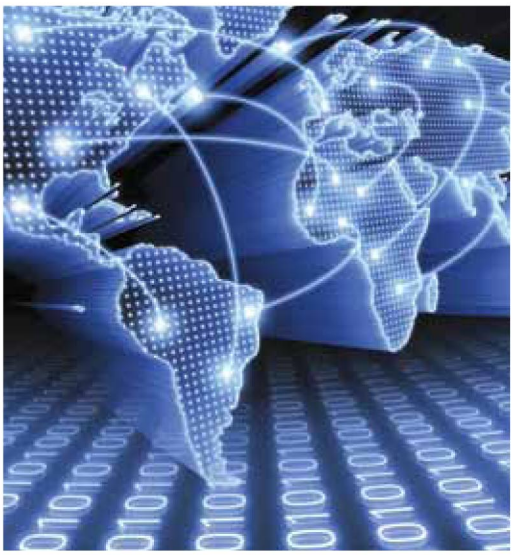
RIAC

Russian International Affairs Council



WORKING PAPER

RUSSIA AND THE CHALLENGES OF THE DIGITAL ENVIRONMENT

№XV 2014

Russian International Affairs Council

Moscow 2014

Russian International Affairs Council (RIAC)

Editor-in-Chief:
I.S. Ivanov, Corresponding Member, RAS, Dr. of History

Authors:
V.S. Ovchinsky, Dr. of Laws; **E.S. Larina**; **S.A. Kulik**, Ph.D. in Political Science

Drafting and copy editing:
I.N. Timofeev, Ph.D. in Political Science; **T.A. Makhmutov**, Ph.D. in Political Science; **A.L. Teslya**

Russia and the Challenges of the Digital Environment: Working paper / [V.S. Ovchinsky et al.]; [I.S. Ivanov, Editor-in-Chief]; [Russian International Affairs Council]. – Moscow: Spetskniga, 2014. – 36 pages – Authors are listed on reverse of title page. – ISBN 978-5-91891-369-7.

This working paper was written as part of the Russian International Affairs Council's project "Information Security, Response to Cyber Threats and the Use of the Internet to Defend Russia's National Interests on the International Scene." In their articles, the authors expound on Russia's presence in cyberspace and suggest the identification of a reference point from which to develop the discussion and seek an effective strategy for Russian participants in global internet processes. The materials place particular emphasis on the use of online tools to improve the quality of foreign policy.

Photo used on the cover is taken from www.heywire.com.

THE WORKING PAPER IS AVAILABLE AT OUR WEBSITE. YOU CAN DOWNLOAD THE FULLTEXT VERSION AND LEAVE YOUR COMMENT HERE – RussianCouncil.ru/en/paper15

TABLE OF CONTENTS

FOREWORD

The past two decades have been characterized by the growth of the internet. It is easy to see that the virtual world increasingly influences current events, and the distinction between the virtual and real worlds is becoming less and less clear.

In the early stages of the development of the internet, it was difficult to imagine that it would become such an integral part of our lives, with its variety of phenomena and processes. We often talk about electronic commerce, telemedicine and the latest means of communication, including video calls and online education. Now the internet has even begun to incorporate elements of public administration, domestic politics and international affairs. The majority of public authorities have developed their own virtual representation in the form of websites and internet portals that provide electronic government services, including electronic voting on significant social issues and digital diplomacy. Users' activity has gained particular importance in virtual social networks, where they can directly and rapidly shape public opinion on current events. The foreign ministries of several countries have even begun utilizing popular social media sites such as *Facebook* and *Twitter*. Every year, the variety and number of online tools increases.

The number of possible internet-related threats facing online participants and web users is also growing, as is the architecture of the entire internet. Developing strategies for the use of online tools is fundamental in setting priorities in the virtual realm. The world's leading nations need to consider these tasks as a priority. Russia is no exception. Considering the global nature of the internet, the key for countries developing internet strategies lies in the appropriate use of network capabilities to protect and promote state interests. In this case, special attention should be paid to both the physical protection of facilities providing internet services and the protection of the state's critical virtual infrastructure.

Intense discussions continue in international forums and the *United Nations* about the possibility of internet regulation. Questions of security, the degree of state regulation in network processes, and the growing number of non-state actors involved in internet communications are the principal themes in such discussions. The most controversial topic of discussion is the aspiration to, and capacity for, individual states to take control of the media. With good reason, the Russian Federation suggests that this would significantly affect the entire architecture of international stability. It therefore demands the development of carefully calculated decisions supported at the international level.

This publication of the *Russian International Affairs Council (RIAC)* invites international relations and information communications technology experts to discuss the prospects and opportunities for Russia to participate effectively in internet governance.

V.S. Ovchinsky, E.S. Larina

THE GLOBAL DIGITAL ENVIRONMENT: OPPORTUNITIES AND RISKS FOR RUSSIA

Introduction

The information environment has been around for as long as humanity. The only things that have changed are the means of communication, the ways of storing and providing information, and the level of its availability. Historically, the development trend for this sphere has been a steady increase in the availability of information resources to individuals, nations, non-governmental organizations and businesses. Communication channels and access to information are simultaneously becoming increasingly diverse and up-to-the-minute. The breadth and diversity of information channels and the ever increasing proportion of the population that they cover are continuously improving the connectivity of the world. Before the internet appeared, any two people in the world were connected by six steps. Today, this number has decreased to four and continues to decline.[1]

Cyberspace, as it is understood today, first appeared during the first industrial revolution, with the massive proliferation of machines and mechanisms. Each machine contained a control panel, through which an operator controlled forces many times greater than his physical abilities. Cyberspace serves as a metaphor for a space characterized by the mass distribution of signals in controlling systems. The concept of cyberspace was first introduced by American writer William Gibson in his novel *Neuromancer*, and soon became popular within the military and among information technology professionals.

Over the past 200 years, cyberspace has been continuously expanding, and the possibility of controlling various machines and mechanisms remotely has been increasing steadily. A quantum leap occurred in this technological advancement with the advent of the internet and its mass application in the industrial, social, communal and other spheres. From this point on, the concept of cyberspace became intertwined with the internet, telecommunications and other networks.

Obviously, both the information sphere and cyberspace developed a fundamentally new quality with the advent of the internet,

[1] **The six degrees of separation theory** – the theory that states everyone and everything is six or fewer steps away, by way of introduction, from any other person in the world (hence six degrees of separation). URL: http://www.en.wikipedia.org/wiki/Six_degrees_of_separation

based on IT and computer engineering. The basis of any calculation lies in operations with real numbers. Therefore, in recent years, official statements and publications, various professional communities including politicians, military strategists, and even people in their everyday conversations, have all adopted the term “digital environment”.

Mapping the Digital Environment

The digital environment includes a wide range of information technologies and covers the whole cyberspace. Accordingly, information security is directly related to the digital environment, but it is only one aspect. Likewise, in the strictest sense of the word, cyberspace is the part of the digital environment in which various types of objects in the physical world are managed using the internet, networks and other telecommunication channels.

The digital environment has its own:

- Infrastructure. First of all, this includes internet and telecommunication lines such as fibre optic cables. Secondly, it includes computer systems of various dimensions, ranging from supercomputers to smartphones and tablet computers. Thirdly, this includes the computational control systems built into different objects in the physical world, from assembly lines to sports shoes and t-shirts.
- Structure. This comprises, first and foremost, software protocol networks that support the transfer of information across networks, including the internet, corporate networks and peer-to-peer networks such as *Tor*. Secondly, it includes programs and programming platforms that store, process and present information. Such systems include everything from databases to familiar operating systems such as *Windows*, *Linux* and others. Finally, this structure includes interface programs that provide end users with usable information (interfaces of sites, blogs, portals, applications, different kinds of programs, etc.).
- Ultrastructure. This includes the infosphere, which contains direct and implicit meanings expressed in text, tables, video and audio content. The ultrastructure first of all includes shared network resources such as websites, blogs, portals, social networks, etc. Secondly, it includes secured information resources only accessible, for example, to authorized users of state or corporate entities. Lastly, it contains shared resources with paid content.

