UNCLASSIFIED//FOR OFFICIAL USE ONLY

Show Full Version

Open Source Center

OSC Report: Russia -- Russia Cyber Focus, Issue 9

FEA20100514004965 - OSC Feature - *Russia* -- *OSC Report* 07 May 10

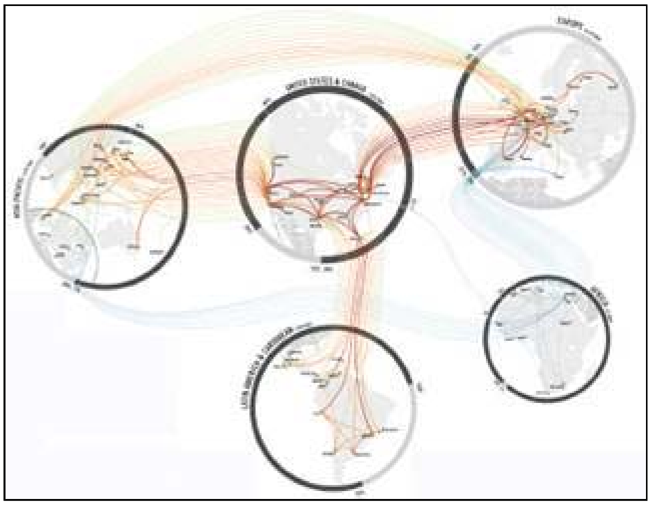
Russia: **Cyber Focus, Issue 9**

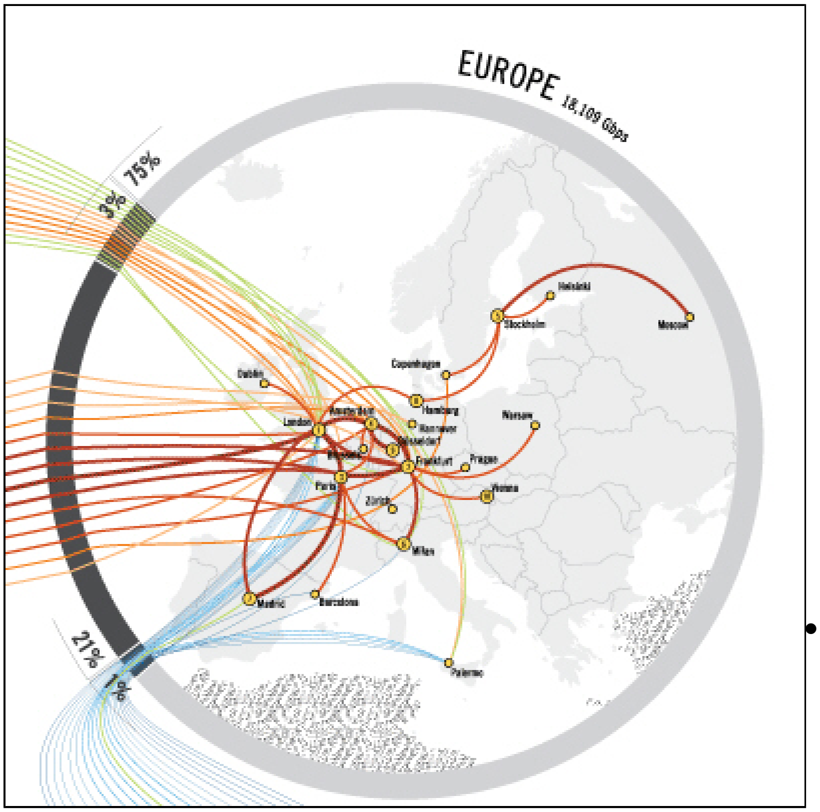
Cyber Focus provides an overview of developments in the Russian-language Internet (or "Runet"). This edition includes the following sections:

1. **Snapshot**
2. **State Censorship & Control**
3. **CyberSecurity**
4. **State Censorship & Control**
5. **Information Operations/Warfare (IO/IW)**
6. **Telecoms & Mobile Telephony**
7. **Social Networks**
8. **Ownership Issues**

Snapshot

Russia Remains Peripheral in Internet Routing





Research by *TeleGeography.com* demonstr
network grid spanning the United States and
remains the backbone of global Internet traf

CyberSecurity

Russian Hacker Claims to Have Stolen 1.
Facebook Passwords

A Russian hacker who offered access to 1.5
accounts and uses the alias *Kirllos*, garnere
coverage from Western media when Verisig
revealed it had observed the hacker in Russ
the accounts for sale (*Infox*, 4 May).

