



www.dds.org

National Dependability Policy Environments

RUSSIAN FEDERATION

Report Version: Final
Report Preparation Date: 1 November 2002
Classification: Public
Preparation led by: RAND Europe (NL)

Contract Start Date: 1 June 2001 Duration: 18 months
Project Co-ordinator: RAND Europe (NL)

Partner: RAND Europe (NL, Project Coordinator); King's College London (UK);
Cell Network (S); IABG (D); Almaweb (I); LINK (P); ELIAMEP (GR);
Ernst Basler + Partner (CH), Isdefe (E)



IST-2000-29202

Project funded by the European Community
under the "Information Society Technology"
Programme (1998-2002)

Table of Contents

Overview of the Country’s Information Infrastructure 3
Main ICT Regulatory and Legal Developments 10
Assessment of Phenomena Undermining Dependability 13
Government Initiatives Aimed at Tackling Cyber-Security 14
Industry and Other Non-Governmental Activities Related to Dependability 16
Public-Private Partnerships 16

Overview of the Country's Information Infrastructure

Economic and political reforms in Russia have had a serious impact on its IT landscape. As IT cannot develop and operate in a society that does not have the social and communications infrastructure to support it, the strengths on which Russia should focus in the short-to-medium term are its contributions to world software production as an offshore haven, as well as using its highly-educated citizenry in technological exchanges with the West to help them develop pockets of IT expertise within Russia. One of Russia's advantages is that, similar to other countries in the emerging world, the advantages of relative backwardness allow the country to focus on the advent of wireless technologies and fibre-optics, directly propelling the nation into the next century of communications. There is no need to waste vast amounts of money and time in new fixed-line networks. In the long run, the return on the investment into the new communications infrastructures will pay dividends far exceeding the costs.

Weaknesses in society, however, are significant. The lack of tax collection and the inability to raise foreign direct investment (FDI) in Russia means that the process of conversion to new networks internally will be slow and laborious. Unless private organisations become confident in the society again, the majority of the funding will have to come from the cash-strapped state. Additionally, legal establishments must conform to the rule of law and adopt contemporary measures to ensure privacy, security, and enforcement to allow the burgeoning IT field to feel secure in their investment.

Societal hurdles are also evident. According to Kraemer and Dedrick,¹ the key assets to competing in the network era are: (i) skilled people, (ii) a good information infrastructure, and (iii) an environment conducive to entrepreneurship and innovation. Russia currently possesses the first, but seriously lacks the latter two. English may be the language of technology, but it has not penetrated into the population; this inability by many to read or understand English will be a hindrance to adopting technology on a personal level. This, in addition to the poverty of the majority of the population, adds to the difficulties of IT adoption by the common Russian.. Finally, Communism devastated the entrepreneurial and liberal economic understanding among many in the older generation; without this, it will be virtually impossible for the dynamic IT field to take root from the inside, at least in the short term.

Communications infrastructure is one of the most important foundations that Russia must continue to fund as a priority. The long-term possibilities will depend on the country's ability to adopt laws to ensure privacy, protection, and ownership; enforce the laws they do adopt; ensure sound and disciplined fiscal measures at home, and continue to push for strong political and civic institutions that will ensure the rule of law and develop democratically-based organisations. Information technology can and will develop alongside these other changes in society as Russia becomes more stable and integrated with the global economy.

The average IT investment in all sectors accounts for 0.1 percent of expenditures (in metallurgy 0.5 percent; financial sector five percent; some banks up to 30 percent).² In 2000, the Russian telecommunications industry as a whole generated US\$5.3 billion (EUR 6.1 billion) in revenue and grew 60 percent faster than the Russian economy.

¹ Kraemer, Kenneth and Jason Dedrick, National Policies for the Information Age: IT and Economic Development (1999).

² Pravdina, Mariya, Roman Kuprin, Igor Pichugin. "Trends. Which Technologies Does Russia Need?" Kommersant-Daily, No.157 (31 August 2001): 6.

In Russia today, as in other emerging markets, IT is a luxury. Home PCs, mobile-phones, and Internet access are generally out of the reach of average citizens, as well as many businesses. Historically, the major consumers and producers of IT were the military and government.

While IT was used to ensure parity in the Cold War, unlike in other countries, there was no trickle-down of IT into the public market from the government and military sectors, adding to the obstacles faced in Russia today in the diffusion of technology within the country. In Russia's segregated society, many feel that the lack of a middle class (through which the economy and technology can proliferate) has remained a major hurdle facing IT diffusion.

The percentage of GDP spent on ICT in 2000 in Russia is approximately three percent.³ Traditionally, financing of technological advancement, even when used to copy foreign technology, never posed a problem. Today, however, this is not the case. With rampant tax evasion and cases of government default on loans, R&D spending has obviously been put aside for the greater necessity of holding together the country during this difficult transition.

Without government funding or FDI in Russia, IT development has not occurred. No wonder that many feel that Russia will be a lost cause in developing the necessary IT infrastructure to be part of the new world economy. A typical example of the lack of financing in the advancing wireless communications sector: the Strategis Group, a Washington, DC-based wireless market research firm and consultancy, notes that there are currently about 160 licensed wireless communications entities in Russia. However, currently only 60 percent are in operation. The problem lies in the lack of domestic and foreign investment to help get these emerging marketplace companies off the ground.

