CHATHAM HOUSE

Chatham House, 10 St James's Square, London SW1Y 4LE
T: +44 (0)20 7957 5700 E: contact@chathamhouse.org
F: +44 (0)20 7957 5710 www.chathamhouse.org

Charity Registration Number: 208223

REP Roundtable Summary

Russian Cyber Security: Concepts and Current Activity

Keir Giles

Conflict Studies Research Centre

6 September 2012

The views expressed in this document are the sole responsibility of the author(s) and do not necessarily reflect the view of Chatham House, its staff, associates or Council. Chatham House is independent and owes no allegiance to any government or to any political body. It does not take institutional positions on policy issues. This document is issued on the understanding that if any extract is used, Chatham House should be credited, preferably with the date of the publication or details of the event. Where this document refers to or reports statements made by speakers at an event every effort has been made to provide a fair representation of their views and opinions, but the ultimate responsibility for accuracy lies with this document's author(s).

As far as cyberspace is concerned, Russia is most worried about the threat posed by content. ‘Internet sovereignty’, i.e. the ability of the state to have control over the information space, is a fundamental concept in Russia. Non-interference in Russia’s cyber space is also seen as crucial and Russia is pushing for the creation of new international arrangements. Its position is supported by countries such as China, Tajikistan and Uzbekistan; members of the Shanghai Cooperation Organization have reached an agreement that is very closely aligned with Russia’s proposals for international cyber security legislation.

There are important contrasts between western and Russian concepts of cyber security. Russia has a statist concept of who should be involved in cyberspace; Russian officials assert the principle of national boundaries, while the established view in the West is that information should - and does - travel freely. In addition, the Russian concept of ‘breach of information space’ has not gained currency in the West, and neither has the view that existing international legislation is not sufficient. Russia has taken part in discussions with the West regarding international cyber security legislation in a range of different fora, but their idea of information space is not clearly defined and negotiations have remained very broad.

How do these Russian standpoints on cyber security reflect on the domestic scene? Russia has well-developed tools for total evidence-collection; furthermore it is easy for officials to close down internet resources at will and without a court order. Russian cyber criminals have until recently appeared to enjoy impunity as long as they do not target domestic Russian victims. Increasing pressure for prosecution of cybercrimes in Russia is both domestically and internationally generated; there has been a recent clampdown on Russian internet resources sharing stolen intellectual property.

Private information security companies in Russia work closely with the law enforcement authorities and augment their capabilities; e.g. 30-40% of the work of Group IB is requested by the police. There is less evidence of information security companies investigating suspicious activity which coincides with Russian state aims, and there are instances where their public statements coincide precisely with government policy.

Freedom of expression is generally accepted on the internet in Russia. The use of distributed denial of service (DDoS) attacks against media outlets critical of the government is not unusual, but at the same time it would be easy and entirely legal for the authorities to close down entire websites if it were felt necessary. Russia avoids overt methods of controlling cyberspace.

There is no overt censorship of social media, as there is in China; at the same time there is investment in monitoring and seeding software. Russia was happy about the West's embarrassment over the WikiLeaks scandal, but the incident heightened the Russian political elite's own sense of vulnerability. The internet continues to be seen by some sectors of the Russian leadership, and by the security agencies, as more of a threat than an enabler. It is difficult to assess how satisfied the Russian authorities are with their control over cyberspace. The important point is that the tools for control are at their disposal, but used only rarely and generally with a light touch.

Several Russian intelligence bodies are concerned with national cyber defence and offensive capabilities. Recently, the military has also been talking about setting up its own cyber command. The Russian government tends by default to present its cyber activity as entirely defensive, i.e. as a measure necessary for countering external threats.

Russians lead the world in developing software and techniques for cyber crime, and Russians remain at the forefront of research and innovation in this area. The nationality of cyber actors does not necessarily dictate their affiliation, whether in Russia or abroad, so criminal activity by Russians should not always be confused with hostile action by the Russian state.