

The RuNet Generation

An Exploratory Study of the Russian Digital Landscape

October 28, 2011

Authors:

UNICEF New York, Division of Communication, Youth Section
Gerrit Beger, Priscillia Kounkou Hoveyda, Akshay Sinha

Collaborators:

UNICEF Russia, Division of Communication, UNICEF Geneva, Division of Communication
John Budd, Lely Djuhari, Viacheslav Tikhomirov

Contributors:

Daniel Kennedy, Melanie Zuch

Contents

ABSTRACT.....	2
SUMMARY OF FINDINGS.....	2
THE DIGITAL CITIZENSHIP AND SAFETY PROJECT & THE YOUTH SECTION AT UNICEF	2
1. INTRODUCTION.....	4
1.1 Background.....	4
1.2 Objective.....	5
1.3 Methodology.....	5
2. CONTEXT.....	7
2.1 Overview of Russia.....	7
2.2 Selected overview: technological context.....	8
3. OPPORTUNITIES.....	10
3.1 Digital access.....	10
3.2 Digital activities.....	11
3.2.1. Communication activities.....	11
3.2.2. User generated content: blogging.....	13
3.2.3. Commercial.....	14
4. IDENTIFYING SAFETY RISKS.....	14
4.1 The risks.....	15
4.1.1. Malicious software and fraud.....	15
4.1.2. Exposure to adult content and child abuse images.....	16
4.1.3. Exposure to extremist content.....	17
4.1.4. Sharing of personal information.....	17
4.1.5. Cyberbullying.....	17
4.1.6. Meeting strangers.....	19
5. MONITORING THE RUNET.....	20
6. LIMITATIONS AND SUGGESTIONS FOR FURTHER RESEARCH.....	21
7. CONCLUSION.....	22
GLOSSARY.....	23

ABSTRACT

This exploratory paper is part of a series examining the role of Internet in the lives of youth living in the Central and Eastern Europe Commonwealth of Independent States. This report focuses on Russia and bases itself on secondary evidence gathered through a desk review of reliable studies and hard data. The first section describes the technological reality in Russia and the peculiarities of its digital landscape. The Internet in Russia is dubbed the RuNet, and provides a range of technological platforms to a population that exchanges overwhelmingly on Russian-bred websites instead of western equivalents. The second section investigates the use of digital networked technologies by Russian adolescents and young people. The third section analyses the research available on the types of safety risks faced by the Russian youth when navigating the Internet. Research shows that youth are facing risks such as cyberbullying, exposure to indecent content, and are often chatting with and meeting strangers offline. The study concludes with the assertion that as the opportunities associated with information and communication technologies rapidly expand for Russian adolescents and young people, so too does the need to educate users on their safe and optimal use.

SUMMARY OF FINDINGS

- The number of Internet users grew from two million in 2000 to 46.5 million by the end of 2010
- The Russian digital landscape is dominated by Russian-bred sites like Yandex, VKontakte and mail.ru
- Meeting strangers is the most widespread risk encountered by Russian adolescents and young people. Forty per cent of Russians aged 9-16 reported meeting someone from the online world in real life
- Significant risks discovered over the course of the study also include adult content, malicious software and cyberbullying

THE DIGITAL CITIZENSHIP AND SAFETY PROJECT & THE YOUTH SECTION AT UNICEF

This exploratory study is part of a series produced by the Youth Section at UNICEF New York through its Digital Citizenship and Safety project. The Digital Citizenship and Safety project aims to get a better understanding of the digital landscape in a range of different countries, mainly those with a developing or emerging economy. The project starts with a data collection phase, during which exploratory, quantitative and qualitative studies are conducted to then produce evidence-based communication materials to raise awareness on the optimal and safe use of the Information and Communication Technologies (ICTs). The concept of Digital Citizenship is then advocated at the local government level through advocacy workshops, seminars and conferences on how to maximize ICTs' opportunities while minimizing risks.

The Digital Citizenship and Safety project aligns itself within the scope of work conducted by the Youth Section at UNICEF, whose mission is to work with traditional and new technologies

including social networking tools, SMS and digital mapping to empower children and young people to play an active role in society.

The Convention on the Rights of the Child (CRC, 1989) guarantees the right to express views and to be heard (Art.12), freedom of expression, including the freedom to seek, receive and impart information (Art.13), the freedom of association and peacefully assembly, and the right to information (Art.17) amongst others. Although drafted before the internet became ubiquitous, the CRC is highly pertinent when it comes to young people accessing, posting and sharing content online. With the rapid development of ICT in the last decade, these rights should be analyzed and clearly applied to this digital age.

1. INTRODUCTION

1.1 Background

“Have decided to write on Facebook, too. Keep in touch!” @Medvedev.

President Dmitry Medvedev has a video blog, a LiveJournal and a Twitter account with 131,665 followers¹. After Medvedev joined all of the aforementioned platforms, 39 regional governors in Russia followed suit.²

Nexted: a term used by the visitors of a one-time popular Russian video chat site called Chatroulette. The website pairs random strangers from around the world for webcam-based conversations. Users can click the ‘next’ button at any point in the conversation, including immediately after seeing what the other person looks like. The experience continues until the user finds the chatter with whom he or she is interested in chatting. Launched in 2009, it had 3.9 million visitors worldwide as of February 2010³, placing the concept of *stranger chat* on the digital map. Created by a then 17 year-old high school student in Moscow, Andrey Ternovskiy, Chatroulette gradually lost the public attention. Indecent exposure by too many users, the selection of chatters at random, and the poor design of the platform made many shy away from the site. Still, Chatroulette is a testament to Russia’s potential in technological innovation, just as it underlines the growing trend of talking to strangers online⁴.

Launched in 2006 by Pavel Durov, *Vkontakte*, (‘In Contact’), is a Russian social network platform used by 23 million people⁵. Originally available in Russia, it is also popular in Ukraine, Kazakhstan and Belarus and can be found in more than 60 languages. *Vkontakte* shares many of the features of Facebook, and is often seen as its Russian clone. Integrating the option to share and download files, a preferred activity for Russian youth⁶, as well as a blogging platform, *Vkontakte* distinguishes itself from Facebook and enjoys high popularity among Russians.

Since the rise of the Internet, the RuNet—the name Russian-speaking Internet users commonly call the component of the Internet written in the Russian language—has developed in response to the societal, cultural and technological realities of a large and diverse country. Russia now

¹ As of 28 October 2011.

² Freedom House, *Freedom On The Net*, 2011. <www.freedomhouse.org/template.cfm?page=664> (accessed 24 July 2011).

³ Schonfeld, Erick, “Chatroulette Quadruples to 4 Million Visitors in February”, 29, March 2010, <<http://techcrunch.com/2010/03/29/chatroulette-4-million-visitors/>> (accessed 12 June 2011).

⁴ Soldatova, G., Foundation for Internet Development, *Российские и европейские школьники: риски онлайн-социализации [Russian and European Schoolchildren: The Risks of Online-Socialization]*. 2010.

⁵ Taylor Nelson Sofres (TNS) 2010, 7 June 2011, <<http://www.tns-global.ru/rus/projects/media/asmi/inet/Reports/index.wbp>> (accessed 2 June 2011).

⁶ Soldatova, G., Foundation for Internet Development, *Российские и европейские школьники: риски онлайн-социализации [Russian and European Schoolchildren: The Risks of Online-Socialization]*. 2010. Thirty per cent of 14- to 16-year-old Russian youth often share files.

has an Internet penetration of 43 per cent nation-wide. While this figure is lower than that of most western nations, Internet penetration is rapidly expanding in Russia. Indeed, the figure more than doubled from 2006 to 2009, and will no doubt continue to grow.⁷ In 2008, Russia was dubbed the country with the fastest growing Internet population in Europe,⁸ and as of 2010, 84 per cent of 12- to 17-year-olds were Internet users.⁹ Russia has made significant progress in allowing its society to enter the digital age, and even implemented a large-scale national programme connecting all institutions of general education to the Internet from 2006-2009¹⁰.

