nournews

شناسه خبر : 53144 2020/08/18 05:59 Tuesday

General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat

The General Staff of the Iranian Armed Forces in a statement on Monday warned that any level of cyber threats against the country will be responded firmly and decisively.

NOURNEWS - “Armed forces of the Islamic Republic of Iran do not initiate any conflict in cyberspace as in the physical space. They regard the policy included in this instrument as a framework for their actions in confronting any threat in cyberspace,” the statement said.

“It is clear that the Armed forces of the Islamic Republic of Iran reserve the right to react to any threat at any level in a firmed and decisive manner if any of the policies included in the present instrument may be violated by any state, group, or any other person or entity supported, controlled or directed by any state,” it added.

The full text of the statement is as follows:

Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace

Armed Forces Cyberspace Center - July 2020

Preamble

The General Staff of the Armed Forces of the Islamic Republic of Iran, in the discourse on national security, has the mandate to deterrent and cyber-defense against any threat in cyberspace.

Taking into account the defensive mission granted to the armed forces and under the command of the Supreme Leader and the grand commandership of all forces, all relevant organizations and institutions shall have coordination and synergy with armed forces. As, in accordance of the cyberspace experts, cyberspace constitutes a new area in the field of defense and security, the present instrument under the title of "Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace" clarifies the concepts, macro policies and the framework of the activities of the armed forces against increasing and various threats of cyberspace.

Article I: General Points

1. Believing that international law applicable to cyberspace shall be a just distributer of benefits and advantages of peaceful cyberspace and involved "access" and "equitable sovereignty" for all states.

2. Emphasizing that while all states shall act responsibly regarding cyberspace, they have common but different responsibilities because of resources and technologies available for each state.

3. Considering that a wide range of general principles of current international law, including equality of sovereignty of states, the prohibition against the use of force and act of aggression may apply to the use of cyberspace.

Article II: Sovereignty Policies of Armed forces of the Islamic Republic of Iran

1. The Islamic Republic of Iran has developed its sovereignty fields consistent with necessary capabilities for protection of its strategic military, economic, social, cultural, and political authority. In doing so, the development of expertise and advanced cyber tools for active and deterrent cyber-defense is, among others, one of the significant priorities for the protection of the strategic authority of the state.

2. Rules of modern international law imply the existence of limited territory in geographical borders of states exercising sovereignty or at least jurisdiction within those borders. According to the armed forces of the Islamic Republic of Iran, the territorial sovereignty and jurisdiction of the states are also extended to all elements of the cyberspace.

3. Any intentional use of cyber-force with tangible or non-tangible implications which is or can be a threat to the national security or may, due to political, economic, social, and cultural destabilization, result in

destabilization of national security constitutes a violation of the sovereignty of the state.

4. Any utilization of cyberspace if and when involves unlawful intrusion to the (public or private) cyber structures which is under the control of another state, maybe constituted as the violation of the sovereignty of the targeted state.

5. The sovereignty of states is not an extra-legal matter. It shall be interpreted under the other fundamental legal principles such as non-intervention, good faith, self-determination, and other basic principles. It must be kept in mind that the sovereignty of states is subject to the principle of equality and the sovereignty of any state is not above the sovereignty of the other states. Therefore, any limiting and freezing measure, including sanctions, constitutes the violation of the sovereignty of independent states because of not respecting the sovereignty of target states.

Article III: Intervention in Internal [and external] Affairs of other States from the View-Point of the Armed Forces of the Islamic Republic of Iran

1. The principle of non-intervention, without any doubt, is an independent principle of customary international law and any measure to change the political regime such as political forceful intervention is a gross violation of this principle. Measures like cyber manipulation of elections or engineering the public opinions on the eve of the elections may be constituted of the examples of gross intervention. The intervention, also, covers situations in which the non-cyber measures may occur in the cyber activities relating to the internal and external affairs of the other state. Cyber activities paralyzing websites in a state to provoke internal tensions and conflicts or sending mass messages in a widespread manner to the voters to affect the result of the elections in other states is also considered as the forbidden intervention.

2. Armed intervention and all other forms of intervention or attempt to threaten against the personality of state or political, economic, social, and cultural organs of it through cyber and any other tools are regarded as unlawful. No state may compel the other state, by resorting to cyber and other means, to use or encourage to use of political, economic, or any other measures to subject that state in exercising its sovereign rights or guaranteeing concessions from that state.

3. All explicit and dainty forms and complicated techniques of duress, overthrow, and outrage (whether Cyber or non-cyber) to intrigue in the political, social, or economic order of other states or destabilizing governments

seeking liberalization of their own economic, political and cultural system form control or intervention of foreigners, is unlawful.

4. Every state enjoys the inherent right to the full development of information system and mass media and their employment, without intervention, to advance their own political, social, economic, and cultural interests and aspirations. Any measure resulting in impediment, denying, and or restricting operation of signals and means of information transfer and providing control systems and exercising the sovereignty of the state is regarded as unlawful.

5. Any capacity-building program in the field of cyber shall be designed and applied under the national plans and needs of states and in consistence with their economic, social, and cultural situations. These programs shall not become a means for intervention in the internal affairs of states.

Article IV: Use of Force and Cyber Attack from the View-point of the Armed Forces of the Islamic Republic of Iran

1. Armed forces of the Islamic Republic of Iran believe that certainly, those cyber operations resulting in material damage to property and/or persons in the widespread and grave manner and or it logically is probable to result in such implications constitutes use of force. Should such operations affect the vital national infrastructures, including defensive infrastructures- whether owned by the public or private sector- they shall violate the principle of the non-use of force.

2. Armed forces of the Islamic Republic of Iran, also, believe that their right to self-defense shall be reserved if the gravity of the cyber operation against the vital infrastructure of the state is reached in the threshold of the conventionally armed attack.

Conclusion

Armed forces of the Islamic Republic of Iran do not initiate any conflict in cyberspace as in the physical space. They regard the policy included in this instrument as a framework for their actions in confronting any threat in cyberspace.

It is clear that the Armed forces of the Islamic Republic of Iran reserve the right to react to any threat at any level in a firmed and decisive manner if any of the policies included in the present instrument may be violated

by any state, group, or any other person or entity supported, controlled or directed by any state.
