



**NATIONAL ASSOCIATION  
FOR INTERNATIONAL INFORMATION SECURITY  
(NAIIS)**

119192 Moscow, Michurinsky prospect №1, room № 4  
PSRN 1187700009606 TIN/IEC 9729271968/772901001  
Phone: +7 (495) 7765999 Mobile : +7 (916) 3043000  
<http://namib.online> e-mail: [info@namib.online](mailto:info@namib.online)

**NAIIS Position thesis for the Seventh substantive OEWG session**

**March 2024**

The application of voluntary, non-binding norms of responsible behavior of states in the ICT environment faces a number of fundamental difficulties. Firstly, they do not stem directly from existing norms of international law, but are aimed at clarifying the interpretation of existing norms in relation to ICT environment, as well as expanding the international regulatory system for activities in the field of ICTs. As a result, in order to apply the norms of responsible behavior of states in the ICT environment, it is necessary to create an appropriate international legal framework, which would on the one hand, establish them as elements of a normative international legal system, and on the other, create certain grounds for their impact on international relations and on public relations regulated by national legislation. In practice, this can be implemented within the framework of the proposed concept of Convention for international information security.

It is necessary to adapt the norms and principles of international law to regulate relations in the field of application of ICTs and the functioning of the global information infrastructure within the framework of the ICT environment as a new space for international cooperation. As part of this process, it seems useful to discuss, among other things, issues of resolving controversial situations regarding incidents in the ICT environment, as well as clarifying the international obligations of states regarding cooperation in the ICT environment from the position of respecting the principle of state sovereignty.

Among the suggestions made, the Second Annual Report of the OEWG states (23b) that “voluntary, non-binding norms... allow the international community to assess the activities of States.” It is worth recalling that in paragraph

1.2 of UN General Assembly resolution A/RES/73/27<sup>1</sup> it is specifically noted that “the indication that an ICT activity was launched or otherwise originates from the territory or objects of the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State. Accusations of organizing and implementing wrongful acts brought against States should be substantiated. In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences.” It is obvious that in the conditions of unresolved fundamental problems of applying the rules and principles of responsible behavior of states in the ICT environment, in particular, determining the areas of responsibility of states, the “assessment” can lead to episodes of unfounded accusations and will not contribute to maintaining peace and stability.

A particular threat today is posed by the uncontrolled development of artificial intelligence technologies. In this context, it is important to note that AI (as a means for processing and transmitting information) is in itself a type of ICT. Relevant tasks for the global community are ensuring the responsible and safe use of ICTs, including AI, as well as preventing the harmful use of AI systems. These pressing issues of information security could be considered within the framework of the UN OEWG.

---

<sup>1</sup> **A/RES/73/27.** Developments in the field of information and telecommunications in the context of international security.