The countries of the FSU have already reached EU-equivalent levels of IT investment relative to size of their economy, spending from 2.2-2.6 percent of GDP on IT. Although growth rates of four percent are projected for the upcoming years, translating into greater IT investment should the spending levels remain constant, this will still fall far short of that necessary for real benefits. The majority of IT investment in the developed world has come overwhelmingly from the private sector. The huge R&D budgets of most high-tech firms is the true cash source for IT, as the need to stay on the cutting edge is paramount in today's high-tech environment. Russian companies received just US\$1-2 billion (EUR 1.15 billion-2.3 billion) from venture capitalists, far less than many developing countries.⁴

At the same time, FDI in Russia has fallen to trickle levels after the 1997 financial crisis and defaults on loans by the Russian government. Without this private sector financing, the majority of Russian IT investment will again have to be drawn from state coffers, at least in the short run. Ultimately, it may be a long time until the flow of FDI and venture capital money will create enough stimulus for the Russian IT revolution to get underway.

³ Reyman, Leonid [Minister for Communication and Informatisation of the Russian Federation], Main Directions of the Development of Infocommunication in Russia as an Element of the Global Information Society. Presentation at the International Conference "Development of Telecommunications and the Construction of an Information Society in CIS Countries", St. Petersburg, 21-23 February 2001. www.contel.ru/rus/actions/report-2p.html.

⁴ Beauprez, Jennifer, "Immigrants Plan Return to Russia with Big Plans for Internet Portal", *Denver Post*, Knight/Ridder Business News (30 August 2000).

The percentage of people working in information products and services (without telecom) is less than one percent (as opposed to about 20 percent in developed countries).⁵

In terms of software and hardware, Russia has had the opportunity to become an emerging player in hardware manufacturing, but has ultimately been forced out from the source of investment and much-needed employment opportunities by the overtaxing of foreign-owned companies. In 1993, IBM established a manufacturing facility near Moscow to produce its computers for the domestic market; unfortunately, this facility had to close in February of 1996 – ultimately, the government overburdened such foreign corporations by taxing away any chance for a profitable enterprise. Other foreign computer manufacturers realised that it would be better to set up facilities in adjacent areas and import the hardware into the country, taking advantage of reduced barriers. Companies such as Hewlett-Packard and Acer, Inc. have established themselves in Finland and find it much easier and profitable just to export the whole demand for computer hardware into Russia.

With a burgeoning demand for corporate and home hardware solutions, Russia has a potential to be a large source of overseas revenue in emerging market penetration of hardware needs. However, the current system of over-taxation is stopping FDI. According to researchers at BIS Strategic Decisions in Paris, the demand for hardware and PCs in Russia should continue to grow at about 20 percent per annum.

Domestic production consists mainly of assembling computers from imported components. The Russian hardware and computer peripheral market was estimated to be US\$2.6 billion (EUR 2.99 billion) in 1998. Major factors for growth are further improvements in the Russian economy, rapidly-growing use of the Internet, hardware price reductions, expansion by large businesses to the regions and the resulting need for co-ordination of their branches' activities, an increasing number of small businesses, development of computer assembling and resulting demand for electronic components, and an increasing number of individual end-users.

Generally, domestic production of office and computer equipment in Russia consists of assembling personal computers, installing local-area-networks (LANs), and producing UPS systems and modems. Today, more than 100 domestic companies in about half of all Russian regions are involved in computer assembly. There is some hardware manufacturing in Russia, mostly in the higher demand areas of St. Petersburg, Moscow, and the large cities on the Pacific coast of the far eastern Districts.⁶ For instance, in the Russian Far East, over 100 small computer firms currently operate, most with less than 20 employees. The components used in these shops usually originate from the US, Taiwan, Japan, and South Korea.

Software appears to be a strong area for Russian IT development. According to McKinsey Global, the Russian software market is characterised by small-scale operations and lower-value products and services, including customisation, localisation, translation, distribution, and technical support. According to Brunswick Warburg, in 1999, Russia provided US\$70 million (EUR 80.5 million) in offshore programming services, with an annual turnover US\$560-580 million (EUR 643.7 million-666.7 million). McKinsey also stated that the Russian business of offshore programming is growing at 50-60 percent per

⁵ *Ibid.*

⁶ Chernobrovkina, Maria, US Foreign Commercial Service Moscow and US Dept. of State, St. Petersburg, 1999; Vyatkin, Sergey, "Computer Hardware and Peripherals in the Russian Far East", US Commercial Service Vladivostok, Russia, Oct. 2000; Wilson, Drew, "IBM: Moscow Tax is a Killer", Electronic Buyers News (CMP Publications, Inc) (1 April 1996).

year, with the expectation that it will obtain international certification and become a force in the world offshore programming market, similar to India.⁷

Russian software programmers work both abroad and at home for foreign corporations producing new algorithms and code for use in proprietary software. Russia has been known recently as an offshore software programming haven, usually in and around the academic institutions of Russia, helping to alleviate the much-needed programming demand from countries around the world. This may lead to export-led growth in the future, as approximately 50 percent of domestic production is sold abroad. Russian programmers can make significantly more money and have steady incomes (unlike most people in Russia today) while working for almost 40 percent less than their Western counterparts.

