RUSSIA

The circulation of this report has been strictly limited to the members of the *Trialogue* Club International and of the Centre russe d'études politiques.

This issue is for your personal use only.

Published monthly in Russian and in English by *Trialogue Company Ltd.*

Issue № 10, vol.1. October 2011.

October 15, 2011

Oleg Demidov, Vladimir Orlov report from Moscow:

CYBER CRIME: A THREAT TO INFORMATION SECURITY

Combat action and massive attacks in the cyberspace have moved on from the realm of media speculation and science fiction to become a very real and urgent challenge to international security. In the 21st century wars are spreading, slowly but surely, to cyberspace and the outer space. There has not been a full-blown war in the Internet for now - but recent events (*Stuxnet, Shady RAT, LulzSecurity*) suggest that such a war is quite likely to happen in the immediate future.

Many of the security threats in cyberspace Russia is facing now are related to economic crime. The existing systems of personal data protection are inadequate. Personal data belonging to Russian users of American or US-registered social networks end up outside Russia, and not just in the United States itself but also in processing centers physically located in developing countries.

Another important aspect of the problem which is becoming ever more pressing with each passing year is cyber espionage. Web sites of US government agencies are being targeted especially often. During our recent conversations with US congressmen it became obvious that in their opinion, this threat is becoming as dangerous as the threat of nuclear proliferation. For Russia this challenge has not yet become quite as pressing - but the attacks against web sites run by Russian government agencies are becoming increasingly frequent and sophisticated.

Computer viruses unleashed by technologically advanced terrorist organizations, as well as state-sanctioned attacks are some of the most dangerous scenarios of the near future. An attack carried out last year with the help of the *Stuxnet* worm against industrial facilities in a whole number of countries was comparable in terms of the damage it did to a military operation. A similar attack against Russia could have very negative effects for the Russian economy unless adequate countermeasures are developed.

REGULATORY MEASURES AGAINST HIGH-TECH TERRORISM

In such context it is becoming obvious that Russia needs a systemic strategy of countering high-tech terrorism, especially cyber terrorism. This kind of terrorism will become one of the most pressing problems for a number of countries, including Russia, in the coming years.

At present the problem of countering high-tech terrorism has yet to be fully addressed in Russia's strategy papers and doctrines. There is no direct mention of cyber terrorism in the Russian Foreign Policy Concept of June 28, 2000 or the Russian Military Doctrine of February 5, 2010. The Russian National Security Strategy until 2020 of May 12, 2009 mentions “unlawful activities in the cybernetic and biological areas, as well as the area of high technologies” as a potential future threat, but does not detail any specific strategies to counter that threat.

On the national level measures against cyber terrorism in Russia are regulated by individual pieces of legislation which do not really add up to a coherent national political or legislative concept. On May 12, 2004 the Russian president signed Decree No 611 "On measures to ensure Russia's information security in the area of international information exchange". The decree prohibits government agencies from using the Internet without any protection measures and details the remit of the Russian secret services in ensuring safe usage of the World Wide Web. The decree is aimed primarily at protecting the web sites run by Russian government agencies from external threats and unauthorized use.

Russia is not a member of the Council of Europe Convention on Cybercrime, which is the most comprehensive and well-known piece of international legislation regulating measures against cyber terrorism on the international level. The convention was signed on November 23, 2001 in Budapest. Although the convention is open for signature, Russia has not joined the 43 Council of Europe member states and 15 other countries who are members of the convention. On November 15, 2005 the Russian president signed a decree "On signing the Convention on Cybercrime”, authorizing the Russian government to join the convention on the condition that Article 32, Paragraph B of the document is revised. Russia is adamantly opposed to that paragraph, which allows authorized agencies from one country to access computer data stored on the territory of another country without obtaining prior permission from that country’s government.

The Russian president later signed a resolution declaring that Presidential Decree “On joining the Convention on Cybercrime” of November 15, 2005 was null and void. The resolution entered into force on March 22, 2008. Since then Russia has shown no interest in the Council of Europe convention, focusing instead on its own initiatives in the area of countering cybercrime. As Pavel Livadny, a representative of the Russian Financial Monitoring Agency (Rosfinmonitoring), said in November 2010, “Russia is advocating an approach which recognizes the need to develop a global convention against cybercrime”.

