Global Threat Research Report: Russia

Eli Jellenc, Senior Threat Intelligence Analyst
ejellenc@idefense.com

Kimberly Zenz, Senior Threat Intelligence Analyst
kzenz@idefense.com

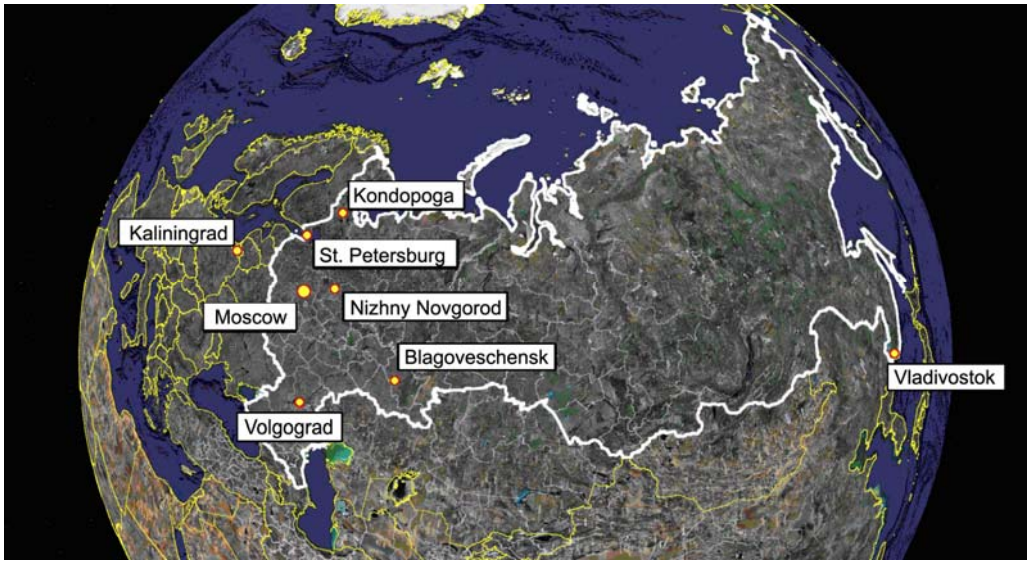
Jan. 10, 2007

An iDefense Security Report
The VeriSign® iDefense® Intelligence Team

VeriSign®

INSIDE THIS REPORT

1 Executive Summary



The Russian Federation

Russia has long been, and remains today, the single greatest source of malicious cyber activity and cyber crime, possibly with the exception of the US. In many ways, Russia's geography and socio-economic conditions clash with the country's difficult recent history and with an often draconian political order to create "perfect storm" conditions in which criminality, including the cyber variant, flourishes. Excellent schools produce tens of thousands of exceptional technical minds who enter a job market with prospects almost universally below many of their abilities. A culture of criminality and increasing apathy toward, or acceptance of, corruption by younger Russians leads many into the criminal underground. There they find easy prestige and money in improperly secured western companies and gullible individuals.

Russia's political leaders are not often of much help in curbing the country's cyber problems. Apathy is a common attitude unless a Russian organization is harmed. The Russian IT sector has good reason to seek its own security, but there are few collaborative efforts among multiple firms to offer the benefits of collective security. Corruption at all levels makes the situation more difficult for western companies in a number of ways. For its part, law enforcement is often riddled with corruption, and the information available suggests that there may be only a few dozen police or security personnel who are competent, intelligent and driven enough to fight cyber crime effectively.

The Russian cyber crime underground has evolved into a sophisticated, if loose-knit community with its own periodical literature and cultural mores. The "Russian hacker" has become a stereotype. But as with many stereotypes, there is some truth involved. Russia does have a large population of talented hackers that are under less pressure from the law than their counterparts elsewhere. Western firms doing business in Russia must not only be able to secure themselves from the relentless challenges of cyberspace, but they must also consider other, often more difficult problems.

The first section of this Global Threat Research Report provides contextual, political and economic background research on the Russian Federation's recent history and current affairs. The second section includes an overview of Russian telecommunications and information technology sectors, Internet penetration and usage trends, and a discussion of those aspects of the Russian regulatory environment pertaining to IT and the cyber landscape as a whole. The third section discusses the major facets of the

cyber threat landscape, beginning with an analysis of corruption in the Russian Federation and its significance for doing business there. iDefense analysts will discuss those law enforcement units responsible for cyber crime before discussing specific cyber crime topics in detail in the fourth section. Among the issues iDefense analysts considered are the hacker culture in general, carding and account theft, phishing, spam, the online market for attack tools, politically motivated hacking and, finally, the insider threat. The final section of this report offers conclusions and summary analysis.

2 Background

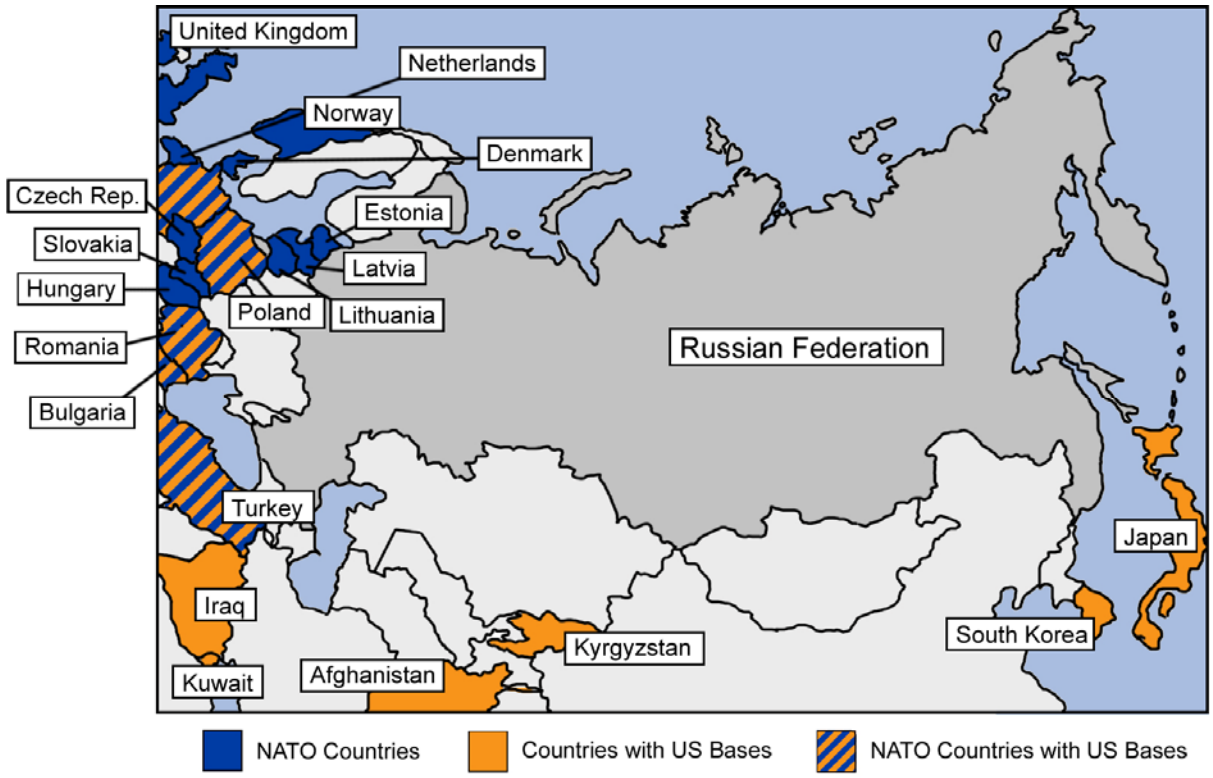
2.1 Foreign Politics of the Russian Federation

The Russian Federation inherited many of the former Soviet Union's foreign policy positions, albeit in a diminished state. The Russian Federation occupies a permanent seat on the United Nations Security Council, and is an active participant in diplomatic efforts to resolve the Israeli-Palestinian and Kosovo conflicts, and issues surrounding nuclear development in Iran. Russia exerts a strong influence over the former Soviet states surrounding it, many of which still have sizable Russian and Russified populations.

President Vladimir V. Putin[1]

Relations between Russia and the US have remained somewhat strained in recent years. The strongest contributing factor to this is the increasing American influence in former Soviet-dominated areas, especially those that there were once parts of the Soviet Union (such as Georgia, Ukraine and Kyrgyzstan). NATO expansion and the presence of US military bases are particularly sensitive issues, as are the war in Iraq and what the United States perceives as Russia's support for Iran's nuclear development. Relations between the two countries worsened significantly in May 2006, during which US Vice President Dick Cheney questioned Russia's legitimacy and called it unjustified for using oil and gas as tools of intimidation and blackmail, interfering in neighbors' territorial integrity and "unfairly and improperly restricting the rights of her people." Relations cooled further two months later when Russian Federation President Vladimir Putin rejected the US president's assessment of the war in Iraq and all but called his plan for that country a failure.[2]

[1] Newslib.com, http://vladimir-putin-news.newslib.com/img/logo/298.jpg
[2] "Putin Rejects Bush's Iraq Democracy Model," July 17, 2006, CNN.com, http://www.cnn.com/2006/WORLD/europe/07/15/russia.g8/index.html



NATO and United States military bases relatively close to the Russian Federation

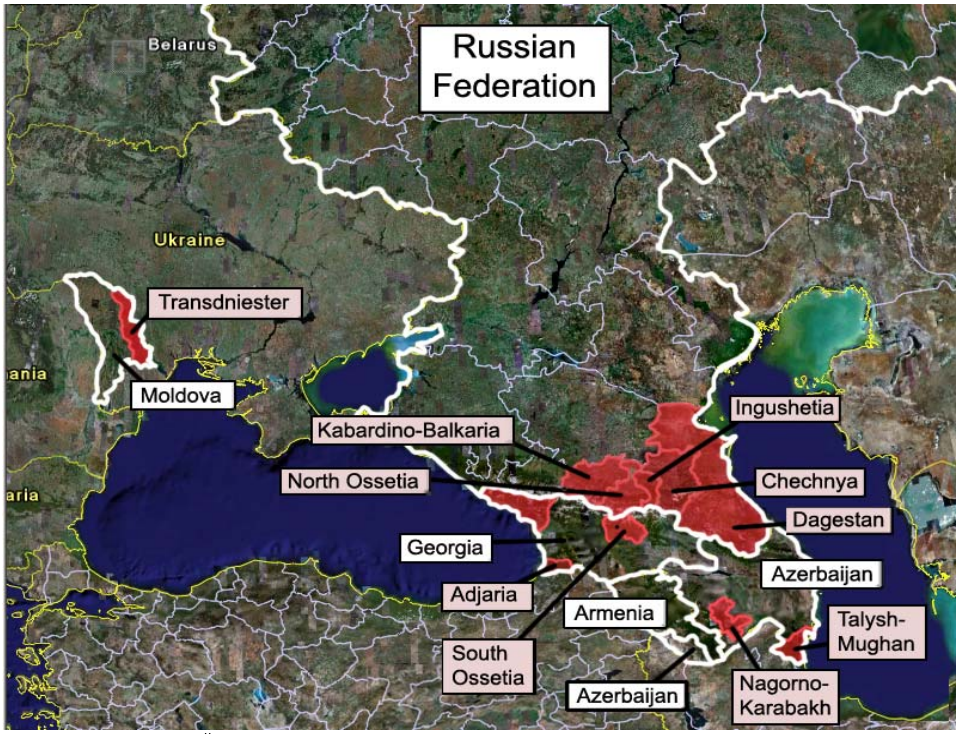
Whereas Moscow views the so-called near abroad states as Russia's rightful region of influence and vital strategic neighbors, foreign policy in these countries is of particular importance. Russia uses a combination of diplomacy, strong-arm tactics, trade, the loyalties of ethnic Russians and separatist regions, and even ethnic tensions within Russia proper to direct the course of events in those countries. The one exception to this is the Baltic States, who have fully repudiated Russia and engaged the West by joining NATO and the European Union. A sizeable majority of Russians reside in these states, and Russia frequently cites discrimination against them as a reason to play a stronger role there.

One country in which Russia remains influential is Belarus, where, despite some strain, strongman leader Alexander Lukashenko trades deference to Russia for support to his regime. The Russian government would prefer a similar relationship with Ukraine, and interfered heavily in the last parliamentary and presidential elections in an attempt to help its preferred candidate Victor Yanukovych and his party win power. Victor Yuschenko ultimately won the presidential race, but not before a messy campaign that included an attempt to assassinate Yuschenko, and voter fraud (which only extensive protests could overturn). Yanukovych's party fared slightly better during the March 2006 parliamentary elections; the Russian government supported Yanukovych and his party again during these elections, and was even implicated in sustained efforts to hack into the Ukrainian Central Election Commission's servers during that time. The areas of Ukraine closest to Russia contain a high percentage of Russian and Russified Ukrainians who feel a strong loyalty to Russia, a useful political tool often wielded by Moscow.

Country	Percentage of the Population Comprised of Ethnic Russians
Russia	79%
Kazakhstan	37%
Latvia	34%
Estonia	30%
Ukraine	22%
Kyrgyzstan	22%
Belarus	13%
Moldova	13%
Turkmenistan	10%
Lithuania	9%
Uzbekistan	8%
Georgia	6%
Azerbaijan	6%
Tajikistan	4%
Armenia	2%

Ethnic Russians in the former Soviet Union as a percentage of the population[3]

The "frozen conflicts" are another policy instrument employed by Russia to exert control over its neighbors. These are regions where independence from the Soviet Union led to hot conflicts that ended in ceasefire, but are not fully resolved. Typically, the region in question operates fairly autonomously, and receives economic, diplomatic and occasionally military support from the Russian government.



"Frozen Conflict" zones in the former Soviet Union

[3] "Ethnic Russians in the Newly Independent States," Map Collection, University of Texas,

One such frozen conflict is in Moldova. The Moldovan central government began efforts to impose greater control over Transdniester, the mostly Russian enclave that attempted to secede from the Romanian majority. The ensuing civil war was ended by a threat of peace enforced by the Russian army, and the Russian state continues to protect Russians in Transdniester and use them as a means to apply pressure on Chisinau. In 2005, the Moldovan government showed signs that it sought to loosen ties to Russia and reassert itself in Transdniester; the Russian government promptly placed a ban on Moldovan wine imports to Russia, a serious economic blow to Europe's poorest nation by its largest trading partner.

The ban on wine imports also included Georgian wine, but where Moldova has made conciliatory overtones towards Russia, this economic pressure only exacerbated anti-Russian sentiment in Georgia. Georgian President Mikhail Saakashvili's foreign policy already adopts a Western orientation in lieu of Georgia's traditional alliance with Russia. When Georgia took steps to reassert control over the frozen conflict regions of Abkhazia, South Ossetia and Adjaria and then expelled four Russian diplomats for spying, this proved too much for Moscow and significant diplomatic tensions developed. In addition to diplomatic conflict on the world stage, Russia instituted a strong domestic anti-Georgian policy, expelling Georgians residing in Russia, harassing Georgians on the street and even investigating famous Georgians such as the best-selling Russian-language author Boris Akunin, whose real name is Grigory Chkhartishvili.

In comparison Nagorno-Karabakh, an ethnic Armenian enclave within the territory of Azerbaijan, is a relatively stable island of Russian influence within that country, as is the other frozen conflict spot within Azerbaijan, the Talysh-Mughan Autonomous Republic. In Kazakhstan, a large Russian population also serves as a base for Russian influence; almost 40 percent of the country is Russian, parliament offers translators for Russian-speaking members and even the currency is written in Russian on one side. Kazakhstan is of particular interest because of the large oil reserves in that country. The majority of the pipelines there (and in its neighbor, gas-rich Turkmenistan) were built during the Soviet era and as such connect to world markets through Russia. Control over these states' access to their markets only enhances Russia's influence. The Russian military forces posted in Tajikistan and Kyrgyzstan further reinforce Russia's dominance in Central Asia.

2.2 Domestic Politics of the Russian Federation

The persecution of Georgians within Russia is not an isolated phenomenon. Although the current political tensions certainly play a significant role in the situation, strong prejudices already existed against Caucasians, especially Chechens. Shortly before the crackdown on Georgians, race riots broke out between ethnic Russians and Chechens in the Russian town of Kondopoga in August 2006; during the incident, two Russians were killed, youths clashed with riot police and each other and Chechen-owned businesses were burned. The tensions in Kondopoga were just the latest example of tensions between ethnic Russians and Caucasians. The most notable example of this is the second Chechen war, which although relatively calm, is still ongoing, marked by accusations of human rights abuses and "disappearances" involving all sides.

Outside of the Caucuses, the political situation is mostly stable. President Putin's policy of recentralizing power is mostly successful, and Moscow is now able to dictate policy to most of the regions. A former KGB officer, Putin was also successful in establishing personal control over the central government. Research by the Moscow Center of Research of Elites showed that 78 percent of leading political figures, including department leaders in the Presidential administration, government members, members of both chambers of parliament, federal leaders and heads of executive power and legislature in the Russian

regions, were somehow connected with the KGB or the organizations that replaced it sometime during their careers.[4]

Legislative and structural changes accompany the recentralization of power; economic, diplomatic and administrative reforms are in the process of restructuring Russia's operational structure, to such an extent that even the internal borders were redrawn; in December 2003 the Komi-Permyak Autonomous Region and Perm were consolidated into one region; this had the dual effects of changing the administrative type of region in Komi-Permyak from an autonomous region to one with less self-determination, and the Komi-Permyak people ceased to be the majority in their own region and became a minority in ethnic Russian-dominated Perm instead.