Public communications networks have been developing for 25 years. Since 1991, when the public was given the opportunity to connect to a closed network, two fundamentally different types of networks have developed.

• The first type of network includes the internet, as well as internal state and corporate networks, which are inaccessible to outside users. These networks are built in a hierarchical manner. There are several levels of hierarchy within the networks, which are used to accumulate and transmit information. Accordingly, rights and opportunities for information management at each level depend on its position in the hierarchy. Therefore, rights and opportunities increase at higher levels in the hierarchy.

• The second type of network to develop is the so called peer-to-peer network.[2] Currently, the most popular of these networks include the *Tor* communication network and the *Bitcoin* payment network. In peer-to-peer networks, information is transmitted between users' computers, which have completely equal rights and opportunities to transmit information. Because of this, peer-to-peer networks are usually much slower than the internet.

These types of networks function independently from each other. Accordingly, the resources of one network cannot be detected or found by other networks' search engines. At the same time, each of these networks has special portals that allow users to access resources in other networks.

The internet has the following mapping:

• Web 1.0 is the oldest and most established segment of the internet. It includes government, corporate, public and personal portals, websites, blogs and other online media. Resources are readily available in this internet segment using search engines such as *Google* and *Yandex*.

• Web 2.0 is the so-called social web, which is home to social networking sites and platforms. This internet segment houses resources such as *VKontakte*, *Facebook* and *Twitter*. It became known as the social web because much of the content in this segment is produced by users themselves. Due to the policies of platform owners and social networking sites, as well as privacy requirements, this segment is only partially visible to search engines. Video and photo sharing are rapidly increasing in this segment.

• Web 3.0 is an internet segment that has appeared in the last two to three years and is the fastest growing. So-called mobile web applications, or apps, have user interfaces that are optimized for viewing on tablets and smartphones. Accordingly, users work directly with apps without the use of search engines by simply connecting their devices to the internet.

---

[2] Decentralized peer-to-peer or P2P networks implement overlay networks based on equality among participants.
URL: http://www.en.wikipedia.org/wiki/peer-to-peer

• The Invisible Web (or Deep Web) contains resources, portals and sites that cannot be found by search engines. Access to this segment is either paid or requires special permission for the use of its resources. According to available data, the Invisible Web contains approximately 90 per cent of the valuable scientific, technological, financial, economic and state open source content available today.[3] The volume of the Invisible Web is constantly growing, because it develops much more rapidly than the web 1.0 and web 2.0 segments. The main reasons behind this increased rate of development are twofold. On the one hand, corporate users are attempting to archive all of their available data. On the other, resource owners are attempting to remove their data from the open internet and move it into paid platforms for monetization purposes.

• The Internet of Things refers to the connection, via the internet, between control centres and the information units embedded in various objects and facilities located in the physical world, including industrial, social and communal infrastructure. For example, this includes the connection of manufacturing lines, water control systems and heating systems to a worldwide network. In the past two years alone, it has become a mandatory default requirement for household appliances and equipment, including refrigerators and washing machines, to have internet connections.

• Bodynet. With the rapid development of microelectronics comes the opportunity to integrate elements that transmit information into clothing items (shoes, shirts, etc.). This technology also allows for the extensive use of microelectronics in the new generation of medical equipment, including various types of implants, ranging from devices that regulate blood sugar to artificial hearts. In addition, the trend in recent months has been the development of a distributed computer with elements imbedded in the human body. In this case, the person wears the computer and interacts with it around the clock.[4]

Most peer-to-peer networks belong to the so-called dark web. The name of this network segment comes from the fact that its extensive resources are used by various criminals, illegal groups and factions. The main segments of this network are the *Tor* network, which was developed in 2002 by U.S. Office of Naval Intelligence, and the *Bitcoin* payment network. Currently, these networks are used predominantly for illegal activities such as cybercrime, drugs and weapons trafficking and targeted actions taken to undermine state sovereignty.

---

[3] Pierluigi Paganini, Richard Amores. The Deep Dark Web. 2012.

[4] For details, see: Larina, E.S. Meet Bodynet! URL: http://www.therunet.com/articles/1877-vstrechayte-bodynet (in Russian).

So-called “money networks” are a special network segment partially located on the internet and partially in specially created peer-to-peer networks. The worldwide trend is to reduce cash payments and turn to using electronic money in all its forms. Money networks include specialized telecommunications network designs linking large banks such as SWIFT and other internet payment systems such as *PayPal* and *Yandex.Money*. Separate, fast-growing segments of these money networks have developed specialized payment systems based on peer-to-peer networks and encrypted messages. The most famous of these is the *Bitcoin* payment system.

Thus, the digital environment has a complex cartography in which individual segments have developed on their own, independent of general patterns and trends. At the same time, there are a number of fundamental tendencies shared by all segments.

The first fundamental trend in the digital environment is the information explosion. In recent years, the amount of available information has been doubling every two years.[5] According to *Cisco*, the volume of data generated in 2012 was around 2.8 zettabytes. By 2020, this number is expected to increase to 40 zettabytes.[6] Approximately one third of this data is automatically generated, i.e., control signals, information associated with machinery and equipment operation, and appliances connected to the internet. Additionally, there is a 40 per cent annual increase in the volume of corporate data that is transmitted and stored online.

At the end of 2013, there were 2.7 billion internet users worldwide, or 39 per cent of the earth’s population. The *United Nations News Centre* estimates that by 2016, this number will grow to 65–75 per cent of the population.[7] It is expected that the number of corporate internet users worldwide will grow from 1.6 billion in 2011 to 2.3 billion people in 2016.

In 2012, more than 90 per cent of users accessed the internet from computers, and only 10 per cent of users accessed it from mobile devices. By 2016, the number of users accessing the internet from tablet computers, smartphones and other gadgets is expected to increase to at least 45–50 per cent.[8]

---

[5] IDC iView.Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East. URL: http://www.emc.com/leadership/digital-universe/2012iview/big-data-2020.htm

[6] Cisco Visual Networking Index: Global Data Traffic Forecast Update, 2013–2020. URL: http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/white-paper-listing.html

[7] The world has seen a rapid growth in the number of subscribers to the Internet and mobile communications / / UN News Centre. URL: http://www.un.org/russian/news/story.asp?NewsID=20390#.U00YSvl_uSo (in Russian);

Report of the International Telecommunication Union, “Measuring the Information Society.” 2013. URL: http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013-exec-sum_R.pdf (in Russian).

[8] Report “Mobile Internet in Russia and the World: Platforms, Consumption, and Tendencies,” presented by Nielsen and the Mail.Ru Group. URL: http://corp.mail.ru/blog/mobileinternet/ (in Russian).

Russia is one of the world's leading countries in terms of internet use. More than 55 per cent of the population currently uses the internet,[9] and in large cities, that statistic is closer to 75 per cent. A year-on-year decrease in the cost of broadband internet access and the transition to new standards of mobile communication that provide coverage to residents of areas not previously covered open up entirely new opportunities for economic, public and social development.

To begin with, opportunities are emerging for the creation of state-wide corporate systems for continuous distance education. Such systems will help people develop competencies for the most in-demand jobs, including trades and professions that did not exist in the past. Just as many opportunities are available in internet medicine, which has been widely distributed in the United States, Western Europe and several other countries in the past several years. It is worth mentioning that, by the end of the 1990s and the beginning of the 2000s, Russia had developed an e-health system within the *Russian Railways* to cover the entire country. Given new technological capabilities, such a system can be implemented nationally or scaled for use by individual regions or large corporations.

Massive opportunities exist in Russian e-commerce (companies that are Russian residents and do business online). It ranks 13th in the world in terms of volume, but in terms of growth, it exceeds Europe.[10] The key issue for sustainable growth in e-commerce is the rapid development of cashless payment turnover in the form of electronic payments by credit card and other online payment methods. The development of Russian e-commerce will also facilitate international legal measures to prevent dumping by foreign e-commerce markets. Such measures are currently in place in Germany, the United Kingdom and other countries.

