U.D.C. 341.211/214:316.276:(007:004.56)
DOI: https://doi.org/10.18524/2411-2054.2020.39.212983

V. V. Muzyka, PhD Student, Assistant
the National University "Odesa Law Academy"
the Department of International and European Law
Fontanska Doroga str., 23, Odesa, 65009, Ukraine
email: viktoriiamuzyka@gmail.com

ANALYSIS OF CYBER-ATTACKS ON UKRAINIAN POWER GRID SYSTEMS IN THE CONTEXT OF ARMED CONFLICT IN DONBAS

Summary

Attribution of cyber-attacks committed by non-state actors is not an easy task; however, it is far from impossible. Being unable to apply the effective control test to invoke state responsibility for state-sponsored cyber-attacks, states have started relying upon multitude of factors for the purpose of public attribution. This approach is not a solution due to political nature of public attribution. By example of Ukraine author demonstrates the potential danger of cyber-attacks against critical infrastructure and the need of attribution. The 2015 and 2016 attacks on Ukrainian power grid systems evidence that private actors posses resources and knowledge to attack the vital objects of critical infrastructure. The article contains the analysis of committed cyber-attacks in the context of armed conflict. Author concludes that these attacks are linked to the armed context in Donbas and stresses out on the need to create an independent body responsible for attribution.

Keywords: cyber-attack; attribution; attacks on Ukrainian power grid systems; industrial systems; critical infrastructure.

Problem statement. The danger and potential effects of cyber-attacks cannot be overestimated, especially when industrial systems are their main target. Our dependence on industrial systems is indisputable – they are not merely underpinning our everyday lives, but became an important part of it.

This article deals with the problem of attribution of cyber-attacks on power grid systems, which distribute electricity to population, keeps heating on and a state economy running. To date, it is almost impossible to attribute a state-sponsored cyber attack by virtue of effective control test, even though cyber-attacks on objects of critical infrastructure may cause humanitarian crisis and millions of deaths. Moreover, without power grid systems operating in a proper way, a country and its people may face the lack of food, medical care, drinking water, heating or cooling during winter or summer respectively.

Increasing number of cyber-attacks shows that hackers became more skillful in attacking industrial systems, notwithstanding the fact that such systems are relatively disconnected from the Internet. Aside from attacks on Ukrainian power grids, cyber-attacks on industrial systems have been committed in other countries. In particular, attacks on Johannesburg electricity supply in South Africa, a nuclear facility in India, as well as attacks at a steel mill in Germany and a petrochemical company in Saudi Arabia – to name just a few.

Cyber-attacks become more and more sophisticated, and most probably attackers receive support from governments due to resources used and plenty of time required for commission of such cyber-attacks. But what distinguishes attacks on Ukrainian power grids is their context, since they are the only attacks committed within the course of armed conflict. Thus, such attacks could have amounted to war crimes [16, p. 391]. Since prohibition of war crimes and other international crimes have *jus cogens* status and *erga omnes* character [1], international community must put best effort to prevent its commission via cyberspace and carry out technical and legal attribution of cyber-attacks.

Analysis of the latest researches and publications. Cyber-attacks attribution is an issue actively discussed by legal scholars and experts of cyber and IT firms due to partially technical nature of this issue. Among law scholars, there are number of scholars whose works dedicated to the issue of attribution of cyber-attacks – M. Schmitt, M. Roscini, J. Richmond, P. Stockburger, D. Hollis, K. Ziolkowski, D. Alperovitch etc. Additionally, technical reports of private sector regarding the nature and effects of 2015 and 2016 cyber-attacks were used.

Purpose statement. The goals of this article are to analyze the 2015 and 2016 attacks on Ukrainian power grids in the context of armed conflict and identify the possible solution.

Main part of the research paper. Acting through proxies is not a new phenomenon for international law. States sponsor and support non-state actors to avoid responsibility and anonymously boost own interests.