Largely dominated by local networks such as VKontakte, Yandex (the most popular Russian search engine), mail.ru (an email service) and Odnoklassniki (a social networking site), the RuNet is different from its western counterpart in that the most used websites remain Russian bred. Consequently, the opportunities and risks of the RuNet are decidedly unique, corresponding to Russian realities and challenges.

Given that young people are active on the RuNet, it is crucial that we gain an understanding of their behavior on the Internet and the risks associated with its use.

1.2 Objective

This exploratory study is the first output of an ongoing research effort to better understand the digital landscape and the types of safety risks faced by Russian youth.

1.3 Methodology

Research process

To reach the study objective, a search was conducted for background information on Russia, particularly pertaining to the use, access, digital behaviour and types of risks faced by Russian adolescents and young people when online.

As an ongoing process during the research, the methodologies of the studies found were checked for their reliability, as were the background and experience of the sources' institutions,

⁷ International Telecommunication Union (ITU), "ICT Statistics 2009—Estimated Internet Users", <<http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx>> (accessed 9 March 2011).

⁸ Comscore, "Russia Has the Fastest Growing Internet Population in Europe" 27 August 2008, <http://www.comscore.com/Press_Events/Press_Releases/2008/08/Russia_Internet_Growth> (accessed 26 May 2011).

⁹ Public Opinion Foundation, "Mobile Internet in Russia", 2010, <http://www.ewdn.com/wp-content/uploads/2011/03/FOM_Mobile_Internet_Q4_2010.pdf> (accessed 2 May 2011).

¹⁰ *The Ministry of Education and Science of the Russian Federation*. Government of Russia, "Provision of all Russian schools with access to the Internet", 2010, <<http://eng.mon.gov.ru/pro/pnpo/int/>> (accessed 7 June 2011).

which consisted of ranking sources like United Nations, government sources, state funded institutions, universities, and private actors. The reliability of the institutions is measured by the methodology including the sampling frame, the type of questionnaire used, and the experience of the institutions in conducting research in the focused area.

The literature search was conducted on the Internet in both Russian and English. Russian and western search engines were utilized, primarily including Yandex and Google. The use of local language and search tools were important in the research process, to ensure that all local sources were identified.

Sources utilized

Only the sources identified as stemming from reputable organizations, containing large sample sizes and reliable methodologies, were utilized. The Russian 2010 Census projections—the data of which are still being analysed by the Federal State Statistics Service—were used in calculation of Internet users by density per location. The primary research explored in this report include studies from the Russian Federal State Statistics Service, United Nations, the Foundation for Public Opinion, All-Russian Public Opinion Research Center (VCIOM)¹¹, the Foundation for Internet Development¹², and the Friendly RuNet Foundation¹³.

Valuing local sources and expertise

A detailed process was carried out in weighing all the international and local sources, in order to gather objective data, which consisted of ranking sources like United Nations, government sources, state funded institutions, universities, and private actors. For the Commonwealth of Independent States (CIS) region, it has generally been found that there are very few international sources that discuss the subject of the digital media through a proper evidence-based approach. Therefore, it became increasingly important to work with Russian-speaking researchers and Russian experts.

Two researchers translated the Russian literature into English, consulting with Russian experts about the validity of results and reliability of sources. Russian language literature came from sources such as foundations, educational institutions, NGOs, and private companies.

¹¹ The All-Russian Opinion Research Center is one of the leading sociological and market research companies in Russia. <<http://wciom.com/>> (accessed 1 June 2011).

¹² The Foundation for Internet Development supports projects concerning Internet development, and the development of legal issues concerning the Internet. <<http://www.fid.ru>> (accessed 1 June 2011).

¹³ The Friendly RuNet Foundation is an organization contributing to the development of Internet as a safe environment, friendly to all its users. <<http://www.friendlyrunet.ru/en/index.phtml>> (accessed 1 June 2011).

In order to validate our findings and gather local perspective, we consulted local experts such as those at STELLIT¹⁴, the writers of the RuNet Echo project¹⁵ and Galina Soldatova, Director of the Foundation for Internet Development.

The findings of this exploratory study were subject to a validation workshop, which took place in Moscow (Russia). The experts identified during the exploratory process were invited to share comments, feedback and any additional research to strengthen the present paper.

Assessing reliability of sources

To assess the reliability of secondary sources, a source valuation matrix was created which weighted the sources by factors of source type, date and expert who wrote a given study. In this process, data were carefully checked against all available sources. This mitigated the risk of valuing any invalid facts and the formulation of false hypotheses.

We found 14 studies that contained information relevant to our objective. These studies were grouped and analysed based on the content of their results.

2. CONTEXT

2.1 Overview of Russia

Russia is the biggest country in the world by land mass size, comprised of 83 federal subjects¹⁶, and is among the emerging economic powers of today.

Most of Russian youth aged 15 to 24 live in urban areas, with 74 per cent of the Russian population residing in urban areas.¹⁷ With a population of 143 million, three fourths of the population lives in the Western and Central-West parts of the country while only one fourth live in the less-populated Siberian and Far East Federal Districts¹⁸. The Far East Federal District is particularly sparsely populated, accounting for 36.4 per cent of Russia's land area but only 4.4

¹⁴ STELLIT's mission is to "improve the health and social well-being of people by assisting a broad range of professionals, including policymakers, to implement evidence-based, efficient social programmes into practice", <<http://eng.ngostellit.ru/>> (accessed: 15 June 2011).

¹⁵ The RuNet Echo project is "a project of Global Voices to expand and deepen understanding of the Russian language Internet and related online communities", <globalvoicesonline.org/-/special/runet-echo> (accessed 3 June 2011).

¹⁶ The federal subject is the basic building block of the Russian federal system. Federal subjects have varying levels of autonomy but equal representation in the Russian Upper House.

¹⁷ 'Youth World Report', Economic and Social Affairs of the United Nations, 2010.

¹⁸ United Nations Statistics Division: Demographic Statistics Division, Search Russia, <<http://data.un.org/>> (accessed 8 June 2011).

per cent of its population. However, the Far East region is still predominantly urban, as the cities of Khabarovsk and Vladivostok both contain over 500,000 people.¹⁹

Unemployment in Russia stands at 7.6 per cent overall, though the figure varies dramatically from one federal subject to another. It ranges from 1.6 per cent in Moscow, to 46.9 per cent in Ingushetia.²⁰ Ingushetia is part of Russia's volatile North Caucasus Federal District, which has experienced two major wars since the break-up of the Soviet Union and a long Islamic insurgency that continues to hinder economic development. Siberia and the Far East also lag behind the rest of the country due to a combination of geographic isolation and poorly developed communication infrastructure.

2.2 Selected overview: technological context

Internet penetration in Russia has grown rapidly with the emergence of government regulated Internet service providers (ISPs) that offer relatively low priced Internet. Internet penetration has grown from 15 per cent in 2005 to 43 per cent in 2010.²¹

RuNet dominates

Russian companies dominate across search engines, social networking, file sharing, and email services. Many of the Russian sites replicate the services of their international equivalents, implementing competitive features of global giants like Google and Facebook.²² Social network site VKontakte, for instance, was launched in September 2006, and quickly captured the Russian market, replicating many of the core functions of Facebook's English-language version.

Yandex is another case of local site domination in Russia. Yandex is the Russian equivalent to Google and provides all of the same services worldwide. In addition to a search engine, Yandex provides detailed maps and real-time traffic information, an e-payments system, and photo posting and sharing.²³

¹⁹ Federal State Statistics Service, 2010 Census.

²⁰ Federal State Statistics Service, 'Занятость и безработица в Российской Федерации в феврале 2011 года (по итогам обследований населения по проблемам занятости)' [Employment and unemployment in the Russian Federation in February 2011 (Based on Surveys of the Population's Employment)], 2011, <http://www.gks.ru/bgd/free/B04_03/lssWWW.exe/Stg/d01/62.htm> (accessed 29 May 2011).

²¹ International Telecommunication Union (ITU), 'ICT Statistics 2010—Estimated Internet Users', <<http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx>> (accessed 28 October 2011).