Protecting "Digital Sovereignty"

Historically, the internet has developed as an environment free for the informal exchange of information. However, it was formed through the rigid technological programs and organizational control methods of the United States, the country that created the World Wide Web. As a result, the world is now in a paradoxical position. The key activities of every state, including commerce, financial op-

[9] The Internet in Russia: Dynamics of Penetration. Autumn 2013, Public Opinion Foundation.URL:http://www.fom.ru/SMI-i-internet/11288 (in Russian).

[10] Russia ranks 13th in the world online trade rating. URL: http://www.cnews.ru/top/2013/11/19/rossiya_zanyala_13_strochku_v_mirovom_reytinge_onlayntorgovli_550401?goback=.gde_135696_member_5808972659395956737 (in Russian).

erations, political and social activism, have all shifted to the internet. Meanwhile, there are no post-Westphalian principles of international law on the internet, like there are in the real world. Of course, "digital sovereignty", joint international internet governance, and dissemination guidelines for the post-Westphalian international system on the internet are important foreign policy objectives for Russia and a growing number of like-minded countries with respect to the principles of international internet regulation.

The second most important trend in the digital environment is the formation of the Internet of Things. This includes a wide variety of technological, manufacturing and infrastructural devices, appliances and tools that are controlled by, communicate with, or are otherwise connected to the internet. There are currently more than 17 billion devices connected to the internet.[11]

According to a forecast by the *IDS*, by 2020 there will be 212 billion devices connected to the Internet of Things. The monetary capacity of this market will be $8.9 trillion. Moreover, an estimated 30.1 billion stand-alone devices, ranging from cars to vacuum cleaners, will be connected to the Internet of Things.[12]

The development of the Internet of Things creates limitless possibilities and opportunities for the Russian and world economies. As real-world experience shows, by analysing the data received from infrastructural facilities connected to the internet, we can achieve a 20–30 per cent reduction in the time motorists spend on congested highways and a nearly 15 per cent decrease in the overhead costs of water and electricity for residential and industrial buildings.[13] Finland and Norway have implemented "smart home" and "smart apartment building" technology, in which every flat and every heat and energy supplier is connected to the internet. This technology allows for a 12–17 per cent reduction in heating costs, while maintaining a constant temperature in residential areas.[14] Clearly, the Internet of Things will have an even more impressive effect in Russia. This effect may be connected with several factors, including Russia's climatic and environmental features, the significant delay in the implementation of various programs aimed at conserving utility resources, and the ample and growing number of megalopolises and agglomerations, where this effect will be most pronounced and on the largest scale.

---

[11] Gartner. The Internet of Everything: Business Models and Scenarios. 2013. URL: http://www.gartner.com/newsroom/id/2621015

[12] Worldwide Internet of Things (IoT) 2013–2020 Forecast: Billions of Things, Trillions of Dollars. IDC, 2013. URL: http://www.idc.com/getdoc.jsp?containerId=243661

[13] Ibid.

[14] Gartner. The Internet of Everything: Business Models and Scenarios. 2013. URL: http://www.my.gartner.com/portal/server.pt?open=512&objID=202&mode=2&PageID=5553&showOriginalFeature=y&resId=2610121&fnl=search&srcId=1–3478922244

As a rule, the threats associated with the Internet of Things can be reduced to different types of cybercrime and even cyber terrorism. When the entire infrastructure of population centres, residential areas, buildings and people's livelihoods are completely tied to the Internet of Things, malicious intrusion can have unpredictable consequences. Therefore, states with highly connected populations whose incomes are high enough to purchase integrated devices need to engage in close international cooperation in the fight against cybercrime and cyber terrorism. It is already clear that this cooperation should not be limited to taking legal action, but should also include a regular exchange of information and effective tools to combat cybercrime and cyber terrorism. Additionally, states should consider the proposal to establish joint voluntary international forces to counter cross-border cybercrime and cyber terrorism groups. Russia, with its first-rate professionals and resident companies,[15] which are leaders in personal and corporate information security, can undoubtedly play a significant role in this work.

There is one more threat from the Internet of Things to Russia's digital sovereignty that has gone relatively unnoticed. Search engines and social network platforms like *Facebook* and *Twitter* currently make it possible to analyse user behaviour, preferences, activities and communications across a variety of user groups. With the emergence of the Internet of Things, not only can internet activities be monitored online, but so can the real life activity of the public, business operations and the workings of municipal and other structures. In the Internet of Things, such information is transmitted to the suppliers of microprocessors or manufacturers of products that connect to the internet. Consequently, complete sets of information about the real world show up in these companies' online networks. The information may also be available to individual, corporate and governmental users of systems outfitted with the Internet of Things. This is precisely why leading internet companies like *Google* have recently begun making deals worth hundreds to billions of dollars to acquire firms associated with it. This issue can be avoided in two ways. The radical method would be to develop a separate microelectronics industry to produce chips for devices, equipment and systems connected to the Internet of Things. The more palliative method would be to set up a mandatory precondition for the sale of articles, equipment and devices connected to the Internet of Things in Russia. This condition would require the relevant companies to establish data processing centres in Russia and in the territories under its jurisdiction.

[15] The activities of a number of these companies can be found on the website SecurityLab. URL: http://www.securitylab.ru (in Russian).

The advent of a wearable internet system, or "bodynet", is taking place before our very eyes. This piece of the internet network comprises three groups. The first takes the form of accessories such as *Google Glass*, which are already heralding a new era of distributed computing. The next is internet-connected garments, such as everyday clothing and shoes, which generally regulate the state of a wearer's health or other such parameters. The third group, which will be most actively developed in the future, comprises the electronic components of micro devices that are implanted directly into a person's body. Today, nearly one million Americans have medical implants that are connected to the internet. These are mostly devices for cardiac monitoring, while some others regulate blood sugar levels. The cost of such implants is falling year by year, not by percentages, but by degrees of magnitude. The number of implants is growing exponentially, due in large part to achievements in biotechnology and micro engineering.[16] There is reason to believe that in the next five to seven years, internet-connected implants embedded in the human body will become commonplace in practically every developed country in the world.

Although medical treatment is generally lagging in Russia, and this includes the commercial application of implants, Russian researchers do have a number of impressive developments under way and are joining the ranks of world leaders in medical cyber technology. Given adequate cooperation between the state and the private sector, Russian hi-tech businesses could not only retain a considerable share of the domestic market, but could also have a greater opportunity to compete in separate sectors of the global market for hi-tech medical internet technology.

The widespread distribution of bodynet items gives rise to new kinds of dangers related to cybercrime, which include grievous bodily harm, homicide and targeted cyber terrorism. In the United States, this threat is already seen as a pressing issue, and concrete countermeasures are being developed on both the state and private level. Considering the worldwide recognition of highly qualified Russian specialists in penetration testing (ethical hackers), Russia has a unique chance to turn such a threat into an opportunity for business and, indirectly, for the government. In order to realize this potential, a Russian public-private initiative needs to be developed as soon as possible to create a pool of microelectronic technology producers, medical implant manufacturers and companies that are engaged in information security and penetration testing. This pool would serve as a reliable defence against mass cybercrime related to malicious interference with the functioning of internet-connected implants.

[16] Nanomedicine – Healthcare in the 21st Century. Cleveland Clinic, 2013.

The Digital Environment and the Third Industrial Revolution

The unfolding third industrial revolution is a critical process that impacts global finance and political structures and effects change in the manufacturing base, the system of economic ties, and the international division of labour. At its core, the third industrial revolution is the total integration of digital technology into the basis of industrial activity. In the early 2000s, digital technologies were already in active use in business, primarily in what is called business analytics, as well as in other forms of business information solutions. At that time, however, information technologies were relegated to management processes.

In the last several years, the situation has changed dramatically due to the mass introduction of robotics, automated production lines, and the expansion of 3D printing.

The United States currently has, or is preparing to launch, 9,000 fully automated production facilities. The United States is unquestionably the world leader in the industrial production of hi-tech robotics. This year, U.S. companies supplied just under 20,000 hi-tech anthropomorphic robots.

To be fair, it should be acknowledged that the United States does not lead in the already established robotics industry. Here, the first place goes to Japan, followed by China and only then the United States. South Korea and Germany round off the top five list.[17] According to expert assessments, Chinese robots are less technological and are primarily utilized for elementary assembly work related to household appliances and other traditional devices.