Pursuant to well-known Nicaragua case, conduct of non-state actors will be attributable to a State "only if it directed or controlled the specific operation and the conduct complained of was an integral part of that operation" [13, p. 47]. In case of cyber-attacks, it means specific orders or instructions should be given by a state to non-state cyber actors. Only in this case actions of non-state cyber actors will be attributable to the state. However, most affected states relied upon other factors (technical indicators, motivation, geopolitical or economic interests, geographic location, level of proximity between state and non-state actors etc.) due to impossibility to apply the effective control test caused by its high threshold. Moreover, decentralized attribution of cyber-attacks came to the fore and gives additional impulse to rethinking current standards in order to find a solution.

A case study of the 2015 and 2016 exemplifies the danger of cyber-attacks on objects of critical infrastructure and demonstrate the importance of analyzing the whole context in which cyber-attacks were committed.

Although cyber-attacks at Ukrainian power grid did not cause physical destruction, a case of Ukraine serves as an example of how cyber-attacks can be used against objects of critical infrastructure. These attacks are not simply malicious cyber activity since they were conducted in wartime.

On 23 December 2015, a group of hackers launched a cyber-attack against electric power stations in Ukraine – the first confirmed cyber-attack to take down an electricity power system. The cyber-attack was directed primarily at three regional electricity distribution companies (oblenergos). Attackers had used spear phishing emails containing Microsoft Office attachments that were infected with the BlackEnergy 3 malware, credential theft, VPNs access and other technical means to get access to the company's computers and SCADA systems. As a result, an interference with oblenergo`s system caused several outages that impacted approximately 225,000 customers in different regions and lasted several hours [18, p. III-IV].

In a joint analysis of the cyber-attack on the Ukrainian Power Grid, the Electricity Information Sharing and Analysis Center and SANS Industrial Control System experts concluded that "[t]he cyber operation was highly synchronized and the adversary was willing to maliciously operate a SCADA system to cause power outages, followed by destructive attacks to disable SCADA and communications to the field. The destructive element is the first time the world has seen this type of attack against OT systems in a nation's critical infrastructure" [18, p. 20].

Importantly, experts have attributed the 2015 attack to the Sandsworm team of hackers [4, p. 10]. This group of hackers is well-known for its planting of BlackEnergy malwares and attacking different networks that manage industrial physical equipment. When FiveEye`s engineers had accessed an unsecured command-and-control servers of Sandsworm in 2014, they discovered the way BlackEnergy operates due to instructions and other files written in Russian. The language of files and the fact that attacks launched by the Sandsworm reflect the strategic interests of the Russian Federation are among the main reasons why this group of hackers is believed to have a strong nexus with Russia [9].

Furthermore, according to Ukrainian Ministry of Energy, hackers made phone calls from Russian Federation and used a Russian-based internet provider within the course of cyber-attack on Ukrainian power grid [20].

Cyber-attacks at Ukrainian institutions and objects of critical infrastructure do not look accidentally chosen targets in the light of the ongoing armed conflict. On 29 December 2015, President of Ukraine made an official statement and announced that within the last two months there were 6500 cyber-attacks against 5 agencies and 31 state information resources. He also added that investigation witnesses about either direct or indirect involvement of the Russian Federation [22].

The time chosen for the 2015 attack and surrounding military-related activities also may shed some light. Firstly, the day of attack had to be the day of ceasefire since the Trilateral Contact Group agreed on a ceasefire during Christmas and New Year starting from midnight of 23 December 2015. But on 22 December 2015 the Ukrainian Ministry of Defense reported that heavy armed DNR group had entered the grey-zone village of Kominternove near the strategic port of Mariupol city. The presence of armed "DPR" members in the village was confirmed by OSCE mission that had been denied the access to that village [11]. Indeed, the presence of DNR armed group in the grey zone may be regarded as a kind of retaliation for Ukrainian Force`s operation in Pavlopil, which for a few moths was within the grey zone, and for gaining the control over seven villages in December [19]; however, the great escalation before and during the cyber-attack was also observed in Luhansk region. While approaching "LPR"-controlled Kalynove, "the SMM observed one rocket being fired from a multiple-launch rocket system (MLRS, BM-21 Grad, 122mm) […]. The SMM assessed that the rocket it saw had been fired in a north-westerly direction. This was the second time in less than a week that the SMM observed MLRS being used in Kalynove" [11].

