A Russian cyber-security expert said today that in order to avoid the “very grave consequences” that could result from cyber-warfare, the world should adopt a non-proliferation treaty for cyber-arms similar in nature to the Nuclear Non-Proliferation Treaty (NPT).

Mikhail Yakushev, chairman of the executive board of the Moscow-based PIR Center, also said that among the cyber-warfare scenarios is the possibility of cyber-attacks that could affect the operations of nuclear facilities.

“In this sense I can say that a well prepared attack could be the equivalent to the explosion of a nuclear arm and it is something that should be avoided,” Yakushev said in an interview with NPSGlobal in Buenos Aires, where he is attending the 48th meeting of the International Corporation for Assigned Names and Numbers (ICANN).

There have been unconfirmed media reports in recent weeks of attempts to breach security at Russian nuclear facilities via cyber-attacks, Yakushev said. But he added that it is premature to judge what if anything happened as the authorities have not yet commented on the matter.

While the possibility of a cyber-attack against national infrastructures has long been a focus of cyber-security experts, the 2010 attack against Iranian nuclear installations brought the subject to the forefront of policy considerations. Iranian nuclear facilities were damaged by the Stuxnet worm in the attack widely reported to have been carried out by the United States and Israel.
Since that time, several countries have opened or strengthened cyber-security command structures as part of their national defense or security efforts.

**Photo Gallery**

{gallery slider=boxplus.carousel width=245 height=200 count=1 crop=1 labels.txt=captions alignment=center orientation=horizontal buttons=1 links=0 counter=0 overlay=1}Yakushev{/gallery}

The PIR Center, or the Russian Center for Policy Studies, is a think-tank focused on the issues of international security and control as well as non-proliferation of weapons of mass destruction. Yakushev is an attorney, former executive of technology companies and information specialist who previously represented the Russian Federation in the U.N. working group on Internet governance.

Yakushev, who visited the offices of the NPSGlobal Foundation in Buenos Aires during a break in the ICANN deliberations, said a non-proliferation treaty for cyber-arms would build off the positive experience of the non-proliferation treaty, which today has 190 signatories.

“We see that it is very evident that the viruses that are used to carry out cyber-attacks, are created by states,” Yakushev. He said that while nobody could object to cyber-defense efforts when these are efforts that reside in the same computers in which they were created, cyber-attacks are transported from one computer to another, or one state to another.

Among the potential objectives of cyber-attacks would the attempt to cripple critical national infrastructure, including telecommunications, airlines, railways or electrical power networks.

“An attack on one of these networks could provoke negative results in another part of the world,” Yakushev said. It is precisely for this reason that cyber-security is a concern of “all humanity” and should be addressed globally.
The Russian security expert said that the proposal for a non-proliferation treaty for cyber-arms is in its initial stages. The Russian Foreign Ministry has expressed interest in the proposal as well as colleagues at the James Martin Center for Nonproliferation Studies of the Monterey Institute of International Studies in the United States. So far there has been no interest from China.

As a result of the revelations made by former U.S. intelligence contractor Edward Snowden, who released information documenting the nature of global spying efforts by the U.S. National Security Agency, Brazilian President Dilma Rousseff has announced plans to host a world summit on Internet governance in April of next year.

The conference will be attended by a broad range of stakeholders in the Internet field, in this instance, including top government officials, industry leaders, civil society organizations and representatives of academia.

Rousseff called the conference in October after it was reported that the U.S. agency had intercepted communications between Rousseff and aides as well as information of the Brazilian oil company, Petrobras, and private citizens. Snowden’s leaks also revealed that the NSA spied on other world leaders.

Yakushev said the conference would be important because it will be the first time that an internet governance meeting is “purely political.” He said the meeting would look at two very significant aspects of Internet governance: the management of root servers, which are responsible for the most basic routing of information across the Internet; and the management of the first level domain names, which currently is in the hands of the U.S. company VeriSign.

On the question of the root servers, Yakushev said, “The problem is not where the root servers are located but rather who manages them.”

Major Root servers, which are responsible for assuring connectivity across the Internet, are currently run by private companies but recent debate has focused on whether management of these servers should not be managed by governments or international organizations.
The ability to advance toward agreement on questions of Internet governance has been blocked so far by the “over-politicization” of the issue, generally around the question of freedom of expression where different countries, including the United States, China and Russia, have not been able to come to terms.

China, for instance, views any reference to human rights as not being positive, he said.

“Unfortunately, as a result of this (lack of agreement), we cannot not reach a compromise on subjects that are much more important such as the fight against cyber-terrorism,” he said. He said the cyber-terrorists are the shared enemies of all states and that these have a common interest to come up with joint defensive measures against potential attacks.