²² Barnett, Emma, 'Runet: Why the Russian Internet doesn't need the West', *The Telegraph*, 13 January 2011, <<http://www.telegraph.co.uk/technology/news/8255183/Runet-Why-the-Russian-Internet-doesnt-need-the-West.html>> (accessed June 13 2011).

²³ Yandex Company Site. About Yandex Section.

<http://company.yandex.com/press_center/press_releases/2009/2009-01-19.xml> (accessed 6 June 2011).

Additional examples of popular Russian-bred sites include mail.ru, the leading email platform, and Rambler, a web portal similar to Yahoo!, which offers services such as web search, email, news aggregation (with Lenta.ru) and e-commerce.²⁴

Digital divide on the RuNet

Rural federal districts in Russia are proportionately underrepresented in the total RuNet audience, while Moscow and St. Petersburg are overrepresented. Despite accounting for 26.3 per cent of Russia's population, rural areas only account for 17 per cent of Russia's Internet audience. While Moscow and St. Petersburg only account for 8.06 per cent and 3.36 per cent of Russia's population respectively, they account for 12 per cent and 5 per cent of its Internet audience.^{25 26}

Residents in more developed federal districts have cheaper Internet rates than the residents of Far East and Northern rural areas. According to the results of a recent survey, residents of the most developed Ural, Volga and Central Federal Districts pay 170-190 roubles (US\$6-7²⁷) monthly for Internet, while the residents of the less inhabited and developed Far East pay 936 roubles (US\$34²⁸).²⁹ The higher prices for Internet connection in less developed areas only serve to exacerbate the digital divide, preventing youth in these areas from accessing the RuNet.

Telephony and mobile internet

About 86 per cent of Russians use mobile phones, but the use of mobile Internet remains low at 18 per cent.³⁰ The Russian 3rd Generation Mobile Telecommunications (3G) licensing process started in February 2007. However, 3G implementation was a lengthy and expensive process

²⁴ Alexa: The Web Information Company. <<http://www.alexa.com/topsites/countries/RU>> (accessed 20 May 2011).

²⁵ Public Opinion Foundation, 'Новый выпуск бюллетеня "Интернет в России, Зима 2009/2010"' [New Issue of the Bulletin 'Internet in Russia, Winter 2009/2010'], news release, 24 March 2010, <http://bd.fom.ru/report/cat/smi/smi_int/int240310_pressr>.

²⁶ Federal State Statistics Service, Census, 2010.

²⁷ Rate considered: US\$1=27.9 RUB as of 13 June 2011.

²⁸ Ibid.

²⁹ Public Opinion Foundation, Yandex, *Taylor Nelson Sofres (TNS)*, RuCenter, 'Internet Development in Russia's Regions', 2011, <http://company.yandex.ru/facts/researches/Internet_regions_2011.xml> (accessed 13 June 2011).

³⁰ Public Opinion Foundation, 'Mobile Internet in Russia', 2010 <http://www.ewdn.com/wp-content/uploads/2011/03/FOM_Mobile_Internet_Q4_2010.pdf> (accessed 20 May 2011).

due to the country's size³¹, and didn't become available until late 2009. The rollout of 3G technology has reportedly increased the use of mobile Internet.³²

3. OPPORTUNITIES

3.1 Digital access

There have been two major studies conducted about digital access among Russian adolescents and young people. A 2010 study by the Foundation for Internet Development surveyed 2,050 urban Internet users aged 9-16 to understand the use, access and types of safety risks users face when online. More than 70 per cent of respondents indicated that they connect at home³³ while 30 per cent say they access it from "anywhere and everywhere".³⁴ Cyber cafes are not as popular among 9- to 16-year-old Russians as they are in other socio-economically similar countries such as Brazil. Only about 10 per cent access the Internet from cafes, while 58 per cent reported having access to his or her own computer.³⁵ According to the study, 45 per cent access the Internet via their mobile phones.³⁶

The Public Opinion Foundation conducted a survey with a random sample of 6,474 Russians aged 12 and over in 2010, finding that, when looking at the 12 to 17 age bracket, 84 per cent were stationary Internet users, while 49 per cent were mobile Internet users. The prevalence of mobile Internet use decreases with age, as 43 per cent of respondents aged 18-24, 26 per cent of respondents aged 25-34, and 11 per cent of those aged 35-44 reported usage.³⁷

³¹ Business Wire, '3G implementation in Russia will be a slow and expensive process', 5 April 2007, See: <<http://www.businesswire.com/news/home/20070405005505/en/3G-Implementation-Russia-Slow-Expensive-Process-Analysys>> (accessed 13 June 2011).

³² MTS Launches 3G Networks in all Markets of Operation, 2 November 2010, <<http://mtsgsm.com/news/2010-11-02-28361>> (accessed 3 May 2011).

³³ Soldatova, G., Foundation for Internet Development, *Российские и европейские школьники: риски онлайн-социализации [Russian and European Schoolchildren: The Risks of Online-Socialization]*. 2010.

³⁴ Ibid.

³⁵ Ibid.

³⁶ Ibid.

³⁷ Public Opinion Foundation, 'Mobile Internet in Russia', 2010.

<http://www.ewdn.com/wp-content/uploads/2011/03/FOM_Mobile_Internet_Q4_2010.pdf> (accessed 4 May 2011).

3.2 Digital activities

3.2.1. Communication activities

Email

Mail.ru has been the largest free email service of the RuNet since 1998.³⁸ According to the Taylor Nelson Sofres (TNS) Web Index Report, 79 per cent of 12-17 year olds and 78.2 per cent of 18-23 year olds who use the Internet use mail.ru every month.³⁹

Social networking sites

As of 2009, Russia's social networking audience was known to be the most engaged in the world.⁴⁰ In fact, the RuNet generation spends an average of 6.6 hours per month online (as opposed to a worldwide average of 3.7 hours), and consumes 1,307 pages per visitor (as compared to 525 worldwide).⁴¹

The Russian social networking market is dominated by two sites: vkontakte.ru and odnoklassniki.ru. Both can be joined free of charge. VKontakte users create profiles, connect with friends, update statuses, create and join groups, share and download files, blog and/or post photos and videos. While it was formerly open to all without invitation, as of February 2011 VKontakte adopted an 'invite only' policy. From now on any person wanting to join the platform must receive an invitation from a current user, then enter a code given by the currently registered user. It is not clear what the motivations are behind this new registration strategy, but it has been noted that it will enable the social networking giant to control the existence of clone and spam accounts. No age restriction applies to registering on VKontakte.

Like VKontakte, Odnoklassniki users can create a profile, connect with friends, publish photos, update statuses and join groups. However, unlike VKontakte, Odnoklassniki is focused primarily on allowing users to search for their classmates and/or colleagues, by name, location, school, year of graduation, etc.⁴² Like VKontakte, registration is free to anyone of any age.

³⁸ Alexa, The Web Information Company, <<http://www.alexa.com/siteinfo/mail.ru#>> (accessed 16 June 2011).

³⁹ Taylor Nelson Sofres (TNS) 2010, April 2011, <<http://www.tns-global.ru/rus/projects/media/asmi/inet/Reports/index.wbp>> (accessed 2 June 2011).

⁴⁰ Comscore, 'Russia Has World's Most Engaged Social Networking Audience', 2 July 2009 <http://www.comscore.com/Press_Events/Press_Releases/2009/7/Russia_has_World_s_Most_Engaged_Social_Networking_Audience> (accessed 2 May 2011).

⁴¹ Ibid.

⁴² Alexa Rankings- Odnoklassniki, <http://www.alexa.com/search?q=odnoklassniki.ru&p=gkey&r=site_siteinfo&s=odnoklassniki.ru> (accessed 3 May 2011).

