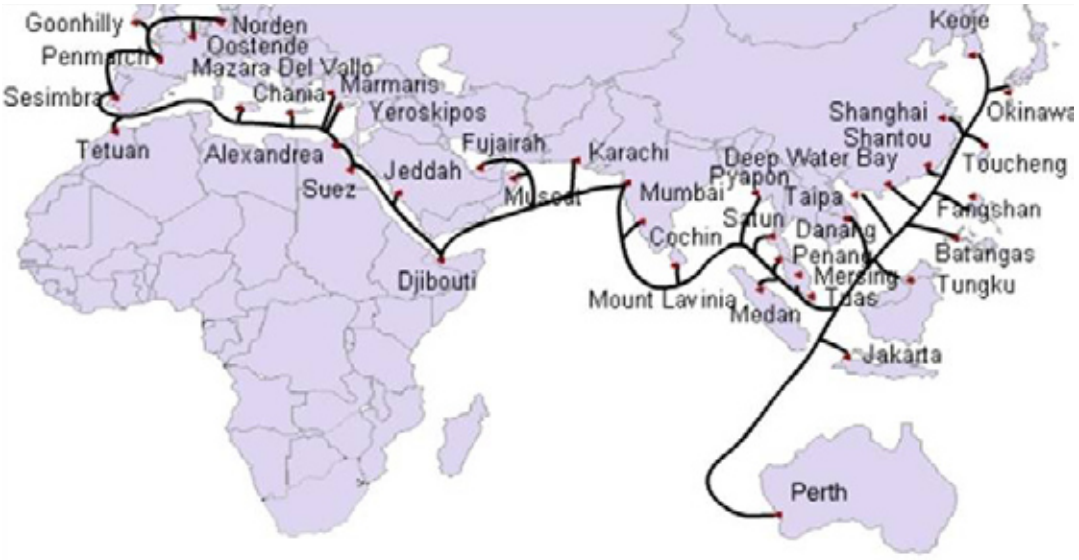


FIGURE 7

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.

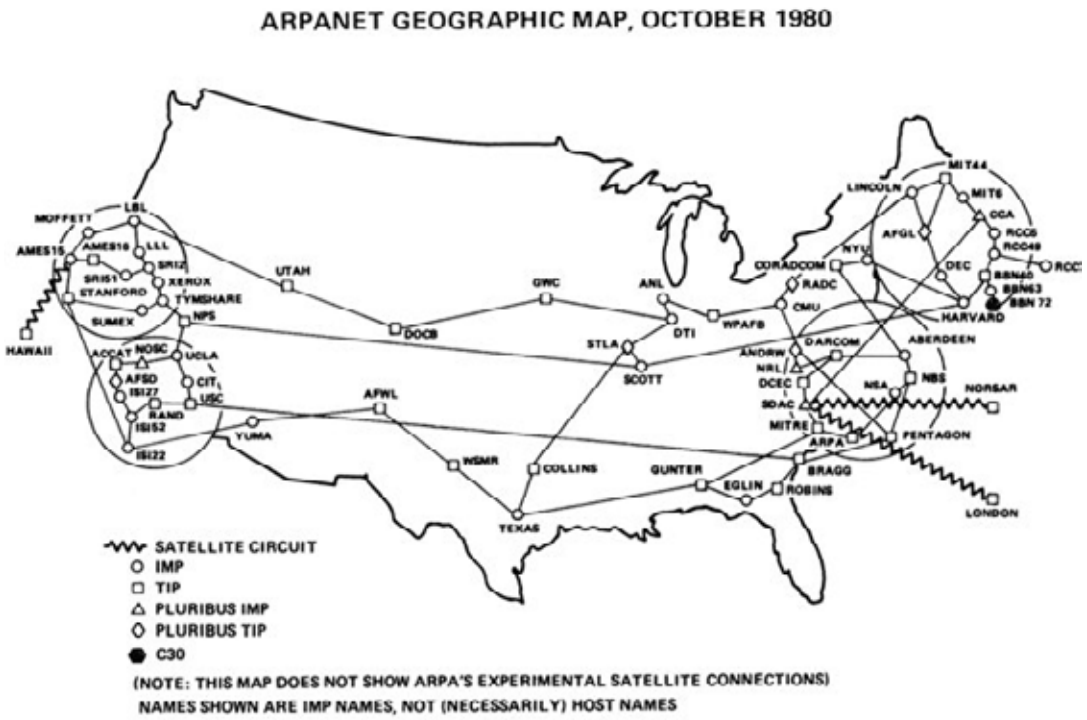
In other words, such outages are especially keenly felt by users in those countries where the national Internet ecosystem is nonexistent. In most cases, however, the Internet has proved fairly resilient to submarine cable outages.

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.