The Russian state also attracts criticism for weakening civil society. All non-governmental organizations must submit to onerous registration regulations; Russia ranks as number 147 of 168 countries on the Reporters Sans Frontiers press freedoms list,[5] and the police are sometimes used as means of controlling unwelcome dissent. For example, in November 2006 police officers detained journalists from Gazeta.Ru, Novaya Gazeta and Panorama Sovremennoi Politiki when they attempted to cover a small protest by the Yabloko Party's youth branch and the youth movement "Da!", keeping the journalists at the station until the protest was over.[6]


Anna Politkovskaya

The disintegration in Chechnya drives the central state's concern over independent-minded minorities. Legislative changes and a system of regional presidential representatives helped consolidate the center's control, but rarely does local instability turn into violence. The most egregious example of this was in December 2004 during a police crackdown in the city of Blagoveschesnk, in the Republic of Bashkortostan. Ethnic Russians compose only 36 percent of the population; 50.9 percent are ethnic Bashkirs and Tatars, and the general trend in the region is pulling for further autonomy from the center and distance from Russian culture. When a group of teenagers reportedly beat three of its officers, the police (dominated by ethnic Russians) sent special units and local police to detain all men under 35 they encountered on the street, in buildings and even inside some apartments, for five days, along with anyone who objected to the arrests. Those resisting were beaten on site. The police brought the suspects to the district department of internal affairs, beat them there, and then released them. After two days of this action in the city of Blagoveschensk proper, the police moved to four surrounding towns and conducted the same operations there. The Moscow Helsinki group estimates that during those five days, more than 1,000 people suffered this treatment, many more than once.[7]

Foreign actors are not exempt from pressure to adhere to the official program in Russia. Anthony Brenton, an ambassador from the United Kingdom to Russia, lodged an official complaint with the Russian Foreign Ministry to protest his harassment by member of Наши (Nashi, which means "ours" in

[4] "78 percent of Russian political elite comes from KGB-FSB," Eurasian Secret Services Daily Review, Dec.12, 2006. http://www.axisglobe.com/article.asp?article=1163, Finn, Peter. "In Russia, A Secretive Force Widens." Washington Post, Dec. 12, 2006.
[5] Press Freedom Index, Reporters Without Borders, http://www.rsf.org/rubrique.php3?id_rubrique=639 2006
[6] "Москва. На Акции Протеста Милиция Задержала Репортеров," Glasnost Defense Foundation, Nov. 23, 2006. http://www.gdf.ru/digest/digest/digest307.shtml
[7] Human Rights in Russian Regions, Moscow Helsinki Group, 2004

Russian), a pro-Kremlin youth group. Nashi members have been following Ambassador Brenton for four months in a campaign the *Financial Times* called "professionally done" and which "borders on violence." Nashi leaders meet regularly with Putin and his deputy chief of staff, Vladislav Surkov, and on Dec. 2 they warned that such protests will continue until Ambassador Brenton publicly apologizes for meeting with Russian opposition members.[8]

Perhaps the most high-profile indication of uncertainty is the series of assassinations that took place over the last few months of 2006. Unlike the mob wars of the 1990s, the targets of these new assassinations include influential figures not specifically linked to organized crime. Recent high-profile murders include Alexander Litvinenko, the ex-KGB spy turned Putin opponent and ally of disgraced Russian oligarch Boris Berezovsky; investigative journalist Anna Politkovskaya[10]; VTB-24 (the retail unit of Russia's second largest bank, Vneshtorgbank) Branch Director Aleksandr Plokhin; TAR-TASS business journalist Anatoly Voronin; chief engineer of BP Plc's Russian gas unit, OAO Russia Petroleum Enver Ziganshin; and central bank reformer Andrei Kozlov. Since 2004, other high-profile murders included Forbes journalist Paul Klebnikov, banker Aleksandr Slesarev and Novosibirsk Deputy Mayor Valery Maryasov.

Shamed oligarch Boris Berezovsky[9]

Despite these very real challenges, the Russian government has made improvements. Economic growth in the country increased employment opportunities, and the chaos of the 1990s has mostly subsided. President Putin prizes stability, and he brought it to many areas of the country with recentralization, legislative reforms and personal efforts. At this point, the greatest challenge to the system he has created is most likely Putin himself; the constitution prohibits him from serving another term, and no clear replacement has emerged. Much debate surrounds the possibility of amending the constitution or which favorite could be the next leader of Russia, but as of yet no reliable predications are possible.

Allegedly murdered former spy Alexander Litvinenko[11]

2.3 Economic Background

2.3.1 General Features

An economic synopsis of the Russian Federation is a complex affair. On many levels, and by most standard measurements, the picture is quite encouraging, but at the same time, there tend to be

[8] Donahue, Patrick and Stringer, Robin. "U.K. Complains to Russia, Says Group Harasses Envoy," Bloomberg.com, Dec. 8, 2006. http://www.bloomberg.com/apps/news?pid=20601102&sid=aobkNJ6SZ.3w&refer=uk
[9] Mosnews.com, http://www.mosnews.com/files/11476/berezovsky-5.jpg
[10] Photo Credit: *Time Magazine*, December 2005, http://img.timeinc.net/time/europe/hero2005/images/ph_politovskya.jpg
[11] Prima News, Moscow, http://www.prima-news.ru/upimg/m_27415.jpg

recurrent incidents that give cause for pessimism. Moreover, there are serious problems specific to Russia that have never been observed on such a large scale, namely its environmental and demographic deterioration, which make any long-term predictions uncertain at best, but potentially catastrophic.

Specifically, growth rates, inflation trends and factor utilization figures over the past several years appear strong and sound. Massive investment flows, mostly from Europe but with significant contributions from newly wealthy Russians, are at an all time high, and show no signs of decreasing. The Russian education system has kept true to its standards, thereby providing a talented pool of problem solvers and workers. However, the endemic corruption of the Russian government, the courts and the Federation's regulatory apparatus remain salient sources of risk. Moreover, the country's heavy reliance on natural resources, especially oil and gas, and the deep inequality among regions and within cities do not look like the model of a healthy emerging economy. Finally, Russia's declining, aging population and deplorable health figures lead many to question the sustainability of long-term growth.

One good index of the risks of doing business in Russia is the Opacity Index, now conducted by the Kurzman Group. Using economic, political and social indicators, this index seeks to frame reprehensible government behavior as an investment risk. According to its calculations, to justify the risks of opacity, investors in the Russian economy (opacity index score: 46) would need to generate a return-on-investment 5.46 percent higher than that of an identical investment in the United States. However, it is notable that Russia, despite its serious problems, still scores higher than India or China, each of which boasts remarkable and growing levels of foreign direct investment. The main reason for this apparent anomaly is simple: the returns in these capital-hungry economies are often great enough to offset the risks.[12]

2.3.2 Macroeconomic Indicators: Attractive on the Surface

The strength of Russia's GDP growth since its recovery from the 1998 economic crisis has made the country a major destination of foreign investment, mostly from Europe. Russia's GDP grew by 7.2 percent in 2004 and 6.4 percent in 2005 to reach $1.6 trillion US (measured by purchasing power parity, PPP) or $765 million in nominal terms.[13] Real GDP growth is expected to be 6.5 percent for 2007, about the same as 2005 and 2006.[14] That places Russia's current GDP at $1.65 trillion (PPP) or $815 billion (nominal).

GDP and GNI increases of late reflect "total factor productivity" gains, the most desirable and sustainable kind. This also strongly suggests that the gains reflect not the increasing levels of investments, but the integration of technologies and organizational schemes that are helping Russia catch up to its factor potential. Direct investments increased 55.5 percent to $10.3 billion throughout 2006, and portfolio investments increased 82.3 percent to $665 million, according to Rosstat figures. Other investments (including commercial and other loans) grew 22.8 percent to $24.4 billion.[15]

[12] The Kurtzman Group, *The Opacity Index: 2005*, at http://www.opacityindex.com/opacity_index.pdf
[13] World Bank Global Development Indicators http://www.worldbank.org and the Federal State Statistics Service, at http://www.fsgs.ru/
[14] IMF, 4
[15] Ben Aris, "A Row over Russia's FDI Figures," *Business New Europe*, Nov. 30, 2006, at http://www.businessneweurope.eu

2.3.3 Macroeconomic Tables:

Macroeconomic Indicators (non-percentage figures in billions USD)

	2000	2001	2002	2003	2004	2005	2006	2007
GDP Growth	10 percent	5.10 percent	4.70 percent	7.30 percent	7.20 percent	6.40 percent	6.50 percent	6.50 percent
Foreign Currency Reserves	24.8	33.1	44.6	73.8	121.5	186.3	288.9	420.9
Ratio of Reserves to Trade Balance	40.6	44.6	52.9	71.5	92.7	113.1	140.8	179.2
Consumer prices (percent change)	20.81 percent	21.60 percent	15.96 percent	13.63 percent	10.90 percent	12.60 percent	9.70 percent	8.50 percent

Source: IMF, Russian Federation: Statistical Appendix, 2006, at http://www.imf.org/external/pubs/cat/longres.cfm?sk=20161.0; and The Economist Country Briefings, http://www.economist.com

Investment Statistics in million USD

Indicator	1999	2000	2001	2002	2003	2004	2005
Direct Investment	1,102	-463	216	-72	-1,769	1,662	13,519
Abroad	-2,208	-3,117	-2,533	-3,533	-9,727	-13,782	-15,386
In Russia	3,309	2,714	2,748	3,461	7,958	15,444	28,905

Source: IMF, Russian Federation: Statistical Appendix, 2006, at http://www.imf.org/external/pubs/cat/longres.cfm?sk=20161.0

2.3.4 Looking Deeper: Sources of Concern

On balance, these indicators suggest a volatile but vibrant economy. Russia's immense gains from its energy exports have enabled it to build up healthy foreign reserves that can help stabilize future shocks and that can also become vital sources of reinvestment into public goods such as the modernization of Russia's aging infrastructure. However the government's willingness to perform such tasks is open to debate. And beneath these figures, many economists point to anomalous fluctuations that indicate distorting effects. To quote a recent *Economist* article, "Distortions are common to all post-Soviet economies, but they are particularly evident in Russia."[16]

The economy's primary source of concern is its overwhelming reliance on energy exports; one 2005 World Bank study gave convincing reasons to think that the energy sector's contribution to GDP, officially nine percent, is closer to 20 percent. The Russian federal government tends to use the energy revenues to prop up inefficient state government offices, which in turn hire more workers without providing strategic direction.[17] If this perpetuates, it would signal a classic case of "Dutch Disease."[18] In late 2005,

[16] The Economist, "Command and Control," *Russia's Economy*, April 7, 2004, at http://www.economist.com/research/backgrounders/displaystory.cfm?story_id=2577463
[17] *Ibid.*

the government paid $7.1 billion to gain more than 50 percent ownership of Gazprom, suggesting that its control over energy revenues will only increase henceforth.[19]

Harmful effects are also evident in the prevalence of oligarchies in private enterprise. The 10 largest ownership groups account for some 60 percent of the Russian stock market, a concentration matched in recent times only in Suharto's Indonesia.[20] Inflation also looks to be growing at undesirable rates. The official figures for 2005 put inflation at 5.8 percent, an improvement over the 11.7 percent of 2004, but more objective sources put the figures closer to 10 percent.[21] In 2006, inflation is estimated to be 10.5 percent at years end.[22]

Within this tangled morass of contradictory trends and ambiguous indicators, the Russian IT sector occupies an undeniably important, but still shaky position.

[18] "Dutch disease is an economic concept that tries to explain the seeming relationship between the exploitation of natural resources and a decline in the manufacturing sector. The theory is that an increase in revenues from natural resources will deindustrialise a nation's economy by raising the exchange rate, which makes the manufacturing sector less competitive.," http://en.wikipedia.org/wiki/Dutch_disease
[19] The Economist, "Told You So", June 23, 2005, at http://www.economist.com/research/backgrounders/displaystory.cfm?story_id=4113527
[20] *ibid.*
[21] *ibid.*
[22] IMF, *The Russian Federation: Country Study*

3 The Russian Information Technology Sector

3.1 Human Capital

Russia's greatest asset for future IT sector development is its highly educated technical labor force. The legacy of the Soviet education system, which intensively emphasized math and science, remains strong today. Despite the country's low income per capita and troubled development history, its people are among the best educated in the world. One anecdotal but telling piece of evidence is the 2006 results of the International Olympiad in Informatics. The Soviet team placed third with three gold medals and one bronze, behind only the Chinese and the Polish teams.[23]

This deep and broad talent pool is all the more attractive because it is cheap to mobilize. The average monthly wage in Moscow is officially only around 17,000 rubles ($630); elsewhere, it is less. A large portion of the population has been left behind by the new prosperity.[24] IT specialists do relatively better than average, but generally only make 15-20 percent as much as their US counterparts. Moreover, Russian IT specialists have a reputation for reliability because most have memories of days when good jobs were difficult to find. According to the latest figures, the Russian software industry has the highest productivity of any major industrial sector in the country, and it is the most internationally competitive.[25] Almost all of this success is due to the sheer skill of the workers.

Despite these formidable strengths, there is one potential weakness in the Russian IT labor market. Profound mathematical and engineering training is almost always an asset when dealing with IT, but it does not always translate directly into expertise on specific systems, many of which have their own, sometimes arbitrary, peculiarities. As a result, although Russians tend to be quite adept at dealing with computational and networking systems in general, there remains an abundant pool of mid-to-high-skilled workers with extensive knowledge of individual software firms but little understanding of the IT industry in general. This generates good employees, but does not augur well for the development of the IT sector as a whole.

This talented but directionless labor pool has become a major source of programming and engineering talent for US and European firms. Roughly 30,000 Russians are engaged in the IT off-shoring market at present, and that figure is set to grow into the indefinite future.[26] Present growth rates stand at 40 percent per year. Moreover, the Russian education system graduates roughly 100,000 new programmers each year, resulting in a huge domestic surplus. Among the US firms that have capitalized on this vast pool of talent are IBM, one of the first western companies to recruit Russian talent, Microsoft, Cisco and Google, which opened two research and development centers in Russia in the past year and acquired one Russian search company to form the core of its operations there.[27] For its part, IBM alone maintains four research centers in Russia, employs more than 200 programmers and engineers and has injected $40-60 billion in research funding alone.[28]

---

[23] OSPINT Staff Writer, "Russians Took gold at the International Olympiad in Informatics," *OSPINT.com*, Aug. 28, 2006, http://www.ospint.com/text/d/2618397/index.html
[24] The Economist, "Building a New Rome", Aug. 24, 2006, http://www.economist.com/research/articlesBySubject/displayStory.cfm?story_id=7830915&subjectid=349002
[25] D. J. Peterson, *Russia and the Information Revolution*, RAND National Security Research Division, May 2005, p. 17
[26] Peterson, Russia and the Information Revolution, Rand, p. 15
[27] Pavel Kupriyanov, "Google opens R&D in Russia," *OSPINT.com*, April 11, 2006, http://www.ospint.com/text/d/2589901/index.html and "Google chose St. Petersburg for its second R&D center in Russia," Oct. 18, 2006, http://www.ospint.com/text/d/3237958/index.html
[28] Igor Lukianenko, "IBM Opens System Lab in Russia," *OPSINT.com*, July 7, 2006, http://www.ospint.com/text/d/2539844/index.html

3.2 Software

While the hardware sub-sector in Russia is average, software is a different story altogether. With its massive reservoir of programming talent, Russian software manufacturers are growing quickly and with strong indications of even greater future success.

The software field's major players are now many, but the more influential among them are Parus, Galactica, Diasoft, Optima and Sterling. Each of these firms produce, among other types, enterprise resource planning software for Russian firms in the banking, power generation and oil production industries.[29] This type of software is currently the major revenue earner for the domestic Russian markets, reflecting businesses' rapid rush to integrate IT into their operations. Kaspersky Lab is a further software firm of note; its anti-virus, anti-spyware and anti-intrusion products are sold worldwide. While domestic software is almost always adequate and generally cheaper than Western equivalents, having foreign software systems is often seen as an indicator of compatibility with Western business norms and therefore can help attract foreign investors.

With domestically obtained profits providing an ample safety net, many Russian software makers are expanding into the international market. During 2006, estimates indicate that Russian firms exported $2 billion in software, a figure expected to grow to $12-14 billion by 2010 even with some reduction in the past few years' impressive 80 percent growth rates in foreign sales.[30]

3.3 IT Hardware

The hardware market is more important in Russia than in most other countries of comparable size, wealth or development. The industry consensus is that Russian-made PCs and networking technologies are not far behind Western models, the best estimate being about one model year. A full 50 percent of Russian IT spending goes to hardware, and 80 percent of that is spent on desktop PCs. This percentage is likely to decline over the next five years, because the present high figures are a result of many Russian firms and local government offices buying their first IT systems in the past several years.[31] Indeed, the most recent figures point to just such a slow down. From 2004 to 2005, the PC market declined from 32 percent to 22 percent. Predictably, laptop sales doubled in share of total spending from 8 percent to 19 percent during 2005, and IDC Corporation predicts an average of 17 percent growth in this market until 2010.[32]

The dominant players in the Russian market are R-Style, Aquarius Group, Kraftway, Formoza, DEPO and K-Systems. Known as "red assemblers," these companies generally buy most of the basic components from abroad. However, foreign PC retailers captured only six percent of the Russian market among them in 2005.[33] Indeed, the only domestic champion component maker is the Micron Chip Factory. This company's recent success has led it to seek larger global market share under the Sitronics brand.