Within the last two years, Russian IT companies have entered the turn-key Internet software solutions market combining widespread database management systems (DBMS) with more sophisticated object-oriented DBMS and e-business technologies. These include web publishing (content management), e-commerce applications (web catalogues, ordering and payment systems, back-integration to ERP and B2B systems, and Internet banking), BackWeb push-technology and others. The companies offering e-business solutions for clients represent (i) software development centres of mature IT companies; (ii) ISP units that provide value-added services to its subscribers; and (iii) independent web application/design companies. The numbers of the latter are growing fast and present a creditable competitive threat to IT majors who are slowly entering Russian e-commerce solutions market.⁸

Russia has six million computers, one-third of which have Internet access. IBS, a major Russian computer and system integration company, estimated that during 2000, this number grew by around 20 percent. In 1999, the Russian PC market grew 26 percent (in terms of units), reaching a penetration rate of four percent, but only two percent in monetary terms; the latter is attributed to considerable price reductions. Portable PCs have a thin margin in Russia and constitute only about 10 percent of PC sales.⁹

There are two major groups of computer and office equipment end-users in Russia. The first group of users includes small companies and individuals, who prefer less expensive computer and office equipment. The second group includes large- and medium-sized government and private enterprises, banks, and financial institutions. The government market is mainly a replacement market with a large number of 486 models still in use. Banks, financial institutions, and large oil and gas companies prefer high quality, sophisticated equipment; they will buy equipment as an integrated system and require installation as well as future upgrade and after-sales service. Public institutional customers such as universities, schools, and government agencies, which depend heavily on government appropriations (and which eventually may become prime customers for large-scale deals), are currently operating under severe budget constraints.¹⁰

PC penetration is still quite low compared to the West. According to the US Commercial Service, Russia has approximately six million computers, one-third of which has Internet access. According to a Gartner

⁷ Lakaeva, Irina, "Computer Software Market in Russia", The US Commercial Service Moscow 28 September 2000); Lakaeva, Irina, "Russian Market for Offshore Software Development", The US Commercial Service Moscow (24 August 2000).

⁸ Nazarova, Inna and Irina Lakaeva, "Overview of Electronic Commerce in Russia", US Foreign Commercial Service Moscow, Moscow (2000).

⁹ Ibid.

¹⁰ Chernobrovkina, Maria, "Computer Hardware Market in Russia", US Foreign Commercial Service Moscow and US Dept.of State, St. Petersburg, March, 2000.

Group report, the Russian Department of Government Information states that there are eight-to-ten million PCs available in Russia; that is, only 5.5 percent–6.5 percent out of the total population.¹¹ IBS, a major Russian computer and system integration company, estimated that during 2000 the number would grow by 20 percent. In 1999, the Russian PC market grew 26 percent (in terms of units), reaching a penetration rate of 4 percent but only 2 percent in monetary terms; the latter is attributed to considerable price reductions. Portable PCs have a thin margin in Russia and constitute only about 10 percent of PC sales. Nevertheless, industry experts say that the sales for portable PCs with built-in modems are on the rise.

There are other factors hindering Internet usage, including poor fixed-line networks in Russia and fees for telephone use on local calls above and beyond the usually expensive ISP charges. One can easily see how these factors will hurt Internet adoption by Russia's relatively poor population. The 300-350 ISPs in Russia will have to find innovative ways of attracting and retaining those customers who are fortunate enough to have the income for Internet service. The advent of ISDN, ADSL, and WAP will help to achieve more Internet diffusion in Russia, but will still fall far short of the numbers currently seen in the EU.

There are conflicting reports for current and projected Internet usage in Russia into the mid-twenty-first century. BIA Financial Network maintains that around two million Russians spend significant time on-line per week while, on the high end, the Russian National Institute of Social and Psychological Research reports that there are currently 5.7 million occasional users of the Internet, with projections reaching as high as 7.8 million by the end of 2001.

Other estimates, such as that by IDT, claim that Internet usage will reach 6.4 percent of the population or 9.4 million by 2004. The exact numbers are elusive and probably dubious, but providing estimates on Internet usage in a vast country such as Russia can be an extremely difficult task. Over half of Internet users access the Internet while at work, 18 percent use the Internet at educational institutions, and 26 percent surf the web at home. One-fifth of Russian Internet users reside in Moscow.

Internet penetration is still low, with only three million people, or two percent of the Russian population, regularly using Internet services. About ten million people have used the Internet at least once. A low computer penetration rate, poor telecommunications infrastructure, inadequate telecom market liberalisation, and lack of capital are stifling the industry development, although some regional infrastructure development projects are on the way. In 1999, there were 350 ISPs operating in Russia. There were 412,000 Internet dial-up accounts, 26.7 million telephone lines and 2.3 million PC owners¹²

International Data Corp projects that the number of Internet users will have grown to 3.1 million in 2000, from 1.8 million at the end of 1999. Investment house Brunswick Warburg (a joint venture between Brunswick Group and Warburg Dillon Read focusing on the Russian securities market) predicts that Internet penetration will rise by 10.5 percent. Another source, the Russian media company Monitoring.ru, optimistically estimates that there are 6.6m persons who use the Internet occasionally, at work, or in places

¹¹ Russia Department of Government Information, www.e-government.ru.