- *Kirllos* posted his offer in Russian on *AntiCh*
hackers and computer security enthusiasts.
the same website hackers posted access de
users of *VKontakte*, a Russian *Facebook* clo
passwords are believed to have been acqui
interactive browser game infected with malic
- The initial post on 1 February included 210 usernames and passwords, which *Kirllos* included "as a freebie for Ac
gave profile details (location and number of friends) of a further 78 accounts, but without passwords. An 8 Februa

"prices start at $8 and end at $30 per 1,000 accounts," depending on country and number of friends.

- *Kirllos* directed potential customers to contact him using his ICQ instant messenger. His account profile suggested he is a 24-year-old male Russian living in New Zealand (ICQ Profile 783464).[2]
- *Kirllos* registered on *AntiChat* on 15 December 2009. He used the same username and ICQ number to register a *WebMoney.ru* account (166862286958) on 8 December 2008. His usernames and numbers appear on various spam sites.

On 4 May New Zealand's National Cyber Crime Centre reported they had traced *Kirllos* to the Russian city of Saransk and notified the Russian police (*New Zealand Herald*, 4 May).

Hacker Imprisoned For Selling Hacking Services to Chechen Extremists

On 9 April Moscow's Kuzminskiy court sentenced hacker Albert Saayev to two years incarceration and a fine of R35,000. His alleged accomplice Oleg Morozov was given a suspended one-year prison sentence. Russia's Prosecutor-General's Office told the court that in 2009 Saayev hacked into the Internet resources of the Chechen and North Caucasus authorities for monetary reward. "Saayev gave unidentified individuals -- clients -- access which he had illegally obtained to the website *chechnyatoday.com*, after which they blocked the website's operation and posted texts on its front page which contained threats addressed to the president of the Chechen Republic." Saayev's clients then claimed responsibility for the attack under the label of "the so-called Ansar cyber subunit of the illegal armed group Imarat Kavkaz (Caucasus Emirate)" on Internet resources controlled by members of illegal armed groups (ITAR-Tass, 9 April).

- After sentencing, Saayev was flown to Chechnya and passed into the care of local penal authorities. Saayev was broadcast on regional television apologizing to President Ramzan Kadyrov (*Gazeta.ru*, 20 April).
- *Kavkazskiy Uzel* reported on 20 April that Saayev "is now kept at the pre-trial detention center in Groznyy and new charges will be brought against him in the coming several days" (NTV, 31 January).
- Anonymous human rights campaigners now fear for the life of Saayev, with one claiming the hacker "just disappeared" and now "nobody knows where he is, what is happening to him, or what awaits him in the future" (*Gazeta.ru*, 20 April).

Blogger Warns of Theoretical PC Virus Injections by Radio

According to an unnamed blogger on Russian telecommunications blog site *Bimchik.ru*, it will soon be possible to inject computer viruses and malware into PCs and networks via a technique dubbed "HF [High Frequency] Overmodulation." The technique would exploit the fact that buses, cables and other conductors in PCs act as resonant antennae that pick up HF signals at certain frequencies. The author claims data embedded in HF signal patterns could pass from resonant conductors into logic and memory devices (*Bimchik.ru*, no date given).

State Censorship & Control

Russian Region Demands Passports for Internet Access

Liberal opposition newspaper *Novaya Gazeta* reported on 21 April that post office branches in the southern Russian district of Krasnodar Kray are demanding to see residents' passports before granting them Internet access, justifying this as an antiterrorist measure. The author expects the regulation will be challenged in court.

Kremlin "Seriously" Considering National Search Engine

On 26 March *RBK Daily* reported that the Russian government is looking very seriously at the possibility of developing a state-sponsored search engine "more oriented towards state needs," an idea first touted by Vladislav Surkov, deputy chief of the presidential staff.

- RBK claims the project, dubbed "*Kremlyandex*," would be entirely owned by Russians, and need a budget of up to $100 million.
- The stated aim of the project's supporters is to "offer access to safe information while filtering sites with illegal content."
- Possible Russian partners named include *Rambler* developer Igor Ashmanov, state communications company Rostelekom, and the developer of ABBYY translation software.

