The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Security First, Technology Second — Why It's Back to the Future For Russian IT

By Andrei Soldatov

December 07, 2016

TASS / DPA

In the Bavarian Alps there is a small mountain resort town, Garmisch-Partenkirchen, famous for its spectacular views and its hosting of the Nazi Olympics in 1936. It has also, since 2007, been the location of a conference between Russian and American top cyber officials and generals.

Every April, they gather in the Hotel Atlas, a traditional Bavarian three-story lodge, to talk cyber. The discussion is private, and by and large participants have tried to be pleasant and friendly to one another. But nothing can hide the fact that the sides have diametrically different views of the Internet.

In 2010, one of participants, American expert George Sadowsky, admitted in exasperation,

“The Russians have a dramatically different definition of information security than we do … They really mean state security.”

The new Information Security Doctrine signed by President Vladimir Putin on Dec. 6 is the very embodiment of the concept of state security. The list of threats listed in the document includes “hostile coverage of Russian state policy” by foreign media; destabilization of Russian regions by “informational-psychological means” i.e. by foreign intelligence services; the use of IT to disrupt the sovereignty, territorial integrity and political stability of Russia, and so on.

On the one hand, none of this is particularly new. Many of the terms were already used in the first Doctrine on Information Security, signed in 2000, while the others came into use after the Arab Spring and the Moscow protests in 2011-2012, when the Kremlin was awakened to the potential of social media.

Read more: In 2016 RuNet, Pressure Shifts from Companies to Citizens

But the new document has also an unmistakably new old Soviet touch. Here, security comes first, technology comes second. The authors of the Doctrine are not happy with “the practice of introducing information technologies without first providing for information security;” they think it increases risks. As far as they are concerned, telecoms and IT companies should always consult with secret services ahead of introducing new services and technologies for their customers.

The Doctrine questions the very essence of the modern information society — the free flow of information across borders. “The possibilities of cross-border flow of information are used increasingly for geopolitical or military-political goals in contradiction of international law,” reads the “Threats” chapter of the Doctrine, a thinly veiled hint at so-called “Twitter revolutions.” There are mentions of ominous forces building the means to disrupt “critical infrastructure” of the Internet.

What this means in practice is that telecoms companies will have to ask secret services where to have their fiber optic cables laid. It also means that the Kremlin is serious in pursuing the idea of an cyber kill-switch — an option which would enable the authorities to cut the Russian Internet off from the outside world in case of “emergency.” All this looks very Soviet, and totally misplaced. After all, the opposition protests in 2011-2012 were not organized or led from abroad.

Strict informational control was, of course, how things were done for 70 years in this country. Soviet authorities traded technological development for the ghost of state security. It didn’t end well then — either for the Soviet system of for Soviet technology. There is little indication it will end well now.

Read more: 1 Million Russians to be Put under Surveillance in 2016, Activists Say

In our book “The Red Web” we describe how the KGB forced the Soviet Communications Ministry to cut international phone lines right after the Moscow Olympic Games. The lines werebuilt for the Games, but were destroyed only months after because the KGB was not comfortable giving Soviet citizens the option of automatic connection. As result, the country

found itself well behind the West in telecommunications.

Ironically, Putin's new Doctrine is full of complaints on the consequences of such decisions. It admits IT development is "insufficient," for example. But the authors of the strategy never come near to learning their lesson. Instead, they lament the "unjust governance of the Internet," and they demand a bigger role for the Kremlin.

Significance change in Internet governance is unlikely to happen soon, but the authors of the Doctrine do have options. While the first Doctrine, written back in 2000, focused mostly on threats and goals, the new Doctrine proudly lists new tools at the Kremlin's disposal — "forces of providing information security", "means of providing information security" and the "system of providing information security."

In other words, in 16 years, the Kremlin has created an entire information security bureaucracy, spread all over the country.

And these new forces are capable of one thing — they can slow down the country's technological progress, once again.

The views expressed in opinion pieces do not necessarily reflect the position of The Moscow Times.

Original url:
https://www.themoscowtimes.com/2016/12/07/security-first-technology-second-why-its-back-to-the-future-for-russian-it-a56458