The VKontakte user base has grown exponentially over the years, and continues to be used most commonly by Russian adolescents and young people. A TNS Web Index report noted that among Internet users, 93.6 per cent of 12- to 17-year-olds and 92.2 per cent of 18- to 24-year-olds have visited VKontakte in the last month, while 39.6 per cent of 12 to 17-year-olds and 49.9 per cent of 18- to 24-year-olds visited Odnoklassniki.⁴³

In the Foundation for Internet Development's study of urban Internet users aged 9-16, 89 per cent reported that they had a profile on VKontakte, while only 16 per cent reported that they had one on Odnoklassniki. Other, albeit less prominent social networking sites are also present on the RuNet, including MoiMir and LiveInternet.⁴⁴

Western social network sites are less often used in Russia, although the user base is slowly growing. In 2010, Facebook use among 9- to 16-year-olds was about 4 per cent.⁴⁵ Anecdotal evidence shows that Twitter use is also gaining popularity, although there is no hard evidence on the scope or frequency of its use.⁴⁶

Online gaming

There is a dearth of research concerning the prevalence and frequency of online gaming among Russian adolescents and young people. According to one 2010 study, 75 per cent of Internet users under 18 years of age who play online games play massively multi-player online games (MMOG).⁴⁷ On average, they play these games 6 days per week, 7 hours per day.⁴⁸ In addition, 25 per cent of this sample play games on social networking sites.⁴⁹ On average, games on social networking sites are played 5 days per week, 4 hours per day.⁵⁰

⁴³ Taylor Nelson Sofres (TNS) 'Web Index Report', 2010, (accessed 7 June 2011).

⁴⁴ Russian Public Opinion Research Center, "Is Facebook Popular in Russia. Rating of Social Networks", 6 June 2010, <<http://wciom.com/archives/thematic-archive/info-material/single/13611.html>> (accessed 8 May 2011).

⁴⁵ Soldatova, G., Foundation for Internet Development, *Российские и европейские школьники: риски онлайн-социализации [Russian and European Schoolchildren: The Risks of Online-Socialization]*. 2010.

⁴⁶ Global Voices, 'Russia: The Twitter Craze. This Time, It's a Worm...' 14 October 2010, <<http://globalvoicesonline.org/2010/10/14/russia-the-twitter-craz/>>, (accessed 3 June 2011).

⁴⁷ J'son & Partners Consulting, 'Market Watch, Online Gaming Market in Russia, 2008-2015', October 2010.

⁴⁸ Ibid.

⁴⁹ Ibid.

⁵⁰ Ibid.

3.2.2. User generated content: blogging

There are several studies that point to the importance of the flourishing Russian blogosphere⁵¹, both in terms of its prevalence and the uniqueness of its content. A 2010 study by the Berkman Center of Harvard University found that there were over five million Russian language blogs, the overwhelming majority of which are found on LiveJournal.⁵²

LiveJournal was invented by an American college student and is now owned by a Russian company with 48 per cent of its audience located in Russia.⁵³ Where traditional media may lag in reportage or analysis of important events, LiveJournal, or blogging more generally, has come to serve a crucial social function in analysing, disseminating and influencing offline events. Anton Nossik⁵⁴ calls LiveJournal “the only uncensored, uncontrolled and unmoderated channel for discussion.”⁵⁵ There have been cases of bloggers exposing corruption and other misdeeds by the authorities. Some, like Alexey Navalny, a prominent social activist, have in recent years gained great prominence amongst Russian bloggers and in mass media. Like many others, Navalny uses his popular LiveJournal blog⁵⁶ to organize large-scale petitions by Russian citizens to address different national issues.

Looking at the 9-16 year old age range, the Foundation for Internet Development study found that 12 per cent blog on a regular basis, more than in any other European country.⁵⁷ The ‘typical’ Russian blogger, however, has been shown to be a 22-year-old female from Moscow, according to a Yandex report from 2010.⁵⁸

Not all Russian blogs advocate for more rights and/or discuss politics. Many rather focus on business and finance, as well as movies and other aspects of pop culture.⁵⁹

⁵¹ Yandex, ‘Trends in the Russian Blogosphere’, Spring 2009 and Berkman Center for Internet and Society, *Public Discourse in the Russian Blogosphere: Mapping RuNet Politics and Mobilization* 2010.

⁵² Berkman Center for Internet and Society, *Public Discourse in the Russian Blogosphere: Mapping RuNet Politics and Mobilization*, 18 October 2010.
<http://cyber.law.harvard.edu/sites/files/Public_Discourse_in_the_Russian_Blogosphere_2010.pdf> (accessed 20 April 2011).

⁵³ “livejournal.com - Traffic Details from Alexa”. Alexa Internet, Inc. 2010,
<<http://www.alexa.com/siteinfo/livejournal.com>> (accessed 16 April 2011).

⁵⁴ Russia’s most prominent start-up manager, journalist and a public figure. Founder of the popular online news sites Vesti.ru, Lenta.ru, Gazeta.ru и NEWSru.com. Former manager of Rambler and SUP Holding. Founder of the charity foundation Pomogi.org («Помоги.орг»). Since 2009 - Managing Director of United Media («Объединённые медиа»), and a free-lance editor-in-chief of Bfm.ru.

⁵⁵ Russians Riled by Attacks on Blogging Service, *New York Times*, 8 April 2011.

⁵⁶ <<http://navalny.livejournal.com/>> (accessed 3 June 2011).

⁵⁷ Soldatova, G., Foundation for Internet Development, *Российские и европейские школьники: риски онлайн-социализации [Russian and European Schoolchildren: The Risks of Online-Socialization]*. 2010.

⁵⁸ Yandex, Trends in the Russian Blogosphere, Spring 2009.

⁵⁹ Berkman Center for Internet and Society, *Public Discourse in the Russian Blogosphere: Mapping RuNet Politics and Mobilization*, 18 October 2010.

More research in this predominantly peer-produced space would enable a better understanding of the degree to which adolescents and young people create content, and the role that Internet can play in promoting dialogue and mobilizing groups.

3.2.3. Commercial

Russian e-commerce

According to a recent study by the Public Opinion Foundation, as much as 24 per cent of all Russian Internet users, approximately 46.5 million internet users, made a purchase online in the last month, a 33 per cent increase from August 2010. Among the most popular product categories are household appliances, cosmetics, clothing, and travel services. This year, the overall volume of Russian Business-to-Consumer e-commerce could reach as much as \$8.75 billion.⁶⁰ A survey conducted by the children's Internet portal Tvidi.ru revealed that 30 per cent of its users aged 10-16 reported paying for online purchases themselves, compared to 64 per cent who had their purchases paid for by parents or relatives. Only 1 per cent noted never having made a purchase online.⁶¹

Thus, research shows a high frequency of Internet use by Russian adolescents and young people, notably on social network sites and blogging platforms, underlining the RuNet generation's desire to be part of an online community.

4. IDENTIFYING SAFETY RISKS

The review of relevant literature revealed that cyberbullying, exposure to adult content, exposure to extremist content, malicious software and fraud, sharing of personal information and meeting of strangers are all safety risks associated with Internet use. The literature did not provide data with regards to hateful content, grooming and gambling, although these safety issues do likely exist in Russia.

⁶⁰ Public Opinion Foundation, 'Новый выпуск бюллетеня "Интернет в России, Зима 2009/2010"' [New Issue of the Bulletin 'Internet in Russia, Winter 2009/2010'], news release, 24 March 2010, <http://bd.fom.ru/report/cat/smi/smi_int/int240310_pressr> (accessed 2 June 2011).

⁶¹ Rambler, '30% юных пользователей сети оплачивают интернет-покупки самостоятельно' [30% of Young Internet Users Pay For Online Purchases Independently], 8 July 2010. <<http://rumetrika.rambler.ru/review/2/4363>> (accessed 3 May 2011).

4.1 The risks

4.1.1. Malicious software and fraud

Russian Internet users are at a heightened risk of encountering malicious software⁶² and fraud⁶³. An estimated 67 per cent of all software is pirated in Russia.⁶⁴ The use of such illicit software increases the risk of attacks from viruses and other malware. Cybercrime is a profitable and highly organized phenomenon in Russia, worth 1.3 billion US Dollars in 2010 according to the research company Group-IB.⁶⁵ The group also noted a rise in fraud committed via SMS. For example, one programme took the form of a Valentine's Day e-card that users downloaded to their mobile phones, which then sent text messages from the victim's phone to a premium number.⁶⁶ In 2010, the Internet security company AVG named Russia the second country most at risk in the world for malicious software attacks on its 'Global Threat Index', noting that a user in Russia had a 1 in 15 chance of being attacked on a given day, compared to the global average of 1 in 73.⁶⁷

More research is necessary to know to what extent adolescents and young people are exposed to or affected by malicious software and fraud.