Communications Ministry Seeks Increased SORM Requirements

According to *Kommersant* the Russian Communications Ministry has requested that the IP addresses of Internet users be gathered by SORM (Means/System of Operative Investigative Activities). The decree is in draft form and suggests SORM technology must record and transmit to relevant agencies information on users' IP addresses (15 April).

Information Operations/Warfare (IO/IW)

Russian Security Advisor Acknowledges Cyber Weapon Program

In a recent interview Vladislav Sherstyuk-- retired Russian four-star general, chief of the Institute of Information Security Issues at Moscow State University, and member of Russia's National Security Council -- discussed his perspective on the militarization of cyber attacks.

- Asked whether Russia is developing offensive cyber weapons, Sherstyuk said: "It is not only Russia. It's just the 21st century [...] Today we are talking about information weapons, about cyber weapons, and there is much in common between nuclear and cyber weapons, because cyber weapons can affect a huge amount of people as well as nuclear. But there is one big difference between them. Cyber weapons are very cheap, almost free of charge."
- When asked about Russia's perspective on dealing with cyber crime, Sherstyuk indicated that Russia currently is more worried about the use of the Internet by terrorists to recruit, organize, plan, and execute conventional attacks inside Russia.

Sherstyuk was interviewed while attending a cyber security conference this week in Garmisch-Partenkirchen, Germany. The conference had 160 attendees including researchers and government officials from India, China, Israel, and other nations, including representatives from the US White House and State Department, according to the report (*TechnologyReview.com*, 14 April).

Yevgeniy Kaspersky Warns of "Civil War on the Internet"

In a lengthy interview with the UK-based *PCR Online* magazine, Yevgeniy Kaspersky, the founder of the global Internet security giant Kaspersky Lab, warned that key cybercriminals already have the power to knock an entire country offline. "In the past it was just kids. They were making viruses for fun, and the global economy didn't depend on the internet [...] Now it's totally different, it's not just kids - it's cyber-criminals. There are particular hackers who run international attacks - it's like a civil war on the internet. Governments still don't have strong data, but I would not be surprised if some attacks were managed by governments - it's logical. I'm 90 per cent sure they do it [...] The Internet is not regulated - it's not stable and it's easy to unbalance. In 2003 or 2004 there was an epidemic of an internet worm and South Korea was disconnected from the internet. Three years ago Estonia was disconnected because of a targeted attack. Cyber crimes load on the global economy, I estimate, at least a $100 billion a year." For the full article see *PCR Online* 13 April.

Telecoms & Mobile Telephony

Vympelkom 4G Tests in Kazakhstan

According to *CyberSecurity.ru*, Kar-Tel Ltd, which is a part of the Russian Vympelkom Group and provides telecom services in Kazakhstan under the trademark of Beeline, has successfully tested the LTE-based 4G network in Kazakhstan's two largest cities, Almaty and Astana. Alcatel-Lucent is said to be a primary equipment supplier for the network (26 April).

Synterra Extends Biopassport Contract Despite Losing Tender

Rostelekom, having won the Communications Ministry tender to manage Russia's biopassport system in February, was forced to bring in Synterra as a subcontractor "to ensure continuity of the service." Synterra had managed the biopassport system since 2007. Rostelekom was the only participant in February's tender; Synterra applied but did not transfer a bidding deposit in time (RBK Online, 1 April).

In a further display of Synterra's close links with the Russian government, the company's executives attended the Russian-Uzbek Intergovernmental Commission March 30-31 in Tashkent. The summit brought together Russian Deputy PM Sergey Ivanov, Synterra CEO Vitaliy Slizen, head of the Uzbek Agency for Information and Communications Hakim Mukhitdinov, and the head of Uzbek national operator Uzbektelecom (*Lenta.ru*, 2 April).

Social Networks

VKontakte Continues to Skirt State Control

RBK Daily reported that Russian state prosecutors are examining video hosting practice at VKontakte after they received "many complaints" from users who had seen "nasty videos of a fascist nature and calls for the overthrow of the political system." Citing a source within law enforcement, the website reported that many of the complaints had been from parents who had monitored their children's online activities (21 April).

VKontakte's culpability in these matters depends ultimately on how the state chooses to define social networks. If a website is defined as a "medium of mass information" it must take responsibility for any content it hosts. Social networks have yet to be formally defined in Russian law, and law enforcers tend to target users and use hosted content as evidence. Most recently, in March 2010 St Petersburg police arrested a 25-year-old VKontakte user for disseminating extremist material in Russian and Arabic.