In the past three or four years Russia has been working hard on addressing the problem of cyber terrorism (and cybercrime as a whole) via UN channels. Russia’s initiative and proposals became the basis of a resolution by the UN Commission on Crime Prevention and Criminal Justice to set up an open intergovernmental group of experts to conduct a comprehensive study of cybercrime. The resolution was adopted in May 2010. One of the main tasks set before the group is to develop and formulate proposals on improving international legislation against cybercrime and cyber terrorism. During the 65th General Assembly session in 2010 a report on issues of information security was submitted to the UN secretary-general. The report was prepared by a group of government experts representing 15 countries and chaired by Andrey Krutskikh, deputy head of the Russian Foreign Ministry’s department for new challenges and threats. The report, which was unanimously approved by the UN General Assembly, focuses on the need to develop common approaches to countering cyber threats and fighting cybercrime (as well as cyber terrorism). It represented a real breakthrough for the group, the first since it was founded back in 2005.

But the ambitious and comprehensive nature of the Russian proposals regulating issues such as some countries’ aggressive behavior in cyberspace is preventing these proposals from being accepted globally. Neither the UN nor the key global powers are at this moment inclined to view the Russian projects for regulating cyberspace seriously. This does not bode well for the latest Russian draft of the UN Convention on International Information Security, which emerged in late September 2011. Moscow is well aware of these risks. It is no coincidence that in recent years Russia has been demonstrating rapidly growing interest in various regional formats of cooperation (such as BRICS, SCO and CSTO) as alternative platforms for the promotion of its initiatives regarding cyberspace regulation.

At the informal CSTO summit in Astana the organization's secretary-general, Nikolay Bordyuzha, said that by 2011 the CSTO was planning to develop a systemic approach to countering the threat of cyber terrorism. He added that the area was one of the organization's priorities. At Russia's insistence the topic of countering cyber terrorism has also become one of the key priorities for the SCO. On June 16, 2009 its member states signed an agreement on cooperation in the area of international information security. The agreement, which was signed in Yekaterinburg, entered into force on June 2, 2011. On September 12, 2011 four CSO member-states (Russia, Uzbekistan, Kyrgyzstan and China) submitted to the UN secretary-general a draft code regulating countries' behavior in cyber space, including prevention of cyber wars and cyber terrorism.

The problem of cyber terrorism is not at the top of the BRICS agenda, but Russia is trying to use that platform as well to promote its initiatives. According to our sources, in 2009-2011 Russia was trying to win the support of other BRICS members (primarily South Africa and China) for the initiative to adopt an alternative piece of international legislation regulating measures against cybercrime and cyber terrorism. In 2011 this initiative did not make any progress, mainly due to lack of support among BRICS members themselves. Nevertheless, the issue of cyber terrorism is increasingly being discussed by BRICS, although nothing firm has been decided yet. The final declaration of the April 14, 2011 BRICS summit says that the member states are committed to “cooperation in strengthening international information security”, and that “special attention needs to be paid to fighting cybercrime”.

USER IDENTIFICATION: PROBLEM №1?

One of the key issues in the discussion of the role of social networks in the context of security is identification of users. According to one leading Russian expert on information law, this is “the key problem facing Russia and other countries in the area of internet governance”. User identification in social networking services is inextricably linked to the overall problem of user identification on the internet. Its importance is highlighted by examples such as the case of the female blogger arrested in Syria on suspicion of spying - although that particular example does not demonstrate all the risks related to so-called active anonymity on the net. A situation whereby a user can easily circumvent the existing identification mechanisms throws the gates open to cyber fraud, socially dangerous and unacceptable content, extremism and social aggression online.

This problem is already on the agenda of Russian national security agencies. According to our source in the Security Council, “the Council’s agenda now includes the problem of terrorism in social networks". The problem is largely rooted in the registration procedure of the *Vkontakte* network, which used to be extremely lax up until June 2011. To this day *Vkontakte* produces hundreds and thousands of search results with pages, groups, articles and videos containing calls for waging “jihad against the infidels”, building “an Islamic emirate in the Caucasus”, launching a rebellion by Russia’s Muslims against the “federals”, etc.

Such a torrent of unacceptable content results from the fact that it is next to impossible to establish the real identities of the users who have posted it. Hence the huge number of profiles of users describing themselves as “mujahedeen”, “warriors of Islam”, and other such things, which would be unthinkable on *Facebook* or *Google+*. Even as these users fill their profile with some personal information, they feel safe in the knowledge of their impunity, unless the FSB takes personal interest in them (which is highly unlikely since there are simply too many of them). In addition, on March 15, 2011 *Vkontakte* won a precedent-setting court case over copyright-infringing content. The judges agreed with the social network’s argument that responsibility for posting such content lies with the users. That gives the green light for similar violations by the users, who effectively remain anonymous.