⁶² Malicious software (often abbreviated to "malware") is "any software programmes developed for the purpose of doing harm to a computer system or create mischief. The most common are Viruses, Worms, and Spyware." Business Software Alliance, 'Cyber Safety Glossary' <<http://www.bsacybersafety.com/threat/malware.cfm>> (Accessed 24 July 2011).

⁶³ Fraud refers to intentional deception with regards to goods, services or contracts with the aim of financial gain. Examples of Internet fraud vary from simple fraudulent online sales, where money is taken but no goods delivered, to more complicated frauds such as re-shipping fraud and advance-fee fraud.

⁶⁴ Gaidar Institute for Economic Policy, 'Protection of Intellectual Property Rights in Russia', 2010, <<http://www.iet.ru/en/comments/ob-o-rane-prav-intellektualnoi-sobstvennosti-v-rossii.html>> (accessed 30 May 2011).

⁶⁵ Group IB, '«Русский» рынок компьютерных преступлений в 2010 году: состояние и тенденции [The 'Russian' Computer Crime Market in 2010: Situation and Trends]. <http://www.group-ib.ru/wp-content/uploads/2011/03/GIB-Issl-rynka_2010.pdf> (accessed 2 June 2011).

⁶⁶ Microsoft 'SMS Mobile Malware Feelin' the Love', 11 February 2011, <<http://blogs.technet.com/b/mmpc/archive/2011/02/11/sms-mobile-malware-feelin-the-love.aspx>> (accessed 20 April 2011).

⁶⁷ AVG, 'New AVG Research Shows Turkey and Russia as Most Risky Places to Surf the Net, Sierra Leone and Japan Among Safest', <<http://www.avg.com/ww-en/press-releases-news.ndi-232210>> 26 August 2010. (Accessed 24 July 2011).

4.1.2. Exposure to adult content⁶⁸ and child abuse images

Russia criminalizes the illegal production, distribution or sale of pornography in article 242 of the Russian criminal code⁶⁹, but fails to define what exactly constitutes pornography.

The research available in the Russian language shows that there is a high exposure of Russian youth to adult content. In a study led by the Foundation for Internet Development, 40 per cent of 9- to 16-year-old Russians encountered images of a sexual nature on the Internet, with 6 per cent seeing it daily and 7.6 per cent once or twice a week. The study further states that 33 per cent of 9- to 16-year-olds see sexual images on social networking sites.⁷⁰

In 2009, the Ministry of Internal Affairs called VKontakte “the largest repository of pornographic materials in the RuNet”⁷¹. The presence of adult content on a site like VKontakte generates concern, as it is a members-only community with a platform primarily geared to adolescents and young people. The Russian Internet community, including a number of top Internet company managers, signed an open letter to the Administration of VKontakte to implore them to introduce strict content filtering.

In a study focusing on the presence of child abuse images and videos, the Friendly RuNet Foundation noted growth in the usage of popular social networking sites, file-hosting sites and photo and video hosting sites for the storage of child abuse images and videos. While in 2009, 68 per cent of child abuse images and videos could be found on sites specifically devoted to this type of content, these sites contained only 39 per cent of the content by 2010.⁷² An increasing amount of child abuse images and videos are now found on social networking and file-sharing websites, heightening the risk that users with no intention of engaging with this content will stumble upon it.

⁶⁸ The terms ‘adult content’, ‘images of a sexual nature’ and ‘pornography’ are used synonymously throughout this paper.

⁶⁹ Article 242 states the following: Illegal making for the purpose of distribution or advertising, dissemination, or advertising of pornographic materials or objects, and likewise illegal trade in printed publications, cine-and-video-materials, pictures, or any other pornographic objects, shall be punishable [...], <<http://russian-criminal-code.com/PartII/SectionIX/Chapter25.html>> (accessed 5 June 2011).

⁷⁰ Soldatova, G., Foundation for Internet Development, *Российские и европейские школьники: риски онлайн-социализации [Russian and European Schoolchildren: The Risks of Online-Socialization]*. 2010.

⁷¹ Newspepper.su, ‘VKontakte accused Yandex in making the porn’, <<http://newspepper.su/news/2011/3/23/managers-runet-called-quotvkontaktequot-get-rid-of-porn>> (accessed 15 June 2011).

⁷² Friendly RuNet Foundation, ‘Отчет о работе горячей линии в 2010 году’ [Report on The Hotline’s Work for 2010], 2010.

4.1.3. Exposure to extremist content

Russian government officials have noted the use of the Internet by extremist groups, such as neo-Nazis and the Movement Against Illegal Immigration (DPNI), to spread their messages.⁷³ Extremists advocating violence against minority groups and immigrants have been a problem in Russia for some time. This study was able to identify only one paper analysing extremist content on the RuNet. In its 2010 paper entitled *Mapping RuNet Politics and Mobilization*, the Berkman Center for Internet and Society explored a range of Russian nationalist bloggers, from extremists advocating violence against Caucasian and Central Asian immigrants, to more moderate nationalists focusing on Russian identity. This paper points to evidence of online political mobilization around often xenophobic nationalist causes, including protests, marches, calls to support extremists who have been jailed, concerts and other offline initiatives.⁷⁴ Further research is necessary to know to what extent adolescents and young people are exposed to, affected by, or engaging with such material.

4.1.4. Sharing of personal information

Social networking sites offer the option for users to display their personal information, including first and last names, date of birth, city of residence, and name of school. This information enables one user to find another on the platform, and gives the platform a feel of an authentic community of friends and acquaintances.

In the Foundation for Internet Development study of 9- to 16-year-olds, it was discovered that 88 per cent listed their last name on their social networking profile, 64 per cent listed their school's name, 25 per cent listed their mobile telephone number and 20 per cent listed their home address.⁷⁵ The level of display of private information is therefore quite high on the RuNet, signaling the need to raise awareness among users on the risks associated with its display.

4.1.5. Cyberbullying

Cyberbullying: child as recipient

According to Article 19 of the Convention on the Rights of the child, all children have the right to be protected from all forms of violence while in the care of parents or other caregivers. General Comment No. 13, of the Committee on the Rights of the Child explains some of the risks that

⁷³ RIA Novosti, 'Russian Official Warns of Dangerous Growth of Race-hate Groups', 28 May 2009 <<http://en.rian.ru/russia/20090528/155111787.html>> (Accessed 25 July 2011).

⁷⁴ Berkman Center for Internet and Society, *Public Discourse in the Russian Blogosphere: Mapping RuNet Politics and Mobilization*, 18 October 2010.

⁷⁵ Soldatova, G., Foundation for Internet Development, *Российские и европейские школьники: риски онлайн-социализации [Russian and European Schoolchildren: The Risks of Online-Socialization]* 2010.

children face through ICTs, one of them being cyberbullying: “As children in contact with others through ICT, children may be bullied, harassed or stalked (child “luring”) and/or coerced, tricked or persuaded into meeting strangers off-line, being “groomed” for involvement in sexual activities and/or providing personal information.”⁷⁶

Cyberbullying is defined by the Berkman Center at Harvard Law School as the "willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices".⁷⁷ Nevertheless, different studies tend to use different definitions and criteria when carrying out research into the phenomenon, which can yield to inconsistent results.

For instance, in the Russian context, Galina Soldatova, Director of the Foundation for Internet Development, defines bullying as “intentional aggressive behaviour, both physical and verbal, directed against someone who is for some reason considered weaker in order to humiliate them”.⁷⁸ Although bullying existed before the creation of the World Wide Web, the Internet has magnified the problem by creating a new venue through which bullying can be perpetrated. When perpetrated online, bullying is eased by the apparent anonymity of the action and distance from the victim.

