# Moscow Pushes Own Approaches to Cyber Security on Rest of CSTO

## by Sergey Sukhankin

Republished in collaboration with the Jamestown Foundation, Eurasia Daily Monitor, Vol. 15, Issue 135, dated 26 September 2018, Edited for *OE Watch*.
For the full article, see: https://jamestown.org/program/moscow-pushes-own-approaches-to-cyber-security-on-rest-of-csto/

**OE Watch Commentary:** Russian military strategists who have analyzed regional military conflicts between 1999 and 2014 conclude that even a less-developed party may be able to at least partly degrade the technological advantage of a stronger adversary if the weaker power can attain information superiority over its opponent. Indeed, one of the key lessons Russia has drawn from its participation in the Syrian civil war is that defeating the enemy on the information battlefield is an integral part of a successful asymmetric counter-actions strategy. The adoption of the new Information Security Doctrine (2016) illustrates Russia's growing determination to ensure its control over the entire information space of the Moscow-led Collective Security Treaty Organization (CSTO), and arguably beyond. On June 11, during the foreign ministerial meeting of the CSTO in Almaty, the participants proclaimed that the regional alliance's top priority for the next seven years would be the consolidation of efforts/actions in the domain of information and cyber security.

In a May 2017 interview with the Russian military publication *Krasnaya Zvezda*, Ara Badalian, the deputy director of the General Secretariat of the CSTO, argued that thanks to key steps taken in 2006–2017, the organization has managed to form "a multi-layered reaction system in the domain of information security". During the first stage of the above-mentioned interim (2006–2009), emphasis was placed on elaborating joint initiatives in the field of targeting "international cyber crimes." This included organizing annual multinational information/cyber trainings (that brought together specialists in information/cyber security, internal affairs, anti-drug trafficking, financial monitoring and migration) under the code name PROKSI (*protivodeystviye kriminalu w sfere informatsii*—"countering crime in the information sphere").

During the second stage (2010–2017), the parties further expanded their level of cooperation, culminating in the decision to create an Emergency Crisis Center (as an integral organ within the CSTO) specifically tasked with enabling further cyber/information policy consolidation, regular information exchange, and establishing a collective security architecture within this field. Despite continuing emphasis on equality in partnership, Russia's full control over the CSTO—and now over the adoption of new cyber and information security guidelines within this bloc—is unmistakable. Namely, the theoretical and practical training of specialists (on the basis of the Moscow Engineering Physics Institute and other Russia-based institutions), as well as the preparation of all CSTO member state military cadres in the area of information/cyber security (at the Krasnodar Higher Military School) remain firmly in Moscow's hands.

Another important trend should not be overlooked: Russia's ambitions clearly extend beyond the CSTO. On June 19, the Russian city of Khanty-Mansiysk hosted the Second International Conference on Information Security (*Infoforum-Yugra*), organized with the support of the Russian parliament, Russian Security Council, the Federal Security Service (FSB), the Ministry of Internal Affairs (MVD) and the Ministry of Foreign Affairs (MFA). The *Infoforum-Yugra* was attended by members of the CSTO, the Shanghai Cooperation Organization (SCO), as well as the BRICS group (which brings together major developing powers Brazil, Russia, India, China and South Africa). During the event, it was proposed to create a "center for monitoring of and reaction to information and cyber threats" that would be located in Russia. This center would, apparently, be jointly used by members of the CSTO and its "partners, including BRICS and the SCO".

In addition to growing ambitions, Russia continues to develop new capabilities in information/cyber security. Notably, Moscow frequently touts the National Defense Management Center (NTsUO). Namely, senior Russian military and civilian experts continually claim the Center's supercomputer (based on the Astra Linux operating system, specifically designed to meet the needs of the Russian military, other armed forces and intelligence agencies) is said to be superior to all existing Western analogues.

Reportedly, the NTsUO's supercomputer features 236 petabits of storage capacity (versus 12 petabits in the most advanced foreign analogues) and computing speeds of 16 petaflops (compared to 5 petaflops of the top rivals). The velocity of information processing is said to equal 50 Lenin Libraries per second, allowing constant monitoring of such complex developments as troop relocations or the tracing of information flows in mass media and online social networks. According to Russian sources, the supercomputer's capabilities have already been tested on several occasions, including during the military strategic exercise Vostok 2014 and as part of regular monitoring of developments in Syria. Additionally, the machine successfully withstood multiple cyberattacks, including the WannaCry ransomware attack.

The intensification of Russian activities in the domain of information/cyber security underscore three main aspects. First, Russia's emphasis on non-military forms of confrontation can be expected to progressively increase, which is likely to be put in practice within the scope of future regional conflicts. Second, Russia will likely continue its efforts to consolidate control over the information/cyber space of its partners inside the CSTO, and probably other actors dependent on Moscow (such as Syria, or Nicaragua). Third, Moscow will almost certainly employ its advancements in the realm of information/cyber capabilities as a means to increase its role in non-Western blocs in order to break its international isolation. **End OE Watch Commentary (Sukhankin)**

Source: "ОДКБ возводит щит кибербезопасности (The CSTO is creating a shield cybersecurity)," *Liter*, 13 June 2018. https://liter.kz/ru/articles/show/47352-odkb_vozvodit_shit_kiberbezopasnosti

*...The interaction of member states in this field has become noticeably active in recent years. In turn, the combined experience and the new standing challenges are reflected in the agreement on cooperation of CSTO member states in the field of information security signed last year in Minsk...The document calls for "holding joint events, especially those of a practical character, aimed at strengthening information security and combating illegal activities in the information space of CSTO member states...*