importantly: the State Enforcement Service is not faced with the task of completing justice. Usually, the State Enforcement Service is engaged in the implementation of an indicative rate of revenues to the state budget, meaning that the completion of enforcement proceedings by non-enforcement of a court decision in cases stipulated by law is quite legal and common.

Not so long ago, a new legal institution appeared on the legal expanses of Ukraine – the institute of a private enforcement officer, which was granted by the state with the right to provide public services for the enforcement of court decisions at the request of participants in the judicial process. It is disputable whether this institute will be able to replace the existing State Enforcement Service in the nearest future. However, as an alternative right of a person interested in enforcing a court decision and other acts, the private enforcement officers can and should function.

As for the fate and subsequent attempts to reform the State Enforcement Service, it is possible that despite the deep respect for the State Enforcement Service officials and their extremely complex and psychologically difficult activities, the legislative and executive bodies of state power need to have the courage and recognize that the creation of the State Enforcement Service as an independent system of state enforcement power was erroneous and it is necessary, as part of the next judicial reform, to restore the institution of liquidated bailiffs subordinated to the judicial authorities in order to ensure the implementation of the constitutional right of a person to judicial protection and the proper implementation of the main task of the court – the administration of justice.

ATTRIBUTION OF CYBERATTACKS COMMITTED THROUGH CYBERINFRASTRUCTURE OF A THIRD STATE AND DUE DILIGENCE OBLIGATION

Viktoriia Muzyka[1]

DOI: https://doi.org/10.30525/978-9934-26-002-5-32

Cyberattacks became a global challenge to international community, which is highly dependent on industrial control systems. They are especially dangerous when launched against objects of critical infrastructure, without proper functioning of which people may suffer from the lack of food, water, electricity, medical care etc, and a state – be subjected to political and economic crisis.

[1] National University «Odesa Law Academy», Ukraine

Cyberattacks may be committed by both state and non-state actors, and it is always difficult to perform an attribution claim and established a required nexus. At the same time, available technical and human resources make it possible to establish that nexus between a certain cyberattack and a private person or a group of persons behind the cyberattack. However, in most cases perpetrators go unpunished.

The world needs significant changes to protect critical infrastructure of states. Nowadays private individuals and some state actors invest in cyberattacks because industrial control systems manage different aspects of human life. Even supply of water or electricity can be disrupted in case of successful cyberattack. In such a scenario, there is a high possibility of humanitarian crisis, serious violation of human rights, political and economic instability.

There were some attempts to eradicate impunity and increase public attention to this problem, however with each cyberattack hackers became more confident in commissioning sophisticated cyberattack on a large scale. Among the most famous cyberattacks on critical infrastructure are the following – cyberattack against one of US dams in 2013, German steel mill in 2014, Ukrainian power grid systems in 2015 and 2016, the National Health Service in the UK in 2017, Saudi Arabia`s safety instrumented systems in 2017, South African electricity supplier and Indian nuclear facility in 2019 [1].

One can also witness increasing number of cyberattacks on railway systems. In particular, in 2014, a 14-year schoolboy hacked tram systems in Poland. His actions caused tram derailments and numerous human injuries [6]. In 2016, UK reported that its railway systems were subjected to at least four major cyberattacks [7]. And in 2017, due to consequences WannaCry attack, Germany`s rail infrastructure suffered system errors [3].

During the first wave of COVID-19 pandemic, even medical sector was attacked by private individuals. Such cases where reported in France, Czech Republic, Thailand, and Turkey. For example, in March 2020, the largest hospital in Brno, Czech Republic, became a victim of a cyberattack against its systems. As a result, it had to postpone surgeries and transfer acute patients to other medical facilities. They also were unable to process coronavirus tests and perform other indispensable functions [4]. In the same vein, Paris-based AP-HP, the largest network of hospitals in Europe, became a victim of cyberattacks [5].

In almost all cases a critical infrastructure of a third state was used to guarantee anonymity. That is a main reason why the duty of due diligence merits a special consideration. This duty is not a panacea against cyberattacks, but it could help to decrease the number of cyberattacks. Indeed, states will pay way more attention if a targeted stated is interested in invocation of responsibility of a third state. It is reasonable to expect state`s interest and

ability to monitor how critical infrastructure within its territory is used. According to the famous dictum in the Corfu Channel case, «it is every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States» [2, p. 22]. This obligation derives from state`s sovereignty over its territory and duty to protect the rights of other states within it.