Philip Breedlove, NATO`s Supreme Allied Commander, also noticed Russian support of proxies in eastern Ukraine and multiple convoys into Donbas, marked as humanitarian support [7]. It is hardly believable that increasing "humanitarian support", entering the grey zone by DNR a day before the cyber-attack and using prohibited weapons in Luhansk region are simple coincidence that has nothing to do with the committed cyber-attack on the day of ceasefire. In contrast, it is reasonable to conclude that these activities were carried out in order to reinforce the positions of armed groups; and that the cyber-attack could have played a key role in weakening political situation and military power of Ukraine.

Finally, a situation around the Crimean Peninsula may be considered as a catalyst for the 2015 blackout. Shortly after the annexation of Crimea, local authorities started the process of nationalization of Ukrainian-owned energy companies. A group of unidentified people attacked power lines supplying electricity from Ukraine to Crimea. Though pro-Ukrainian activists of so-called "Civil Blockade of Crimea" and Crimean Tatars prevented repair of pylons that blown up on 22 November 2015, they denied their responsibility for the attack. In any case, the 2015 cyber-attack might be the direct consequence of and revenge for the Crimean blackout [6].

Shortly after the first attack against a power grid system in 2015, the Security Service of Ukraine declared that Russian special services were behind this attack [15].

On 17 December 2016, the Ukrainian critical infrastructure was again attacked. In comparison with the 2015 cyber-attack, the 2016 cyber-attack on the Ukrainian power grid had smaller scale and impacts. However, in terms of intentions, the 2016 attack was more sophisticated and could lead to greater effects [5, pp. 2, 13-15]. The attack resulted in outrages in certain districts of the capital city and lasted one hour fifteen minutes.

There is also a difference in chosen target. In 2015, cyber-attack was launched against electric distribution system. In worst scenario, it could potentially cause outrages within limited geographical areas. The attack on a transmission system, which took place in 2016, in contrast, could promptly result in uncontrolled cascading outages in power systems. And then, cascading outrages can impact large populations within a wider geographic area and seriously damage components of power system that are impossible or difficult to replace [10]. According to Dragons Inc. experts, "CRASHOVERRIDE evolves from an immediate disruption event to a delayed potential physical destruction attack. […], the disruption of transmission through remote terminal unit (RTU) manipulation is a precursor to a final, more serious stage: inhibiting protection systems so when service is restored, the target circuit is no longer safe and is subject to damage” [5, p. 9].

Researchers of the Dragon firm also concluded that the aim of using CrashOverride was not to cause a short-time blackout but to create a lasting destructive scenario that could have led to cascading outrages for weeks or even months. This fact puts this blackout malware in one line with the most dangerous codes that have been ever employed to destroy physical components of industrial systems (for instance, the Stuxnet malware in late 2009 or early 2010 destroyed one-fifth of Iran`s nuclear enrichment centrifuges, and the Triton malware that was designed to affect an oil refinery in a Saudi Arabian in 2017) [14].

If one takes a look at the armed conflict in Donbas, he or she will find out that at the day of the 2016 attack a conflict greatly escalated. Increasing number of shellings was reported by the press-center of Anti-Terroristic Center of Ukraine on 17 December [21], while on 18 December non-governmental military groups started an offensive attack to change the position of Ukrainian militaries [23]. The report of SMM OSCE confirms the escalation of situation and gives some important data: “The SMM recorded more ceasefire violations in Donetsk region on both 17 and 18 December, including some 700 and 2,900 explosions respectively, compared with some 100 explosions in the previous reporting period” [12]. As in case with the 2015 attack, such intensification at the day of cyber-attack and after does not look accidental and may be considered as a part of integral operation against Ukraine.

