NATIONAL CONVENTION ON THE EUROPEAN UNION IN NORTH MACEDONIA (NCEU-MK)

RECOMMENDATIONS

11th session of WG-4, Justice, Freedom, and Security (Chapter 24), Skopje, 24 April 2023

***Topic:* "INCREASING RESILIENCE OF THE INSTITUTIONS TO ADDRESS HYBRID THREATS"**

1. The Government should take the initiative to create a systemic national approach to increase the resilience of institutions through an appropriate normative framework for the preparation of acts and procedures for cyber security management and protection against hybrid threats.
2. To increase the institutions' resilience to hybrid threats, the Government should take the initiative to define the specific standards and equipment (information infrastructure) that will be installed in the institutions.
3. To develop national resilience to hybrid threats, it is necessary for the Government to increase communication, cooperation, and coordination with all stakeholders (companies from the IT sector and other companies in the field of security, civic associations, the academia, the media and other expert public).
4. An operational team to address cyber security and hybrid threats, should establish a list of institutions that may be targets of hybrid threats, including to implement prioritization because all institutions do not require the same level of protection, nor do all institutions have the same importance.
5. An operational team to address cyber security and hybrid threats, should establish security standards, operational procedures, and protocols to protect institutions from possible hybrid threats, as well as to address the consequences thereof.
6. The Government should take the initiative to define the need for trainings of the managerial staff and the employees in the institutions, as well as to determine the concept and forms of the trainings in order to familiarize them with the security standards, operational procedures, and protocols for protection of the institutions from possible hybrid threats.
7. Given the fact that the country is moving in the direction of mass application of information technologies (IT) in all spheres of social action, the Government should take the initiative to change the approach to the IT sectors in the institutions through appropriate human resources management, which would imply:

- Attracting highly qualified staff with special material incentives (appropriate to the sector as a whole);
- When recruiting IT staff, it is necessary to strictly apply the expert criterion, i.e., professional qualifications;
- Optimization of the number of employees according to the complexity, criticality, and vulnerability of the institution;

8. The justice system institutions (the public prosecutor's office and the courts) should invest in all aspects of strengthening the investigative and judicial processes. It implies having a dedicated budget and the ability to use the services of external specialized organizations.
9. The Government should initiate closer cooperation and partnerships between the national institutions with those from the neighboring countries, as well as with the countries from the Region to share experiences from realized cases of cyber-attacks and hybrid threats.
10. The Government should reconsider the possibility of changing the procedures of public procurement announcements in the field of IT, which provide many details of a technical nature that increase the risk of hybrid threats.
11. Cyber culture - as a whole of technologies (of a material, organizational and intellectual nature), but also practices, attitudes, ways of thinking and values about cyberspace - is built in a spontaneous way by all members of the community. However, encouraging and supporting public debates by different stakeholders can increase citizens' sensitivity to these issues.