BIURO BEZPIECZEŃSTWA NARODOWEGO

Sankt Petersburg, 7 June 2012

Consolidation of international efforts towards information security

Dear Secretary Patrushev!
Dear Excellencies! Ladies and Gentlemen!

It is our honor and indeed a pleasure to attend this important event in such a beautiful and historic place. Both Saint Petersburg and President Boris Yeltsin (patron of the venue) represent the spirit of cooperation and the desire to participate in shaping a common European future.

Contemporary security environment is evolving dynamically. The changes are determined by rapid technological growth as well as new political and social phenomena, among which growing participation of citizens in shaping state's actions takes prominent place. During last decades we may observe a growing scale of asymmetric threats. Those are perceived by many researchers and analysts as becoming more important than conventional threats. Thus new security aspects emerge, including information security.

The cyberspace is becoming a new worldwide security environment. One of the most important characteristics of this new environment is the fact that there are many problems in the area of identification and monitoring of new threats, risks and opportunities. Those processes of identification and monitoring are necessary conditions of correct analysis, evaluation and creation of optimal cyberspace security mechanisms. That is the reason why information security has become the strategic issue for most countries.

The development of information and communication technologies directed the contemporary world towards the new information era, and created a new societal

model: information society. It is a global society. For this reason alone benefiting from positive effects of information revolution as well as countering its negative consequences demand common action by states and international organizations. Main sources of threats in this security area are intentional disruptions of information systems, illegal input or copying of data, hacking the security mechanism in order to seize control of individual elements on critical infrastructure (for example in case of war). It is important to remember that such threats can emanate from both: states (their armies and intelligence services) as well as non-state actors (criminal or terrorist groups).

Cyberterrorism is one of the most important threats among many challenges and threats that are generated by information society age. Many critical sectors of state's economy have to be protected from the threat posed by this phenomenon – mainly by the state itself in close cooperation with private sector. Among the most important targets of potential cyberterrorist attacks are key elements of critical infrastructure supporting the functioning of public administration, internal security, national defense, communications and financial systems, rescue systems and basic services (providing citizens with water and energy).

It should be underlined that in the long run most of the traditional security threats will be mirrored in the virtual environment. We are already witnessing cyber attacks in the form of cyber protests or cyber demonstrations that disorganize the functioning of public administration on unprecedented scale. We need to be looking for new means and procedures to respond to those new challenges adequately.

It is very important to remember that information security influences civilian as well as military sphere of state's actions. Both of those spheres are dependent on correct functioning of critical infrastructure. Development of information technologies influences greatly how the conflicts are played out – more and more often cyber warfare may be used during those conflicts. States as well as their citizens are universally present in cyberspace. This is the factor that makes information warfare and its manifestations capable to influence the political stability outside of virtual world on national and international scale.

Those facts generate the necessity to intensify efforts and improve capabilities of states in the area of responding and protecting their own assets. Those actions have to be undertaken within the framework of legal and institutional cooperation. In order to effectively counter threats to information security the states should focus on shaping the correct legal framework and procedures that enable them to punish perpetrators. Another important area is creation and improvement of adequate deterrence mechanisms in cyberspace through perfecting the effectiveness of threats detection.

Optimizing activities in this area is all the more important due to the fact that in cyberspace state loses great part of its sole attributes connected with jurisdiction. State administration acting in this environment has to cooperate closely with the private sector because differentiating between public and non-public actors (including economic ones) in cyberspace is almost impossible.

States are also facing an important challenge of generating new types of legal, organizational and functional tools adequate to cyberspace characteristics. Keeping abreast of technological development is extremely demanding even if limited only to the legal aspect. Long-lasting legislative processes mean that keeping up with evolution in information environment is extremely difficult in the aspect of legal and organizational changes.

Discrepancy between the law and the specific characteristics of cyberspace (due to the lack of borders, difficulties in interpretation of jurisdiction, large potential of non-state actors) may necessitate application of the "code of conduct" to regulate various phenomena in cyberspace. It may be described as a "half measure", but taking into account serious problems with setting up imperative norms, it may well become one of the most effective solutions.

Additionally it is important to say that lack of borders in cyberspace makes this category a global one. Protection of this environment is a challenge faced by the whole international community. This calls for the necessity of common action to counter dangerous phenomena and common response to existing threats by the whole international community.

Cyber security has been a recurrent subject in the international debate within NATO, the European Union and the United Nations. This proves its important role and significance in protecting global security. The direct consequence is institutionalization of activities in cyberspace. Many countries have either already created or are planning to create specialized bodies that are supposed to deal with cybercrime, cyber intelligence, cyberterrorism and cyberwar in an integrated manner. In Poland those kinds of actions are being implemented on legal level – through introducing to the Polish legal system the concept of cyberspace, creation of governmental programme of cyberspace protection and development of institutionalized tools for cyberspace protection (Cyber-Security Center, CERT).

The next stage of guaranteeing global information security is deepening international cooperation in the area of response to cyber threats. Actions in this area are being realized on daily basis, mainly through international organizations that create specialized institutions (like NATO's Cooperative Cyber Defence Centre of Excellence in Tallin or European Network and Information Security Agency). Creating a mechanisms that allow for testing common procedures of responding to threats would also improve cyberspace security.

Consolidation of international community efforts towards global information security should be a priority in strategic actions of its members. It is necessary to increase the pressure to create global institutions and agreements as well as maintain action towards the improvement of individual capabilities and optimizing the level of protection of national assets.

It is my opinion that the current formula of conferences organized regularly by our Russian friends creates a very good forum for discussion and searching for much needed, possible and admissible solutions.

Let me conclude by quoting the late President Yeltsin, who once said: "It is especially important to encourage unorthodox thinking when the situation is critical. At such moments every new word and fresh thought is more precious than gold. Indeed, people must not be deprived of the right to think their own thoughts". This year Security Council of the Russian Federation is celebrating the

20th anniversary of its founding. Let me wish you on this occasion, Secretary Patrushev, further contribution to international standing of the Security Council by bringing in the new ideas – more precious than gold!