---

[29] Peterson, Russia and the Information Revolution, Rand, p. 10
[30] OSPINT Staff Writer, "Russia Exported 2 billion USD Worth of Software," *OSPINT.com*, Nov. 21, 2006, http://www.ospint.com/text/d/3527934/index.html
[31] RAND, p. 34
[32] OSPINT Staff Writer, "Russian PC Market Slows Down," April 25, 2006, http://www.ospint.com/text/d/2558327/index.html
[33] Peterson, Russia and the Information Revolution, Rand, p. 36

3.4 Mobile Telephony

Russia's has three main providers of wireless telephony, MTS, Vympelcom and Megaphon, (which together claim almost 90 percent of total market revenue of $10.2 billion in 2005.[34] Between 2002 and 2006 more than 110 million Russians became mobile phone subscribers, constituting a 50-100 percent each year since 2000.[35] Currently, Russia's mobile penetration rate is more than 90 percent with 50 million new subscribers in 2005.[36] This stands in remarkable contrast to the fixed-line market, which consisted of only 40 percent of Russians in 2005. Moscow and St. Petersburg are already nearing the saturation point of 100 percent of the adult population, though many people will end up with more than one mobile phone.

Interestingly, with seven percent of the "big three's" revenues coming from non-voice services, some could view these wireless giants as poised to enter wireless Internet markets as ISPs.[37]

Indicator	2003	2004	2005
Total Market Size	11,900	18,000	20,600
Total Equipment Market Size	1,900	3,300	4,100
Total Equip. Exports	275	391	420
Total Equip. Imports	n/a	2,740	2,860
Total Services Market Size	10,000	14,700	16,500

Source: US commercial service, doing business in Russia, February 2006

The market leaders in service provision have been perhaps a bit too successful in recent years. In October 2005, the Russian government's anti-monopoly task force called MTS and Vympelcom to task for their overwhelming power in the market. Of course, by definition, neither of these firms could be considered a monopoly, but the main charge levied against them was that they were involved in price fixing and collusive market division.[38] This, said a group of regional mobile service providers, put the giant firms in breach of Article 6 of the Federal Law on Competition which criminalizes the following: "coordinate action of dominating market players entailing significant breach of competition laws and infringing the interests of other business enterprises."[39]

The most interesting questions are, why the mobile providers, and why now? Hundreds of Russian companies stand in violation of this law every day, yet are never questioned about it. The most likely answers are a good organizational scheme on the part of the regional operators or the government's desire to take more of a cut of their revenue.

3.5 Internet-Specific Technologies

In 2005, the Economist Intelligence Unit ranked Russia number 52 out of 65 countries, behind India and Saudi Arabia, in terms of IT sector development potential. In 2002, Russia ranked number 42 out of 60

[34] US Commercial Service, *Doing Business in Russia: A country Commercial Guide for US Companies*, US Department of State, Feb. 13, 2006
[35] RAND, 2005
[36] OSPINT Staff Writer, "Every third Russian owns a mobile phone," Sept. 19, 2006, http://www.ospint.com/text/d/2752217/index.html
[37] Russia Profile Staff Writer, T*elecommunications Overview,* Russia Profile, 2006, at http://www.russiaprofile.ru
[38] Julia Koldicheva, "Russian Mobile Operators caught breaching anti-monopoly law," *Network World*, Oct. 25, 2006, at http://www.ospint.com/text/d/3282342/index.html
[39] i*bid.*

countries according to the same measurement.[40] Despite this gloomy assessment, some sectors of the digital economy in Russia have shown strong and consistent growth. In 2004, communications showed $19 billion in revenues, while the IT sector generated $9-10 billion, together constituting about five percent of Russia's GDP.[41]

3.6 Broadband

Revenues from broadband services in Moscow alone are estimated to have grown by 45 percent to $195 million by the end of 2006 from a year earlier. More than 800,000 Moscow households were broadband customers by mid-2006, up 18 percent in six months. Another million had adopted the technology by the year's end. The present penetration rate stands now at 26 percent of households. Moscow accounts for more than 25 percent of all broadband subscribers in Russia, with the national penetration rate at 3.5 percent as of the end of summer 2006; however, this is expected to expand rapidly in the larger cities. As of mid-2006, about 57 percent of Moscow broadband connections were made via Ethernet technology, about 37 percent via ADSL technology and about six percent via cable TV networks.[42]

3.7 Wireless Internet

By November 2006, Golden Technologies had emerged as the undisputed leader of wi-fi Internet access in the Moscow area. The company claims to have built roughly 5,000 hotspots, which together cover a circle in central Moscow with a radius of up to five kilometers from Red Square. Market indicators suggest this is just the beginning, with analysts expecting market volume to double in 3-4 years to about $70 million. Golden Technologies itself aims to capture 15 percent to 20 percent of the market with 350,000 to 400,000 subscribers by 2010.[43]

Just as the first wi-fi networks become accepted, WIMAX technology is already in the planning phases for rollout in Moscow. Comstar UTS has applied for frequencies in the 2.5 to 2.7 gigahertz range to build a WiMAX network in several Russian regions, but will concentrate first on Moscow. Ultimately, every Russian city with more than a million residents will have a Comstar WIMAX network at its center, probably by 2015.[44] However, these initiatives are still young and should pick up as new enterprises with similar goals enter the market.

3.8 Internet Penetration and Use

According to the Public Opinion Foundation, which has the latest available Internet use data, there are a total of 27 million Russian Internet users, constituting about 20 percent of the country's population. Of these, 9.1 million use the Internet daily while another 4.9 million use it weekly; the rest connect either monthly or once every three months. The Russian Internet audience is ranked number 23 in the world, just after Brazil but generally well above most countries except northern European and the native English-speaking countries.[45] Although Russia's Internet audience has grown from 8.7 million total users in 2002, the proportions of use frequency have held more or less constant, with roughly one-third of all users being daily users in any given observation period.

Levels of wealth, population and technological sophistication are highly divergent from region to region and between the cities and the countryside. Indeed, although Moscow holds only about nine percent of

[40] Peterson, Russia and the Information Revolution, Rand, 26
[41] Peterson, Russia and the Information Revolution, Rand, 28
[42] Russia Profile Staff Writer, T*elecommunications Overview*
[43] Lyudmila Yaremchuk, "Golden Telecom to compete for Moscow broadband access customers with Wi-fi technology", *Computerworld Russia*, Oct. 30, 2006, at http://www.ospint.com/text/d/3317182/index.html
[44] Russia Profile Staff Writer, T*elecommunications Overview,* p. 5
[45] Peterson, Russia and the Information Revolution, Rand, 2005

Russia's roughly 142 million people, almost 17 percent of all Russian Internet users, or just more than 4.5 million people, are also Muscovites.[46] The following table lists the absolute and relative distribution of Internet users throughout Russia's federal administrative regions:

Internet users in Russia by federal administrative region

There are three basic trajectories followed by Russia's different regions since 2002. Moscow's and St. Petersburg's Internet user population, as percentage of the total population, has nearly doubled from 27 percent to 52 percent and from 13 percent to 31 percent, respectively. The percentage of Internet users among the total has quadrupled in the Far East, from six to 25 percent. In the Central, Southern, Ural, Volga Basin and Siberian regions, the percentage has tripled, from around 6-8 percent to 17-20 percent.[47]

3.9 Nearing Saturation?

Findings from the "Expert Committee" of the [Russian] National Institute for Regional Researches and Political Technologies" report on Information and Communications Technologies (ICT) diffusion and E-Russia's progress, follow. The number of PC users in Russia increased by 10 percent since the end of 2005. A robust 25 percent of Russian urbanites use computers on a regular basis (multiple times weekly).[48] The Internet was classified as "indispensable" by 13 percent of Russians, and one-third of all urbanites use it multiple times weekly. Dial-up connections are still the norm for 57 percent of Russians, but broadband connections are increasing rapidly, moving from 13 percent to 39 percent in the past year. Moreover, the Russian appetite is still vibrant. For every one Russian Internet user, there are two who expressed a desire for regular access.[49] Of course, Moscow and St. Petersburg will soon reach a critical saturation point, which is currently estimated to be near 88-90 percent of the population, if observations in highly digitized countries like Denmark and South Korea are any indicators. However, it will take at least another decade, and quite possibly longer, before the other regions reach this point. Indeed, massive Wi-fi rollout may be necessary to achieve this. It is important to remember that almost two-thirds of all Russian homes still lack a fixed telephone line, and tens of thousands of villages and far-flung towns have no telecommunications infrastructure at all.

[46] "The Internet in Russia," Public Opinion Foundation Poll, Oct. 12, 2006, at http://bd.english.fom.ru/report/map/eint0603
[47] "The Internet in Russia", Public Opinion Foundation Poll, Oct., 12, 2006 at http://bd.english.fom.ru/report/map/eint0603
[48] Lyudmila Yaremchuk, "Russians increasingly use PCs and Internet, report says," *OSPINT.com*, Dec. 13, 2006, at http://www.ospint.com/text/d/3707508/index.html
[49] Lyudmila Yaremchuk, "Golden Telecom to compete for Moscow broadband access customers with Wi-fi technology", *Computerworld Russia*, Oct. 30, 2006, at http://www.ospint.com/text/d/3317182/index.html

3.10 Government Influence in the IT Sector

It is hard to overestimate the influence that the Russian government has over the revenues and, to a lesser extent, the direction of the Russian IT sector. Unfortunately, according to one IT sector CEO, "The development of the IT sector has so far not been on the [Russian] government's list of priorities."[50]

Russia was a relatively late entrant into the information revolution. When the Soviet Union collapsed in 1991, the new Russian Federation inherited an antiquated system that was designed for and adapted to the needs of the military-industrial apparatus. Thus, it is unsurprising that considerable changes were necessary before Russians could even begin to participate in the IT revolution.[51] The real boom began roughly in 2000, when recovery from the 1998 crash took hold. Rapid economic growth and increased government spending helped to fuel the growth of new firms and the creation of new ones. Since then, growth in the Russian IT sector has varied between 20-25 percent per year compared to roughly 5.5— 6.0 percent in the US. In 2004, the federal government spent more than $640 million on IT products and services while other levels of government spent just below $1.2 billion.[52] In 2005, RAND analysts estimate that the federal government itself spent $1.2 billion.

This year, The Ministry of Information Technologies and Communications (MinInformSvyaz or МинИнформСвяз) has initiated the process of forming a joint stock company, the Russian Investment Fund for Information and Communication technologies. Several different ministries and other independent government agencies will also participate in the establishment of this fund. The startup costs, $54 million, will be totally provided by the Russian Investment Fund. MinInformSvyaz will be a shareholder on behalf of the Russian Federation.[53]

3.11 Regulatory Environment

Although many more recent elements of the Russian regulatory system are modeled on EU or European countries' national regulatory schemes, it also retains features and cultural traits dating back to the Soviet period. Moreover, there are uniquely Russian elements blended in. Any unfamiliar regulatory environment can be daunting, but the Russian one can be especially so given its propensity to frequent change and the selectivity with which officials sometimes apply the rules.

A 2005 OECD evaluation of the Russian regulatory environment claimed that businesses faced too many rules, some of which are contradictory, that changed frequently and were inconsistently applied. The justice system, the authors claimed, is unresponsive and nepotistic. The gas, electricity and railway industries are monopolies that often seem to follow a different set of rules. From these assessments, the OECD concludes that the Russian economy is growing, in general, "more interventionist [and] less rule-governed."[54] Along the same lines, A Foreign Investment Advisor Council Survey showed that nearly all foreign investors in the Russian market listed licensing procedures and obtaining work visas as the greatest barriers to effective engagement of the market in Russia.[55]

The 2003 Communications Law, *O svyazi* (On Communications) provides the backbone of the Russian ICT regulatory system. Russian legislators crafted the law specifically to respond to blatant shortcomings that were perceived to contribute to the risky and crime-ridden ICT sector. In practice, however, enforcement fails to live up to both the spirit and the letter of the law, which itself can be vague or even

[50] Peterson, Russia and the Information Revolution, Rand, 27
[51] *ibid*, p. 38
[52] *ibid*, p. 51
[53] OPSINT Staff Writer, Russian Government getting ready to launch technology venture fund," OPSINT.com, Nov. 27, 2006
[54] The Economist, "Told you so," http://www.economist.com/research/Backgrounders/displaystory.cfm?story_id=4113527
[55] Foreign Investment Advisory Council, *Russia: Investment Destination 2006*, FIAC Survey, May 2006, p. 55

contradictory on critical issues. Persistent problems include inconsistent licensing procedures, a universal service provision tax, disparities in the rights and privileges of different firms, a lack of transparency and, of course, corruption.[56]

Another important legislative package of direct consequence for the Internet and IT industries is the so-called "Extremism Law." Enacted by the Duma in June 2002, the law is meant to enable the state to respond effectively to terrorist activity on or against the telecommunications and IT sectors, but also carries the additional implication of giving the government greater powers of censorship. Another function of the law is to prevent radical right-wing groups from fomenting violence through the Internet. The provision states that should such material appear on a website, the telecommunications operator is responsible for deactivating it as soon as possible or risk losing its license.[57] The most relevant language in the article is:

> *"Use of public telecommunication networks for engaging in extremist activity is prohibited. Remedies envisaged by this federal law, taking into consideration peculiarities of relations regulated by legislation on communication, will be implemented in case public telecommunication networks are used for engaging in extremist activity."*[58]

3.12 Regulated Deregulation

In July 2006, President Putin approved amendments to the 2003 Communications Law that will help dissolve the state's controlling interest in fixed-line telecom operator Svyazinvest. The sale of most of the government's shares will further telecom privatization efforts, but before this could occur, special provisions had to be agreed upon that would ensure military and law enforcement access to the network. Some investment houses have already begun to speculate that the sale will soon lead to increased efficiencies in connected regional networks.[59]

Government oversight laws require retention of many documents in hard-copy format, making IT storage and transmission superfluous.[60] This is an unfortunate holdover from communist-era legislation, but the legal basis for change already exists. The 2003 Communications law, for instance, contains numerous provisions detailing the legal rationale for electronic signatures being functionally equivalent to physical, handwritten signatures, provided certain safeguards are in place.[61]

3.13 Intellectual Property

The formation of the Russian Federation's intellectual property standards stemmed from its accession to the World International Property Organization Treaties in 1996. In September 2006, a presidential spokesman for Legislative Activities and Monitoring announced that Russia had finally met its obligations under that treaty, in terms of having all necessary laws and procedures in place. Enforcement, as ever, may still remain a problem, but the Kremlin and the Duma are expected to allay concerns over this aspect in parts of Russia's WTO accession push.

---

[56] US Commercial Service, *Doing Business in Russia: A country Commercial Guide for US Companies*, US Department of State, Feb. 13, 2006
[57] Alexander Lakhov and Haik Karapetyan, "Russia: New Law Could Seriously Restrict Internet Activities," *Regulatory Digest*, August 2002, at http://www.bnai.com (subscription required)
[58] *ibid.*
[59] BNAI, "Russia: Telecommunications", *Regulatory Digest*, August 2006, at www.bnai.com (subscription required)
[60] Peterson, Russia and the Information Revolution, Rand, 42
[61] Oxana Iatsyk, President Putin Signs Law on Electronic Digital Signatures", *BNAI Regulatory Digest*, February 2002, at http://www.bnai.com (subscription required)

As part of their new commitment to intellectual property integrity, Russian officials also instituted a series of laws designed to clamp down on Internet piracy. Russia currently ranks third behind China and Indonesia as a haven for software piracy, but the new round of laws promises to treat material published on the Internet as equal to materials published on CD or DVD formats.[62] Although this may be the right language for the legal community, such a claim is very ironic considering the notorious abundance of pirated music, cinema and software in Russia.

Indeed, that said, Russia's accession to the WTO, whether or not it is currently in compliance with WTO standards, will drastically speed up anti-piracy efforts, though given the current levels of piracy in Russia, even an ideal clean-up could take more than a decade.

3.14 Website Security Certificates, Data Protection and Encryption

The theft of Russian's personal data has not been nearly as serious a problem as for US and European citizens. Thus, it is not surprising that Russia did not have a first-rate data protection law until December 2005. Federal Law no. 160-FZ, "On Ratifying the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data," is drawn from the eponymous convention ratified by the Council of Europe in 1981. The primary intent of the law is the protection of individual privacy, although in practice it is more about forcing compliance among negligent corporations.[63]

All website security certificates are handled through the state, in contrast to most of the developed world, which relies on private companies for such security services. One Russian official responsible for the federal certification scheme claimed that, because it was managed by the government, there were rarely any problems with spoofing of Russian sites. Of course, Russian malicious actors who spoof foreign websites are an entirely different matter.[64]

The same official told iDefense analysts that his present focus rests on new encryption techniques that could potentially ease the tension between the government's concern for security and private businesses interest in confidentiality. At present, federal level prohibitions on strong encryption have deterred potential partners, especially financial services firms, from doing extensive business in Russia. Some see this as a way for the government to retain extensive control over key economic sectors while others believe it is meant to privilege domestic firms.[65] Either way, staunch regulations on encryption make it difficult to develop secure online transactions and have been a persistent point of contention for foreign financial services firms wishing to do business in Russia.[66]

[62] BNAI, "Copyright Protection Takes Effect for Works on the Internet," October 2006, at www.bnai.com (subscription required
[63] US-Russia Business Council, "New Russian Legislation: 2005 Year-End Update," December 2005
[64] Interview with senior official of the Ministry of Information Technology and Communications, Sochi, Russia, Sept. 13, 2006
[65] Interview with senior official of the Ministry of Information Technology and Communications, Sochi, Russia, Sept. 13, 2006, and Interview with Russian ex-hacker, Sochi, Russia, Sept. 15, 2006
[66] Peterson, Russia and the Information Revolution, Rand, 39

4 The Russian Threat Landscape: Corruption, Cyber Crime and Those Who Fight It

4.1 Corruption

Corruption is perhaps the most well-known negative feature of the Russian economy and its political underpinnings. The apparent majority of empowered individuals, from top-level Duma members and Kremlin mandarins to traffic police and customs agents, appear to be "on the take." Unfortunately, this stereotype has a strong basis in fact. While people's perceptions of corruption can often be higher than its actual frequency or severity, the notorious "bribe tax" is a fact of life in many sectors of the Russian economy.