Proliferation of Smaller, Niche Social Networks Continues

While the social network market worldwide tends to be monopolistic, with users generally gravitating towards networks their friends and relatives use, Runet continues to experience a proliferation of smaller social networks aimed at niche communities. Some are simply commercial exercises; others have more political or religious agendas. This could mean that an ever increasing quantity of online content will be closed off from public access by registration requirements on these niche sites.

- Russia's Communication Ministry launched *Regionalochka* (*www.regionalochka.ru*), a social network for "employees of Russia's regional administrations, charged with IT development, administrative reform and transition to providing state and municipal services online." To register, users must provide personal and professional information, which is then checked by regional officials. As of 28 April there were 537 registered users, with Moscow, Kirov Oblast, St Petersburg, Ulyanovsk Oblast, and Nizhniy Novgorod Oblast the regions with most registrations (RIA Novostey, 11 April). *Gzt.ru* reported that current membership includes a number of regional governors (13 April).

- On 8 February Muscovite Igor Gulyev launched *Odnodolshiki* (www.odnodolshiki.ru) ("fellow stakeholders"), a social network for consumers who have been cheated out of money while investing in property developments. The site raised the ire of ruling party United Russia, which claimed the project was failing to make "constructive suggestions" (*The Moscow Times*, 27 April).
- *World-Muslim.com*, a social network for Muslims with a Russian interface was set up in September 2009. The site also offers incomplete English and Turkish language capabilities, and currently claims to have 9,307 registered members.

- Earlier in the year a social network for villagers in the North Caucasus was in the national media spotlight. NTV reported that in Dagestan the website *Odnoselchane.ru* is gaining popularity. The name of the network can be translated as "Fellow Villagers," a play on the more popular Odnoklassniki ("Classmates"). Unlike most social networks, users are grouped by village or town (NTV, 31 January).
- On 31 March *Lenta.ru* reported the launch of *Nuara*, a social network for "vampires...goblins, werewolves, ghouls, monsters, and other mutants." The site is part of the St Petersburg "Multer" company, which publishes fantasy books, cartoons, and online games. As of 6 May the *Nuara* social network currently has 1,457 members.

Ownership

Digital Sky Technologies Buys ICQ

On 28 April Digital Sky Technologies Limited (DST), the largest Internet company in the Russian-speaking and Eastern European markets, announced that it had agreed to acquire instant messaging service ICQ from US firm AOL Inc for $187.5 million.

"The acquisition of ICQ is a strategic enhancement of our business in Russia and Eastern Europe. ICQ's long-standing brand name and its sizeable loyal customer base together represent a very attractive opportunity to further strengthen our position in the region," said Yuriy Milner, Chief Executive Officer of DST (*AOL Corporate*, 28 April).

The move is the latest in DST's rapid expansion into social media, with a portfolio that includes stakes in *Mail.ru*, *Vkontakte*, *Odnoklassniki*, and *Facebook.*

AOL was reportedly approached by six other companies interested in buying ICQ, which has over 40 million Russian users. DST edged out *Rambler*, *Yandex*, *Yahoo!,* Chinese group Tencent Holdings, South African group Naspers, and Czech group Seznam. The deal was ultimately worth less than expected, reputable Russian business daily *Kommersant* had reported sources close to negotiations valuing ICQ at $200-$250 million (15 February). One of DST's main bidding rivals, Tencent Holdings, joined forces by purchasing a 10% stake in DST just two weeks before the conclusion of a deal with AOL (Hong Kong *South China Morning Post*, 14 April).

---

[1] See 14 August OSC Analysis **Hacker Group Released Stolen Vkontakte Account Information** (CEF20090814592001)

[2] An ICQ account registered today will have a nine-digit user number. Older user numbers with five or six digits are seen as prestigious in Russia's Internet subculture, and short ICQ numbers can be bought and sold on popular auction site *Molotok.ru* for hundreds of dollars. [http://molotok.ru/search.php?string=icq&order=pd]

[This item was originally filed as CEP20100507510001]

Submit Review

This OSC product is based exclusively on the content and behavior of selected media and has not been coordinated with other US Government components.

UNCLASSIFIED//FOR OFFICIAL USE ONLY