Interestingly, CrashOverride`s dangerous capabilities can be used to launch automated power-killing cyber-attacks against other states and types of critical infrastructure water facilities, transportation, or gas lines. For this, the code should be rewritten and adapted to protocols of a particular state. “The way it is built and designed and run makes it looks like it was meant to be used multiple times. And not just in Ukraine”, said Robert M. Lee, the founder of the security firm Dragos and a former intelligence analyst focused on critical infrastructure security [3].

Although investigations of the 2015 and 2016 cyber-attacks have been carried out by state and private agents (Ukrainian and foreign), these attacks did not attain enough attention. Partially, it is due to geographic limitation of attacks that were directed exclusively against Ukrainian infrastructure. The absence of international body with the power to establish attribution and make authoritative findings also contributed to international ignorance. At the same time, there is a reason to believe that Ukraine was only an ‘experimental laboratory’ for cyber-attacks and that next time hackers` main target for successful destructive attacks may be located in another country.

Understanding the potential effects and danger of cyber-attacks gave a strong impulse for increasing public attribution of cyber-attacks by states. In 2017, WannaCry cyber-attack was attributed to North Korea and the Lazarus Group that allegedly acted on behalf of North Korean government. In 2018, cyber-attack campaign of APT 10 group targeting intellectual property and sensitive commercial data in Europe, Asia and the US was publicly attributed to the Chinese government. The NotPetya cyber-attack is the most prominent example here. In 2018, the United Kingdom, Denmark, the United States, Canada and Australia publicly attributed the NotPetya cyber-attack to the Russian government. The UK was the very first state to declare that “the Russian Government, specifically the Russian military, was responsible for the destructive NotPetya cyber-attack of June 2017” [9]. New Zealand, Norway, Lithuania, Estonia, Latvia, Sweden, and Finland joined them by issuing statements of support. The White House also recognized that NotPetya “… was part of the Kremlin’s ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia’s involvement in the ongoing conflict [17]”.

The European Union as a result of blooming cyber-attacks adopted a new framework on May 17, 2019, that foresees imposition of targeted restricted sanctions for cyber-attacks constituting external threat to the EU or its members. For this, a cyber-attack should have a significant effect and be launched from the outside of EU. Council`s Decision covers not only cyber-attacks ‘directed’ or ‘under control’ but also cyber-attacks ‘supported’ by natural persons or legal entities [2].

Conclusions and suggestions. Attribution of cyber-attacks against object of critical infrastructure merits a special consideration, especially when cyber-attack committed in war time. These objects are of extreme importance for people, and cyber-attack against electricity and water grids could lead to humanitarian crises, millions of death and collapse of a whole state.

The 2015 and 2016 attacks have demonstrated the near reality of cyber wars and thus the possibility of commission of international crimes via cyberspace. Without appropriate attribution, it is impossible to take legal actions and there is a high risk of wrong attribution with the subsequent state reaction amounting to internationally wrongful act. These attacks also show the importance of both governmental and nongovernmental attribution. Decentralized nongovernmental attribution is normally much faster that those done by a governmental agencies. Moreover, it is more detailed and contains information that may enable industrial security professionals from all over the world to defend industrial systems against future cyber-attacks. Governmental attribution also plays important role; however sometimes it could face various challenges at the political level.

From our perspective, creation of an independent body responsible for technical attribution may be a possible solution for deterrence and responding to dangerous malicious cyber-attacks. A high confidence exists that states are involved in commission of the most serious cyber-attacks owing to the resources used by hackers and the level of sophistication. Therefore, international community need a special technical body for technical attribution, the outcomes of which could be used for invocation of state responsibility. Only state responsibility may be that very means for decreasing the number of cyber-attacks.