A survey conducted by the Foundation for Internet Development reveals that 11 per cent of 9- to 16-year-old Russian respondents have reportedly been bullied on the Internet, 6 per cent through their mobile phones, and 13 per cent face-to-face.⁷⁹

When asked about where they encounter cyberbullying, social networking sites emerged as the leading answer⁸⁰. Respondents reported cases of insults within a post, as well as instances where fake pages have been created under the name of the victim to spread insulting content.⁸¹

Cyberbullying: child as actor

The literature revealed very little information as to who is perpetrating the cyberbullying. The only data gathered in this regard stem from the Foundation for Internet Development study, where 6 per cent of children aged 9-16 admitted to bullying other people on the Internet⁸².

⁷⁶ Committee on the Rights of the Child CRC/C/GC/13 , Fifty-sixth session, Geneva, 17 January - 4 February 2011

⁷⁷ Shrock, Andrew, boyd, danah, *Online Threats to Youth: Solicitation, Harassment, and Problematic Content*, Harvard University: Cambridge, 2008
<http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/RAB_Lit_Review_121808_0.pdf> (accessed 10 August 2011).

⁷⁸ Soldatova, G., Foundation for InternetInternet Development, *Российские и европейские школьники: риски онлайн-социализации [Russian and European Schoolchildren: The Risks of Online-Socialization]*. 2010.

⁷⁹ Ibid.

⁸⁰ Ibid.

⁸¹ Ibid.

⁸² Ibid.

4.1.6. Meeting strangers

Meeting strangers is an opportunity vastly expanded by Internet activity. It can open the door to potentially long-lasting and/or international relationships, or it can open the door to unwanted and/or deceitful interactions. With the omnipresence of Internet, many users are accustomed to the idea of meeting strangers they once talked to online.

This meeting can take several forms. On classifieds websites such as Craigslist in America or avito.ru in Russia, the buyer and seller may meet to proceed with a transaction. As it is likely a one-time occurrence, the exposure is typically brief and business-oriented. On a social networking site or in a chatroom, however, a meeting of strangers is much more likely a continuation of a more personal, online relationship, and the nature of the meeting will be less easily defined. There may be a false feeling of safety that comes along with such a meeting, as the counterparts may have been communicating for a period of time before the face-to-face meeting and thus feel like they know each other. Social networking sites also provide users the opportunity to meet friends of friends. This scenario may likewise lead to the feeling that an offline meeting will be safe, since a friend or acquaintance will have met the person before.

A review of the literature shows that meeting online strangers is a significant occurrence for Russian children. It should be noted that adolescents and young people might not perceive strangers as a risk and more as a friend who they have been interacting with online for a longer period of time. The survey conducted by the Foundation for Internet Development shows that 50 per cent of 9- to 16-year-old Russians constantly interact online with people to whom they are not connected in any way, while 40 per cent meet these strangers in person. These interactions are reported to happen mostly on social networking sites, in chatrooms and through online games.⁸³

As adolescents and young people become increasingly active on the RuNet, they also more frequently encounter the risks associated with Internet use. While malware, fraud, cyberbullying and exposure to extremist content all warrant attention, it seems that chatting with and meeting strangers is the most ubiquitous hazard faced by Russian adolescents and young people today according to the research findings presented in this paper. Future research will need to carefully examine the nature of these interactions, to ensure that young RuNet users are not falling prey to ill-intentioned online contacts.

The research obtained in the course of this exploratory study indicates that the most pressing and unique risk faced by Russian adolescents and young people is chatting to and meeting online strangers in real life. Here Russian adolescents and young people seem to sharply distinguish themselves from their western European counterparts, who are far less likely to

⁸³ Soldatova, G., Foundation for Internet Development, *Российские и европейские школьники: риски онлайн-социализации [Russian and European Schoolchildren: The Risks of Online-Socialization]*. 2010.

engage in such behaviour⁸⁴. There is also a strong indication that viewing indecent content such as adult content and spam is a high risk for Russian adolescents and young people.

5. MONITORING THE RUNET

Russia became party to the CRC at the time of its ratification on August 16, 1990⁸⁵. Russia then attempted to bring its domestic legislation in accordance with international obligations with regards to children's rights. The Federal Law on Basic Guarantees of the Rights of the Child in the Russian Federation, enacted on July 21, 1998, repeats all the provisions of the CRC.⁸⁶ With the growing use of Internet, particularly among adolescents and young people, steps have been taken to address the attendant risks that come with digital activity.

Research shows that both governmental and private actors are taking such initiatives. While governmental actors have typically focused on the adoption of relevant legislation, private actors have established hotlines where users can denounce indecent content and receive counseling services if affected by it.

Hotlines for Internet safety

The Friendly RuNet Foundation maintains a hotline to report the presence of child abuse images and has been very active in pursuing such cases. The Foundation issues an annual report of its work, detailing the complaints it received, the nature of the content contained in the complaints, and on what type of sites child abuse images were discovered.⁸⁷ In June 2011, the Foundation launched a separate helpline, which allows Internet users to report websites that promote the use of illegal drugs.⁸⁸ The work of the Friendly RuNet Foundation led to a total of nine criminal cases in 2009 and 24 in 2010.⁸⁹

The Internet Safety League

Talks of improving the policing of the Internet have led to the creation of the Internet Safety League in February 2011. The Internet Safety League is comprised of the three major mobile

⁸⁴ Ibid.

⁸⁵ United Nations Treaty Collection, Chapter IV: Human Rights, 11. Convention on the Rights of Child, November 20, 1989, <http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-11&chapter=4&lang=en>.

⁸⁶ World Organisation Against Torture, Rights of the Child in the Russian Federation, 30 September 2005, available at: <<http://www.unhcr.org/refworld/docid/46af4d420.html>>.

⁸⁷ Friendly Runet Foundation, 'Отчет о работе горячей линии в 2010 году' [Report on The Hotline's Work for 2010], 2010.

⁸⁸ RIA Novosti, 'Russian Runet Launches Hotline to Fight Drug Promotion' <<http://en.rian.ru/russia/20110531/164338344.html>> (accessed 3 May 2011).

⁸⁹ Ibid.

providers, Mobile Telesystems, VimpelCom and Megafon, as well as the state telecom company Rostelecom. The League's priority for 2010 was reportedly to fight against child abuse images and videos. Critics, however, comprised mostly of Russian bloggers and human rights activists, are skeptical as to whether or not the League will also be used as a tool to further monitor political dissidents. Considering Russia's growing history of monitoring and regulating the RuNet, this possibility is realistic.

Governmental policing of the Internet

In a 2011 report entitled *Freedom on the Net*, a study evaluating the level of online freedom enjoyed by Internet users, Freedom House deems the Russian Internet to be "partly free." Online monitoring and regulation is a reality on the RuNet, as content is at times removed on the grounds that it violates Russia's laws against extremism. Under article 282 of the Russian criminal code⁹⁰, the offence is defined as the "incitement of national, racial, or religious enmity, abasement of human dignity, and also propaganda of the exceptionality, superiority, or inferiority of individuals by reason of their attitude to religion, national, or racial affiliation" towards an "organized group". Following a non-transparent procedure, the Russian Ministry of Justice lists all prohibited materials found on the Internet, and communicates it to Internet service providers who are instructed to block the content or face legal consequences. In January 2009, the Ministry of Information and Communication officially required telecommunications companies and Internet service providers to allow the Federal Security Service (FSB), to tap telephones and monitor information over the Internet.⁹¹ The practice of exerting pressure on service providers and content producers can result in self-censorship and/or an exodus of websites to foreign site-hosting providers.⁹²

6. LIMITATIONS AND SUGGESTIONS FOR FURTHER RESEARCH

The primary limitation of this study lies in the scarcity of literature available on the digital behaviour and risks faced by adolescents and young people in Russia. This prevented a thorough cross-referencing of data. There were also no randomized control trials (RCT) of Russian youth found in the search, though an RCT may have provided a more representative

⁹⁰ Article 282 states: Actions aimed at the incitement of national, racial, or religious enmity, abasement of human dignity, and also propaganda of the exceptionality, superiority, or inferiority of individuals by reason of their attitude to religion, national, or racial affiliation, if these acts have been committed in public or with the use of mass media shall be punishable by [...] The same acts committed: a) with the use of violence or with the threat of its use; b) by a person through his official position, c) by an organized group, shall be punishable by [...], <<http://russian-criminal-code.com/PartII/SectionX/Chapter29.html>> (accessed 2 June 2011).