The INDEM Fund, a corruption watchdog group, estimates the present cost of corruption in Russia at more than $3 billion per year and climbing.[67] INDEM also estimates the volume of business corruption to exceed the federal government's budget by 40 percent for any given year since 2000.[68]

The Public Opinion Foundation often conducts surveys on corruption. In the latest, 28 percent reported giving bribes in the last year while 34 percent said they would if demanded.[69] Of those who responded in the affirmative to giving bribes, 45 percent were Muscovites.[70] Survey respondents overwhelmingly cited police officers as the most corrupt public officials. Foreign investors in Russia, on the other hand, cited tax officials, trade policy officials, and Federal Licensing Authorities as the most corrupt.[71]

INDEM Corruption Characteristics	2001	2005
Percent of Citizens who engaged in Corruption	50.4	54.9
Corruption pressure on citizens	25.7	35
Citizens' readiness to bribe	74.7	53.2
Average no. of bribes per year	1.92	0.882
Average bribe amount (USD)	69.1	105.72
Average yearly bribe cost (USD)	82.22	93.25
Bribes as percent of income	0.0121	0.0117
Average volume of corruption (USD billions)	2,825	3,014

Source: INDEM, "Corruption process in Russia: level, structure, trends," INDEM Fund, 2005
http://www.indem.ru/en/publicat/2005diag_engV.htm

Despite the ubiquity and severity of corruption, the situation seems to be improving. A recent World Bank report, drawing upon triennial survey data from thousands of firms in the EU and FSU, concludes that progress in reducing corruption in the Russian Federation is evident and unambiguous.[72] Of course, corruption there remains significantly more serious there than in the EU countries, but the important

[67] INDEM Staff Writer, "Corruption process in Russia: level, structure, trends," INDEM Fund, 2005 http://www.indem.ru/en/publicat/2005diag_engV.htm , page 1
[68] ibid., page 2
[69] Svetlana Klimova, "Corruption in Russia Today," *Public Opinion Foundation Population Poll*, http://bd.english.fom.ru/report/map/ed064722, page 3
[70] *ibid.*
[71] Foreign Investment Advisory Council, *Russia: Investment Destination 2006*, FIAC Survey, May 2006, p. 41
[72] "Progress on Corruption Mixed in Russian Federation: Corruption Eased in Transition Countries from 2002-2005, Reports World Bank", World Bank Press Release, July 26, 2006, at http://media.worldbank.org/secure

point is that legal, institutional and economic reforms, when properly implemented, do tend to reduce corruption. Moreover, barring a severe economic downturn or shift in government policy, the trend is likely to hold. In general, Russian businesses pay smaller bribes and do so less frequently when compared to data points in 2002, 1999, and 1996.[73] However, some key sectors, notably licensing and procurement, show either no change or an increase in bribery.

Official corruption can also enable criminals to evade prosecution for their misdeeds. A senior MVD investigator told iDefense analysts about a particularly unsavory criminal, "Flyman," in St. Petersburg who worked with Russian cyber criminals by hosting their malicious code and content on his Russia-based servers. Flyman is also one of Russia's, and perhaps the world's, largest purveyors of child pornography. When the MVD investigator sought to arrest this individual, his efforts soon met forceful, official resistance. Flyman's father is an influential St. Petersburg politician who used his leverage and money to persuade law enforcement authorities to prevent do-gooders from pursuing the case.[74]

To minimize exposure to corrupt practices, the US Commercial Service advises dealing only with large, well-known companies or publicly visible officials whenever possible. However, recent incidents indicate that larger organizations may simply engage in larger corruption schemes. In October 2006, the MVD's Economic Security Division exposed eight Russian banks that had laundered more than $8 billion over the past three years.[75] In the IT sector, the most recent high-profile incidence of corruption was made public in early December 2006, with a dramatic SWAT-style raid by Russian police into IBM's Moscow headquarters.[76] The initial reports suggest that the scandal involves the possibility that IBM, along with other hardware vendors R-Style and Lanit, each reportedly bought equipment at a price not commensurate with the price at which they sold the equipment to the Russian State Pension Fund. IBM reportedly sold the pension fund no less than 1,000 servers and 50,000 PCs while Lanit and R-Style sold various pieces of equipment to the fund for "$655 million and $590 million, respectively."[77]

This is not the only manner in which corruption can impact the future health of Russia's IT industry and network. Many of the so-called technology parks in Moscow, Volgograd, Nizhniy-Novgorod and other cities are thought by many to be little more than corrupt pork-barrel largesse in disguise. The problems are worsened by the fact that significant talent may be drawn to attractive sounding firms in these parks, and some firms may draw significant foreign investment, much of which may never produce returns. Driven by corruption, poor planning and inexperienced management, many technology parks are likely to remain simple funding sinks. The Russian government has indicated plans to funnel another $80 million into such technology parks throughout the Moscow area during 2007.[78]

4.2 The Economic Theory of Corruption: Motives of the Russian State

Classical equilibrium market theory views corruption as a price balancer in markets where, by informational asymmetries or by fiat, prices are incommensurate with the value of a good. The entire Russian federal government runs on a budget smaller than that of Texas, suggesting that most public servants and officials are underpaid, relative to the services they perform, the costs of acquiring the skills

[73] Ibid.
[74] Interview with MVD investigator, Moscow, Russia, Sept. 20, 2006
[75] RBC Daily, Economic Security Division Accuses Banks of Fraud," Oct. 18, 2006, reprinted at http://www.russiaprofile.org/resources/business/sectors/banking/index.wbp
[76] "Carl Schreck, "IBM, Lanit, R-Style Accused of Fraud," Moscow Times, Dec. 8, 2006, at http://www.moscowtimes.ru/stories/2006/12/08/001.html
[77] ibid and John Oates, "Armed Police Raid IBM's Moscow Office," The Register, Dec. 7, 2006, at http://www.theregister.co.uk/2006/12/07/ibm_moscow_raided
[78] "From Russia with Technology?," *Business Week*, Jan. 30, 2006. http://www.businessweek.com/magazine/content/06_05/b3969420.htm

they use and the opportunity costs of using those skills elsewhere.[79] If the "bribe tax" were too high, the classicists argue, people would simply forego the purchase.

Corruption can be seen as a service with supply (officials pressure on citizens to pay bribes) and demand (people's willingness to pay).[80] Depending on the nature of an official's position, he/she can leverage control of supply to demand more or less illicit compensation. If there are similar officials with comparable power, then competitive pricing may emerge and could even reach an equilibrium stability point. For instance, a police official can threaten someone with jail time more or less arbitrarily while a real-estate official can only make the purchasing process more difficult for a potential buyer. The real estate official, also, is more at the mercy of the market for real estate than a police officer is to the crime rate.

Modern theorists have disputed that official corruption is more than just a price equalizer for two reasons: first, it injects an element of uncertainty and arbitrariness into whichever market it touches, and second, it can be backed by the state's monopoly on jurisdictionally legitimate violence. Thus, these "unseen" collective costs of corruption far outweigh any benefit they may bestow upon the few who (or the many, in the case of Russia) exercise the privilege.[81] Ultimately, corruption distorts the information content of the economy to such a degree that the market becomes nothing more than a sophisticated system of banditry.

Russia is an interesting case through which to observe the interplay of these different theoretical approaches to corruption. It is so endemic to the country that it tends to punish only the most strictly honest and ethical individuals. So many individuals participate in corrupt practices that, as young people are learning about their economic and civic system, they come to view it as a normal state of affairs even though it is considered to be "wrong." Indeed, in one population poll, 70 percent of respondents claimed they thought acceptance of bribes was wrong while 68 percent believed others thought the practice to be wrong.[82] In the same poll, 67 percent of Russians said they believed that corruption could not be fought.[83] In a 2004 poll conducted in Vladivostok by Management Systems International, the overwhelming majority of all respondents said they believed corruption was wrong, but 60 percent of people under 28 said they believed it was sometimes justified to get what one wants.[84]

This attitude of mass "honor among thieves," the proverbial wink and nudge, amounts to far more than the officially powerful benefiting at the expense of the weak and poor. Much of modern economics and finance scholarship tends to show that economies function best which are the most transparent and least arbitrary. Such conditions allow for market participants to plan with greater reliability and also give a clearer picture of the relationship between fiat money prices and the functional value of the good or service in question.

With this in mind, the recent anti-corruption efforts of the Kremlin become more interesting. What some see a crackdown on corruption, upon further analysis, could just as easily be an example of supreme hypocrisy. Indeed, given that so many Russian government officials and businesspeople are corrupt, what led the Kremlin to select the targets it did? There are two likely answers. The first is money. The Kremlin simply selected targets that promised to provide the most financial gain for the authorities' efforts to expose them. The other possibility is power. Because of Russia's abundant pool of world-class IT talent, the sector is recognized as a critical engine of future growth that should also help increase the diversity

[79] *Symposium on Corruption in the Developing World*, University of Westminster, London, UK, June 15, 2001
[80] INDEM Staff Writer, "Corruption process in Russia: level, structure, trends," INDEM Fund, 2005 http://www.indem.ru/en/publicat/2005diag_engV.htm
[81] *ibid.*
[82] Svetlana Klimova, "Corruption in Russia Today," page 3
[83] *ibid.*
[84] Management Systems International, "Public Opinion of Corruption in Vladivostok," June 11, 2004, at http://www.bisnis.doc.gov/bisnis/bisdoc/0411RFE percent20Public percent20opinion percent20of percent20corruption.htm, page 2

of the Russian economy. Recognizing this, the Russian government has in recent years channeled significant funding into IT-related initiatives and is positioned to continue doing so for years to come.

Ultimately, both motivations are probably at play, but it is too soon to tell which, if either, will prove to be the dominant rationale for future crackdowns. The lesson to be drawn here is that, despite the burgeoning growth of the Russian IT market, among others, the political risk of state opposition remains higher than many other countries boasting similar growth rates.

4.3 Law Enforcement

The structures and functions of the Russian law enforcement apparatus are of considerable concern to businesses— foreign and domestic— operating in Russia. The problems associated with Russian police forces, at all levels, are both acute and pervasive. Major issues include strong tendencies toward corruption, abusiveness, apathy, incompetence and under provision of essential resources. Because an analysis of the entire Russian law enforcement community could fill volumes, this section focuses only upon those police units and practices of direct consequence for information security. This analysis draws not only upon secondary sources, but on extensive interviews by iDefense with Russian police investigators.

MVD Uniform Patch (St. George Insignia) [85]

The primary federal police unit responsible for cyber crime investigation is Department K of the Ministerstvo Vnutrennikh Del (MVD— Ministry of the Interior). As a ministry-level unit, it has a far wider scope of powers than any other domestic law enforcement bodies. Moreover, its investigators are the best available in the country, excepting those who perform similar functions for the FSB (Internal Security Service). For cyber crime affecting businesses, however, the FSB is not likely to be of significant consequence, focused as its activities are upon issues of national security.


FSB Official Seal[86]

According to one senior investigator, there are at most 20 to 30 federal-level police involved in cyber issues who are at once honest, dedicated and competent. While police corruption is generally the greatest fear of Western companies, apathy is often of greater consequence. Unfortunately, cyber crime investigation is not generally considered a worthwhile use of officers' time. The more ambitious and able investigators find greater prestige benefits in more salient fields such as counterterrorism, narcotics, organized crime investigations and, of course, building cases against the enemies of powerful political figures.

Cyber crime, by contrast, is known to be a serious problem, but is generally sidelined by decision makers who rightly acknowledge that more serious problems deserve the majority of Russia's limited law enforcement resources. Moreover, so long as cyber criminals' main victims are foreign entities, it becomes even more difficult to justify extensive police attention. However, the converse of this attitude is that once a cyber criminal acts upon important domestic companies or government assets, the invasive powers of the Russian police are often brought in to bear down swiftly and forcefully. With fewer legal checks on their investigative strategies,

[85] Retwa Image Library, http://www.retwa.org/admin/imageLibrary/public/thumb_200px-MVD_russia_stof.gif
[86] FAS.org, http://www.fas.org/irp/world/russia/fsb/fsb_logo.gif

Russian police can, under such circumstances, operate in ways that would contravene Western norms of due process and civil liberties, but which can often be more expedient from the investigators' point of view.

Compared to the US counterparts, Russian law enforcement investigators have more access to information with fewer bureaucratic hurdles to surpass. For example, Russian investigators routinely access and record server logs without having to notify the owner.

4.4 The Positive Aspects of Russian Law Enforcement

Despite the extensive structural and organizational-cultural problems in the Russian law enforcement community, those few honest, dedicated and competent investigators are remarkably effective. When bureaucratic hurdles are minimal, when resources are sufficient and with the support of key officials, the best Russian cyber cops demonstrate world-class levels of skill and innovation. Under such amenable circumstances, federal level police have scored several notable victories against the Russian cyber crime underground.

Still, the career choices of Russia's most capable cyber cops are telling indicators. Most officers either become corrupt or disillusioned after several years on the force, one investigator told iDefense analysts. Those who do not grow corrupt often move on to the private sector after several years to higher salaries and better equipment. This is bad for the police forces, who do put resources into training investigators and need all of the talent they can muster. However, on the other hand, it is good for the private sector, which also needs experienced talent with solid connections to law enforcement departments. Cooperation among security professionals and law enforcement personnel is extensive, not least of all because many of each category were once in the other. The two roles are often complementary, with each having access to different types of information and different advantages in investigative techniques.

The law enforcement investigators whom iDefense analysts interviewed were both honest men who were eager to establish international cooperative efforts. Several weeks after the on-site visit, iDefense analysts participated in an international conference call with law enforcement from Russia, Poland and the UK. Such relationships are the sharpest tools of cyber cops in any country, and Russia's best understand it well. Concerning cooperation with US authorities, one senior investigator told iDefense that the FBI was quite difficult to work with, but that the US Secret Service was a model of competence and fairness in cooperation.[87] Such perceptions probably helped generate the recent official memorandum of understanding signed by the USSS and the MVD. Although this official gesture to facilitate joint investigations of financial cyber crime solidifies and helps institutionalize cooperation between the two agencies, they have cooperated on serious, high-profile cases for years. Indeed, the US Secret Service's 2004 Operation Firewall owed some of its success to cooperation with foreign law enforcement agencies, especially the MVD.[88]

4.5 The Resourceful Russian Carder

The Russian carding scene remains the most populated and active (in terms of monetary flows) of any in the world with the exception of the US. In fact, the two scenes are well connected, as shown by the tendency of US or English-language carders rushing to Russian sites in the aftermath of significant operations by US authorities. This happened almost immediately in the wake of 2004's Operation Firewall and appears to be happening with lesser intensity since 2006's Operation Cardkeeper.

[87] Interview with MVD Investigator, Moscow, Russia, Sept. 19, 2006
[88] Mike Bucken, "US, Russian Authorities Sign Law Enforcement Agreement," *Computerworld*, Oct. 13, 2006

Over the past several years, the Russian carding population has developed a robust market with well-established procedures and networks. A key result of this market development is the increasing specialization of Russian carders. The most sophisticated attack tools and techniques of 2006 all emerged from Russian groups: WebAttacker, MetaFisher, Snatch and now Rock Phish not to mention thousands of Trojans.[89]

Both Russian police officials (MVD) whom iDefense interviewed indicated that, although the Russian carding scene was advanced and large, authorities had nonetheless scored several major victories in the past year. The three carders which, a year ago, were recognized as the most successful have all been apprehended, two of them by Russian police and the other through cooperation between Russian and Ukrainian law enforcement. This increase in law enforcement success appears to have led some ambitious carders to think more strategically.

In August 2006, iDefense received intelligence that some Russian carders were searching for inside information on law enforcement agencies, bank personnel and academic materials related to information security studies. It was immediately evident that the carders were engaging in advanced data mining and correlation exercises that amount to tactical reconnaissance of the financial industry and law enforcement cyber crime units in Russia, the US and Europe.[90]

An analysis of the types of data collected by the attackers and the methods they employ suggests a level of strategic sophistication, organizational capacity and ambition never before seen among common Russian (or any other) carders. Regarding their logistical attack methods, the attackers have constructed efficient and powerful interfaces to control bot armies and to continually customize their malicious code. This enhanced system of command and control dramatically increases the number of victims targeted in a given time period while simultaneously expanding the proportion of targets from which desired information will be stolen. All of the control tools used by the attackers are open source, easily obtainable and extensively customizable. Thus, the possibilities for refinement are much greater than those exhibited at present.

Serious though the above may be, the greatest danger is evident in the types of information that the attackers are collecting. Before this investigation, iDefense held no prior evidence that common carders have obtained (or even sought) the types of information listed above, and if other researchers have uncovered such evidence, they have not published it. Despite the absence of precedent, the information sought by the attackers leads to some disturbing insights into their motives and strategies.

