CAPACITY TO MANAGE LARGE-SCALE CYBER CRISES OF UKRAINE

Pohorila V. M., Klymenko D. V.
National Aviation University, Kyiv
Supervisor – Martyniuk H. V., PhD., associate professor

For preventing the belief of basic cyber threats tons of nations area unit used world indexes, like National Cyber Security Index, world Cybersecurity Index, ICT Development index, Network Readiness Index. victimisation statistics from 2020, land isn't within the worst place (fig. 1). however in terms of cyber management crisis land is at zero and it's sensible that it's not within the red. sadly, the Law of land doesn't contain the idea of cyber crises in and of itself generally.

Figure 1. The place of Ukraine by Cybersecurity global indexes

Large-scale cybersecurity incidents which cause disruption too extensive for a concerned Member State to handle on its own or which affect two or more Member States or EU Institutions are considered a cybersecurity "crisis". These cybersecurity incidents can have a wide-ranging and significant impact of technical or political significance that they require timely policy coordination and response at Union political level.

The Cyber Crisis Management provides the strategic framework and guides actions to prepare for, respond to, and begin to coordinate recovery from a cyber incident.

The first step to improve cyber management crisis in Ukraine is creating cyber crisis management plan. The government has established a crisis management plan for large-scale cyber incidents. It's going to has such elements: clear definition of roles and responsibilities of every stakeholder; identification of potential negotiation experts; templates of statements tailored for purchasers, business partners.

Over the past three years, there is no information about exercise documents or press releases about conduction of a national-level cyber crisis management exercises or a crisis management exercise with a cyber component. Ukraine needs tangible assistance from the West to confront current threats. In cyber space this will entail projects in three areas: cyber defense skills and capabilities development; cyber security policy, legislation and strategy development; and material and technical assistance.

An equally necessary facet of rising the crisis state of affairs in land is participation in international cyber crisis exercises. NATO and their member states ought to invite experts and officers from Ukraine to their cyber defense exercises (Cyber Coalition, Cyber Europe). Within the framework of the Annual National Program, the Alliance ought to strengthen cooperation for cyber defense capability development within the Ukrainian defense force. just in case of a cyber crisis, international organisation allies ought to deploy their “Rapid Response Teams”within 24 hours.

The procedures for victimisation volunteers within the field of cyber security aren't established by legislation therefore, land should establish a Cyber Civilian Corps, a new law, which permit volunteers to service a broader vary of entities in would like of crisis help. underneath bill broadening powers for the civilian corps, it permits these volunteers from the community to bring cyber-defense services to non-profit-making organizations, non-public businesses, instructional teams, and alternative non-governmental associations.

As a result, we can say that in Ukraine there are attempts to change and improve this area, but unfortunately, these attempts are scanty in comparison with the development of other areas and the development of this area in other countries. In this situation, it is desirable to continue to develop and take more significant measures.

References:

1. International Centre For Defence and Security EESTI – Estonia. What Ukraine needs to defend against cyber, information and psychological operations [Electronic resource]. – Electronic magazine. – September 19, 2014 – Access mode: https://icds.ee/en/what-ukraine-needs-to-defend-against-cyber-information-and-psychological-operations/

2. Developing Cyber Crisis Response Capabilities. [Electronic resource]. – Access mode: https://cyberstartupobservatory.com/cyber-crisis-response-capabilities/

3. Chris Galford. New Michigan law assigns cybersecurity volunteers to network security assistance during cyberattacks [Electronic resource]. – Electronic magazine. – October 30, 2017 – Access mode: https://homelandprepnews.com/stories/25017-new-michigan-law-assigns-cybersecurity-volunteers-network-security-assistance-cyber-attacks/

4. Official resource: National Cyber Security Index (NCSI) Ukraine. [Electronic resource]. – Access mode: https://ncsi.ega.ee/country/ua/

5. Dr. Jnaneswar K, Gayathri Ranjit. Exploring the Cyber Threat Landscape and Cyber Crisis Management Model. // International Journal of Science and Research. [Electronic resource]. – Electronic magazine. – 2016 – Access mode: https://homelandprepnews.com/stories/25017-new-michigan-law-assigns-cybersecurity-volunteers-network-security-assistance-cyber-attacks/