China-Russia cyber-security pact: Should the US be concerned?

The Russia-China deal on cyber-security could send a warning signal to the U.S., which might view the deal as a growing threat to its economic and security interests in cyberspace.

Originally written for Russia Direct and published on May 21 2015

The applicability of the international law and the law of armed conflict to cyberspace is generally accepted and its nuances are being debated at global platforms. Photo: AP

A host of agreements signed by Russia and China marked the recent visit of Chinese President Xi Jinping to Moscow. Among them is an agreement in the field of international information security – an agreement that has already been branded a "cyber pact" by the media. This agreement received the most attention because it is viewed as an important and symbolic move of Russia and China towards each other in one of the most debated spheres of international relations.

The document identifies the key threats to global information security, which both countries intend to stand against together. These threats include the use of technology "to carry out acts of aggression aimed at the violation sovereignty, security and territorial integrity of states," "to interfere in the internal affairs of states," to cause economic damage, to commit crimes, including data breach, for terrorist purposes, or to disseminate information that "harms political and socio-economic systems, or the spiritual, moral and cultural environment of other states."

What the new cyber-security deal means for Russia and China

Russia and China have pledged to cooperate closely to address these threats jointly through enhanced interaction and information exchange between the respective law enforcement agencies on cybercrime and terrorism, through sharing expertise in cyber-security technology

and by establishing communication channels allowing prompt response to the world's cyber-threats.

The two sides agreed on a range of trust and confidence building measures and joint "promotion of norms of international law in order to ensure national and international information security," especially under the auspices of the platforms of the relevant international organizations: the UN, OSCE and ITU.

The agreement looks like an ambitious attempt at setting the rules of the game in cyberspace at the time when no such consent on norms of behavior seems currently feasible at a global scale. As the Global Conference on Cyberspace in The Hague in April showed, the decision on signing such a treaty is not ripe enough for the states to commit.

Due to dual use technologies at the heart of what could be seen as cyber weapons, at present it is very hard to set up an efficient oversight mechanism to implement any international treaty banning cyber weapons in the environment of increasing distrust in the world.

Despite calls for global peace and security, the policies of some countries appear to boost the cyber arms race, affecting non-proliferation and disarmament efforts as well as global security in general.

In this context, Russia and China, seeing more eye-to-eye on a range of information and cyber-security than other partners, found it possible to come up with a non-aggression pact and put on paper the key points for strategic partnership in information security.

The Russia-China deal as a response to the U.S. cyber defense strategy

The deal appears logical, as Russia is throwing more weight behind cooperation with its Eastern partners in the situation of an economic and diplomatic "siege" at its Western border.

In addition, the recently released U.S. Department of Defense Cyber Strategy directly identifies Russia and China among its key adversaries, which "have developed advanced cyber capabilities and strategies," while only mentioning the need for keeping a dialogue with China.

"Russian actors are stealthy in their cyber tradecraft and their intentions are sometimes difficult to discern. China steals intellectual property (IP) from global businesses to benefit Chinese companies and undercut U.S. competitiveness," it reads, clarifying the U.S. perception of Russia and China.

Moreover, in April the U.S. announced the launch of a new sanctions program that "authorizes the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to sanction malicious cyber actors whose actions threaten the national security, foreign policy, or economic health or financial stability of the United States."

Remarkably, the Russia-U.S. cyber-security confidence-building agreement in 2013envisaged similar cooperation and information exchange between the U.S. and Russian

computer emergency response teams (CERTs), the creation of a working group on emerging threats and the use of the existing nuclear hotline to communicate directly in a cyber-crisis.

Unfortunately, it has never meaningfully got off the ground and has stalled in the current geopolitical context.

The China-U.S. cyber dialogue has been patchy since a similar attempt at a confidence-building measures (CBM) agreement in the same year. Snowden's ill-timed revelations in 2013 didn't help the implementation of the deals either.

The third link in this triangle was rumored back in late 2014 and was expected to exceed in scale both attempts. At present, the Russia-China agreement looks more like a framework document, in many ways building on previously identified shared values and expectations.

Yet, it develops the new Section 10 of the reviewed SCO proposal, referring to the development of practical confidence building measures, "aimed at increasing predictability and reducing the likelihood of misunderstanding and the risk of conflict" – the least debatable area among policy makers as well as the least assessable and controlled.

The two sides have not experienced big public fallouts on mutual hacking so far, which makes, what seems a non-aggression pact, look more like a pre-emptive declaration of understanding, making a special point of this consensus to the external world.