The information being mined by the attackers can be classified into several categories beyond standard cardholder data: fundamental research, countermeasure research and confidential insider data on organization's structures and processes. First, the academic theses databases and news archives constitute basic research that attackers can use to hone their methods and target selection schema.

Second, the information pertaining to fraud software sellers and financial industry training firms indicates that the attackers recognize that their long-term prospects for success in the cyber crime underground are enhanced by "knowing their enemies." Equivalent to reconnaissance by military or intelligence personnel, this information will allow the criminals to design more stealthy attacks and to conduct campaigns of disinformation and obfuscation to thwart law enforcement and security personnel. Less than a year ago, in the aftermath of operation firewall, most English-language carding forums contained only the most rudimentary discussions, even among veteran fraudsters, on how to spot and evade security professionals. By contrast, the Russian groups examined here are incredibly more aware of their relationship to their adversaries.

[89] See any back issues of the iDefense Bi-Weekly Malicious Code Review and most 2006 issues of the *Weekly Threat Report*
[90] Internal iDefense Analysis, unpublished, August 2006

Third, the job/resume repositories and bank employee portals indicate two things. One, the attackers are trying diligently to understand the inner workings of the institutions they target, and can easily do so if they are focused enough in their data collection and analysis. And two, the attackers are most likely looking for financial service employees, current and prospective, who can be planted to facilitate larger scale data theft with greater chance of impunity. Most implications of this are obvious, although it is worth stressing that targeted social engineering is a likely goal, as is skillful manipulation of internal information flows to aid in covering the criminals' tracks.

iDefense analysts drew the following conclusions from the evidence. First, the groups already possess significant financial resources and are staffed by multiple, experienced, intelligent criminals. In short, these activities do not fit popular profiles of the members of the carding community: lone, free-agents with highly specified skillsets exchanging information and services anonymously from their basements or alleyway cafes. The attackers above are organized team-players who may remain anonymous, but who can trust one another and who know well each other's working styles and expertise.

Second, their likely goals are either or both of two possibilities: sell the information to the wider carding community for a profit; or analyze and employ the information to craft unstoppable attack strategies evolving faster than security personnel's countermeasures. If fully utilized, this knowledge could help the group steal tens (maybe hundreds) of millions from banks and hitherto underexploited targets such as mutual funds and brokerage accounts. Indeed, the latter appear to be a new favorite target of Russian cyber criminals, as indicated by the recent capture of an ethic Russian working out of Estonia who used compromised brokerage accounts to inflate the price of penny stocks which he himself then sold short to reap more than $300,000 in profits.[91]

The recent history of the carding community suggests that the individuals involved tend to be reactive to changes in their environment rather than anticipatory. Moreover, they do not seem to be able to work together closely on long-term projects although they do forge lasting buyer-seller relationships. The attackers discussed in this article do not conform to that modus operandi. Instead, the evidence above seems to support more recent conjectures that Russian organized crime syndicates are becoming heavily involved in online fraud.

4.6 Motivation/Weltanschauung: Perceptions and Targets

The general hacking environment in Russia can be characterized as financially driven. Some "ethical hacking" for the sake of the challenge does take place, as does politically motivated hacking (or "hacktivism"). For the most part, however, the Russian cyber crime scene is exactly that, criminal, and its aim is to maximize the amount of money the participants can make. Despite this, condemnation of criminal hacking in Russia is not as great as one might expect. As long as hackers avoid targeting "regular Russians," their activities are generally tolerated, and even admired.

Russian cyber criminals overwhelmingly prefer targets outside of the Russian Federation, with foreign companies operating in Russia as the second most favored choice. The need for cross-border cooperation complicates investigation and prosecution efforts, while investigating crimes against foreign interests is not a priority for overstretched and often unmotivated law enforcement officers in Russia (see section 4.3 Law Enforcement). Internationally based foreign entities are also less likely to possess any sort of protection operations in Russia proper, which adds a further level of safety for criminals within Russia's borders.

[91] Floyd Norris, "SEC Says Russian Trader Used Stolen Online Passwords," *New York Times*, Dec. 19, 2006, at http://www.nytimes.com/2006/12/20/business/worldbusiness/20pump.html

Of these Western targets, financial institutions in Western Europe and the US are the most attractive. They are generally wealthier than most Russian targets and, in the case of Western Europe, are geographically close, which makes making connections and finding collaborators easier. What is more, reputation is very valuable to financial institutions, so even when it is possible for Russian law enforcement officials to investigate domestic hackers, the victim organizations are quite reluctant cooperate out of fear that their vulnerabilities will become known and their reputation compromised.

Hackers' intelligence and skills, ability to "put one over on the big guys," and even nationalist pride in Russians successfully attacking [wealthy] foreign targets, all contribute to a positive perception of hackers by many Russians, as does a generally higher opinion for those members of society who make their living from technically illegal methods. The ubiquitous corruption in Russia means that virtually all successful people are compromised to some degree, which in turn breeds tolerance of illicit behaviors. The general population also does not view hacking as an inherently harmful pursuit; to the contrary; successful Russian hackers are often viewed with pride and respect for their ability to live well by tricking wealthy foreigners, especially those in the West who are often portrayed in the media as arrogant and deserving of being taken down a peg.

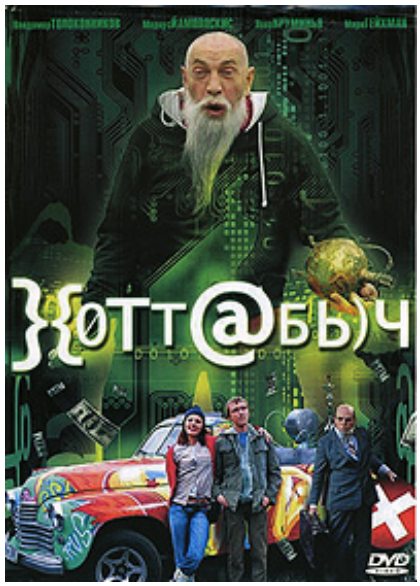
The portrayal of successful hackers as "cool," successful and powerful is exhibited by the March 2006 cover of *Хакер* (*Hacker*), the primary hackers' magazine in Russia. The cover shows hackers adopting poses more commonly encountered among Western rap stars, wearing flashy jewelry and surrounded by scantily dressed women. The magazine invites, *"we have conquered the world – are you with us?"* A poster included in the same issue depicted a money tree sprouting dollars and bearing the caption "I LOVE WMZ," WMZ being the equivalent of dollars on the WebMoney electronic money exchange.

What is most interesting about magazines such as *Hacker* is not so much what the authors choose to offer readers, but that such publications openly operate within Russia, despite their advocacy of what is essentially a criminal lifestyle. Officially, such publications are protected by regulations protecting free speech, but the degree of successful control exerted over media outlets that are critical of the Putin government suggests that magazines such as Hacker could not operate as openly or as widely if the state strongly disapproved.

March 2006 cover of Khaker magazine – Moscow, "We have conquered the world – are you with us?"

Another recent example of such attitudes is the hit Russian comedy *Хоттабыч* (*Khottabych).* The original Khottabych is a genie in the 1930s Soviet children's classic book of the same name. In that book and the 1950 movie based thereon, Khottabych is a genie freed after a 1,000 years by a model Soviet boy, who astounds the genie with the rights and high quality of life enjoyed by the common Soviet man. In the 2006 version Khottabych, spelled in Cyrillic "Leet" as "}{0TT@бь)ч" is freed by Gena, an affable, highly skilled hacker who spends his days breaking into the systems of wealthy, Western corporations. Gena purchases the copper kettle containing Khottabych on an online auction site, and the genie helps Gena's attempts to handle life offline, evade corrupt law enforcement officers who are in league with the mafia, and foil the combined efforts of the Russian Secret Service, the FBI and Microsoft in stopping Gena from hacking. In the process, Gena falls in love with the beautiful female FBI agent sent to apprehend him, and with the aid of Khottabych, convinces her to help him escape her former employers and generally make fools of them. Although entertaining, what is most interesting about this remake is that it is the hacker who is portrayed as the new model Russian boy and the law enforcement

agents sent to catch him are portrayed as dishonest and bungling. Instead of being amazed by the sanatoriums for the workers and educational opportunities provided by the state as he is in 1950, the 2006 Khottabych is horrified by the system in place and instead helps the fundamentally honest hacker Gena thumb his nose at the powers that be.



The Genie Khottabych watches over hacker Gena and "reformed" FBI agent Annie

Despite what would appear as an obvious repudiation of the Soviet system and ideals among hackers, a great deal of Soviet nostalgia and awareness is apparent among much of the hacker discourse. This suggests that at least a significant portion of those hackers active in the semi-public sphere are old enough that they lived more than just their earliest years during the Soviet Union, and that many feel a level of nostalgia for those times. Examples of hacker's enduring interest in that time are evident in hacker magazines and forums. The hacker magazine *Khaker-SPETS* specifically dedicated the April 2006 edition to Soviet nostalgia and dates many of its readers as former "Octoberists and Pioneers," which would make them approximately 25 or older. The Mazafaka hacker eZine opens with the tolling of the Kremlin bells, while even law enforcement officials dedicated to tracking down hackers employ similar imagery to identify themselves, such as the following avatar graphic used by one as his ID in an instant messaging program.

Soviet soldier with the star symbolizing the five continents to which Communism will supposedly spread and the initials "USSR"

Even more, iDefense research analysts sent to Russia were given a mock induction into the Communist Young Pioneers youth group, complete with Lenin lapel pins, the Pioneer salute and the Pioneer oath ("always prepared"). This is not to say that Russian hackers embrace the ideals of the Soviet era. They are still dedicated to their craft and maximizing the money gained by their talents. The following image was posted on the Russian hacker forum *Mazafaka*, and while the design is that of a Soviet-era poster promising the spread of socialism the text reads "Cashier" at the top and "We are automating the payment system" at the bottom.

"We are automating the payment system"

Officials have criticized some hackers and hacking in recent weeks, primarily when discussing the threat to critical infrastructure posed by hackers hostile to the Russian Federation, but for the most part official concern is not high. This may change as Russian targets are increasingly targeted, particularly major Russian banks (see section 4.9.3 Financial Fraud). A few more high-profile cases of this nature or an increase in the number of Russians targeted could damage Russians' perception of hackers, but for the time being their reputations and self images are predominantly positive.

4.7 Insider Threat in the Russian Threat Landscape

During a September 2006 on-site research project in the Russian Federation, iDefense analysts discussed various threats with six private-sector information security professionals, three government (Ministry of Information Technologies and Communications) officials, two police officers, one Gazprom executive and one former hacker. When asked, "What is the greatest class of threat in the Russian cyber landscape?" every subject indicated the insider threat.[92]

The primacy of the insider threat stems from the same factors that explain the country's thriving hacker culture. Specifically, the legacy of a world-class education system, especially in mathematical, scientific and engineering fields, has produced a relatively large and talented population with insufficient employment opportunities. The economic instability and high unemployment of the 1990s led many such tech-savvy Russians to lives of cyber crime. However, as indicated by figures from the World Bank, IMF, various governments and investment banks, the Russian economy is improving, with the IT sector showing particularly strong growth.[93] Thus, many formerly unemployed technical experts now have jobs, but some of them have chosen to continue their criminal activities. The threat is compounded by the rampant corruption and graft that have become caricatured features of the Russian economy. Workers and even leaders in many Russian industries are occasionally dishonest, and those in IT-related sectors are no exception; they simply require a more technically advanced skillset to achieve their ends.

None of this is at all surprising. The insider threat is a preeminent fear in most countries, especially among financial firms and those with extensive intellectual property assets. In the Russian Federation, however, the insider threat manifests itself in unusually bold ways. For instance, one former doyen of the international, underground carding community, a St. Petersburg-based criminal calling himself "Leroy," based much of his operation on using financial sector insiders. The lead investigator who captured Leroy told iDefense analysts that the carder first corrupted existing insiders, mostly tellers, but later grew so bold as to plant his own insiders at various banks in the Russian Federation.[94] Few carders have ever evinced such long-term strategy. In the most extreme case, Leroy was able to obtain from a corrupted IT security insider the algorithms used to generate credit card numbers. Using insiders in this way made Leroy, for a time, the most successful carder known to Russian law enforcement.

One interviewee, the IT security director of a major St. Petersburg bank, told iDefense that nearly all serious threat incidents affecting his bank over the past several years were due to insider threat. One senior official in the Ministry of Information and Communications provided a similar synopsis. "Only things the government fears is [sic] terrorists, spies and criminals inside," he said.[95] A senior executive of Gazprom echoed this refrain. When asked which threats he feared the most, he first noted insiders, including espionage. One former hacker who is now an information security professional expressed concern over the potential recurrence of an incident like the 1999 takeover by hackers of a major Gazprom pipeline.[96]

A recent publication by McAfee Inc. analyst David Marcus claims that organized crime syndicates are recruiting IT-savvy adolescents between the ages of 14-18 to work as hackers and malicious insiders. Marcus argues that some recruits are selected for their likelihood to end up in the IT departments of successful companies, Russian or Western, which often become victims of elaborate attacks months or years later. Considering the pervasiveness of the inside threat, organized crime and cyber crime in the

[92] Interviews conducted between Sept. 12 and Sept. 21, 2006, in Sochi, Russia and Moscow. iDefense interviewed four interviewees more than once.
[93] See this report's Economics Section above.
[94] Interview with MVD Senior Investigator, Moscow, Russia, Sept. 18, 2006
[95] Interview with bank security director and MITC official, Sochi, Russia, Sept. 16, 2006
[96] Interview with Gazprom executive, Sochi, Russia, Sept. 15, 2006; Interview with former hacker, Sept. 15, 2006, Sochi Russia

Russian Federation, it is certainly possible, perhaps even likely, that some criminal groups attempt to complement their ranks with IT talent. However, iDefense analysts believe that Marcus is overstating his case, which may mislead readers about the actual significance of the threat.

One serious problem is that McAfee has not provided any sources to reinforce his claims. One journalist specifically asked one of the report's authors for specific instances, but he was unable to provide any evidence. Of course, such instances are highly clandestine by nature, so few, if any, researchers would be able to cite specific instances. Another source of confusion is the meaning of "organized crime." In the Russian Federation, police investigators usually attempt to classify as an organized crime syndicate any group of four or more conspiring to commit a crime. Laws on organized crime are harsher than upon common criminals, and this gives police extra leverage with which to elicit cooperation from some suspects. Thus, an organized crime group recruiting a high school student with IT skills could be as simple as one college-aged member of a five-member hacking team trying to convince a former schoolmate to join his team. This is, of course, bad news for the Russian threat landscape, but it is hardly as serious as millionaire Mafiosi from Moscow attempting to build a cyber criminal cell. That said, it is likely that the traditional mob syndicates in Russia do have some cyber crime specialists among them, but the problem is not as institutionalized as the McAfee report suggests.

Finally, even government employees can be insider threats. From time to time, information stolen by government employees or officials becomes available on the black market. In 2005, for instance, a CD titled "Incomes of Muscovites for 2003" was sold on the street for less than $200.[97]

4.8 Piracy and Intellectual Property Infringement

Although the situation is improved, Russia remains an area of concern regarding intellectual property rights and the enforcement of anti-piracy measures. For this reason Russia is one of 13 countries on the highest level of the United States Trade Representative's priority watch list for its failure to sufficiently protect intellectual property rights. Russia shares this distinction with China, followed by Argentina, Belize, Brazil, Egypt, India, Indonesia, Israel, Lebanon, Turkey, Ukraine and Venezuela. The Russian government did officially identify the protection of intellectual property rights as a priority, and is in the process of changing the civil code to strengthen existing intellectual property rights regulations. However, although these regulations are a step toward stricter controls on intellectual property, if adopted they would not bring Russia into full compliance with international norms and would permit much of the current abuses to continue.

Most famously, the pirate website www.allofmp3.com remains operational, despite international pressure and lawsuits within the country. This is due to a combination of the copyright laws in Russia, which contain enough loopholes for the site to continue operating at least quasi-legally. Popular opinion sympathizes with allofmp3.com to such an extent that the major Russian IT news site www.cnews.ru reported on measures taken by Visa and MasterCard to prevent customers from paying Allofmp3.com using their cards as "Allofmp3.com Falls Victim to the Americans."[98]

In November 2005, the Russian government did take steps to restrict the sale of counterfeit wares sold in a serious of police raids on some of the largest markets for such products, including the largest such market, the Gorbushka market in Moscow. Although the raids initially reduced the amount of counterfeit goods sold, most sellers since moved their operations to other markets, such as the Rubin trade center, the Tsaritsinio and the Mitino. Smaller raids and prosecutions have taken place outside of Moscow, but

[97] Peterson, Russia and the Information Revolution, Rand, 64
[98] "Allofmp3.com Вновь Стал Жертвой Американцев," *CNews*, Oct. 19. 2006. http://spb.cnews.ru/news/top/index.shtml?2006/10/19/214522

they mostly target smaller businesses instead of the major producers and distributors. Even Russia's second city, St. Petersburg, only prosecuted its first intellectual property cases in 2005.[99]

The lack of prosecution is partly a function of corruption and the difficulties law enforcement agencies face in investigating and prosecuting intellectual property violations, and partially a function of the general population's acceptance of such activities, at least on a small scale. Legitimate software and music is very expensive in Russia, where the average monthly salary is slightly more than $400 US,[100] and "sticking it to the big guys" is a recognized cultural value. Many Russians are therefore unwilling to pay very much for software or music, and therefore do not view complaints concerning most intellectual property violations as particularly important.