According to estimates from various sources, in the coming years, a mass-scale application of robotics will unfold in the United States, South Korea and Japan. Mass robot production already under way. This technology is more cost effective compared not only with the work performed by workers with specific qualifications, but also with the work done by lower skilled assembly line workers. Without exception, all automated and robotic production lines, as well as select industrial robots, are linked up both to corporate networks and the internet.

Alongside robotics, 3D printing is a key element of the third industrial revolution. Three-dimensional printing uses a technology known as additive manufacturing, in which an item is manufactured through the progressive addition of raw material. Three-dimensional printers do not print ink onto paper – they “grow” objects from plastic, metal or other materials.

[17] A Good Year for Robots. URL: http://www.computerra.ru/90864/horoshiy-god-dlya-robotov (in Russian).

Initially, 3D printers were utilized primarily in design. Now 3D technology is used in a variety of fields, from manufacturing furniture and clothing to operating in hi-tech branches of industrial operations. This year, major corporations made breakthroughs in the industrial application of 3D printers. Three-dimensional production lines are currently being built by *Boeing*, *Samsung*, *Siemens*, *Canon*, *General Electric* and others. By the end of 2013, the global market for 3D printer sales was valued at $3–3.5 billion, and on average sales are growing at an exponential rate, doubling every 18 months.

The undisputed leader in the production and use of 3D printers is the United States. It is responsible for almost 40 per cent of global production. Japan is responsible for about 10 per cent, as are Germany and China. The UK completes the top-five list, with a share of 6 per cent. Russia comes in at tenth.[18]

3D printing, like robotics, is closely linked to information technology. The vast majority of 3D factories are connected to the internet and use remote systems to store information and make the computations needed to ensure that the printers operate smoothly.

The third industrial revolution is changing the industry, and this is a highly dynamic process. Because of this, Russia has a great chance to maximize its own potential. In the United States, Europe and China, the mass use of the aforementioned technologies is constrained by an inevitable reduction in the capitalization of existing production facilities. These facilities are in good working condition, have short service lives, well-adjusted logistics, and systems in place for marketing and sales. In Russia, production facilities are characterized by a high degree of wear and tear and an abundance of machinery, equipment and technological lines that have extremely long service lives. Accordingly, there are no obstacles to introducing more progressive technologies to industry in Russia. In addition, the technology of the third industrial revolution is fully immersed in the digital environment and requires highly trained professional programmers, developers and equipment operators. Russia is globally competitive in this regard, and it boasts a substantial number of specialists in the information sciences, ranging from mathematicians and cognitive linguists to developers and programmers. The country also has a well-established regimen for training and retraining operators.

The most apparent threat that the third industrial revolution poses to Russia stems from the fact that the country missed the two previous revolutions in information science, the microelectronics revolution and the internet revolution. Consequently, Russia lost its position as a leader in science and technology and is on the same level

[18] World 3D Printing (Additive Manufacturing). Fredonia Group, December 2013.

as emerging states. The danger now is that Russia will miss the third industrial revolution. It will require a joint effort on the part of the government and the business sector, as well as maximum widespread international cooperation, to avert this danger. This can happen in many different ways – not only by inviting professors, leading product engineers and designers, but also by purchasing smaller, innovative venture firms that manufacture robotics and 3D printers. There are a considerable number of such firms with innovative technologies overseas, and they are experiencing a significant shortage of capital. Because of strong competition coming from the North American, European and Asian markets, these firms have limited opportunities to advertise and create a market for their products. As such, there is room to take advantage of Russian and overseas expertise, so that Russia could assume a leading role even in the early stages of the third industrial revolution.

A distinctive feature of our time is that practically all branches of science and technology, including the life sciences, are integrated into the digital environment. In the last ten years, information sciences and technologies have been combined with life sciences and biotechnology at an increasing rate. Bioinformatics and its myriad practical applications, generally referred to as genetic information engineering and industrial biotechnologies, have already been formulated. The most apparent manifestation of industrial biotechnology is individualized medicine, which both pharmaceutical giants and young, rapidly developing pharmaceutical companies are banking on. Various kinds of “regenerative medicines” are also included in industrial biotechnology. Three-dimensional printers are being used to produce donor organs and have been adopted by medical facilities in France, Germany and the United States. This may seem like science fiction, but it is a clinically tested routine.

A special area of biotechnology is synthetic biology. Synthetic biology enables new kinds of bacteria and other living organisms to be produced directly from a computer. This is done using special solutions and programming codes that are transmitted by a computer into a growth medium.

The cost of equipment for computer-based genomic surveying is dropping several times over on a yearly basis. Five to seven years ago, this research cost tens of thousands of dollars, and the equipment for it cost millions. Today, that same research is conducted by hundreds of companies around the world with equipment whose cost has decreased by orders of magnitude. Computer-based genetic research technology truly opens up boundless opportunities for genetic engineering and creating fundamentally new types of medicine.

Russia's capabilities in bioinformatics and biotechnology are marked by a long history of ground-breaking developments that can be broken down into several parts. Until 1991, Soviet microbiology and bioengineering were foremost in the world. According to American experts such as *Project Socrates* founder Michael C. Sekora, it was thanks to a specialized Russian committee – *Glavmikrobioprom* (the chief administration for the microbiological industry) – along with a large network of subordinate scientific research centres and educational institutions, that the Soviet Union surpassed all other governments in several fields of biotechnology and genetic engineering.[19] However, a significant amount of this potential was lost as a result of international measures to dispose of biological weapons, as well as the degradation of the hi-tech branches of Russian domestic industry in the 1990s. Today, Russia could, by properly mobilizing its resources, make up for lost time. Such resources include existing designs and scientific accomplishments, active schools of science, and the diaspora of Russian biotechnologists working abroad.

If bioinformatics and genetic engineering were to develop without regulation, the ruinous consequences could exceed the damage done by nuclear weapons. Political, legal and technological instruments have been established to regulate nuclear weapons, control their distribution, and prevent them from falling into the hands of terrorist groups. Similar tools for biotechnology do not yet exist. According to several experts, this will present the greatest threat to Russia and the rest of the world within the next three to five years. The threat is sharply enhanced by current achievements in bioinformatics that make it possible to create "bio-cyber" weapons with a directional effect (i.e. weapons that can affect groups of people with certain genetic markers). Accordingly, the top priority should be to implement a multilateral initiative for international cooperation to prevent the development of bio-cyber weapons or dual purpose biotechnology. This would exist on both the state level and among public organizations and foundations, to be backed by leading universities and corporations. In order to have a serious impact on such a pertinent issue, several things must occur. Not only must multilateral agreements be signed to develop a legal regime against bio-cyber terrorism, but measures must also be implemented in the framework of national legislative bodies on the basis of direct ties among the scientific, technological and commercial structures of various countries.

[19] For more information, see Ervin Ackman. President Reagan's Program to Secure U.S. Leadership Indefinitely: Project Socrates. URL: http://www.amazon.com/President-Reagans-Program-Leadership-Indefinitely-ebook/dp/B00G1RJWXW

The emergence, development and introduction of expert systems into various spheres of business, politics and daily life are rapidly gaining momentum. In the last two to three years, the United States, and to a lesser extent the United Kingdom, have made genuine breakthroughs in developing expert systems. These expert systems apply principles of programming that, inspired by examples in biological systems, simulate neural networks. The most famous expert system is *IBM*'s remarkable computer Watson, which won the very human-oriented game show Jeopardy. After the win, Watson went on to achieve impressive results as an expert system in the fields of medical oncology, pharmacology, police investigations and the stock exchange. According to the estimates of various professionals, expert systems will displace up to 70 per cent of workers in routine intellectual labour across a variety of fields in the next 7 to 12 years.[20] Expert systems afford users immense intellectual capabilities, multiplying the wealth of human knowledge by the power of computational algorithms. Note that *IBM* is not a monopoly. *Google*, *Facebook*, *Amazon* and others have all announced work in this area.

There is a powerful school of programmers, computational linguists and mathematicians in Russia now working in the field of expert systems. The first functioning expert system in the USSR was created as early as the late 1980s. A substantial number of specialists in natural language processing algorithms – the basis of expert systems – left the USSR and Russia and now work for leading international companies.