This has been ascribed by some experts to Russia's desire to sting the U.S. and build up a joint front to counter potential cyber-intrusion, which is seen as more than probable in the current standoff. At the same time, the stumbling Sino-American dialogue on cyber cooperation gives additional incentive to China to team up with Russia.

There are fears in the West that the private sector might lose business if Russia and China edge closer on mutual technology exchange. Photo: AP

The Russia-China cyber agreement as a strategic move

However, to discount the agreement to mere attempt at "ganging up" on America would be to oversimplify things. In other words, what we are seeing might be just the tip of the iceberg.

Even if symbolic, the pact strengthens the Russia-China axis of cooperation and marks a further shift in Russian foreign policy towards the East. This makes the agreement more of a priority for Russia in the current tight diplomatic environment.

The win for China is not obvious but there may well be a trade-off in the bigger basket of deals signed in early May 2015 in Moscow between the two countries. It would also help bring additional legitimacy to domestic cyber-governance policy in both countries and strengthen the incumbent regimes. This goes in line with the SCO code of conduct provisions creating a multi-level support to this norm-building effort.

The framework deal still leaves room for future amendments and extensions to the agreement, with more detailed spelling out of the technological, infrastructural and policy alignment moves at the national segment level. This might be something Russia hoped for initially and the Chinese have not been able to commit to up to now - but the option is out there.

In this sense, the underwater part of the iceberg might exist, but might not be revealed for a long time. However, it is still not obvious how feasible and desirable intentional cyber deterrence and due diligence is for both sides in practice. Only the future implementation of the agreement's CBMs should show the real level of commitment to transparency and mutual trust.

Promoting global cyberspace governance

On a larger scale, the agreement illustrates the ongoing Russian efforts to promote a norms-driven approach to cyberspace governance. The applicability of the international law and the law of armed conflict to cyberspace is generally accepted and its nuances are being debated at global platforms including the UN Group of Government Experts (GGE) format, where Russia has historically been one of the key drivers of the responsible behavior agenda in cyberspace.

The SCO proposal is the only international effort so far to adopt a self-regulatory approach to non-aggression in cyberspace whereby all interested parties are welcome to join. However, due to conceptual differences in qualifying threats in cyberspace, not helped by an exceptionally low level of diplomatic contacts between Russia and the West, it has not seen much support so far outside the SCO group.

In this sense, the bilateral agreement clearly builds on the points already mutually accepted and reinforces Russia's lead on norms formation, backed up by the important partner from the East.

All of the above neatly fits into the "securitization" of the information space agenda, which Russia has been highlighting for years. As it is felt now in some fora, the ongoing radicalization of the online public sphere due to extremism and terrorism helps somewhat narrow the existing gap in understanding of threats and risks in cyberspace.

The diplomatic tensions might thwart tangible international rapprochement in this area but regional and bilateral steps have been taken.

The blurring of the line between offense and defense in cyberspace

The question still remains how meaningful the pledge 'not to hack' is – and it goes beyond the Russia-China deal. The U.S. Cyber Strategy states it is "appropriate for the U.S. military to conduct cyber operations to disrupt an adversary's military related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations."

This stems from the assumption that "deterrence is partially a function of perception," which "will not be achieved through the articulation of cyber policies alone, but through the totality of U.S. actions," including warning and response capabilities, defensive posture, and the overall resiliency of U.S. networks.

This stance displays quite a loose reading of potential threats to U.S. interests and gives carte blanche to the U.S. government in the assessment and response to what is perceived as aggression, further blurring the line between defense and offense in cyberspace.

Keeping this in mind, the Russia-China deal, built around the idea of the supremacy of sovereignty in cyberspace governance and countering external actions against the internal stability and integrity of states, could be well taken, if or when implemented, as a growing threat "against U.S. interests."

Therefore, if further stepping up this cooperation looks aggressive, there is no guarantee the response will be symmetric. What is 'symmetric' in cyberspace has not been clearly defined yet.

The practical implications from the Russia-China agreement are probably too early to formulate before any implementation steps are taken. Nevertheless, it would certainly be interesting to see if these are in any way highlighted at the BRICS summit in July 2015 in Ufa.

More precisely, whether or not the Russia-China bilateral pact inspires other parties to follow suit (at least at a bilateral level within the group) in the absence of a clearly articulated joint approach on information and cyber-security.

While there are also fears in the West that the private sector might lose business if the two countries edge closer on mutual technology exchange, the key concerns still lie with the matters of peace and security: The best advertisement for the advocated approach to cyber security would be a safer global community.