¹² Pyramid Research, 1999 figures

of education. Even if such an Internet penetration rate is true, the majority of these users are students and thus have little purchasing power. About 60 percent of active domestic buyers are in Moscow.¹³

In the 1990s, the telecommunications infrastructure improved substantially in Russia, especially in the area of mobile telephony, where the entry of some private companies into the market increased competition and investment. Russia currently has more than five million mobile phone users in 2001 and should have 45-48 million by 2010.¹⁴

Russia, a country of great distances, has uneven telecommunications coverage. Some 40,000 or 26 percent of villages in Russia have no telephone access. About 50,000 villages have one-to-three phone lines per settlement. There is an average of ten phone lines per 100 people. In 2000, over 130,000 phone lines were installed in rural areas, which is one-tenth of the total number of installed lines. Over 535,500 people are on a waiting list for basic telecom services. Most equipment and cable used in rural areas is outdated and worn out. Only 56 percent of phone users in rural areas can make long-distance calls automatically. No sizeable state funding has been made available to develop rural telecom networks since 1996.¹⁵

External fibre-optics have been placed connecting Russia with various countries, such as Denmark, China, Finland, South Korea, and Italy. Internally, the most ambitious plan for fibre-optics has been undertaken by Andersen Group, a New York-based company, along with its local partner ComCor, which has set out to rewire the entire Moscow metro area with broad-band access. Of course, such endeavours are usually set on the capital and most prosperous business districts first, of which Moscow has the distinction of being both. The result of the work has been 2,400 kilometres of fibre cable servicing 3.5 million apartments and businesses.¹⁶

In 2001, the Russian government committed about US\$250-300 million (EUR 287.4 million- 345 million) to upgrade their satellite communications in Russia and the Commonwealth of Independent States (CIS). Four new satellites were launched in 2000, with Alcatel relay stations in the Russian Federation carrying the signals across this vast country.

There are different estimates relating to the volume of B2B e-trade in Russia, but all assessments concur that the level remains extremely low. ICD puts the size of this market in 2001 at US\$285 million (EUR 327.6 million), and expects it to grow to US\$3 billion (EUR 3.45 billion) by 2005. The Gartner group estimates that today, only nine percent of B2B financial transactions are done over the internet, and anticipates this figure to grow by the end of 2002 to 26 percent and by 2006 to 35 percent. According to the Russian Al'fa-bank, turnover in the Russian internet in 2000 was US\$179.3 million (EUR 206.1 million), out of which US\$121.8 million (EUR 140 million) was generated in the B2B sector. Al'fa-bank

¹³ "EIU e-Readiness Survey - Russia: E-business marketplace", Economist (August 2001): www.e-businessforum.com/index.asp?layout=rich_storyanddoc_id=691andcountry_id=RUandcountry=Russiaandchannelid=6andcategoryid=22.

¹⁴ Deputy Communications Minister Yuri Pavlenko, St. Petersburg Conference (7 November 2001) "Russia to have up to 48m mobile users by 2010", Reuters (10 September 2001).

¹⁵ Nazarova, Inna, "Rural Telecommunications in Russia", Business Information Service for the Newly Independent States (BISNIS), US Commercial Service- Moscow, Russia (16 April 2001): www.bisnis.doc.gov/bisnis/country/010420RuralTelecom.htm.

¹⁶ "ComCor-TV", Internet World (Meckler Media Corporation) (15 September 2000).

forecast a growth in overall turnover to US\$1,454.4 million (EUR 1.67 billion), out of which US\$615.4 million (EUR 707.4 million) would come from B2B¹⁷.

Contrary to experience in Western Europe, where small business started e-commerce, big Russian corporations are establishing large-scale ventures to open new markets (use the Internet as a marketing vehicle), and/or to increase operational efficiency. Metallurgical plants are making the most impressive investments, followed by oil companies.

The number of Internet trading systems has grown dramatically from one online brokerage in November 1999 to over 40 in June 2000. Most offer Internet interfaces to trade commodities, including steel, metals, oil products, and grain. Major projects include the already-operational Zerno On-line (grain), Oil On-line, and Grin.ru (universal exchange). Scheduled for launch in 2000 were Global Steel Exchange, Europe-Steel.com, Emetex (metals), and Business.ru (universal). Privacy concerns and an existing lack of pricing transparency that some companies find beneficial may impede the growth of online trading.

Online financial services are just emerging in Russia, which is still recovering from the collapse of the banking system in 1998. People lack confidence in domestic financial institutions and typically convert their savings to US dollars and euros kept “under mattresses.” Nevertheless, several banks are pioneering new online services. Online financial brokerage is rapidly developing, growing from a single firm in November 1999 to over 40 in June 2000.¹⁸

E-commerce retail sales estimates for 1999 ranged from US\$1 million (EUR 1.15 million) to US\$3 million (EUR 3.45 million). Russia’s population of 146 million (spread over vast distances) may eventually be quite receptive to using on-line services, but weak consumer purchasing power, low computer penetration rate, insufficient telecommunications infrastructure, and inadequate postal delivery systems significantly limit the potential of B2C e-commerce. Russians have ambivalent attitudes about new technologies and most have no confidence in virtual transactions, something Western consumers have been accustomed to through catalogue purchases. Moreover, Russians lack non-cash payment forms: debit and credit cards are rarely used outside Moscow and St. Petersburg. Furthermore, the population is wary of the banking system (especially since the 1998 financial crisis).