Russian mathematics and linguistics schools remain some of the finest in the world, and professionals in these fields are in high demand by leading transnational companies and government agencies. As such, Russia has the opportunity to catch up in the clearly lagging production of work-ready expert systems, which could be broadly utilized in various aspects of life. However, targeted national programs are needed to turn this possibility into a reality. As far as implementation goes, the decisive role will be played not so much by the availability of financial resources, but rather by the ability to form a team of experts distributed across different companies and educational institutions, domestic and overseas, and to create comfortable conditions for them to focus on the project.

The continuation, not to mention deepening, of Russia's lag in intellectual expert systems can be considered one of the most serious national threats. Without powerful and accessible expert systems

[20] For more information, see Erik Brynjolfsson and Andrew McAfee. Race Against The Machine: How the Digital Revolution is Accelerating Innovation, Driving Productivity, and Irreversibly Transforming Employment and the Economy. URL: http://www.amazon.com/Race-Against-Machine-Accelerating-Productivity-ebook/dp/B005WTR4ZI/ref=sr_1_3?s=digital-text&ie=UTF8&qid=1396004715&sr=1–3&keywords=machine+against

that are able to interact with the end user in a natural human language and are furnished with a powerful computing core, the country may encounter problems in practically all fields in the next five to seven years. Most importantly, a lack of such systems could make it difficult to maintain national defence capabilities and to make difficult policy decisions. It could also result in the systemic weakening of the overall competitiveness of Russian business.

The Digital Environment and the Expansion of Big Data

The widespread expansion of big data will perhaps be the defining factor of the dynamics of the digital environment in the coming years. The term "big data" emerged five years ago after the publication of a special edition of the journal *Nature* in 2008.[21] Since then, big data has played a leading role in information technology. Paradoxically, there is no strict definition of big data. However, those who work with it have an intuitive understanding of what big data implies:

- An enormous mass of information from various sources about events, processes, items and phenomena that are continuously occurring online. According to known statistics, 60 per cent of this information is unstructured and mostly textual. Forty per cent of it consists of structured, tabular information;[22]
- A specially designed programming platform in which big data of any volume can be stored in a form that is convenient for computation;
- The presence of various mathematical – primarily statistical – tools for processing big data and producing results in an understandable format.

At the largest ever conference on big data, it was stated that no more than 0.6 per cent of all information currently available is being accumulated, stored and processed.[23] That is, only 0.6 per cent of available information can be categorized as big data. Calculations estimate that 23 per cent of currently stored information can potentially be used in sucha way. This means that, at the present time, slightly more than 3 per cent of this information is being processed and analysed as big data. Meanwhile, recent advances in accumulation, storage and processing platforms for volumes of data in all formats allow potential big data to increase from 23 per cent to about 40 per cent of all network-transmitted information.

---

[21] Issue of Nature dedicated to big data. URL: http://www.nature.com/nature/journal/v455/n7209/index.html

[22] Gartner. Survey Analysis: Big Data Adoption in 2013 Shows Substance Behind the Hype. URL: https://www.gartner.com/doc/2589121/survey-analysis-big-data-adoption

[23] Predictive Analytics World. London, October 23–24, 2013. URL: http://www.predictiveanalyticsworld.com

In 2011, the *McKinsey Global Institute* declared that big data is "the next frontier for innovation, competition and productivity."[24] Its effect on business today is apparent. For example, in transnational *Fortune 500* companies – where with procedures and processes are streamlined – big data technology has increased resource efficiency in labour, chief production assets and energy by 5–7 per cent, and sales figures by 7–9 per cent. On average, the same figures for medium-sized businesses have increased by one-and-a-half to two times. These numbers were obtained in the aftermath of a severe global financial crisis, when economic growth was being calculated at 1–2 per cent at best.[25]

From 2011 to 2013, the United States and the United Kingdom implemented state initiatives aimed at indirectly stimulating the public adoption of what these governments consider to be rational solutions regarding the integration of big data technology, behavioural economics and politics.[26]

Why is big data effective? Big data technology, primarily methods of statistical analysis, computer-based pattern recognition, etc., based on enormous quantities of constantly updating data, makes it possible to:

- carry out the most varied classification of any number of people, companies or other objects using a variety of qualifiers, at any level of detail. Such classifications make it possible to obtain an accurate understanding of the relationship between the various characteristics of any object – from a person to a company or organization – and any of its actions;
- perform multivariate statistical or other mathematical analysis. This analysis makes it possible to find correlations between the most varied parameters, characteristics, events, etc. Correlations do not answer the question of why; they show the likelihood of a change in one factor causing a change in another factor. In a sense, big data is an alternative to traditional science. Science based on theoretical models answers the question of why, and then, after finding an answer, makes recommendations on how to act. In the case of correlation, there is no search for reasons, and action originates from cases in which factors are closely interrelated and a targeted impact can be made on one of the factors.
- predict. Predictions are based on classifications and analytic calculations. The essence of prediction is to identify the easiest way

[24] Big data: The next frontier for innovation, competition, and productivity. URL: http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation

[25] Cisco Connected World Technology Report. URL: http://www.cisco.com/c/en/us/solutions/enterprise/connected-world-technology-report/index.html

[26] For more information, see Cass R. Sunstein. Why Nudge?The Politics of Libertarian Paternalism. Yale University Press, 2014. URL: http://www.amazon.com/Why-Nudge-Politics-Libertarian-Paternalism/dp/0300197861/ref=pd_sim_b_17?ie=UTF8&refRID=043MRV8BETG3ZVZ55RZA

to have an impact so that one set of factors characterized by any object, person, company or event is converted into another.

Big data has primarily been used in marketing, the investment business and sales; that is, in areas where behaviour is indirectly and inconspicuously managed. Another application for big data is processes described by a multitude of parameters, in which a particular resource can be saved by making changes to a routine, mode or regime. Therefore, besides marketing and sales specialists, the most active big data users are government institutions and the energy sector.

When carrying out surveys, top managers at large corporations say that they use big data, but they are actually utilizing standard business analysis platforms, which are not capable of multidimensional classification and high quality prediction. They are generally satisfied with the analytical function. Besides that, an overwhelming number of Russian companies simply do not have large quantities of data that are constantly being updated online. In addition to this, Russia essentiallyhas no commercial big data brokers – companies that buy, gather, store and sell anonymous big data – which are active primarily in the United States and Japan.

At the same time, Russia has all of the essential prerequisites to achieve a real breakthrough in the big data sector. Since crucial software solutions for storing and processing big data are open and free, and considering Russia's colossal potential in statistics, mathematics and programming, Russia has every opportunity to make maximum use of big data technologies in all spheres, ranging from state administration to utilities and living needs, not to mention business.

For that, the government needs to provide target financing for big data platform developers oriented towards specific fields, from defence to small business, through its venture organizations, such as the *Internet Initiatives Development Fund*, *Skolkovo* and *Rusnano*. For comparison: last year, the United States financed about 80 big data startups through state channels, while more than 300 U.S. startups participated in a competition for the best international big data startup.[27] Today, experts recognize fewer than ten big data startups in Russia that meet international standards to a certain extent.[28]

If there is not a drastic change in the development of national platforms and services that work with big data oriented towards various state segments, economic sectors and business of all sizes – from transnational companies to small business – in the next two to three years, Russia will face a whole host of threats.

[27] Data of the authors.
[28] Data of the authors.

Perhaps the most visible of these threats would be a loss of the competitiveness that Russian businesses have obtained. It will not help to focus on foreign platforms, because as the events of last year show, the use of foreign services, software and other technology exposes countries to data leaks, including direct industrial espionage.

A far more serious threat is that big data technologies could be used against our country and society in conjunction with the instrumental implementation of achievements in the behavioural sciences. As indicated above, such techniques are currently being tested in the United Kingdom and the United States. It should be understood that big data was largely born in the marketing and sales sector and focused on the targeted management of group behaviour. Accordingly, advanced solutions based on combining big data with behavioural technologies offer endless opportunities for remote, undetected and effective control over the behaviour of large populations. This control can exist in various fields, ranging from boosting the consumption of certain goods and services, to remotely manipulating electoral behaviour. Big data is a typical dual-use technology, and in this regard it is not only important to have effective Russian solutions, but also to take timely initiatives within international organizations to legally ban the cross-border use of tools and solutions that combine achievements in big data technology and the behavioural sciences.