⁹¹ United States Government: Bureau of Democracy, Human Rights, and Labor. *Report on Human Rights Practices*. 2009, <<http://moscow.usembassy.gov/hrr-2008-russia.html>> (accessed 3 May 2011).

⁹² Freedom House, *Freedom On The Net*, 2011. <www.freedomhouse.org/template.cfm?page=664> 2011 (accessed 24 July 2011).

picture of the extent of Internet use in Russia. There was likewise a dearth of literature exploring Internet use in rural areas, as well as in the North Caucasus and Far East Federal Districts.

This exploratory study has identified several areas for which further research is needed. These areas include:

- Internet usage by rural adolescents and young people
- The digital landscapes of North Caucasus, Far East and Siberian Federal Districts
- The presence of hateful content, grooming and gambling on the RuNet

The second phase of this project will entail the use of quantitative and qualitative methods to collect original data on Internet use, access, digital behaviour, and safety risks faced by adolescents and young people in Russia. Quantitative methods will include a questionnaire with a large sampling frame. Qualitative research will be conducted primarily through focus groups.

7. CONCLUSION

Although Internet penetration remains low, Russia's digital landscape is expanding, particularly among adolescents and young people. While western societies see its youth corresponding on major western platforms such as Facebook, Twitter or Google, Russian youth have been interacting on a range of Russian platforms and networks. These sites have been duplicated and adapted from their western equivalents to not only offer the options available on the western leading platform, but also to provide features that are favoured by Russian youth, such as file sharing and blogging. These emerging communication tools play a political as well as social role, as Russian bloggers discuss serious national topics and address issues that are at times ignored by the government. Parallel to the spread of ICTs, attendant safety risks have arisen, including the massive presence of malicious malware on the RuNet, and the high frequency with which adolescents and young people are talking to and meeting with online strangers. Russian youth, while enjoying the opportunities created by the digital world, need to arm themselves with the tools and skills to navigate, judge, create and consume digital content in a safe and optimal way.

GLOSSARY

3G: Generic name for third-generation networks or services under the IMT-2000 banner, for example W-CDMA. (Source: ITU, <<http://www.itu.int/osg/spu/ni/3G/technology/SPU%20Mobile%20Glossary%202003.pdf>>).

Access: The right, opportunity, and/or means of finding, using or retrieving information. (Source: International Standard ISO/TR15489-1, Clause 3.1).

Adolescent: Males and females aged 10-19 years. (Source: United Nations Children's Fund (UNICEF), "The State of the World's Children 2011", <http://www.unicef.org/sowc2011/pdfs/SOWC-2011-Main-Report_EN_02092011.pdf>).

All-Russian Public Opinion Research Center (VCIOM): One of the leading sociological and market research companies in Russia. <<http://wciom.com/>>.

Blog: A Web site that contains dated text entries in reverse chronological order about a topic. Blogs serve many purposes from personal journals to online newsletters. Written by one person or a group of contributors, entries may contain commentary, observations and opinions as well as images, audio, video, and links to other sites. (Source: PC Magazine, <http://www.pcmag.com/encyclopedia_term/0,2542,t=blog&i=38771,00.asp>).

Broadband: A transmission capacity with sufficient bandwidth to permit combined provision of voice, data and video, with no lower limit. Broadband is implemented mainly through ADSL, cable modem or wireless LAN (WLAN) services. (Source: ITU <http://www.itu.int/wsis/tunis/newsroom/stats/The_Portable_Internet_2004.pdf>).

Caucasus: *See Federal District.*

Chatroom: An online discussion forum. Everyone who is logged into a chatroom sees what everyone else is typing, although two people can decide to break off and have a private chat. (Source: PC Magazine, <http://www.pcmag.com/encyclopedia_term/0,2542,t=chat+room&i=39614,00.asp>).

Child pornography: Child pornography means any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes. (Source: Article 2 of the Optional Protocol to the CRC on the sale of children, child prostitution and child pornography (OPSC)).

Cyberbullying: Willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices (Source: Center for International Development at Harvard University, Information Technologies Group, <http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/RAB_Lit_Review_121808_0.pdf>).

Cyber café: Public establishments offering access to Internet-enabled terminals in addition to other services, such as food and drink. Also known as an "Internet Cafe". (Source: Center for International Development at Harvard University, Information Technologies Group, <<http://cyber.law.harvard.edu/readinessguide/glossary.htm>>).

Cybercrime: Refers broadly to any criminal activity that pertains to or is committed through the use of the Internet. (Source: Center for International Development at Harvard University, Information Technologies Group, <cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Cybercrime.doc>).

Digital Behaviour: The way in which an individual behaves and interacts with other users online and in groups.

Digital Divide: The gap between individuals, households, businesses and geographic areas at different socio-economic levels with regard to their opportunities to access information and communications technologies (ICTs) as well as to use the Internet. (Source: Patricia, J.P, (2003) 'E-government, E-Asean Task force, UNDP-APDIP', <<http://www.apdip.net/publications/iespprimers/eprimer-egov.pdf>>).

Digital Media: Digitized content that can be transmitted over the Internet or computer networks. This can include text, audio, video, and graphics. News from a TV network, newspaper, magazine, etc. that is presented on a website or blog can fall into this category. (Source: Penn State University, "The Fourth Amendment Relating to Technology", <<https://wikispaces.psu.edu/display/IST432SP11Team14/Definition+of+Digital+Media>>).

E-commerce: "The conduct of transactions by electronic means." (Source: Center for International Development at Harvard University, Information Technologies Group, <<http://cyber.law.harvard.edu/olds/ecommerce/introduction.html>>).

Email (electronic mail): A computer-based form of sending and receiving messages via the Internet. Users may have their own e-mail account or use a shared account. (Source: Center for International Development at Harvard University, Information Technologies Group, <<http://cyber.law.harvard.edu/readinessguide/glossary.html>>).

Emerging Economies/Emerging Markets: Developing countries' financial markets that are less than fully developed, but are nonetheless broadly accessible to foreign investors. (Source: International Monetary Fund (IMF): Global Financial Stability Report 2004).

Far East: *See Federal District.*

Federal District: Administrative zones composed of several federal subjects, created in order to more easily facilitate the governing of the country. Each district is headed by a plenipotentiary envoy, appointed by the president. There are eight federal districts: the Central Federal District, the Far East Federal District, the North Caucasus Federal District, the North West Federal District, the Siberian Federal District, the South Federal District, the Urals Federal District and the Volga Federal District. (See Decree 849 of 13 May 2000 "On the Plenipotentiary Representative of the President of the Russian Federation in the Federal District").

Federal Security Service (FSB): An integral part security forces of the Russian Federation within the authority granted to them to ensure the safety of the individual, society and state. (Source: Federal Law of 3 April 1995 "On the Organs of the Federal Security Service in the Russian Federation").

Federal Subject: The federal subject is the basic building block of the Russian federal system. Federal subjects have varying levels of autonomy but equal representation in the Russian

Upper House. (See Chapter III “The Federal Structure” of the Constitution of the Russian Federation).

File Sharing: Copying files from one computer to another. (Source PC Magazine, <http://www.pcmag.com/encyclopedia_term/0,2542,t=peer-to-peer+network&i=49056,00.asp>).

Foundation for Internet Development: Organization supporting projects concerning Internet development, and the development of legal issues concerning the Internet. <<http://www.fid.ru>>.

Friendly RuNet: Organization contributing to the development of Internet as a safe environment, friendly to all its users. <<http://www.friendlyrunet.ru/en/index.phtml>>.

Grooming: “As children in contact with others through ICT, children may be bullied, harassed or stalked (child “luring”) and/or coerced, tricked or persuaded into meeting strangers off-line, being “groomed” for involvement in sexual activities and/or providing personal information.” <Committee on the Rights of the Child CRC/C/GC/13, Fifty-sixth session, Geneva, 17 January - 4 February 2011>.