Nevertheless, some B2C projects are expanding. As of summer 2000, Russia has about 500 online stores. Major B2C projects include Ozon.ru, a copycat of Amazon.com; XXL.ru, an online supermarket; Dostavka.ru (computers); and Torg.ru, an online shopping mall. Most retailers require on-delivery cash or credit card payment. The above-mentioned projects are very aggressive in brand development and have catchy names for the 2.5 million Russian Internet users. Most industry experts believe that B2C electronic commerce will become economically viable only when Internet reaches about 10 percent of the population, or 15 million users, which may happen in 2003.¹⁹ There are 500 online stores available in

¹⁷ A.V. Sokolov [General Director of OAO ‘Elvis-Plyus’]. Information security: Directions and Prospects for Developments – Technological and Legal Aspects. Third All-Russian Conference “Information Security in Russia in the context of a Global Information Society”. Moscow (26 November 2001): [ww.infoforum.ru](http://www.infoforum.ru)

¹⁸ US Department of Commerce, Guide to E-Commerce Markets in Europe. (Washington, May 2001).

¹⁹ US Department of Commerce Guide to E-Commerce Markets in Europe. (Washington, May 2001).

Russia with an overall retail turnover of US\$700,000 (EUR 804,600) per month, with approximately 25,000-27,000 purchases online.²⁰

The best progress has been in the advancement of wireless capabilities since 1992 when modern cellular systems were introduced. Although no real production of wireless products is evident in Russia today, the most up-to-date networks are being implemented/installed rapidly. The cellular phone density is believed to be only at 0.3 per hundred as opposed to the 24 per hundred in the USA.²¹ Aggregate figures from Brunswick Warburg estimated the total number of mobile phone users to reach 3 million by the end of 2001. Other estimates by the Strategis Group put total cellular revenue in 1999 at US\$1 billion (EUR 1.15 billion) and may even reach US\$9.2 billion (EUR 10.57 billion) by 2007. On the other hand, paging services have been approximated at half-million subscribers in 2000.

Despite these lacklustre numbers, a few of the most transparent and well-managed companies in Russia today deal in wireless paging and cellular technology. Vypelcom, half owned by Telenor of Norway, and its main competitor MTS, a partner with Deutsche Telekom, have been battling over ownership of the emerging GSM, CDMA, 3G, and paging networks in Russia. Telenor estimated the potential for wireless to be US\$7.2 billion (EUR 8.28 billion) by 2003, up from US\$3.6 billion (EUR 4.14 billion) in 1999, with 3G communications networks accounting for an ever increasing share in the upcoming years.

Main ICT Regulatory and Legal Developments

Russia remains a country in the throes of a long and tumultuous transition process that is affecting every sphere of public life. The heavy regulatory legacy of the Soviet Union continues to affect the country's attempt to catch up with the international marketplace, including in the critical field of ICT. The Russian government itself remains a huge apparatus that continues to impose considerable regulatory and other hurdles and thus remains more part of the problem than of the solution.

Until recently, the Russian government's main policy focus in the ICT field was on privatising parts of state ownership on the one hand, and on 'information security' on the other.. There was no real policy on e-government or e-commerce. Russian technology firms used to complain that the government did not recognise the existence of their sector, focusing all of its efforts instead on traditional heavy industry, especially the fuel and energy sector.²² With Vladimir Putin, the government is slowly recognising the importance of new technologies for Russia's development. Mr Putin has repeatedly stressed his ambition to make Russia a digital superpower and, as a result, we are witnessing some recent political and legislative activism in this sphere.

As was the case with the entire economy, the ICT sector suffered from an onerous Soviet legacy: total state ownership; poor infrastructure (lack of installed telecommunication-lines with outmoded switchgear,

²⁰ "Russian Internet survey", *Expert* (June 2000): www.expert.ru. See also Readiness For the Networked World Assessment: Russia. Information Technologies Group. Center For International Development: Harvard University, 2002.

²¹ Breiter, Maria, "Encryption Regulations in Russia", US Foreign Commercial Service Moscow (August 1999).

²² "EIU e-Readiness Survey - Russia: E-business marketplace", Economist (August 2001): www.e-businessforum.com/index.asp?layout=rich_storyanddoc_id=691andcountry_id=RUandcountry=Russiaandchannelid=6andcategoryid=22.

minimal and obsolete computer equipment, and inadequate investment in all of these spheres); and a pent-up demand for service. Although progress has been made in all of these areas, much remains undone.

Until 1993, the entire Russian telecommunications network was fully controlled by the Russian Ministry of Communications. That year, local network operators were privatised in such a way that each region received one telecommunications provider. Rostelecom became the single national network operator, and 85 regional telecommunications companies were formed. In 1995, Svyazinvest, a holding company which consolidated the government stakes in all of the 85 regional telecommunication companies, was created. The government held 51 percent of Svyazinvest, with the remaining shares sold off at a controversial auction.

