# FEATURES OF NATIONAL CYBER DEFENCE

**Borysenkov D., Rozhok S.**
*National Aviation University, Kyiv*
*Supervisor – Martyniuk H.V., PhD, Associate Professor*

Because of Russia's actions in April 2014, the Ukraine decided to make a step from historic alignment with Russia to find itself in NATO membership. On September 20, 2018 Ukraine's president Petro Poroshenko said "We need to amend our constitution to make NATO membership a long-term goal" [1]. These words played an irreversible role of transformation our country toward European and Euro-Atlantic course integration. And one of the main goals was to transform consciousness of Ukrainian people to convince them that Ukraine is not a part of Russian Federation. The importance of this message made by Ukrainian law was directly counter to Putin's influence operations attempting to convince the entire world that Ukrainians were ethnically Russians.

The main objective of the new Cyber Security Strategy of Ukraine (hereinafter – Strategy) is to create circumstances for the protected operation in cyberspace, its use for the advantages of individuals, society and the state. It should be noted that in linking with the Strategy the National Security and Defense Council of Ukraine has decided to establish a special new government body as its working body – National cyber security coordination center [2].

The most innovative measure among aforesaid ones is to establish a special sub-unit of the Armed Forces of Ukraine which didn't exist before, and development of such sub-unit in other government bodies. This arrangement implies attraction of IT-specialists to these bodies which, in its turn, implies additional money from the government budget. At the same time it is very important to guarantee sufficient qualification for such specialists in cyber defense.

Last three years, the main goals for cybersecurity sphere was [3]:

- achieving the relevant standards of EU and NATO in cyber security field;
- creating a terminology framework, regulation in field of electronic communications, information protection in accordance with international standards;
- development of mobile communication security sphere;
- improvement of state control system of information security;
- development of national response teams for computer emergencies;
- development of international cooperation with EU and NATO in order to increase Ukraine's capability in cybersecurity sphere.

A center of excellence (COE) is a team, a shared facility or an entity that provides leadership, best practices, research, support and/or training for a focus area. As of 2018, there are twenty-four of them. COEs are international military organizations that train and learn leaders and technicians from NATO member and partner countries. They help in doctrine improvement, identify lessons educated, improve interoperability and capabilities, and test and validate concepts through experimentation. They propose

recognized expertise and experience that is of benefit to the Alliance, and support the transformation of NATO, while bypassing the duplication of assets, resources and facilities which were already presented within the Alliance." [4]

In addition to employing information as a tactical level of power, there is a number of other reasons to expedite Ukraine's membership application and approve the Ukraine as the future layout of the IW (Information Warfare) COE.

As stated by the Strategy, development of security potential and defense sector in the cyberspace must include the next realization steps:

- creating a safe environment for the existence and development of a free society by the formulation and implementation of the internal affairs policy;
- enhancing public confidence in the Ministry of Internal Affairs;
- continuing the development of Ukraine as a safe European state which is based on the needs of its citizens and high efficiency of each MIA component;
- establishment and implementation of protocols of joint actions, including information interchange in real time;
- implementation of state strategic planning and software in the field of electronic communications, information technology, information security and cyber defense in the cyberspace;
- creating a sole sub-unit to ensure protecting and defending in the cyberspace of the Armed Forces of Ukraine on strategic, operational and tactical levels;
- development of quick reaction to computer emergencies [5].

Anyway, when it comes to cybercrimes, the most important part of the operation is immediate reaction of intelligence agencies, but obtaining a court decision may delay such reaction. That's why it is still hard to say whether our new cyber security strategy helps to decrease the level of cybercrime or not. Thought, it is absolutely sure that Strategy still requires making a lot of changes in Ukraine legislation, toughening measures of responsibility for violations in the cyber space sphere and increasing fines.

However, it is too obvious that Ukraine has to make some serious steps in the way of changing the policy of data protection in cyberspace and Strategy is undoubtedly a good beginning of positive changes.

**References:**

1. AP NEWS. Ukraine pushes ahead with plans to secure NATO membership. Retrieved on 25/02/2021 from https://www.apnews.com/dff40992fcc446f6808d02d03b35e4bc

2. Cyberdominance. Ukraine as a NATO Centre of Excellence: Information Warfare. Retrieved on 24/02/2021 from https://www.cyberdominance.com/cyberdominance/ukraine-as-a-nato-centre-of-excellence-information-warfare/?history=0&pfid=1&sample=2&ref=0

3. Nekrasov V, Polyakova A (2017) This is war: Ukraine was shaken by the largest cyberattack in history. Ekonomichna Pravda (Text in Ukrainian). Retrieved on 24/02/2021 from http://www.epravda.com.ua/publications/2017/06/27/626518/

4. NATO. Centres of Excellence. Retrieved on 25/02/2021 from https://www.act.nato.int/centres-of-excellence???history=4&pfid=1&sample=11&ref=0

5. KMU. National Security and Defense. Retrieved 03.03.2021 from https://www.kmu.gov.ua/en/reformi/bezpeka-ta-oborona