References

1. Bassiouni M. Cherif (1996). International Crimes: Jus cogens and obligation erga omnes, Law and Contemporary Problems, vol 59 (4). P. 63-74.
2. Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, ST/7299/2019/INIT, OJ L 129I , 17.5.2019. URL: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32019D0797.
3. ‘Crash Override’: The Malware That Took Down a Power Grid. URL: https://www.wired.com/story/crash-override-malware/.
4. CrashOverride: Analysis of the Threat to Electric Grid Operations. URL: https://dragos.com/wp-content/uploads/CrashOverride-01.pdf.
5. CrashOverride: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack. By Joe Slowik, Dragos Inc. URL: https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf.
6. Crimea without power from Ukraine after electricity pylons ‘blown up’. URL: https://www.reuters.com/article/us-ukraine-crisis-crimea-electricity-idUSKCN0TB04920151122.
7. Emmott, R. Russia unlikely to meet Ukraine peace deal deadline, NATO says. Reuters. URL: https://www.reuters.com/article/us-ukraine-crisis-nato-idUSKBN0TL1FA20151202.
8. Foreign Office Minister condemns Russia for NotPetya attacks (15 February 2018). URL: https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks.
9. How an Entire Nation Became Russia`s Test Lab for Cyberwar. URL: https://www.wired.com/story/russian-hackers-attack-ukraine/.
10. How do you say Ground Hog Day in Ukrainian? URL: https://ics.sans.org/blog/2016/12/20/how-do-you-say-ground-hog-day-in-ukrainian.
11. Latest from OSCE Special Monitoring Mission (SMM) to Ukraine, based on information received as of 19:30hrs, 23 December 2015. URL: https://www.osce.org/ukraine-smm/212656.
12. Latest from OSCE Special Monitoring Mission (SMM) to Ukraine, based on information received as of 19:30, 18 December 2016. URL: https://www.osce.org/ukraine-smm/290026#_ftnref1.
13. Military and Paramilitary Activities in und against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986. URL: http://www.icj-cij.org/files/case-related/70/070–19860627-JUD-01–00-EN.pdf.
14. New Clues Show How Russia’s Grid Hackers Aimed for Physical Destruction. URL: https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/.

15. SBU Press Center, Russian Hackers Plan Energy Subversion in Ukraine, Ukrinform, December 28, 2018. URL: http://www.ukrinform.net/rubric-crime/1937899-russian-hackers-plan-energy-subversion-in-ukraine.html.
16. Schmitt, M. N., & NATO Cooperative Cyber Defence Centre of Excellence. (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. 598 p.
17. Statement from the Press Secretary, February 15, 2018. URL: https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/.
18. TLP: White Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case March 18, 2016. URL: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.
19. Ukraine clashes signal end of truce (5 January 2016). URL: https://www.euractiv.com/section/europe-s-east/news/ukraine-clashes-signal-end-of-truce/.
20. Ukraine sees Russian hand in cyber attacks on power grid. URL: https://www.reuters.com/article/us-ukraine-cybersecurity/ukraine-sees-russian-hand-in-cyber-attacks-on-power-grid-idUSKCN0VL18E.
21. Summary of ATC`s press-center dating on morning of 17 December 2016. URL: http://www.mil.gov.ua/news/2016/12/17/zvedennya-pres-czentru-shtabu-ato-stanom-na-ranok-17-grudnya-2016-roku/ [in Ukrainian].
22. Poroshenko: State agencies suffered from 6.5 cyber-attacks, RF is involved in some of them. URL: https://www.ukrinform.ua/rubric-polytics/2148600-porosenko-derzstrukturi-zaznali-65-tisaci-kiberatak-do-deakih-pricetna-rf.html [in Ukrainian].
23. ATC forces repulsed the enemy`s attack in the Donetsk direction. URL: http://www.mil.gov.ua/news/2016/12/18/sili-ato-vidbili-nastup-voroga-na-doneczkomu-napryamku/ [in Ukrainian].