In general, ‘natural monopoly reform’ is proceeding at a very slow pace and with little transparency.²³ Although plans to reform these natural monopolies regularly surface, little real progress has been made to date. The latest government plan intends to liberalise further the telecommunications market through imposing interconnection services, through improved price regulation, and to impose more reporting requirements on telecommunication operators.

Generally speaking, both domestic and foreign businesses operating in Russia complain about the excessive burdens imposed on them in the current legislative framework surrounding the ICT sector. In Russian legislation today, for instance, there are over 90 different laws covering at least 40 different types of secrets that can be invoked to limit the normal exchange of information. As one well-placed Russian observer puts it, “even with the most honest will possible, it is impossible to observe all requirements”.²⁴

Key legislative issues involve intellectual property, privacy protection and electronic commerce. There continue to be major problems with the laws on trademarks and with intellectual property in general, which greatly affect the ICT sector (both domestic and international).

Privacy is a relatively new concept in the Russian legislative process, as witnessed by the fact that there is no Russian equivalent for the word. Although the Russian legislature is trying to address the protection of personal data in cyber-space, the balance between the right of individual and the right of various government layers continues to be skewed in favour of the latter. According to the Russian Constitution and a number of laws, the privacy of electronic information and exchange must be protected. Yet through a variety of legislative measures, the Russian security services have obtained the right to monitor all forms of electronic correspondence— from postal deliveries over cell-phone conversations to all forms of Internet communication. Thus, the Federal Security Service (FSB), the domestic successor to the KGB, was running a project codenamed SORM to monitor electronic communications, including private correspondence; and other parts of Russia’s intelligence community have access to this system. Although all these authorities are required by law to obtain a court warrant before reading any of this communication, many human-rights groups worry that this legal safeguard is hard to check and easily overridden with modern technologies.

²³ Even the Anti-Monopoly Ministry has started voicing complaints about the lack of transparency in the government-driven program. Elisabeth Wolfe, “Yuzhanov: Telecoms Reform Too Secretive,” *The Moscow Times* (15 October 2001): 9.

²⁴ A.V. Sokolov [General Director of OAO ‘El’vis-Plyus’]. *Information security: Directions and Prospects for Developments – Technological and Legal Aspects*. Third All-Russian Conference “Information Security in Russia in the context of a Global Information Society”. Moscow (26 November 2001): www.infoforum.ru.

Articles 160(2) and 434(2) of the Russian Civil Code now recognise electronic signatures, but only where there is a mutual agreement between the parties to use electronic signatures. The State Duma is poised to adopt a draft Federal Law on Electronic Digital Signatures that regulates the use and verification of electronic digital signatures. Unfortunately, however, electronic transactions and signatures now have no equivalence under the law with paper-based transactions and signatures, and most courts simply do not recognise claims based on electronic signatures.

Given Russia's current budgetary situation, its relative backwardness, and the continuing obsolescence of its infrastructure coupled with the enormity of its territory, universal e-access has not been a priority for the government. Still, the Ministry of Communications has decided to install computers with Internet connectivity at 1,800 postal offices throughout Russia.

Because of the Russian Government's insatiable penchant for secrecy, rules governing the use of the Internet are even more stringent than in many other countries. The government network has been limited and entirely isolated from the Internet.²⁵ The governmental Internet presence is also lagging behind considerably on the private, and until recently more effort seems to be spent on securing the modest existing infrastructure than on expanding it.²⁶

Yet under the Putin administration, there are signs that a new impetus has been given to e-government, this being one of the four areas singled out in the Russian Government's 3 billion EURO programme 'Electronic Russia 2002-2010', which intends to increase the efficiency of the economy both in the public and private sectors, to make wider use of information technologies in government departments, and transfer much of the state's work online. The E-Russia plan seeks to improve information transparency of Russia's state entities, to improve the use of IT in governmental communication at all levels,²⁷ to deliver an increasing number of government services on-line, and to alleviate some of the heavy bureaucratic burden on Russia's citizens and businesses.²⁸ Russian citizens will be able to declare their taxes via the internet from 2002 onwards.

The main obstacles to the development of e-commerce in Russia appear to lie with factors over which the government has little direct control. The new 'Electronic Russia' program is more targeted at public areas (such as government and education), although it does foresee more B2G interaction for state procurement and other commercial activities of the state.²⁹

²⁵ According to a presidential decree, government officials are prohibited from connecting computers that are connected to governmental intranets onto the Internet.

²⁶ With respect to government websites, in December 2001, FAPSI started introducing new security mechanisms for government websites.

²⁷ All regional authorities, for instance, are in the process of being hooked up to the "Special Purpose Information and Telecommunication System" (Russian acronym: ITKS). See V.S. Gorbachev. [The Role of FAPSI in Implementing the Foundations of the Federal Policy for Information Security in the Subjects of the Russian Federation and the Federal Districts](#). All-Russian Conference "Information Security in Russia in the context of a Global Information Society": www.infoforum.ru/detail.php?pagedetail=219

²⁸ See Vladimir Rubanov, [Electronic Government: From Idea to Practical Realisation](#). Third All-Russian Conference "Information Security in Russia in the context of a Global Information Society". Moscow (26 November 2001): www.infoforum.ru/detail.php?pagedetail=221

²⁹ Lakaeva, Irina, US and Foreign Commercial Service. [Electronic Russia Program](#) (28 September 2001): www.bisnis.doc.gov/bisnis/country/011001E-Russia.htm

On behalf of the Russian government, the Ministry of Communications is working on a federal e-commerce development programme, which would create a framework for public and private sector initiatives.