Information and communication technologies (ICTs): The building blocks of the Networked World. ICTs include telecommunications technologies, such as telephony, cable, satellite and radio, as well as digital technologies, such as computers, information networks and software. (Source: Center for International Development at Harvard University, Information Technologies Group, <<http://cyber.law.harvard.edu/readinessguide/glossary.html>>).

Internet: A linked global network of computers in which users at one computer can get information from other computers in the network. (Source: ITU <http://www.itu.int/wsis/tunis/newsroom/stats/The_Portable_Internet_2004.pdf>).

Internet-service providers (ISPs): ISPs provide end-users, and other ISPs, access to the Internet. ISPs may also offer their own proprietary content and access to online services such as e-mail. (Source: ITU (2009), “Glossary, Acronyms and Abbreviations”, <http://www.itu.int/ITU-D/ict/publications/wtdr_99/material/glossary.html>).

Internet users: Subscribers who pay for Internet access (dial-up, leased line, and fixed broadband) and people who access to the worldwide computer network without paying directly, either as the member of a household, or from work or school. The number of Internet users will always be much larger than the number of subscribers, typically by a factor of 2–3 in developed countries, and more in developing countries. (Source: ITU <<http://www.itu.int/ITU-D/ict> >).

ITU: International Telecommunication Union. The United Nations specialized agency for Telecommunications, <<http://www.itu.int/>>.

Malicious Software: (Also known as malware) Any software program developed for the purpose of doing harm to a computer system or create mischief. The most common are Viruses, Worms, and Spyware. (Source Business Software Alliance, “Cyber Safety Glossary” <<http://www.bsacybersafety.com/threat/malware.cfm>>).

Massively Multiplayer Online Game (MMOG): A game on the computer played by many people. People can log in, join the action and leave whenever they wish, although the game continues. (Source: PC Magazine <http://www.pcmag.com/encyclopedia_term/0,2542,t=MMOG&i=56862,00.asp>).

Mobile Phone: Portable telephone device that does not require the use of landlines. Mobile phones utilize frequencies transmitted by cellular towers to connect the calls between two devices. A mobile telephone service provided by a network of base stations, each of which covers one geographic cell within the total cellular system service area. (Source: ITU, <http://www.itu.int/wsis/tunis/newsroom/stats/The_Portable_Internet_2004.pdf>).

Mobile Internet: Internet accessed via mobile devices such as mobile phones through advanced wireless technologies like Wi-Fi, WiMax, IMT-2000, ultra wideband and radio frequency identification (RFID) tags. These operate at long, medium and short ranges. Handheld devices that are Internet enabled could open up the information gateway in a new and exciting market, that could help further the goals of universal access while challenging manufacturers and service providers to meet different users' needs across the globe. (Source: ITU, <<http://www.itu.int/osg/spu/publications/portableInternet/ExecSummFinal2.pdf>>).

Online: A resource that is available over the Internet or a network. (Source: Center for International Development at Harvard University, Information Technologies Group, <<http://cyber.law.harvard.edu/readinessguide/glossary.html>>).

Online Content: Information that is available online. The "message" rather than the "medium." (Source: Center for International Development at Harvard University, Information Technologies Group, <<http://cyber.law.harvard.edu/readinessguide/glossary.html>>).

Penetration: A measurement of access to telecommunications, normally calculated by dividing the number of subscribers to a particular service by the population and multiplying by 100. (Source: ITU (2009), "Glossary, Acronyms and Abbreviations", <http://www.itu.int/ITU-D/ict/publications/wtdr_99/material/glossary.html>).

Platform: A hardware and/or software architecture that serves as a foundation or base. (Source: PC Magazine <http://www.pcmag.com/encyclopedia_term/0%2C2542%2Ct%3Dplatform&i%3D49362%2C00.asp>).

Population: The number of all residents in a country, regardless of legal status or citizenship, excluding refugees not permanently settled in the country of asylum. Data are midyear estimates. (World Bank, "Country At a Glance technical notes", <<http://go.worldbank.org/WG51XXDWB0>>).

Portal: refers to the starting point, or a gateway through which users navigate the World Wide Web, gaining access to a wide range of resources and services, such as e-mail, forums, search engines and shopping malls. (Source: ITU Glossary 1-ITU (2009), "Glossary, Acronyms and Abbreviations", <http://www.itu.int/ITU-D/ict/publications/wtdr_99/material/glossary.html>).

Randomized Control Trials (RCT): studies that randomly assign individuals to an experimental variable or to a control group, in order to measure the effects of the intervention. Source: Andre Marchand, Stephane Guay, Richard Boyer, Soledad Iucci, Annick Martin, Marie-Helene St-Hilaire, 'Randomized Controlled Trial of an Adapted Form of Individual Critical Incident Stress Debriefing for Victims of an Armed Robbery', Stanford University School of Medicine, March 2006, Published by Oxford University Press, <<http://btci.stanford.clockss.org/cgi/reprint/6/2/122>>).

RuNet: The component of the Internet written in the Russian language.

RuNet Echo: Organization which describes itself as "a project of Global Voices to expand and deepen understanding of the Russian language Internet and related online communities", <globalvoicesonline.org/-/special/runet-echo>.

Rural: Any area that cannot be classified as urban. Rural areas are less dense and are usually devoted to agriculture. The status of a region as urban or rural can change based on the decision of the federal subject it finds itself in. (See: Legislative Assembly of Krasnoyarsk Krai. Law 21-5541 of December 26, 2006 "On Changing the Category of the Settlement of Aban of Abansky District to That of a Rural Inhabited Locality"; State Duma of the Russian Federation. Federal Law 131-FZ of October 6, 2003 "On General Principles of the Organization of Local Self-Government in the Russian Federation").

Search Engine: A web site that maintains an index and short summaries of billions of pages on the web. Examples include Google and Yandex. (Source PC Magazine <http://www.pcmag.com/encyclopedia_term/0,2542,t=Web+search+engines&i=54339,00.asp>).

SMS: Short Message Service. A service available on digital networks, typically enabling messages with up to 160 characters to be sent or received via the message centre of a network operator to a subscriber's mobile phone. (Source: ITU, <<http://www.itu.int/osg/spu/publications/portableInternet/ExecSummFinal2.pdf>>).

Social Networking Site: A web-based service that allows individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site. Examples Include Facebook, Odnoklassniki, VKontakte Tvidi.ru and MoiMir. (Source: Boyd, d. m., & Ellison, N. B. (2007), "Social network sites: Definition, history, and scholarship", <<http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>>).

Software - The programmes or other "instructions" that a computer needs to perform specific tasks. Examples of software include word processors, e-mail clients, web browsers, video games, spreadsheets, accounting tools and operating systems. (Source: Center for International Development at Harvard University, Information Technologies Group, <<http://cyber.law.harvard.edu/readinessguide/glossary.html>>).

Spam: The abuse of electronic messaging systems to send unsolicited bulk messages, which are generally undesired. (Source: ITU <<http://www.itu.int/ITU-D/cyb/cybersecurity/spam.html>>).

STELLIT: Russian NGO whose mission is to "improve the health and social well-being of people by assisting a broad range of professionals, including policymakers, to implement evidence-based, efficient social programmes into practice". (Source: <<http://eng.ngostellit.ru/>>).

Urban: In Russia, cities and urban-type localities, officially designated as such, usually according to the criteria of number of inhabitants and predominance of agricultural, or number of non-agricultural workers and their families. (Source: UN Demographic Yearbook 2005, UNSD, <http://unstats.un.org/unsd/demographic/sconcerns/densurb/Defintion_of%20Urban.pdf>).

World Wide Web: The complete set of electronic documents stored on computers that are connected over the Internet and are made available by the protocol known as HTTP. The World Wide Web makes up a large part of the Internet. (Source: ITU, <<http://www.itu.int/ITU-D/ict>>).

Youth/Young People: Males and females, aged 14-24 years old. (Source: United Nations Children's Fund (UNICEF), "The State of the World's Children 2011", <http://www.unicef.org/sowc2011/pdfs/SOWC-2011-Main-Report_EN_02092011.pdf>).