* * *

The digital environment is dynamic and malleable, and it does not always change in a predictable way. These changes are occurring as the third industrial revolution unfolds. Moreover, the digital environment is being transformed in the midst of increasingly uncertain global, economic, financial, political, military and social processes. All these factors are superimposed on the ever increasing complexity of human civilization and the strengthening of the network interdependence of all its components – from states to individual groups of people. Under these conditions, any conflicts, regardless of their nature and causing factors, are fraught with unpredictable development dynamics, as well as with a significantly growing tendency for escalation and reduced opportunities for timely reconciliation. In such circumstances, philosophy and practice of international multilateral cooperation is more important than at any other time in history. This philosophy should provide warnings of new outbreaks of confrontation, and should also prevent attempts at unilateral advantages by any member of the united but diverse world, which consists of an array of independent entities.

S.A. Kulik

NETWORKING TOOLS AND FOREIGN POLICY: MATERIAL FOR DISCUSSION

The rapid development of networking tools – information and communication technologies (ICT), social networks and the blogosphere – is more clearly seen during global and regional processes, and it has an effect on the ranking of problem agendas for the international community and individual states. This brings about a growing influence on state services involved in foreign affairs.

The topic of networking tools and foreign policy is rapidly becoming more sophisticated and extending beyond the scope of politicians' and experts' established patterns of thinking. New questions and surprises are likely to lie ahead. This is already increasing the burden on foreign ministries and expanding their field of activity. At the very least, it compels them to think more rapidly and carefully on this area in the priorities of Russia's international activity, as well as on the appropriateness of gradually and adequately reconfiguring this activity, including in terms of management. It is in the interests of state structures to set the clear task of reviving the expert community and enhancing interaction with it.

Intellectual resources, which at the present time are noticeably sparse, need to be brought together on an interdisciplinary basis – "techies", lawyers, "soft power" experts, etc. Without an understandable prescription of the values of networking tools, at least for "soft power" policy, the state focuses them more on technological issues in ICT security, protection from external influence and internet regulation. Despite the importance of these issues, the mountain of problems and challenges growing behind them on the international stage both for Russia and for other leading states may go unnoticed. It is useful to bear in mind that our major foreign partners are working consistently and very seriously on disciplinary compliance.

When analysing the opportunities that arise from the acquisition of networking tools, a clear preference is given – and not only in Russia – to the use of these tools for "soft power" needs, for raising the efficiency of "feedback" from state agencies with the public and other foreign addressees, and for generally playing games in the information realm in order to strengthen the state's position and reputation beyond its borders. In a rather simplistic view, this concerns the weight of network tools for foreign policy, as well as their use in this direction by authorities involved in international issues.

In addition to new opportunities, networking tools have also posed obvious challenges for these state services and have given rise to another set of tasks. With the development of ICT at the end of the last century, the governments of many countries has begun to worry about network leverage in the hands of terrorists and organized crime units, as well as about the disabling of critical infrastructure. These questions have started to transcend national borders, prompting bilateral and authoritative international forums at the highest level; for example, at the *G8*.

Later, prospects for and changes to the current internet regulation regime, with central servers in the United States, have begun to top the agendas of negotiating mechanisms. A number of countries, including Russia, express dissatisfaction with the fact that the World Wide Web falls outside the purview of the *United Nations* and its specialized agency, the *International Telecommunication Union*. Countries are also dissatisfied with the fact that the status quo does not consider the interests of all participants on an equal footing. Many leading nations, and not just those in the West, oppose any intentions to change this situation. Without mutual understanding, there arises a danger of "Balkanizing the internet" (the technical isolation of individual sectors and the establishment of one's own regulations in these sectors).

These issues have intensified and are gaining momentum on the global agenda. As before, difficult discussions and a negotiating battle lie ahead for several of these issues, particularly internet regulation.

Lately, foreign policy services have had their hands even fuller than usual. Of no less importance is the fact that the governments of leading countries and international structures have started rushing negotiations with respect to networking tools in an expanding list of formats.

The degree of dependence on global networking tool infrastructure is forcing the national leadership to start cooperating more closely and with greater speed in order to avoid a lot of undesired effects from the rapid development of ICT. The need has also arisen to try to jointly identify previously unconsidered future threats.

When looking at the *World Economic Forum's* report "Global Risks 2014," published in January 2014, it becomes clear that the dangers brought about by the development and spread of hi-tech and ICT have literally soared to the top at the international level, based on risk ratings beginning in 2007.[29] These dangers, which include cyber attacks, data theft and disrupting critical infrastructure, have begun to shadow even traditional geopolitical threats. One problem is that

[29] World Economic Forum report "Global Risks 2014." URL: http://reports.weforum.org/global-risks-2014

the latter has been counteracted on the basis of more or less effective experience and regulatory mechanisms. As far as dangers in cyberspace are concerned, however, we have a clear shortage of experience, understanding and management technologies.

Only recently, for example, have political leaders become aware that ICT does not merely help a nation's social and economic development; ever increasing malfunctions and various crimes in the use of networking tools are fraught with slowing down economic growth and weakening financial stability. This problem is knocking ever louder on the door of the *G20*'s negotiating rooms – it may even be posed as an entirely separate problem.

There is a risk of "digital disintegration" – the reinforcement of national protective measures against cybercrime without strengthening global cooperation. This would lower the status of networking tools as a reliable means of financial and economic dialogue and doing business. This would come with social and other costs.

For now, the threats arising from the networking space are mainly invisibly touched upon by many documents from international forums, including the *G20*. To varying degrees, this is characteristic of the basic foreign policy documents of leading states. It is sufficient to read the second part of the Concept of the Foreign Policy of the Russian Federation (dated February 12, 2013), called "Foreign Policy of the Russian Federation and the Modern World", more carefully. However, a number of challenges noted in this document – including those of a transnational scale – notably stem from networking tools. It should come as no surprise that the networking problems in these documents will start to be outlined in more detail and be of special focus for foreign affairs agencies.

More substantive official materials are already offering foreign policy structures more understandable arrangements. For example, the "Basic Principles for State Policy of the Russian Federation in the field of International Information Security," adopted on July 24, 2013, provides guidance for working with foreign partners on networking issues.[30]

A significant dynamic can be observed at the *United Nations*, which deals not only with new issues, but also with analytical work aimed at finding harmonized approaches. In the latter area, our participation is seen in the productive efforts of the *UN Group of Governmental Experts*.[31]

[30] Basic Principles for State Policy of the Russian Federation in the field of International Information Security. URL: http://www.scrf.gov.ru/documents/6/114.html (in Russian).

[31] See the Ministry of Foreign Affairs of the Russian Federation press release from 08.11.2013 on the adoption of the resolution "Developments in Information and Telecommunications in the Context of International Security," which took place at the meeting of the First Committee of the 68th session of the UN General Assembly. URL: http://www.mid.ru/brp_4.nsf/0/9C738EC38849040244257C1D004302B7 (in Russian).

The group has been successful in breaking the deadlock in disagreements over what seemed like a simple issue: one "club" of states prefers the term "cyber security" (all of the Western countries and many other leading players, such as Brazil and India), while the second club prefers "international information security" (Russia, countries in the *Collective Security Treaty Organization* and the *Shanghai Cooperation Organisation*). Amid a relative blur in suggested definitions, this issue has blocked a fruitful discussion on object of analysis itself and has provoked negotiators and experts to exchange mutual suspicions and claims. Their logic is that Russia wants to set high national barriers to information flows, while in the interpretation of their definitions, all the Western countries are primarily oriented towards maintaining the status quo in internet regulation. This has demonstrated the lack of any particular desire to go beyond a discussion of the internet's operating modes and deal with other topics on forming an international code of conduct in the use of network security tools.