One should recognise that there are certainly islands of excellence within Russia in a number of different ICT fields. These undoubtedly include theoretical computer science but also a small number of applied areas (such as anti-viral software). Furthermore, ru.net (the Russian segment of the Internet) is an extremely dynamic environment, in which, for instance, news and analysis websites are probably superior to those in many Western countries, both in form and substance. So far, however, little of this ICT-ingenuity seems to have spilled over onto the public sector.

Assessment of Phenomena Undermining Dependability

Given the slow development of ICT networks in Russia, it should not come as a surprise that dependability problems have remained modest so far. Although it is generally recognised that Russia is home to a large and sophisticated computer crime community, there is little evidence that this community is having a commensurate negative effect on their home country. Although computer crime did go up fourfold in 2000, for instance, there were only 436 criminal cases, and the amounts of money involved remained fairly modest (not surprising given the modest role of e-commerce in the country). At the same time, however, it has to be recognised that the presence of this community may also have a deterrent effect on the further development of e-commerce. Thus, for instance, both America Online and CompuServe (before they merged) shut down their Russian services after evidence of rampant credit-card fraud.³⁰

Also, the commercial information security market in Russia is extremely small, but on the increase (very crude estimate by Informzashchita of US\$20 million (EUR 22.3 million) in 2000; in 2001, estimated at US\$40 million (EUR 44.6 million).³¹ One of the few serious surveys of this issue was done by Ernst and Young, and showed that security concerns and lack of resources, skills, and expertise are the main inhibitors to the expansion of e-business. Information security issues are being addressed, with 99 percent of the survey respondents implementing at least one type of security solution. The most commonly used security measures are anti-virus software and firewalls.

There is a higher emphasis on implementing technical security solutions (such as firewalls) as opposed to organisational security measures (such as formal security policies and procedures). 32 percent of respondents do not test their security measures to ensure that they are operating effectively. 65 percent of respondents said that they experienced a security breach in the past 12 months. Virus attacks form 43 percent of the breaches reported. Other common incidents are denial-of-service (DOS) attacks, system penetration from the outside, and unauthorised insider access. 41 percent of companies that reported security breaches were not involved in any e-business activities, hence dissipating any myths that computer crime only focuses on companies conducting business via the Internet. 26 percent of respondents experienced critical business systems failures in the past 12 months.

³⁰ "EIU e-Readiness Survey - Russia: E-business marketplace", *Economist* (August 2001): www.e-businessforum.com/index.asp?layout=rich_storyanddoc_id=691andcountry_id=RUandcountry=Russiaandchannelid=6andcategoryid=22

³¹ Сетевые атаки и системы информационной безопасности 2001 [Network attacks and information security] www.cnews.ru/comments/security.

Government Initiatives Aimed at Tackling Cyber-Security

Contrary to most other countries, where developments in the ICT sector typically ran ahead of policymakers, Russia appears to follow the opposite path. The development and introduction of new network technologies continue to proceed at a fairly slow pace, yet the regulatory and (public) security framework surrounding this fledgling sector is quite overwhelming – and this long before the events of 11 September 2001. There have been many curious attempts by the Russian government over the past few years to interfere with various new media, for both political and financial reasons, probably partially based on the idea that it could be a new source of tax revenue.³²

A clear example of this was the 'National Doctrine on Information Security'³³ signed into law in 2000 by President Putin. Although the doctrine pays lip service to the principles of freedom of information, the document also contains a number of far-reaching provisions that appear to restrict severely those principles. Recent government attitudes towards all media – both printed and electronic – in the centre, as well as in the regions, also shows an increasing trend towards more direct state control over various types of media.

The model that emerged in the Russian Federation on dependability policy issues was thus a fairly peculiar one, certainly prior to the 11 September 2001 events, in which the government arrogated for itself – at least on paper – wide and intrusive powers of control over virtually all forms of communications in the name of national security. What is unclear is to what extent these paper competencies have actually been implemented, especially in light of various practical, financial, organisational, political, and other limitations brought about by Russia's size and history.

There is currently no genuine central co-ordination mechanism in Russia on these issues. The Security Council is, on paper, responsible for co-ordination, but its real role appears to be limited to issuing broad policy guidelines that are frequently interpreted or implemented differently by different agencies.