This opinion was substantiated in a poll conducted by a St. Petersburg committee on counterfeit wares. St. Petersburg is a relatively wealthier city where the average monthly income is approximately $500 US. Of the more than 500 St. Petersburg residents polled, 36 percent were willing to pay 70 to 150 rubles for a software or music disc, 13 percent 150 to 400 rubles and only 2.6 percent were willing to spend 400 to 700 rubles. About 44 percent of those polled said that they did not purchase discs at all, either because they did not own their computer or obtain their software free of charge.[101]

Amount willing to pay for software or music disc	Percentage of those polled willing to pay that amount
400- 700 rubles ($15.00 - $26.50)	2.6 percent
150 - 400 rubles ($5.50 - $15.00)	13.0 percent
70 - 150 rubles ($2.50 - $5.50)	36.0 percent
Do not purchase discs	44.0 percent

Amount St. Petersburg residents are willing to spend on software and music discs[102]

Neighboring countries offer minimal assistance; although many did reduce their own intellectual property violations, they continue to serve as trans-shipment points for Russian products, particularly pirated discs. Ukraine, Lithuania, Latvia and Poland are particularly important trans-shipment points for goods destined for the Western EU states.

Despite these challenges, Russia has made some progress. Increased monitoring and enforcement decreased the production of pirated optical discs in factories located on government-owned land,[103] and specific software manufacturers such as Microsoft encountered success in cooperating directly with local customers and officials to restrict the use of counterfeit versions of their software among major corporations and government bodies. Such phenomena are exceptions rather than the norm, however, and intellectual property rights remain far from secure.

Companies seeking to protect intellectual property in Russia should register with the country's patent agency and its Customs service. The US and Russia are both members of the Madrid Protocol, which means that companies in each may apply for trademark and patent protection in the other. For American firms, this entails registering with Rospatent, the Russian Federal Service for Intellectual Property,

[99] "В Петербурге За Год Изъят 1 Млн. Единиц Контрафакта," *CNews*, Nov. 23, 2006
http://safre.cnews.ru/news/line/index.shtml?2006/11/23/218344
[100] BOFIT Russia Review, Suomen Pankin Siirtymätalouksien Tutkimuslaitos (BOFIT) , Aug. 12, 2006
http://www.bof.fi/bofit/eng/4ruec/index.stm
[101] Пиратов-Питерцев Накажет Совет, *CNews*, Nov. 21 2006., http://spb.cnews.ru/news/top/index.shtml?2006/11/21/218064
[102] Пиратов-Питерцев Накажет Совет, *CNews*, Nov. 21 2006, http://spb.cnews.ru/news/top/index.shtml?2006/11/21/218064
[103]" Report Notes Continued Progress on Intellectual Property Rights, Identifies Significant Improvements Still Needed in China and Russia ," Office of the U.S. Trade Representative, April 28., 2006
http://www.ustr.gov/Document_Library/Press_Releases/2006/April/Report_Notes_Continued_Progress_on_Intellectual_Property_Rights,_Identifies_Significant_Improvements_Still_Needed_in_China_R.html?htm

Patents and Trademarks. US companies should also register with the Russian Customs Service, which is committed to blocking the exports of counterfeit products (when able to identify them) and will aid in the investigation and prosecution of suspects. Most importantly, taking these measures will provide American companies with the legal basis when requesting investigation and prosecution of cases that the company itself has encountered; as with many other aspects of the Russian legal system, successful enforcement of intellectual property rights most often originates in the efforts of the rights holders to identify violators.

Russians may begin affording greater importance to the enforcement of intellectual property rights in the near future, however. While Russians traditionally benefited from copying one another's intellectual property, Russian organizations' own property is increasingly at risk, and with this risk comes a strengthened support and advocacy for stronger regulations and enforcement. A recent example of such threats to Russian intellectual property is the theft of Kaspersky Lab's anti-virus database by Jiangmin, a large Chinese anti-virus software producer. The Kaspersky lab software developers located their own names, written in Cyrillic, in Jiangmin software code, code which is very similar to what Kaspersky developed. The Kaspersky lab is in the process of negotiating for reparations from Jiangmin, but declared that if the two firms cannot come to a satisfactory arrangement that it will sue Jiangmin in all relevant courts.[104] As more Russian firms find themselves victims of intellectual property theft, interest in protecting intellectual property will rise.

4.9 Internet-Based Scams

4.9.1 Extortion

Direct financial fraud is not the only weapon in the Russian hacker's arsenal; many have adopted and adapted extortion, a favored method of more traditional organized crime. This most commonly comes in the form of threats to interfere with the victims' operations if they do not pay, or in the form of ransom demands after the hackers have already accessed the victims' systems and deleted and/or encrypted important data.

In January 2006, iDefense reported on a high-profile, yet very straightforward, example of the first type of extortion. British student Alex Tew's popular advertising site, Million Dollar Homepage, suffered a denial of service (DoS) attack involving as many as tens of thousands computers, which began Jan. 11 and brought the site down by Jan. 12, although the hosting company of the site, InfoRelay Online Systems Inc. was able to restore the site by the next day. The details are unclear, but press accounts indicate that hackers demanded $5,000 to prevent an attack, and then $50,000 to end it.[105] InfoRelay Online Systems, the company that hosts the Million Dollar Homepage, said that it appeared as if a Russian group was responsible.

In October 2006, the Saratov court convicted a group of three Russian hackers in their early twenties, Saratov resident Ivan Maksakov, Astrakhan resident Alexander Petrov and St. Petersburg resident Denis Stepanov, for engaging in a more sophisticated version of the same extortion type directed at the Million Dollar Homepage. According to Saratov prosecutor Anton Pakhmanov, the group, founded by then-20-year-old Maksakov, installed spyware onto the systems of more than 50 UK online casinos and bookmakers, used the information they obtained to show the site operators that they were capable of interfering with their operations, and then demanded payments to avoid further DDoS attacks. At least

[104] "Kaspersky Blames Chinese Counterparts," OSP International. Nov. 04, 2006. http://www.ospint.com/text/d/2570512/index.html
[105] Stanciu, Adrian. "Hackers Claim $50K for the Million Dollar Homepage," *Softpedia News*, Jan. 19, 2006. http://news.softpedia.com/news/Hackers-claim-50K-for-the-Million-Dollar-Homepage-16659.shtml, Sanders, Tom. "Extortionists Behind Million Dollar DDoS Attack," *IT Week*, Jan. 19, 2006. http://www.itweek.co.uk/vnunet/news/2148849/cyber-criminals-target-pixel

one firm paid more than $40,000 to prevent such an attack.[106] Firms that did not pay lost even more; one such company, Canbet Sports Bookmakers, suffered a DoS attack during the Breeders Cup, costing Canbet more than £100,000 in lost revenue for each day the site was down. Although the case focused on British companies, the Saratov court estimated that the group extorted more than $4 million US from various companies in about 30 countries. The court sentenced all three members of the group to eight years in a high-security penal colony and a 100,000 ruble ($3,800 US) fine.[107]

In some cases, Russian hackers do not threaten to interfere with victims' operations, but instead focus primarily on ransoming data. This process can even be automated using programs such as the KillFyl.A Trojan to allow less experienced hackers to extort funds.[108] While some so-called "ransomware" programs encrypt data, this particular Trojan disables various system features of explorer.exe, which can be reactivated by the hacker at will. Although the author of KillFyl.A appears to reside in Ukraine, this is still considered a Russian threat, as the payment demand is in Russian, and many Russians and Russian-speaking Ukrainians move and collaborate between the two countries. Furthermore, the e-mail address associated with this incident is cdsg@rambler.ru; rambler.ru is a free Russian e-mail service akin to yahoo! or gmail.

In other cases, the extortion is closer to blackmail. Russian hackers might access an organization's site, copy data, and then demand payment for keeping said information private. In March 2006, two hackers were arrested in Sverdlovsk; the Ministry of Internal Affairs of the Russian Federation accused them of hacking into a Kaliningrad company, copying proprietary data, and then demanding $10,000 up front and $1,000 per month thereafter to prevent their publicizing what they found.[109]

4.9.2 Social Engineering

Russian criminals are skilled at social engineering, often considered the least technical type of cyber crime, although due to distance and language issues, they will not always use it when targeting foreign victims. That said, social engineering techniques are improving, and many Russians can conduct such attacks in languages other than Russian, including English. Those Russian cyber criminals who specialize in social engineering are called синжери (sinerzhi), which is a contraction of социальные инженеры (sotsialnie inzhiniri, or social engineering).[110] Smaller-scale attacks tend to be focused attempts to gain passwords or administrative rights, sometimes through targeted phishing or through phone calls and even personal interaction. Large-scale attacks can be quite sophisticated, incorporating different techniques (phone, e-mail, post, in person), prior practice on targets of no interest to improve attackers' abilities and even technical assistance, such as voice and video surveillance.[111]

4.9.3 Financial Fraud

Russian hackers are well known for their criminal abilities, particularly those involving financial institutions. The scale and number of the attacks prompted Russian Interior Minister Rashid Nurgaliyev to warn of a coming cyber crime epidemic in April 2006, citing the threat posed by hackers from the Former Soviet Union, especially Russia, followed by the Ukraine and Belarus. More cyber criminals originate from or operate within that triad than any other region in the world,[112] to such an extent that according to Boris Miroshnikov, head of the Bureau for Special Technical Events of the Russian Interior

[106] "Российские Хакеры Осуждены За Вымогательство Через Интернет," *YTPO.ru*, March 10. 2006. http://www.utro.ru/news/2006/10/03/589278.shtml
[107] "Хакеры Заработавшие" $4 Млн, Получили 8 Лет Тюрьмы," *Korrespondent*, Oct. 3, 2006. http://www.korrespondent.net/main/165972/
[108] iDefense Weekly Threat Report, June 5, 2006
[109] iDefense Weekly Threat Report, March 20, 2006
[110] iDefense Weekly Threat Report, March 20, 2006
[111] iDefense Weekly Threat Report, 2004
[112] Bigg, Claire. "Authorities Warn of Cyber Crime Epidemic," RadioFreeLiberty/Radio Free Europe, April 20. 2006. http://www.rferl.org/featuresarticle/2006/4/7D821779-4411-43D1-BF7B-D19743879DF6.html

Ministry, there were 15,000 crimes related to computer technologies reported in 2006. Of those, 80 percent were offenses linked to illegal access to information and fraud.[113]

Whereas concerns about reputation or privacy often prompt victims to conceal the thefts, it is likely that the majority of such crimes go uncounted and that the true scale of Russian financial cyber crime is much greater. Interpol estimates that Russian hackers stole more than $65 million from foreign banks since July 2005. It is important to note that this figure is based solely on Interpol's estimates of the amount stolen directly form foreign citizens' bank accounts and transferred back to Russia via intermediaries in other countries; the true cost of all financial cyber crime could be much higher. According to Vladimir Basov, the Deputy Division Chief of the Interpol information Technology Division of the Department for the Fight Against International Crime, this practice of multiple transfers makes locating and prosecuting Russian cyber criminals that much more difficult, as it is not always possible to follow the money and the hackers frequently do not know each other personally and only communicate online or via intermediaries.[114]

In some cases, the attacks on financial institutions are relatively simple, where the criminals break into a bank's system and transfer money to and from the account(s) of their choosing. A typical example is a Rostov student recently convicted of stealing more than 3 million Rubles from American companies utilizing this method. Specifically, he accessed bank systems and transferred 3,120,000 Rubles ($120,000 US) to accounts held by his foreign accomplices, who then transferred the money to his own accounts. [115]

Although some Russian cyber criminals choose to break into banks' systems themselves, it is often easier and less risky to steal the passwords and account information using other means, and then use that to access the funds. This is sometimes done through phishing or social engineering. Other times the actors go directly after the passwords, as did one group consisting of 12 Russians, all in their twenties, who stole more than €1 million ($1,300,000 US) from French banks over a period of 11 months. The groups used malicious code hidden in e-mails and websites that installed itself on the victims' computers and remained dormant until the victims accessed their online bank accounts. At that time, the virus recorded the victims' user names, passwords and account information and then forwarded the information to the hackers. The Russian hackers then used this information to create and validate new accounts belonging to third parties. Those accomplices then accepted fund transfers from the victims' accounts and forward them to the hackers' in return for a commission of 5-10 percent of the amount stolen.[116] A more sophisticated, larger-scale version tactic is currently employed by hackers somewhere in Russia. In this version, a Trojan horse operates in conjunction with a rootkit element to conceal its presence. Whenever victims access a site requiring identification, the program connects to a server in Russia and sends all information entered by the victim.[117]

Money is not the only item of value which Russian cyber criminals can steal from banks; the theft and sale of account holders' information increased dramatically in the last sixth months of 2006, to such an extent that the sale of black market credit information threatens the development of Russia's legitimate credit rating agencies. This most recent case is also of an unprecedented scale; the names, telephone numbers, home addresses, places of work and negative credit information (including late and missed payments, defaults and other compromising information such as arrests) of almost four million Russian borrowers and would-be borrowers are, as of Dec. 14, 2006, available for sale on the Russian black market. The cost of the database is quite low; only 2,000 Rubles (or $75 US), for which the buyers receive

[113] Alikina, Svetlana. "Russian Police Report Increasing Cyber Crime Rate", Itar-Tass, April 19, 2006
[114] "Российские Хакеры Украли 50 Млн Евро," Hacker Magazine, Dec. 12, 2006, http://www.xakep.ru/post/35713/default.asp
[115] "Ростовского Хакера Приговорили к 6 Годам Лишения Свободы Ксловно," Computer Crime Research Center, Dec. 6, 2006. http://www.crime-research.ru/news/2006.12.06/3079
[116] iDefense Weekly Threat Report, Feb. 13, 2006 and Willsher, Kim. "'Sleeper bugs' used to steal €1M in France," The Guardian, Feb. 7, 2006, http://money.guardian.co.uk/news_/story/0,,1703779,00.html
[117] "Trojan Horse Channels Web-Users' Passwords to a Server in Russia, OSPit, April 4, 2006. http://www.ospint.com/text/d/2573737/index.html

the records for clients of 10 major Russian banks, including Russian Standard Banking, HKF-Bank, Rosbank, FinansBank and Impeksbank.[118]

The precise source of this information is as yet unknown, but the type of information available suggests that the information was stolen by members of one of the bank's internal security service, or someone from one of the bank's IT departments with access to the security service's records.[119] This particular database lists delinquent borrowers and those denied credit, and while several departments have that information, only the security services would also have the reasons for denial of credit and other compromising information on borrower's histories, while the IT departments could gain access to the security services' records.

Although unprecedented in the number of accounts compromised, this leak is the third large-scale sale of Russian banking data in the last half of 2006. In mid- August a database reportedly containing more than 700,000 retail outlet credit records appeared for sale on the black market;[120] two weeks later, a database of 3,000 delinquent borrowers also appeared for sale.[121] In November 2005, an even greater data loss occurred when data from sales contracts for more than 9.9 million residents of Moscow and the surrounding Moscow Oblast appeared for sale on the black market.[122] Thieves also offered a database containing an unknown number of records from the Russian central bank's 2003-2004 operations in early 2005, and subsequently offered an updated version of the same containing more records in May 2005.[123] The following is a table illustrating the progression of publicized Russian data theft incidents since 1992:

Date	Details	Resolution (if any)
1992	Compact discs containing the records of the Moscow Metropolitan Telephone Network subscribers were offered for sale on the black market.	The source of the leak was never found and the discs (with some updates) are still available.
1996	Records of subscribers to the telecommunication provider WimpelCom were offered for sale on the black market.	WimpelCom representatives claim that the company found and punished the guilty parties.
Nov. 2002	The first run of compact discs containing information about subscribers to mobile phone operator MTS were offered for sale on the black market. In January 2003 the second print run containing the information of approximately 5.5 million subscribers disappeared.	The source of the leak was not found.
May 2003	Discs containing data concerning 4.5 million clients of the telecommunications firms MegaFon, Telecom XXI, North-West Telecom and Peterstar appeared on the black market.	According to one version of events, the leak originated from law enforcement structures.