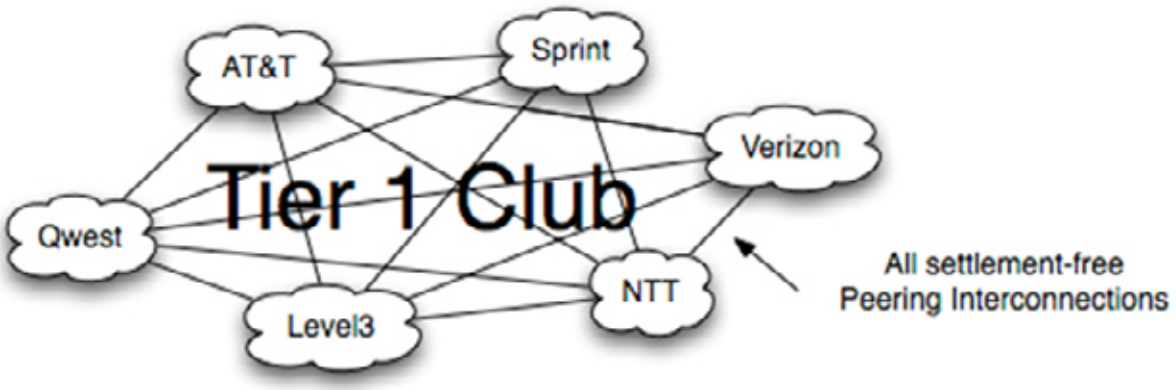
GLOBAL TIER 1 OPERATORS: GLOBAL INTERNET'S FIRST BACKBONE INFRASTRUCTURE

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]

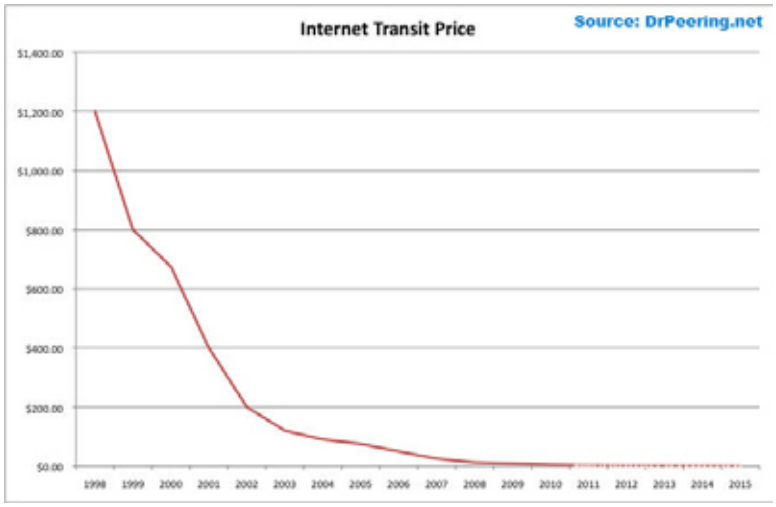
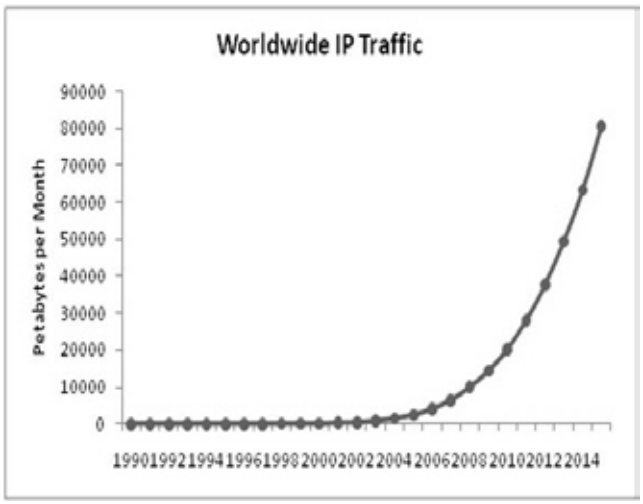


FIGURE 11

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).

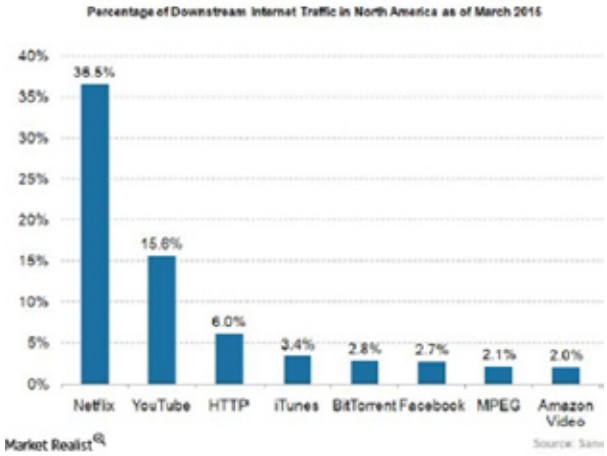
The plummeting IP transit prices forced the global Tier 1s to launch a regional expansion. Their expansion in Europe led to the following trade-off: the global Tier 1s were allowed to do business at the end-user level by granting them access to European infrastructure at the last mile. In exchange, a 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.*