Meanwhile, the social networks themselves – at least in Russia – are trying to find their own ways of solving the problem of user identification. The results are not always good. On July 11, 2011 *Vkontakte.ru* introduced a new registration system requiring users to submit their mobile phone number, a compromise between their previous open registration system and a closed one. Linking a user account to a phone number is a fairly effective mechanism of user identification in countries such as Russia, where citizens need to present a national ID in order to obtain a mobile phone number. But this mechanism also has gaping holes because *Vkontakte* users are not all Russian citizens. About 40 million of them live in other countries, meaning that they buy mobile phone numbers under different rules. As of early 2011, *Vkontakte* had about 16.5 million accounts of users from Ukraine, where buying a SIM card does not require any form of ID. In some European countries, such as Spain, mobile phone numbers are not even fixed to any specific mobile service provider. As a result, about 30 per cent of *Vkontakte* users cannot really be identified, even though their phone numbers are known. The approach chosen by *Vkontakte* (which could well be followed by other social networks) therefore needs to be augmented by other solutions to close the aforementioned loopholes.

One possible mechanism is to link a social network account to the user's bank details, i.e. follow the approach already used by electronic payment systems such as *PayPal*, *Webmoney*, *Yandex.Money* and others. One clear advantage of such an approach is highly reliable user identification and higher value of the account in the eyes of the user (especially if the User Agreement includes a provision under which a certain sum of money in the bank account is frozen in the event of a breach of the agreement's terms by the user). But the idea has two vulnerabilities.

First, it will not cover the entire user base. As of March 2011, only 47 per cent of Russians had bank accounts - although the figure is much higher for young people, who form the core of the social networks' user base. Also, it is not clear what to do with users who have accounts in foreign banks which do not work in the Russian market. *Second*, linking social network accounts to the users' bank accounts could face resistance from the social networks themselves and from other stakeholders in this area, as well as from the banks, which will have to process a flow of information they have no use for.

On the second point, any progress is possible only if the social networks successfully commercialize their services, i.e. if the users start to pay for them using their bank accounts. First steps in that direction were made in July 2011 by Russia’s two largest social networks, *Vkontakte* and *Odnoklassniki*, whose users can now pay for premium services using credit cards issued by certain banks (previously the only way was to send a text message to a premium number). The key question is, will the social networks be able to turn what is now a payment option into a compulsory mechanism, and will their security measures be enough to protect their users' bank details? In terms of security *Odnoklassniki* seems to have come up with one of the better solutions. During the initial registration the network’s users work in a secure database operated by the bank itself before being directed to the *Odnoklassniki* user interface.

In any event, all of these measures do not offer a complete solution to the problem of user identification - that will require a holistic approach that encompasses the entire internet. At this moment such an approach is absent in Russia. First, there is no consensus about the role government should play in this area. Second, there is no single vision of the problem by technology experts and the legal profession. Given the situation, there is a clear need for a detailed and comprehensive study of international experience, both positive and negative. According to one renowned Russian expert on information law, “the Russian government needs to monitor the solutions and practices being used in other countries and international organizations in this area”.

Confidential

Among the foreign countries the most interesting proposals have been voiced in the United States. One initiative actively discussed in recent years is to introduce *internet passports* - and not just for the social networking services but for all internet users. In late 2010 the White House published a draft of the National Strategy for Trusted Identities in Cyberspace. The idea is to have a universal, comprehensive, multi-level and secure internet environment in which users are securely identified and personal data is reliably protected. The strategy is aimed at individuals and other entities, including organizations, services, and software products. It takes into account the global nature of the internet and the need for the proposed user identity instruments to work across the national borders. The key principle of security arrangements for the internet environment is to enable the entities exchanging information to provide only the minimum of information that is required for each individual situation, with a multi-level and very flexible range of requirements to each individual type of transaction or entity. In all other cases users remain anonymous and are not forced to disclose any personal information that is not required by the situation.

THE STRATEGY

Firstly, there needs to be a detailed and comprehensive study of internet security and user identification projects such as the *Identity Ecosystem*. This project, which is now being developed by the United States, is a promising example of a comprehensive approach to the identification problem. It could serve as a starting point for developing Russia’s own national strategy on user identification. User identification in social networks must be an integral part of such system.

Secondly, establishing routine cooperation with the internet community, which can serve a variety of useful purposes in the area of security, should be a priority for the Emergencies Ministry, the Interior Ministry, the Federal Security Service (FSB), the Defense Ministry and other security agencies. At present, cooperation between the government and the internet community is developing too slowly.

Thirdly, the problem of cybercrime and cyber terrorism must be properly addressed in Russia's strategies and doctrines. Modernization of national legislation can serve as an adequate basis for international and multilateral cooperation in fighting cybercrime.

The authors are research fellows at the PIR Center.

Edited by Irina Mironova.

Trialogue Club International*:* trialogue@pircenter.org

Centre russe d’etudes politiques: crep@pircenter.org

Moscow - Geneva, October 2011