The principal government agencies responsible for information security are the Federal Security Service (FSB – domestic successor to the KGB), Directorate for Computer and Information Security (in the FSB's First Department on Counter-terrorism), the Federal Agency for Government Communications and Intelligence (FAPSI)³⁴ – roughly comparable to the NSA in the US or GCHQ in the UK. Unlike the FSB, which has been restructured a number of times over the past decade, FAPSI has a reputation for being unreconstructed; it also has more employees than the FSB or SVR, the Russian Foreign Intelligence Service. Finally, there is The Russian Security Council (and, more specifically, its Directorate for

³² According to Anton Nosik, one of the best-known Internet specialists in Russia, "the internet community had been awaiting an attempt by the authorities to regulate it since 1995-96. Internet professionals realised that officials--likebandits--could not allow the existence of a sector that is developing fast and produces advertising income, but that is totally outside their regulation. Since the beginning the questions were 'when will authorities understand that they can make money regulating the internet?' How could they do that? Either extorting shares in exchange of a registration document, or directly asking bribes for the registration of new internet projects": www.rferl.org/nca/special/rumedia5/babitsky2.html

³³ For the full text, see ng.ru/politics/2000-09-15/0_infodocctrine.html

³⁴ On FAPSI, see Gordon Bennett, [The Federal Agency of Government Communications and Information](#) (August 2000). Conflict Studies Research Centre. FAPSI's competencies in the information security field emerged primarily because historically speaking, this was the main source of government expertise on cryptography.

Information Security), which has a general co-ordinating role in the area of information security, although its actual political weight at any given moment depends largely on its chairman.

Russia is currently preparing to join the international standard ISO/OSI 15408:1999 'Common Criteria'.³⁵ Russia has apparently also set up an expert group on critical infrastructure protection to develop a program of action, which will be developed in consultation with the private sector.³⁶

Given the relative backwardness of the Russian ICT sector, its development is viewed as more important than ensuring its security. Nevertheless, given the official penchant for secrecy and 'national' security, the government has imposed a number of requirements that could theoretically also enhance network dependability.

Overall, however, the Russian government appears to have been more interested in protecting itself and its citizens against various internal and external threats than in establishing a dependable environment for the country's transition into a networked information society. Despite this, some of the basic elements are now starting to fall into place, including the draft law on electronic signatures, which has passed its third reading in the Duma and will likely become legislation very soon.

In the first instance, the financial resources of the Russian government are extremely limited, and are not expected to grow dramatically in the anytime soon. Furthermore, Russia is confronted with a wide array of 'traditional' infrastructural problems after years of neglect. Some of these have already led to various disasters, and therefore put 'information security' in a somewhat different perspective.

Within these confines, the main emphasis of the Russian government appears to have focused on securing the federal communication systems themselves, rather than on helping the private sector proactively with CIP threats. We have found limited evidence of government information sharing, no evidence of federally-funded education and training programs, and very limited R&D in this field.

Internationally, Russia has nevertheless tried to put ICT dependability on the agenda by taking an initiative that led to the adoption by United Nations General Assembly in December 1998 of Resolution 53/70 'Developments in the Field of Information and Telecommunications in the Context of International Security.' The document invited member-states to inform the UN Secretary-General of their views and assessments on (i) the issues of cyber-crime and terrorism; (ii) definition of basic notions related to information security; and (iii) the advisability of developing international principles that would enhance global information and telecommunication systems and help combat information terrorism and crime. Russia has also been active in the G8 framework. At the same time, however, Russia did not provide responses to the APEC Working Group dealing with CIP or e-security issues.³⁷

³⁵ Sokolov, *op cit*.

³⁶ APEC Telecommunications and Information Working Group. Business Facilitation Steering Group. E-security Task Group. Minutes Of Meeting, 17 September 2001, Jeju, Korea. www.apectelwg.org/apecdata/telwg/24tel/bfsg/18_percent20ESTG_percent20Minutes.htm

³⁷ www.apectelwg.org/apecdata/telwg/24tel/estg/9percent20Mappingpercent20-percent20roundpercent202percent20slides.files/frame.htm

Industry and Other Non-Governmental Activities Related to Dependability

RU-CERT: the Computer Emergency Response Team of Russia was founded and is maintained by the Russian Institute of Public Networks (RIPN). Since March 2002, RU-CERT is the official service for RBNET backbone constituency and is based on RBNET Network Operation Centre (NOC). The primary purpose of RU-CERT is responding to computer security incidents that occurred or can happen with RBNET users, providing a single trusted contact point for RBNET users to deal with computer security incidents and problems³⁸.

The Computer Security Analytic Centre (AC) is a non-commercial project formed and co-ordinated by RIPN (Russian Scientific Research Institute of Public Networks Development, www.ripn.net). The main goals for the first stage of the project are the co-ordination of the Internet-user efforts in Russia towards the control of information security incidents; gathering, analysing, and processing of the incident log; response to network security violations, detection of incident sources, and prevention of incident source appearance in the future; co-operation with the foreign IRT for joint activities; information server support for the location of the documentation archive and the information security facilities; analysis of existing procedures, facilities, and resources intended for the prevention of security violations, production of the recommendations related to attack detection, and protection and elimination of attack consequences; distribution of incident information reports; and conducting seminars and conferences dedicated to procedures regarding the control and prevention of network security threats.

Public-Private Partnerships

Genuine public-private co-operation in the field of information security remains very limited when compared to other countries. This should not come as too much of a surprise given that the Russian government has traditionally had limited expertise in ICT matters and fairly idiosyncratic views on its own role in security provision. Thus, the Russian ICT industry remained fairly weak and fragmented (also politically). Both sides are currently changing their stance, making more co-operation a much likelier prospect.

³⁸ www.cert.ru/Eng/Operation/framework.html.