[118] "Пришли На Базу," Kommersant, Dec. 12, 2006. http://www.kommersant.ru/doc.html?path=/daily/2006/232/13185437.htm
[119] Пришли На Базу," *Kommersant*, Dec. 12, 2006, http://www.kommersant.ru/doc.html?path=/daily/2006/232/13185437.htm. "БД-"Пустышка" Дискредитирует Российские Банки," CNews.com, Dec. 12, 2006, http://safe.cnews.ru/news/top/index.shtml?2006/12/12/227868
[120] "Пришли На Базу," Kommersant, Dec. 12, 2006, http://www.kommersant.ru/doc.html?path=/daily/2006/232/13185437.htm
[121] "Пришли На Базу," Kommersant, Dec. 12, 2006, http://www.kommersant.ru/doc.html?path=/daily/2006/232/13185437.htm
[122] "Пришли На Базу," Kommersant, Dec. 12, 2006, http://www.kommersant.ru/doc.html?path=/daily/2006/232/13185437.htm
[123] "Пришли На Базу," Kommersant, Dec. 12, 2006, http://www.kommersant.ru/doc.html?path=/daily/2006/232/13185437.htm

July 2004	WimpelCom filed a complaint with Russian police concerning the website Sherlok.ru, which offered information concerning WimpelCom, MegaFon and MTS subscribers in Moscow and Saint Petersburg.	Seven suspects were detained on November 26, 2004, of which three were WimpelCom employees. In March 2005 the local court sentenced them to various fines. Sherlok.ru is still operational.
Feb. 2005	A database containing bank operations of the Central Bank in 2003 and 2004 was offered on the black market. In May 2005 a larger version of the same was also offered.	In October 2005 government security forces and the information protection service of the Moscow government stated that the sources of each leak were connected, but did not name specific suspects.
Nov. 2005	A database containing contracts entered into by more than 9.9 million residents of the Moscow region were offered for sale on the black market.	In November 2006 the FSB declared that officers detained the people responsible for the leak, but the names of the accused are not known.
Aug. 2006	Several credit bureaus and banks received an e-mail offering a database containing more than 700,000 records of borrowers, lenders and consumer credit information.	The national credit history bureau claimed that the leak originated in two or three banks, but the specific banks are unknown.
Dec. 2006	A database containing over three million records from 10 major Russian banks of delinquent payers, defaulted loans and a black list of people to whom credit should not be given, and compromising personal information of said borrowers, was offered for sale on the black market. The database contains information from ten major Russian banks.	The type of information offered suggests that the leak originated in the security services or IT departments of one of the affected banks

Major Russian data thefts[124]

What is most troubling about these leaks is not their existence, but the approach taken to them by the Russian banking authorities, whose primary concern is the harm that the availability of black market credit information will do to legitimate credit rating agencies seeking to compete. According to the Bank of Russia, the 23 credit rating agencies that currently operate in Russia possess information on 10 million people between them, or only seven percent of the population. The aforementioned cases, which are only the best known, offer almost half again that many records for a fraction of the cost and time; purchasing the databases costs pennies per record and is almost instantaneous; to purchase the information legitimately would cost about $.50 per record and take several days.[125] The concern is therefore that banks will choose to buy their credit information on the black market instead of from the credit rating agencies; the ethical or legal issues surrounding purchasing stolen data do not appear to be a major consideration. In fact, the primary risk cited by officials is that posed by false data, (i.e., that banks will deliberately sell false information on the black market to their competitors.[126]

Banks are not the only targets for financial crime; Russian cyber criminals target stores and even governments for financial gain. In February 2006 the Russian magazine *Hacker* published claims of such an attack on Shop-Script PHP shopping carts.[127] Shop-Script is an open-source, turnkey PHO product, where each client has a personal account where they can access customers' contact information,

[124] "Пришли На Базу," Kommersant, Dec. 12, 2006. http://www.kommersant.ru/doc.html?path=/daily/2006/232/13185437.htm
[125] "Пришли На Базу," Kommersant, Dec. 12, 2006. http://www.kommersant.ru/doc.html?path=/daily/2006/232/13185437.htm
[126] "БД-"Пустышка" Дискредитирует Российские Банки," CNews.com, Dec. 12, 2006. http://safe.cnews.ru/news/top/index.shtml?2006/12/12/227868
[127] iDefense Weekly Threat Report, April 17, 2006

shopping and visit history, their own address book, and affiliate commissions and payments. Despite guarantees of "hacker safe" status published by WebAsyst Llc (the company selling shop-Script) in March, the February article written by a Russian hacker using the handle "k00p3r," or "buyer," details the attack sequence and even provides a CD containing a video of the same.[128]

Although Russian hackers do not target governments as commonly as financial or commercial institutions, they do target them, and as more processes are conducted online, their attraction to hackers will only increase. The sale of contracting data taken from the Russian Central Bank mentioned above is only one such case. Nor is the Russian state the only target. In January 2006 a Russian hacker used Google to locate PHO vulnerabilities, and then employed a brute-force attack to gain passwords to the government of Rhode Island's website.[129] Many financial transactions take place on this website, a great deal of which are conducted using credit cards. The hackers claiming credit for the attack stated that they stole the information for nearly 53,000 cards, but Rhode Island Governor Donald Carcieri claimed that the hackers stole only 4,118 credit card numbers.[130] The attack was first reported in the January online edition of *Hacker* magazine,[131] which included a detailed description of the attack. The original article was written in the first person by one person claiming to have executed the attack, but was actually written by two hackers using the nicknames "fan" and "virgoz." Upon discovering the incident, iDefense brought this issue to the attention of the authorities and notified responsible parties.

It is unlikely that this attack would ever have become public knowledge had the hackers not published a detailed account of exploits. High-profile cases of this type are publicized very rarely, and victims make such events even less often. It can therefore be assumed that the frequency of such attacks is much greater than reported, and that the aforementioned known cases are only a sample of the true scale of these activities.

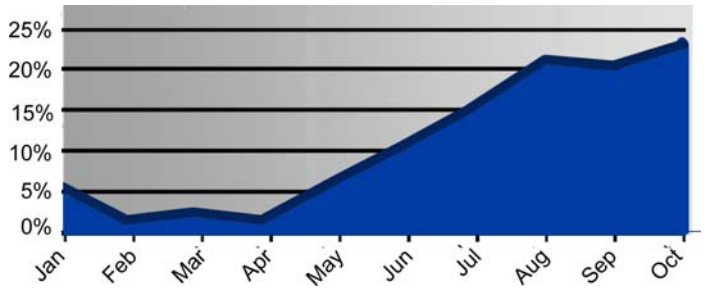
4.9.4 Phishing

Although it is possible to steal victims' password using malicious code, it is far easier for Russian cyber criminals to trick victims into turning them over via phishing, both through social engineering endeavors designed to trick victims' into handing over personal information and the use of worms and Trojans that record victims' online activity and send the relevant information to their creators.

Over the past year, Russian cyber criminals significantly increased their participation in such activities; in February through March 2006 the percentage of phishing-based Trojans and downloader's hosting countries as determined by their IP address hovered at around 2 percent of the worldwide total.[132] By August of the same year Russia surpassed the US as the hosting location of the most phishing-based keyloggers and Trojan downloaders by hosting 32.12 percent, with the US hosting 25.45 percent.[133] Although the US regained the preeminent position September and October by hosting 30.91 percent to

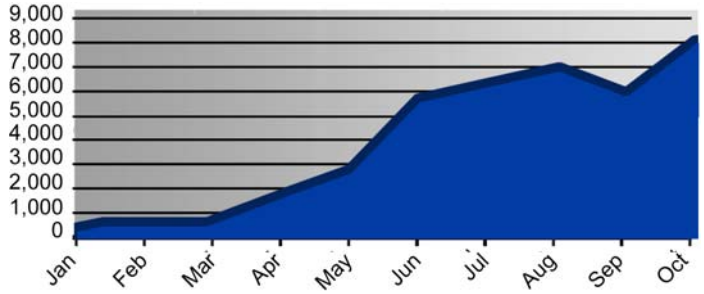
[128] k00pr, "Берем Магазин Под Контрол," *Хакер*, February 2006.
[129] iDefense Weekly Threat Report, Jan. 30, 2006
[130] Parker, Paul. "Hackers Stole 4,118 Credit Card Numbers," Rhode Island News, Jan. 27, 2006. http://www.projo.com/digitalbulletin/content/projo_20060127_hack28x.215a78fc.html
[131] Fan and virgoz, " Конкурс: Как Был Взломан Ri.Gov Или Как Стать Владельцем Острова," *Хакер*, January 2006, http://www.xakep.ru/post/29550/default.asp
[132] "Phishing Activity Trends Report," Anti-Phishing Working Group. February 2006. http://www.antiphishing.org/reports/apwg_report_feb_06.pdf, "Phishing Activity Trends Report," "Phishing Activity Trends Report," Anti-Phishing Working Group. March 2006, http://www.antiphishing.org/reports/apwg_report_mar_06.pdf "Phishing Activity Trends Report," Anti-Phishing Working Group. April 2006. http://www.antiphishing.org/reports/apwg_report_apr_06.pdf
[133] "Phishing Activity Trends Report," Anti-Phishing Working Group. August 2006. http://www.antiphishing.org/reports/apwg_report_August_2006.pdf

Russia's 28.5 percent,[134] no doubt exists that Russia remains an area of concern for phishing and related crimes.



Percentage of all-new phishing-based Trojans hosted in Russia by month Jan – Oct 2006[135]

During the same period, the number of reported new instances of phishing using Russian IP addresses rose from 390 in January to 7,700 in October.[136]



Reported new instances of phishing by Russian cyber criminals by month, Jan. – Oct. 2006[137]

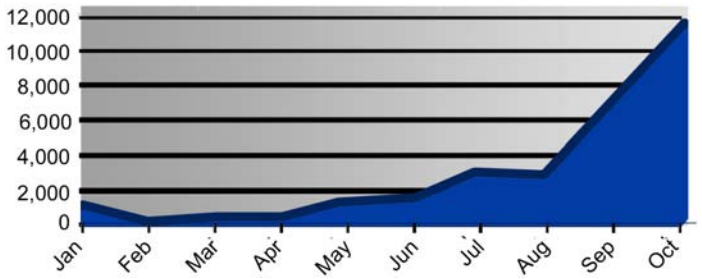
[134] "Phishing Activity Trends Report," Anti-Phishing Working Group. October 2006." http://www.antiphishing.org/reports/apwg_report_september_october_2006.pdf

[135] "Phishing Activity Trends Report," Anti-Phishing Working Group. January 2006. http://www.antiphishing.org/reports/apwg_report_jan_2006.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. February 2006. http://www.antiphishing.org/reports/apwg_report_feb_06.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. March 2006. http://www.antiphishing.org/reports/apwg_report_feb_06.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. April 2006. http://www.antiphishing.org/reports/apwg_report_apr_06.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. May 2006. http://www.antiphishing.org/reports/apwg_report_May2006.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. June 2006. http://www.antiphishing.org/reports/apwg_report_june_2006.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. July 2006. http://www.antiphishing.org/reports/apwg_report_july_2006.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. August 2006. http://www.antiphishing.org/reports/apwg_report_August_2006.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. September and October 2006. http://www.antiphishing.org/reports/apwg_report_september_october_2006.pdf

[136] "Phishing Activity Trends Report," Anti-Phishing Working Group. January 2006. http://www.antiphishing.org/reports/apwg_report_jan_2006.pdf , "Phishing Activity Trends Report," Anti-Phishing Working Group. February 2006. http://www.antiphishing.org/reports/apwg_report_feb_06.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. March 2006. http://www.antiphishing.org/reports/apwg_report_feb_06.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. April 2006. http://www.antiphishing.org/reports/apwg_report_apr_06.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. May 2006. http://www.antiphishing.org/reports/apwg_report_May2006.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. June 2006. http://www.antiphishing.org/reports/apwg_report_june_2006.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. July 2006.

[137] "Phishing Activity Trends Report," Anti-Phishing Working Group. January 2006. http://www.antiphishing.org/reports/apwg_report_jan_2006.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group.

The number of reported new phishing sites based in Russia also increased; from 675 in January to 10,700 in October.



Reported new instance of phishing by Russian cyber criminals by month, 2006[138]

The ascendancy of Russian phishers is so widely recognized that phishers themselves even incorporate it into their scams to make them more believable. Earlier this year CFCU, a New York credit union, reported a phishing e-mail warning recipients that multiple attempts to access their accounts had been made from Russian IP addresses, and even included a manufactured list of those addresses.[139] Bank customers were then asked to follow an included link to a website with an address similar to the credit union's, but which in reality directed users to a website hosted in Singapore that resembled that of the CFCU.[140]

While a great many Russians may be involved in phishing, a small number of organized and highly capable groups dominate the practice. It is believed that only 50 or 60 such groups, based in Russia, Ukraine, Estonia, Latvia, Lithuania and Romania, are responsible for two thirds of all phishing e-mails.[141] Phishing can be highly lucrative for such groups; investigators believe that any of these major groups

---

February http://www.antiphishing.org/reports/apwg_report_feb_06.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. March 2006 http://www.antiphishing.org/reports/apwg_report_feb_06.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. April 2006. http://www.antiphishing.org/reports/apwg_report_apr_06.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. May 2006. http://www.antiphishing.org/reports/apwg_report_May2006.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. June 2006. http://www.antiphishing.org/reports/apwg_report_june_2006.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. July 2006. http://www.antiphishing.org/reports/apwg_report_july_2006.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. August 2006. http://www.antiphishing.org/reports/apwg_report_August_2006.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. September and October 2006. http://www.antiphishing.org/reports/apwg_report_september_october_2006.pdf

[138] "Phishing Activity Trends Report," Anti-Phishing Working Group. January 2006. http://www.antiphishing.org/reports/apwg_report_jan_2006.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. February 2006. http://www.antiphishing.org/reports/apwg_report_feb_06.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. March 2006. http://www.antiphishing.org/reports/apwg_report_feb_06.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. April 2006. http://www.antiphishing.org/reports/apwg_report_apr_06.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. May 2006. http://www.antiphishing.org/reports/apwg_report_May2006.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. June 2006. http://www.antiphishing.org/reports/apwg_report_june_2006.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. July 2006. http://www.antiphishing.org/reports/apwg_report_july_2006.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. August 2006. http://www.antiphishing.org/reports/apwg_report_August_2006.pdf, "Phishing Activity Trends Report," Anti-Phishing Working Group. September and October 2006. http://www.antiphishing.org/reports/apwg_report_september_october_2006.pdf

[139] iDefense Weekly Threat Report, Jan. 30, 2006

[140] Anbinder, Mark H., "CFCU Credit Union Says Customers Received "Phishing" Scam E-mails," *WVBR News*, Jan. 24, 2006, http://today.14850.com/0124cfcuscam.html

[141] Ward, Mark. "Boom Times For Hi-Tech Fraudsters." *BBC News*, Sept. 28, 2005, http://news.bbc.co.uk/2/hi/technology/4286276.stm

earns between $100,000 and $300,000 US per month. Russian organizations are particularly difficult to investigate, as they tend to be fairly closed groups and use closed communications channels.[142]

As with their carding counterparts, Russian phishers have begun to specialize in 2006. Those who use social engineering to gain victims' gaining passwords and those who use worms and Trojans work separately more and more. The first group is also more specialized in its approach. Instead of sending out huge amounts of e-mails to many people, they prefer to send out fewer e-mails to those they feel are most likely to respond or have access to a desired target.[143] In comparison, cyber criminals who use worms or Trojans tend to prefer to send out many e-mails to catch more victims. For this they frequently use a "spam cannon," where phishers seize control of a computer and use it to send out thousands (or even millions) of messages using a template with the victims' e-mail addresses, names and personal data inserted automatically.[144] Russian phishers who employ malicious code are split into those that use it themselves against victims and those who sell kits to others who wish to launch phishing attacks but lack the technical expertise.

4.9.5 Spam

Although the US remains the greatest single source of spam in the world, a great deal also originates from Russia. According to Spamhaus, eight of the world's top spammers are in Russia, including the number three spammer, Alexey Pano. The elite Russian spammers tend to cooperate with one another through loose networks. For example, spammer Leo Kukayev is part of large criminal group including Alex Blood and the Pavka/Artofit gang, while Alex Blood (also known as Alex Polyakov, AlexseyB and Alexander Mosh) is a sometime partner of Send-Safe proxy spamware author Ruslan Ibragimov, who himself runs a larger criminal operation.[145]

Russian spammers typically adopt one of three approaches; the first is to simply purchase a list of e-mail addresses and send them all spam. This makes it difficult to target spam, however, and it is therefore preferable to hack into phpBB forums and steal the list of users. This approach provides the spammer with a list of legitimate e-mail addresses. It also allows hackers to target the spam, but only within the subjects of the forums. The third approach entails the use of a "spider" program to collect e-mail addresses from the Internet. Spiders can be directed to collect the addresses from specific types of sites, which allow them to target the recipients, but the process is complex and time consuming.

Those spammers not willing or able to go through such procedures can purchase spamming software such as Direct Marketing System (DMS). Written by Alexey Panov, DMS reportedly costs $1,500 to $2,000 US and includes malicious code that can be attached to spam and then coordinated from the users' computer(s). It also allows would-be attackers to sort and edit e-mail addresses that are no longer

---

[142] Ward, Mark. "Boom Times For Hi-Tech Fraudsters." *BBC News*, Sept. 28, 2005.
http://news.bbc.co.uk/2/hi/technology/4286276.stm
[143] Young, Tom. "Localized Attacks Add to Phishing Increase," *Computing*, Sept. 7, 2006.
http://www.vnunet.com/computing/news/2163690/localised-attacks-add-phishing
[144] Young, Tom. "Localized Attacks Add to Phishing Increase." *Computing*, Sept. 7, 2006.
http://www.vnunet.com/computing/news/2163690/localised-attacks-add-phishing
[145] "Spammer Profile: Pavka / Artofit," Spamhaus Registry of Known Spam Operations,
http://www.spamhaus.org/rokso/listing.lasso?-op=cn&spammer=Pavka
Ruslan Ibragimov / send-safe.com, "Spammer Profile: Ruslan Ibragimov / send-safe.com," Spamhaus Registry of Known Spam Operations. http://www.spamhaus.org/rokso/evidence.lasso?rokso_id=ROK5880, "Spammer Profile: Ruslan "Inkey" Hakimov / iNkus LTD," Spamhaus Registry of Known Spam Operations." http://www.spamhaus.org/rokso/listing.lasso?-p=cn&spammer=Ruslan, "Should ISPs Be Profiting from Knowingly Hosting Spam Gangs?" Spamhaus, Feb. 2, 2006. http://www.spamhaus.org/news.lasso?article=158, "Spammer Profile: Alex Blood / Alexander Mosh / AlekseyB / Alex Polyakov," Spamhaus Registry of Known Spam Operations."
http://www.spamhaus.org/rokso/evidence.lasso?rokso_id=ROK5521

valid.[146] Another popular program is the Send-Safe proxy spamware, by another major spammer, Ruslan Ibragimov.[147]

Some spammers are also capable and motivated to attack those that seek to stop their operations. A Russian spammer who calls himself "pharmamaster," suspected to be Leo Kukayev, launched a major DDoS attack against Israel-based Blue Security beginning May 2, 2006. Blue Security ran a "Do Not Intrude" list linked to Blue Frog, a spam tracking application that bombards the spammers with "opt-out" requests and bogs down the spammers' servers. Some additional Blue Frog customers were also attacked. Pharmamaster may also have tried to change the routing configurations for traffic to Blue Security's website, although this is not confirmed.[148]

In response, Blue Security redirected its traffic to its journal on the blog-hosting service Six Apart. Pharmamaster then shifted the DDoS attack to Six Apart, which brought down that company's TypePad and LiveJournal services for nearly eight hours.[149] Pharmamaster is also suspected to be behind the series of threatening e-mails sent to users who registered with the Do Not Intrude list, sending them high numbers of spam messages and extortion e-mail messages threatening to continue the campaigns if they do not un-register the Do Not Intrude registry.

