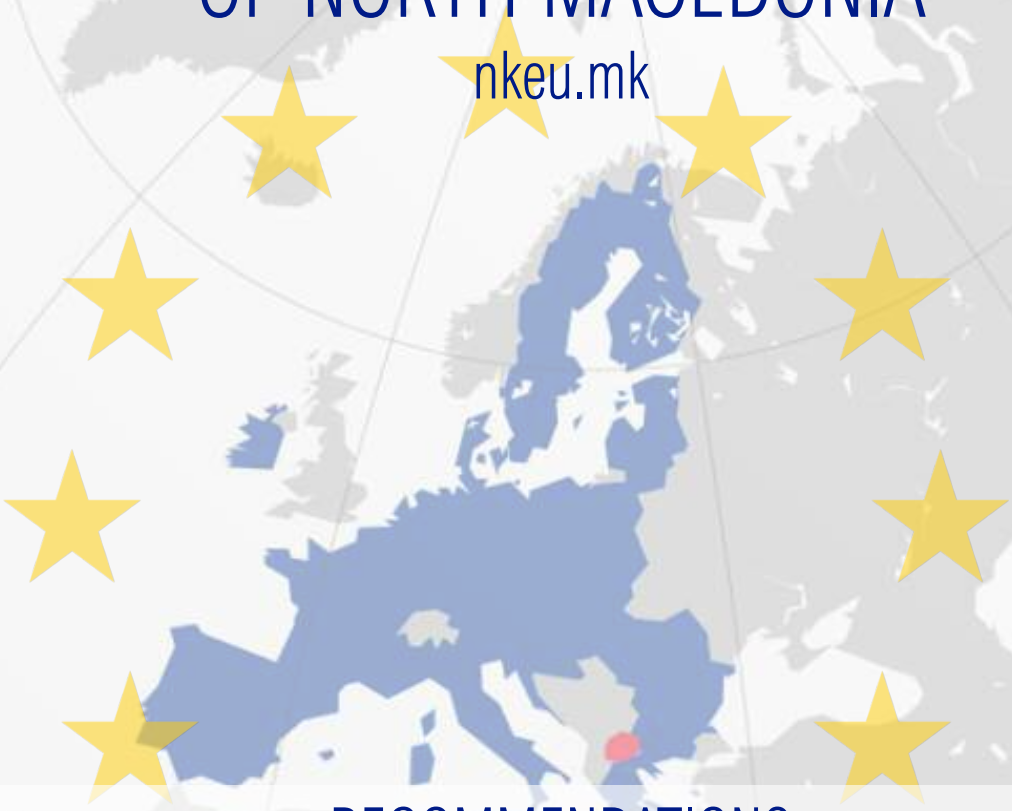
Финансирано од
Европска Унија

Европско движење Северна Македонија
European Movement North Macedonia

NATIONAL CONVENTION ON THE EUROPEAN UNION IN THE REPUBLIC OF NORTH MACEDONIA

nkeu.mk



RECOMMENDATIONS
11th Session of the Working Group 4 – Justice, Freedom and Security

Topic: “Strengthening the Institutional Resilience Response to Hybrid Threats”

1. The Government should take an initiative to develop a systemic national approach through a normative framework that should serve as a basis for drafting legal acts and procedures for managing cyber-security and hybrid threats protection in accordance with EU directives and NATO standards.

2. The Government should consider the necessity of changing the procedures of public procurement calls on IT technologies, in which many technical details are disclosed that may increase the risk of hybrid threats.

3. In order to strengthen the institutions' resistance against hybrid threats, the Government should pay special attention to the extremely important technical standards for security (protection) of the institutions' IT systems (i.e.IT infrastructure).

4. The Public Prosecutor's Office and the courts including other competent institutions responsible for the implementation of laws should increase their investigative capacities (technical and resource ones) for dealing with criminal acts in the area of cybercrime. This implies having a dedicated budget and the option of using services of external specialized organizations (outsourcing).

5. In order to achieve greater national resilience to hybrid threats, the Government needs to strengthen communication and cooperation with all stakeholders (enterprises from the IT sector and other enterprises in the area of security, civil associations, the academic community, the media and other experts) as well as develop a concept for public-private partnership in this area.

6. The operational team for cyber-security and hybrid threats should accelerate the process of making a list of institutions that may be a target of hybrid threats, including their prioritization, since not all institutions require the same level of protection, nor all institutions have equal importance.

7. Considering the inevitable mass application of information technologies (IT) in all spheres of social life, the Government is recommended to take an initiative to change its approach towards the IT sectors in the institutions by adopting an adequate human resources management, which requires:

8. The government should initiate closer cooperation and partnerships between national security institutions and those from neighboring countries for regular sharing of experiences from successfully closed cases of cyber-attacks and hybrid threats (regular meetings with EU representatives and regional experts).

    - attracting highly qualified personnel while ensuring personal income that corresponds to the IT sector as a whole;

    - during the recruitment of IT personnel, the professional qualifications i.e. the experts criterion should be strictly applied;

    - optimization of the number of employees according to the complexity, criticality and vulnerability of the institution;

9. Considering the fact that successful dealing with hybrid threats requires involvement of all stakeholders, including institutions' employees, it is recommended that: The Government takes the initiative to identify the requirement for an adequate training, in order to familiarize the employees with security standards, operational procedures and protocols for protection against potential hybrid threats.

10. Cyber-culture as a set of technologies (material, organizational and intellectual) as well as practices, standpoints, mindsets and values for the cyber-space is being developed in an organic manner by all members of the community. However, the encouraging and supporting of public debates among various stakeholders can increase citizens' sensitivity to these issues and develop critical awareness and a culture of tolerance, through an active involvement and support of the civil sector.

11. Ensuring protection of the electoral process from hybrid threats, hostile cyber-activities, dissemination of information carried out by other state and non-state entities, from financing of political parties, politicians and non-governmental organizations by external, adversary entities. To effectively achieve this goal, national actors will apply lessons learned and expertise from NATO and the EU.