The group's compromise proposals were developed and, most importantly, enshrined in a legal document dated June 17, 2013 – a joint statement by the presidents of the United States and Russia "On a New Area of Cooperation in Trust-Building."[32] The document concerns security threats in the use of ICT and of ICT itself. It also elaborates ways to counteract these threats. Having overcome the terminological dilemma of cyber security and international information security, the leaders of both "clubs" finally identified a clearer view of areas of cooperation. This succeeded in clearly prescribing certain tasks. Among them – more effectively protecting critical information systems, as well as addressing hazards caused by events that could endanger safe ICT use and ICT itself. In other words, setting tasks finally has become broader than the traditional set of issues surrounding information flows and internet regulation.

With the introduction of this initiative, it has become easier to reach agreements in international structures. The acceptance of the "Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies" became a landmark legal event at the regional level in December 2013. This also relates to security in using ICT and of ICT themselves.[33]

This does not concern just the considerable work that has already been done; it is also about the serious efforts that lie ahead in the implementation of these documents by foreign ministries and their

[32] Joint statement by the presidents of the United States and Russia "On a New Area of Cooperation in Trust Building." URL: http://www.kremlin.ru/ref_notes/1479 (in Russian).

[33] OSCE.Permanent Council Decision No 1106."Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming From the Use of Information and Communication Technologies." December 3, 2013. URL: http://www.osce.org/pc/109168

colleagues. This includes reaching a consent in the *Organization for Security and Cooperation in Europe* (*OSCE*) by October 2014 in a more detailed understanding of the terminology and, accordingly, the topic of further negotiations to expand the list of confidence-building measures. And this requires the consent of several dozen states with very different positions, and of varying "interest clubs". In the meantime, the main thing is that members of such a complex structure as the *Organization for Security and Cooperation in Europe* have understood that they have all ended up in the same boat in an ocean of risks associated with ICT.

Both events show the substantial success of Russian diplomacy, and in the coming months, a busy schedule of specialized forums and summits concerning networking tools with high official representation lies ahead. Serious battles will also occur in internet regulation in anticipation of the Plenipotentiary Conference of the *International Telecommunication Union* in October–November 2014.

It is necessary to take note of probable surprises that force networking tools into offices where there are discussions on topics that have nothing to do with it. Recent examples are talks between the United States and the European Union on creating a transatlantic partnership for trade and investment. The scandal surrounding Edward Snowden on the openness of cyberspace for American special services has given European negotiators a reason to heighten demands on an entire range of trade, economic and legal questions, which have added problems and work for Washington. And in general, these types of setbacks have increased the burden on the foreign ministries of both sides to rectify the transatlantic relationship. It is possible that Russia could also see this kind of surprises.

These exposures stimulate even more of the *UN*'s interest in networking tools, lifting them to new heights. The organization is closely and actively connected to the resolution of various problems, from internet regulation to the impact of cyber tools on civil rights and socio-economic development. This, in turn, will surely affect the plans of the Ministry of Foreign Affairs of the Russian Federation. Moreover, in the Concept of the Foreign Policy of the Russian Federation, international information security is mentioned specifically in the framework of this organization: Russia "will work under the auspices of the *UN* to develop an international code of conduct for information security" (Paragraph 32 i).[34]

The list of examples could be expanded upon, but we will limit ourselves to two considerations. First, the role of cyber issues in

[34] Concept of the Foreign Policy of the Russian Federation. URL: http://www.mid.ru/brp_4.nsf/0/6D84DDEDEDBF7DA644257B160051BF7F (in Russian).

foreign policy is increasing significantly, as is the part it plays in the expansion of the foreign policy agenda – and likely changes to its priorities – in Russia and its partner countries. These topics are increasingly extending into different negotiating dossiers. Secondly, this obvious and dynamic process leads to some interference by agencies involved in international affairs. Still present – and not only in Russia – is a deficiency in understanding of the real challenges posed by ICT development, which prevents a clearer formulation of the tasks arising from them. At the same time, concern for the next set of "surprises" is growing for the respective services.

Unlike the subject of networking tools **in** foreign policy, problems with networking tools **for** foreign policy are much more clearly defined in official documentation and analytical works for a number of leading countries, above all for the United States, Canada, leading European Union countries and China. Most importantly, these problems rely on a significant amount of practical experience. They also dominate expert discourse, official basic positions and official statements by the Russian authorities, but with an obvious deficiency in the prescribed view of the use of networking tools.

A whole host of tasks concerning "soft power" is enshrined in the Concept of the Foreign Policy of the Russian Federation, particularly in the provisions directly related to it – "International Humanitarian Cooperation and Human Rights" and "Information Support for Foreign Policy Activities." This is, however, only with brief mention of the fact that "possibilities offered by new information and communications technologies will be widely used in these activities."

In general, this base, as well as other official materials (e.g., those of *Rossotrudnichestvo*) offer a list of tasks, the successful implementation of which (including cost effectiveness criteria) depends largely on the scale of networking tool connectivity, as evinced by the experience of the United States, the United Kingdom and Australia, for example. It is still necessary to prescribe the role of the latter in separate guiding documents or in broader documents on the information component of foreign policy.

At a meeting of the Ministry of Foreign Affairs of the Russian Federation in July 2012, the Russian president noted, "Colleagues, our diplomats are well versed in the traditional and familiar methods of international relations, if not masters in this field, but as far as using new methods goes,'soft power' methods, for example, there is still much to reflect on."[35] This observation to some extent revived our

[35] Meeting with Russian ambassadors and permanent representatives of Russia. July 9, 2012, Moscow. URL: http://www.eng.news.kremlin.ru/news/4145/print

expert community, including those involved in networking tools. This was, however, only noticeable in the very beginning.

The language of networking technology for foreign policy has far been given rather free treatment with different understanding each of them.

There is a wide spectrum of definitions: “digital diplomacy”, “networking diplomacy”, “diplomacy Web 2.0” (in the last few months, the concept of “diplomacy Web 3.0” has also appeared), “*Twitter* diplomacy”, etc. This lack of consistency is quite understandable, not only in Russia, but throughout various other countries, which do not have their own official interpretations of such terms. To some extent, this resembles the debate on cyber security and international information security. For example, under the overarching banner of “*Twitter* diplomacy”, a number of questions have been raised that are rather unrelated to this particular tool. The subjects and objects of analysis have been blurred.

At a Moscow press conference on Russian diplomacy on January 21, 2014, Minister of Foreign Affairs of the Russian Federation Sergey Lavrov noted for the first time that “it is appropriate at this point to discuss information diplomacy.”[36] Earlier, representatives of the ministry had proposed a discussion of “innovation diplomacy”, which was taken to mean increasing work in the information sphere. At the end of 2012, Deputy Director of the Department of Information and Press at the Ministry of Foreign Affairs of the Russian Federation Yevgeny Panteleyev shared his detailed vision of “innovation diplomacy.”[37]

Evidently, the time has come for a more concrete set of tasks to be established in order to tackle the issue of networking tools for foreign policy. The issue has its own particular dimensions and differs from the concept of networking tools in foreign policy in form and content. Clear signals from the Ministry of Foreign Affairs of the Russian Federation to the expert community have been given and it’s time for useful collaborative work, including bottom-up collaboration. It is worth evaluating the pros and cons of the experience of several leaders in this diplomacy, primarily the United States and the United Kingdom.

This author published a report on the United States’ approaches to the subject, in which the official term “e-diplomacy” was coined. This term has been encountered in the titles of various structures, and also in some of the state department’s activi-

[36] Press conference by Minister of Foreign Affairs of the Russian Federation Sergey Lavrov on the results of Russian diplomacy in 2013. URL: http://www.mid.ru/bdomp/brp_4.nsf/2fee282eb6df40e643256999005e6e8c/b748284d938d69b144257c67003ac3cb!OpenDocument

[37] Panteleyev Y. Foreign Policy and Innovation Diplomacy // International Life. 2012. No. 12.

ties.[38] It is certainly understood there in a rather more generalized sense, such as in the use of the World Wide Web and new information technology to aid foreign policy goals. It is worth noting that this term is acknowledged in the European Union.

The experience of the British Foreign and Commonwealth Office drew on American knowhow, approving a "Digital Strategy" at the end of 2012.[39] Unlike the United States, the document refers to "Digital Diplomacy" (although without elaboration).