To establish the violation of due diligence, two principal preconditions should be met. Firstly, the knowledge of a third state about the use of cyber infrastructure within its territory is required. This knowledge should not be actual, rather constructive. It means that knowledge may be attributed to a state if within the normal course of events a state would have been aware about the use of its territory for cyberoperation [8, p. 41].

If a governmental infrastructure is used, it is undeniably that a third state should have possessed knowledge about the use of its cyber infrastructure. Indeed, attribution of constrictive knowledges will also take place if well-known vulnerabilities or malwares, which has been already discovered and reported, are used. For instance, a third cannot avoid responsibility by claiming it was unaware about Heartbleed [8, p. 41] or Zerologon [9] vulnerabilities discovered in 2014 and 2020 respectively.

Secondly, a cyberattack have to cause 'serious adverse consequences'. Although a threshold for the required harm is unsettled in international law, it is clear that serious consequences excludes minor disruptions and inconvenience. At the same time, there is no need for physical damage to objects of critical infrastructure of a targeted state or human injuries. It will be assessed a on case-by-case basis [8, p. 37].

Therefore, states have to actively engage in establishing state responsibility based on the due diligence obligation. It may force states to monitor carefully how critical infrastructure located within its territory is used, and, as a result, to prevent and cease wrongful actions that breach obligations owned to a targeted state.

References:

1. Caltagirone S. (2019). Industrial cyber attacks: a humanitarian crisis in the making. ICRC Blog. URL: https://blogs.icrc.org/law-and-policy/2019/12/03/industrial-cyber-attacks-crisis/

2. Corfu Channel case, Judgment of April 9th, 1949: I.C. J. Reports 1949, P. 4. URL: https://www.icj-cij.org/public/files/case-related/1/001-19490409-JUD-01-00-EN.pdf

3. Cyberattack hits German train stations as hackers target Deutsche Bahn. URL: http://www.telegraph.co.uk/news/2017/05/13/cyber-attack-hits-german-train-stations-hackers-target-deutsche/

4. Mačák K., Rodenhäuser T. and Gisel L. (2020). Cyber attacks against hospitals and the COVID-19 pandemic: How strong are international law protections?

URL: https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/

5. Naveen G. (2020). Failed Cyber Attack on Paris Hospital Authority // Cybersecurity Insiders. URL: https://www.cybersecurity-insiders.com/failed-cyber-attack-on-paris-hospital-authority/

6. Schoolboy hacks into city`s tram system. URL: https://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html

7. UK rail network hit by multiple cyber attacks last year. URL: http://www.telegraph.co.uk/technology/2016/07/12/uk-rail-network-hit-by-multiple-cyber-attacks-last-year/

8. Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge: Cambridge University Press.

9. Zerologon Vulnerability: Analysis and Detection Tools by Igor Kovalenko & Itamar Meydoni. URL: https://www.cynet.com/zerologon/

LOCAL GOVERNMENT REFORM IN UKRAINE: CURRENT STATE AND PROBLEMS

Vladislav Oliinyk[1]

DOI: https://doi.org/10.30525/978-9934-26-002-5-33

The start of the reform of local self-government in Ukraine was given after the approval by the government on April 1, 2014 of the Concept of Reforming Local Self-Government and Organization of Power in Ukraine. It was based on the provisions of the European Charter of Local Self-Government, which was ratified by the Verkhovna Rada on July 15, 1997. The implementation of the provisions of the document began in 2015 and provided for the consistent solution of the following tasks:

– Determine the territorial basis for the organization of local self-government and executive power.

– To delimit powers between local self-government bodies of various levels.

– To delimit powers between local self-government and executive power.

– Determine the required amount of resources for each level of government.

– Establish the responsibility of local self-government bodies to the voter and the state.

The goal of the reform of local self-government is the transfer of significant powers from the executive authorities to the level of local self-

[1] Academy the State Penitentiary Service, Ukraine