Ultimately, pharmamaster proved victorious. The security firm was forced to cease operations on May 17, stating that "as we cannot build the Blue Security business on the foundation we originally envisioned, we are discontinuing all of our anti-spam activities on your behalf and are exploring other, non-spam-related avenues for our technological developments."[150]

4.9.6 Products and Services for Sale

Russian cyber criminals do not work only for themselves; they also sell or rent their expertise to others. This trade is almost always one-way, with the Russian working for outside actors. There are some exceptions, such as the Iran Hackers Sabotage (IHS) group, a political anti-US, anti-Israeli Iranian hacker group made up of three members who use the handles "NT," "c0d3r" and "LorD," and who frequent Russian IRC chat rooms, claim to have sold scripts to at least one Russian hacker with the handle, "aqust1ck."

Groups such as the IHS that sell to Russians do exist, but the majority of the trade is in the reverse. In some cases it is a relatively simple matter of selling a program. Simple-to-use kits like WebAttacker, which only requires users to send spam directing victims to a compromised website, proliferate[151] The hackers who create these programs often advertise, and postings appear on popular hacking forums. iDefense analysts observed one such advertising endeavor by someone using the handle "ГлавНа-Deception" (or GlavNa-Deception), who offered spyware and malicious code for sale, including an "advanced polymorphic keylogger." For $800 US, ГлавНа-Deception guarantees his program for six months, with support and upgrades during that period should it be detected. Although he writes in English, his handle (which is half in Russian), his avatar (which is a Russian flag) and the syntax he uses

[146] iDefense Weekly Threat Report, Feb. 27 2006
[147] "Should ISPs Be Profiting From Knowingly Hosting Spam Gangs?" Spamhaus, Feb. 2, 2006. http://www.spamhaus.org/news.lasso?article=158
[148] "Alleged Russian Spammer Hits Israel's Blue Security and Related Targets with Massive DDoS Attacks," *Six Apart*, May 8, 2006. http://www.sixapart.com/typepad/news/2006/05/typepad_update_1.html
[149] Espiner, Tom. "Blue Security Attack Linked to Blog Crashes," *ZDNet*, May 4, 2006. http://news.zdnet.com/2100-1009_22-6068607.html
[150] Vijayan, Jaikumar, "Blue Security Waves White Flag on Spam Attack," *Computerworld.com*, May 17, 2006. http://www.pcworld.com/news/article/0,aid,125752,00.asp#
[151] iDefense Weekly Threat Report, March 2006

while typing in English all strongly suggest that he is Russian.[152] The comments section even includes positive reviews of ГлавНа-Deception's programs and services form other users.

It is difficult to gather comprehensive data as to the prices charged by Russian cyber criminals, but anecdotal evidence suggests that the prices for exploits are in the low hundreds of US dollars, with a few, more powerful, exploits costing thousands. Pricing trends are suggested by a sale held by a Russian hacker using the handle "xoce" (khsoe) offered his entire hacking toolkit on Web-Hack.ru when he decided to give up cyber crime. The toolkit included more than 30 exploits for Windows, an Internet filtration system, 10 methods for circumventing anti-virus programs, a simple injection method in C++ and xoce's website for selling those programs. The asking price was $8,000 US, or about $260 per exploit.[153] In a poll conducted by the Russian hacker website www.inet-lux.com, the greatest number of respondents (38 percent- 80 responses of 208), were only willing to pay $100–300 US for an exploit. Some 20 percent, or 41 voters, said that they would "try to grab [exploits] for free," while 14 percent would pay "more than a $1,000 US."[154]

Amount respondents reported they would pay for an exploit[155]

In addition to specific programs, Russian cyber criminals offer services, such as the hourly, daily and monthly use of botnets, which are networks of compromised working controlled by the hacker, frequently to launch extensive denial of service attacks. A Russian hacker using the handle "Fargal" offered anonymous use of botnets for the "technically illiterate" customer for the following prices. Set-up and consulting services are included in the price, and discounts are offered to potential partners.[156]

Service	Cost (in USD)
10 bots for a 24-hour test and familiarization	$5
50 bots for 24 hours	$10
50 bots for one month	$60
100 bots for one day	$15
120 bots per month	$120
500 bots for 24 hours	$30
500 bots for one month	$220

[152] iDefense Weekly Threat Report , April 3, 2006
[153] iDefense Weekly Threat Report, Aug. 14, 2006
[154] iDefense Weekly Threat Report , July 24, 2006
[155] "Сколько Вы Готовы Платить За Эксплойт?" *Inet-lux.com*, http://www.inet-lux.com/index.php?go=Voting&in=result&id=1
[156] iDefense Weekly Threat Report, June 19, 2006

1,000 bots for 24 hours	$60
1,000 bots per month	$550

Source: http://forum.web-hack.ru/index.php?showtopic=38947[157]

Should someone wish to launch a DDoS attack with even less skill or effort required to rent botnets, Russian hackers also offer DDoS attack services. A Russian hacker calling himself Дата (Data) posted an offer on the Web-hack.ru forum offering a "quality DDoS service for $80 to 250 USD for a 24-hour attack." Another hacker, Dies' Irae, agreed that this price was reasonable, but another hacker using the handle "Freder" objected that the price was too high. More recently, Fargal offered a DDoS attack for only $35 US for 24 hours, which is more in alignment with Freder's impressions as to what the price should be.[158]

Russian cyber criminals actively solicit clients, but clients actively seek them as well. In October 2006 iDefense analysts observed darkangel11012, a member of the 3asfh.net Arabic hacker website describe seeking to purchase exploits for sale by "Russian programmers," and solicited the assistance of other members in locating the Russian-designed WebAttacker tool. Another member posted exploit code by Tritrat Puttaraksa, but the darkangel1012 replied that that exploit was deficient, and that the Russian program was in order. He later posted a link to the Russian hacker website www.inet-lux.com, where he claimed that WebAttacker could be purchased for $65, and provided a link and instructions for online translation software for non-Russian speakers.[159] While the Russian sellers of programs such as WebAttacker may not be political, at least some of their customers most certainly are, and such evidence that the two groups are attempting to strengthen their collaboration is a troubling development that iDefense continues to monitor.

4.9.7 "Hacktivism," or Political Hacking

The Russian political hacking sphere does not fit the stereotypical pattern of politically motivated private citizens launching attacks on sites representing interests they oppose or seeking to draw attention to their causes. Such people do exist, but in Russia the most powerful "hackivist" actor is the state itself. Some hackivism is directed against the Russians, most commonly surrounding the war in Chechnya, while other politically related hacking is not for a specific political cause, but rather personal politics.

The most infamous case of hackivism by the state took place in March 2006 during the Ukrainian parliamentary elections. The server of the Ukrainian Central Electoral Commission was attacked nearly 29,000 times from March 23-30. The attacks were mostly unsuccessful, and the servers involved continued to operate. The Russian state was strongly involved in the 2004 presidential elections, and they were equally involved in those for parliament. Whereas nothing has been proven conclusively, indications exist that Russian actors were behind the actions.[160]

One area where the Russian state's involvement is also suspected is in the so-called "Botnet Project." This refers to a botnet and spam war and DDoS attacks on pro-Chechen websites by Russian hackers, which included claims that the Russian Federal Security Service (FSB) was allegedly targeting some of the websites and hosting servers that support the Chechen terrorists.[161] On a more informal level, Russian hackers frequently attack pro-Chechen sites, most notably the flagship Chechen news and propaganda site, Kavkaz Center (www.kavkazcenter.com). The site is almost continuously under attack;

[157] Fargal, Forum Post, Webhack.ru, June 9, 2006 http://forum.web-hack.ru/index.php?showtopic=38947
[158] iDefense Weekly Threat Report, June 26, 2006
[159] iDefense Weekly Threat Report, Oct. 2, 2006
[160] iDefense Weekly Threat Report, April 3, 2006
[161] "FSB Launches a SPAM-War Against Kavkaz Center, *Kavkaz Center*, Oct. 18, 2005.,http://www.kavkazcenter.com/eng/content/2005/10/18/4157.shtml

similar addresses lead users to Arabs and Western porn sites. Russian hackers have even gone so far as to set up the GavGav Center (literally the "Sh*tSh*t Center" http://www.gavgavcenter.com) a website spoofing the Kavkaz Center. The GavGav Center website is noteworthy not for its name, but for its elaborateness and the collective nature in its construction; the satirical news articles are written by contributors, allowing the GavGav Center to offer a large degree of content and updates.

A screenshot of the KavKaz Center homepage (http://www.kavkazcenter.com/russ/)[162]

A screenshot of the GavGav Center homepage (http://www.gavgavcenter.com)[163]

One area where the involvement of the Russian state is undisputed is that of a campaign by the Liberal Democratic Party of Russia (LDPR) against "russophone elements." The LDPR is an extremist right-wing party known outside Russia primarily for its racist and ultra-nationalist views and within Russia for its populist appeal and corruption. During a Duma meeting LDPR member and State Duma Deputy Nikolai Kuryanovich publicly promised to encourage the hacking of terrorist and extremist sites and to give a certificate of appreciation to each hacker who personally carried out such actions.

Kuryanovich kept his promise when he awarded the first State Duma certificate of appreciation during a ceremony in the Duma building. A hacker was given an official Duma certificate of appreciation in return for defacing www.evrey.com, a Jewish site based in Jerusalem three times and posting a photograph of LDPR deputy Kuryanovich. The site was singled out in general because of the LDPR's anti-Jewish stance and in specific because of an article published thereon discussing the destruction of Orthodox Christian symbols.[164]

---

[162] *KavKaz Center*, http://www.kavkazcenter.com/russ/
[163] *GavGav Center*, http://www.gavgavcenter.com
[164] с.т.а.л.к., "Intro," *Mazafaka Ezine*, August 2006. http://www.mazafaka.com

A March 2006 screenshot of extremist site pro-Russian site Demushkin.com celebrating the defacement of the Israeli site www.evrey.com, showing a part of that defacement.[165]

ФЕДЕРАЛЬНОЕ СОБРАНИЕ РОССИЙСКОЙ ФЕДЕРАЦИИ
ГОСУДАРСТВЕННАЯ ДУМА

ДЕПУТАТ
ГОСУДАРСТВЕННОЙ ДУМЫ
четвертого созыва (2004–2007)

«21» марта 200 6 г. № КНВ-3/94 и

Отдел информации НСД «Славянский Союз».

21 век – это век информационный. И такая часть жизни человека как Интернет становится все более значимой, нужной, важной и в тоже время опасной. В сети Интернет есть свои законы, есть свои правила, тут идет немного другая жизнь, чем в реальности. И в скором времени многие конфликты будут проходить не на открытом поле сражения, а на Интернет-просторах, с помощью информационных Воинов – хакеров. Это значит, что небольшой отряд хакеров – это сильнее, чем многотысячный отряд настоящих вооруженных сил.

Отдел информации НСД «Славянский Союз» это доказывает на своем примере, вы – настоящие информационные Инквизиторы, которые беспощадны к врагам Русского народа, всегда готовы опустить карающий меч возмездия на головы русофобов и террористов, разжигающих межнациональную ненависть и рознь.

Как депутат Государственной Думы, член Комитета по безопасности, хочу выразить благодарность Отделу Информации НСД «Славянский Союз» за бдительность и недавнее пресечение размещения в Интернете русофобских и иных разжигающих межрелигиозную рознь материалов. Надеюсь, и впредь ваша работа будет не менее продуктивна и идеологически выверена.

Слава России!

член Комитета по безопасности
Государственной Думы РФ Н.В.Курьянович

Certificate awarded by the Duma (source: Slavic Union Website http://www.demushkin.com/engine/index.php?module=news&a=showme&id=1125397631)[166]

A translation of this certificate of appreciation reads:

> "The 21st century is the century of information. And during this period in the life of mankind the Internet becomes even more unavoidable, necessary and important. At the same time it becomes more dangerous. The Internet has its own laws, its own rules and to a degree within it run another life outside of reality. In the very near future many conflicts will not take place on the open field of battle, but rather in

[165] "Отдел Информации СС Награжден Депутатской Грамотой," Slavic Union, March 22, 2006. http://www.demushkin.com/engine/index.php?module=news&a=showme&id=1125397631
[166] "Отдел Информации СС Награжден Депутатской Грамотой," Slavic Union, March 22, 2006. http://www.demushkin.com/engine/index.php?module=news&a=showme&id=1125397631

> spaces on the Internet, fought with the aid of information soldiers, that is hackers. This means that a small force of hackers is stronger than the multi-thousand force of the current armed forces.
>
> "...As Deputy of the State Duma and member of the Security Committee, I want to present you with the thanks and appreciation of the Information department of the NSD "Slavic Union" for your vigilance and your recent suppression of Russophobe and others on the Internet, Russophobes that fan the flames of inter-religious discord and provide related materials. I hope that from now on your work will not become any less productive or ideologically adjusted."[167]

The Russian state is also the target of politically motivated attacks. In June 2006, Victor Gorbachev, spokesman for the Russian Federal Security Service (FSB) stated that the number of attacks on Russian government website increased throughout 2006, to a total of almost one million attacks. Gorbachev claimed that the attackers were primarily US and Chinese hackers attacking the Ministry for Emergency Situations site, websites connected to the Russian Ministry of Internal Affairs and Russia's Foreign Intelligence Agency, respectively.[168]

Not all political attacks in Russia are directed at a government body. The Russian site Compramat.ru (http://www.compromat.ru/) suffered intermittent DDoS attacks beginning at the end of May and continuing into June 2006. According to the *Moscow Times* (www.MoscowTimes.ru), the Compromat.ru site contains "controversial dossiers on hundreds of politicians, public figures and businessmen;" these dossiers are reportedly regularly updated with republished news and Internet media reports.[169]

Russia even occasionally finds itself embroiled in other countries' political difficulties. In March 2006 the Russian ISP Ariadna Media shut down a pro-terrorist children's website, Al-Fateh.net, which it was unwittingly hosting. The website is now hosted by an ISP in Malaysia, but the incident suggests that Ariadna Media and other ISPs could also be hosting other radical political sites unknowingly.

[167] с.т.а.л.к., "Intro," *Mazafaka Ezine*, August 2006. http://www.mazafaka.com
[168] iDefense Weekly Threat Report, June 19, 2006
[169] Abdullaev, Nabi, "Hackers Down Muckraking Web Site," *Moscow Times,* http://www.moscowtimes.ru/stories/2006/06/09/044.html and iDefense Weekly Threat Report, June 12, 2006

5 Conclusions

Russia underwent a momentous year in 2006. Political violence increased, the economy surged ahead, the criminal underground grew larger and more sophisticated and the police scored a few notable but ultimately token victories. Carders and bot herders in particular grew more advanced, generating the most sophisticated tools ever for commanding bot armies and stealing the personal financial information of (mostly Western) consumers. Moreover, there is no end in sight; all of the elements driving the Russian cyber crime underground remain robust, and no checks to its growth are evident.

Western companies doing business in Russia face a number of challenges, including corrupt officials at all levels of power. The interests of these companies will often clash with oligarchic domestic companies with deep connections and a lax enforcement environment. They will encounter cumbersome and shifting regulatory schemes that can disrupt perceptions of risk and preferred strategy. Finally, and almost surely, they will experience repeated, attempted attacks on their information systems; on the other hand, companies not physically doing business in Russia will also face challenges from the Russian underground.

For all of the dangers of the Russian threat environment, there is a great deal of money to be made there. The educated Russian population is capable of solving many difficult problems, but it lacks the permissive environment of the more advanced economies and the management skill that accompanies it. Many Russian minds set to useful work with Western investment capital and leadership experience have the potential to generate immense growth and profit. The Russian IT and telecommunications sectors are booming, if more quietly than in the past three years, but with much potential growth that remains untapped. Indeed, Russia needs the telecom sector to thrive to lessen its dependence on energy and raw materials exports.

The political environment of Russia is currently uncertain and can be expected to become more chaotic as Russian President Putin nears the end of his constitutionally mandated term. Should instability increase, the economic setbacks could be substantial, but not irrevocable. Russia is poised to become a major center of power and growth in the emerging international order, but it sits in a shaky position. Irrespective of the political outcome, it is difficult to see whether or how any significant change could begin to curb the dangers posed by underground criminal elements.

The next year, and the several after that, will see Russian hackers and their successors develop more intricate and effective tools as they group together in synergistic ways to extract money from the global information networks. Any company working in Russia itself should take note of these dangers and be aware that the best security posture in Russia is one that provides for one's own needs after careful study and deliberation, and after engaging legitimate security professionals who are intimate with the Russian cyber threat environment.