Of late, the following picture has been observed. Within the whole set of definitions referred to by experts, "Digital Diplomacy", alongside "e-diplomacy", has gradually begun to overtake the other terms. At the same time, use of the term "cyber diplomacy" has become increasingly linked to the topic of networking tools for foreign policy and to those issues touched upon in the first section of this research.

The focus points and tasks outlined in the Foreign and Commonwealth Office's strategy seem to be constrained mainly by references to distinct examples of activities from embassies and central departments, in order to increase the impact of "digital technology and other areas of foreign policy." This list includes: "following and predicting developments", "formulating foreign policy", "implementing foreign policy", "influencing and identifying who to influence" and "communicating and engaging on foreign policy."

The list appears to offer a rather scant choice of examples and is far from complete, testifying to the Foreign and Commonwealth Office's entirely natural unwillingness to open the door wide (only the United States' door is open wider). Even the range of issues which affects public opinion, including the underhand manner in which back-door methods and "know-how" are used to achieve goals, not to mention "formulate foreign policy", which is rather a touchy point. It is thus unsurprising that a significant part of the document and the list of examples is given over to a separate section on the use of networking tools to facilitate support, thereby improving the perception of the country for visa recipients, as well as its citizens that travel abroad.

Moreover, two rather important messages can be clearly discerned from the document, which were publicized earlier and then officially adopted by the U.S. Department of State. First, it is acknowledged that "the use of digital has expanded from a communi-

[38] For more information, see Kulik S. A. E-diplomacy – The Beginning / Institute of Modern Development, February 2013. URL: http://www.insor-russia.ru/files/EDiplomacy.pdf (in Russian).

[39] The Foreign and Commonwealth Office Digital Strategy.
URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/39629/AB_12–11–14_Digital_strategy.pdf

cations team activity to increasingly involving policy teams directly. A number of policy teams have taken direct charge of using digital to achieve policy outcomes, while others maintain digital channels themselves."[40]

In order to better understand the nature of this message, it is worthwhile examining activities and documents from the U.S. Department of State and their expert analysis. The preference to limit oneself primarily to social networking sites when analysing the use of networking tools in foreign policy creates a limited picture of "digital diplomacy". Aside from this, there are other important subjects and objects in the use of networking tools, both within and outside state mechanisms and foreign policy authorities.

If one proceeds from the assumption that this results in the increased effectiveness of such diplomacy for foreign policy, then this also includes some improvement in the coordination and running of the whole decision-making process. Networking tools afford new opportunities – opportunities for savings, optimizing the selection and distribution of evaluations and proposals by and within departments, managing large flows of information, etc. Therefore, when evaluating their potential use in foreign policy, one must be aware of the conditions required to reconfigure internal processes. However, at this juncture, outside experts inevitably run into entirely explicable restrictions, which are due to the closed nature of this mechanism, even in the leading democratic countries.

The world of foreign policy is too sensitive and risky to be completely open to third-party analysis. This is particularly the case regarding the issue of the "correct" use by diplomats of network infrastructure for service needs and external communications. However, it is worth noting that certain matters concerning networking tools within the foreign policy mechanism have already been outlined by the Deputy Director of the Department of Information and Press at the Ministry of Foreign Affairs of the Russian Federation, Yevgeny Panteleyev, in his vision of "innovation diplomacy."

Secondly, the impression created by intentions to increase the significance of networking tools for use not only outside, but also inside the mechanism for developing and adopting foreign policy decisions, is reinforced by stated plans of promoting those responsible for using network technologies and expanding HR training programs. This inclination was confirmed by A. Bye, responsible for strategy implementation at the Bri-

[40] The Foreign and Commonwealth Office Digital Strategy. P. 6. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/39629/AB_12–11–14_Digital_strategy.pdf

tish Foreign and Commonwealth Office. However, in a short annual report posted on his blog in December 2013, Bye maintained that the "formulation" and "implementation" of foreign policy, limited with examples of "initiatives" at the annual meeting of ambassadors, where the use of networking tools for "aiding foreign policy work" had been discussed.[41]

In this regard, we can see that the foreign ministries of many countries (including the field-specific civil service) are attempting to reinforce their "networking power" by actively engaging representatives of the private sector that deal with technology, PR companies, and other links to their area of expertise. There is a more active cooperation with large private networking companies. Cooperation with non-profit organizations in the use of networking tools to suit the state's foreign needs is expanding. It is no accident that the Foreign and Commonwealth Office in this vein has developed its strategy in a more prosaic document entitled "Leadership for Executives on Politics in the Social Media Sphere" (June 2013).[42]

All is quiet on this front in Russia for the time being. Despite the well-known Russian particularities, sooner or later this situation will have to change, both along the lines of a public-private partnership and the tangible but not declaratory broadening of non-profit involvement in "soft power" politics, with all their potential for effective work in networking.

Upon careful examination of U.S. and UK experience, as the leaders in harnessing networking tools for foreign policy, it may be useful to further analyse and evaluate the possible stumbling blocks. To a great extent, the pitfalls concern the use of networking tool-aided open channels of communication used by official personnel and diplomats.

In assessments of both countries' foreign policy departments, Western experts are generally united in their opinion that they prefer to proceed with caution on external platforms and not to take risks. Even small mistakes here can result in extremely serious consequences. Many officials work in an environment where strict control over channels, information content and reporting dominates the desire to expand the space and take advantage of new technologies.

Things are even worse for their allies. For example, according to data gathered in mid-2013, the ambassadors of the United States

---

[41] Bye A. Foreign Office Digital Strategy: One Year On // Digital Diplomacy – the FCO's Digital Work. December 20, 2013. URL: http://www.blogs.fco.gov.uk/digitaldiplomacy/2013/12/20/foreign-office-digital-strategy-one-year-on

[42] See Paris R. The Digital Diplomacy Revolution: Why is Canada Lagging Behind? / Canadian Defence and Foreign Affairs Institute, June 2013. P. 3.

and the United Kingdom outperform their Canadian colleagues many times over in the use of open information channels (*Twitter*, *Facebook*, blogs). This same gap can be observed through the embassies in the number of followers per *Twitter* account. The explanation lies in the "excessive centralized and restricted control on communication." Ottawa takes a relatively long time to approve public statements on social networking sites.[43]

Another question arises: How can the desired balance between granting permission for officials to create their own *Twitter* pages or *Facebook* accounts for their contacts with the general public and granting permission for them to exchange professional opinions and assessments through the very same channel be achieved? In turn, the U.S. Department of State has encountered a tough choice between maintaining a proper level of control over the accuracy of information communicated to audiences and providing its employees with greater flexibility in their external communications, in more understandable and less official language.

Internal filters ensure that officials using networking tools are strictly following the official line. On the other hand, the need for a swift reaction to an event risks the possibility that officials may offer a political assessment without the approval of the higher authorities. This last point may have destructive consequences, which could be difficult to remedy. Generally, the necessity of a rapid reaction to an event is one of the dominant subjects of expert analysis of what ought to be altered appropriately to work with external audiences through networking channels.

We are now faced with the task of attempting to understand what new technologies could mean for foreign policy work. There are some helpful reference points, taking into account foreign expertise and Russian specifics and resources: how and to what extent to implement information technologies "within the system", in view of the safety demands and the risks involved; what organizational measures need to be taken and what changes need to be made to what has become known as "document workflow", etc. However, it should be emphasized that the leading role in support of innovation and the dissemination of opportunities for networking tools in foreign policy, including the United States and the United Kingdom, is played by the state. It has also been the initiator in including the private sector, non-profit organizations and civil society in formulating and implementing decisions in this area of foreign policy work.

It is also useful to weigh the strengths and weaknesses of the state's networking potential impartially, and consider formulating

[43] Ibid, P. 6.

a clearer and more understandable arrangements for developing networking tools in foreign policy requirements. We should proceed from the assumption that the preference given to setting various barriers in the global dialogue is unlikely to have the desired results. It would be more promising to tackle those problems and decisions linked to cooperating with common and global networking tool hubs in Russia's interests.

Russian International Affairs Council

Printed in Russia