Список використаної літератури

1. Bassiouni M. Cherif (1996). International Crimes: Jus cogens and obligation erga omnes, Law and Contemporary Problems, vol 59(4). P. 63-74.
2. Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, ST/7299/2019/INIT, OJ L 129I , 17.5.2019. URL: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32019D0797.
3. ‘Crash Override’: The Malware That Took Down a Power Grid. URL: https://www.wired.com/story/crash-override-malware/
4. CrashOverride: Analysis of the Threat to Electric Grid Operations. URL: https://dragos.com/wp-content/uploads/CrashOverride-01.pdf.
5. CrashOverride: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack. By Joe Slowik, Dragos Inc. URL: https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf.
6. Crimea without power from Ukraine after electricity pylons ‘blown up’. URL: https://www.reuters.com/article/us-ukraine-crisis-crimea-electricity-idUSKCN0TB04920151122.
7. Emmott, R. Russia unlikely to meet Ukraine peace deal deadline, NATO says. Reuters. URL: https://www.reuters.com/article/us-ukraine-crisis-nato-idUSKBN0TL1FA20151202.
8. Foreign Office Minister condemns Russia for NotPetya attacks (15 February 2018). URL: https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks.
9. How an Entire Nation Became Russia`s Test Lab for Cyberwar. URL: https://www.wired.com/story/russian-hackers-attack-ukraine/.
10. How do you say Ground Hog Day in Ukrainian? URL: https://ics.sans.org/blog/2016/12/20/how-do-you-say-ground-hog-day-in-ukrainian.
11. Latest from OSCE Special Monitoring Mission (SMM) to Ukraine, based on information received as of 19:30hrs, 23 December 2015. URL: https://www.osce.org/ukraine-smm/212656.
12. Latest from OSCE Special Monitoring Mission (SMM) to Ukraine, based on information received as of 19:30, 18 December 2016. URL: https://www.osce.org/ukraine-smm/290026#_ftnref1.
13. Military and Paramilitary Activities in und against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986. URL: http://www.icj-cij.org/files/case-related/70/070–19860627-JUD-01–00-EN.pdf.
14. New Clues Show How Russia’s Grid Hackers Aimed for Physical Destruction. URL: https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/
15. SBU Press Center, Russian Hackers Plan Energy Subversion in Ukraine, Ukrinform, December 28, 2018. URL: http://www.ukrinform.net/rubric-crime/1937899-russian-hackers-plan-energy-subversion-in-ukraine.html.
16. Schmitt, M. N., & NATO Cooperative Cyber Defence Centre of Excellence. (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. 598 p.
17. Statement from the Press Secretary, February 15, 2018. URL: https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/.
18. TLP: White Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case March 18, 2016. URL: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

19. Ukraine clashes signal end of truce (5 January 2016). URL: https://www.euractiv.com/section/europe-s-east/news/ukraine-clashes-signal-end-of-truce/.
20. Ukraine sees Russian hand in cyber attacks on power grid. URL: https://www.reuters.com/article/us-ukraine-cybersecurity/ukraine-sees-russian-hand-in-cyber-attacks-on-power-grid-idUSKCN0VL18E.
21. Зведення прес-центру штабу АТО станом на 17 грудня 2016 року. URL: http://www.mil.gov.ua/news/2016/12/17/zvedennya-pres-czentru-shtabu-ato-stanom-na-ranok-17-grudnya-2016-roku/
22. Порошенко: Держструктури зазнали 6,5 тисячі кібератак, до деяких причетна РФ. URL: https://www.ukrinform.ua/rubric-polytics/2148600-porosenko-derzstrukturi-zaznali-65-tisaci-kiberatak-do-deakih-pricetna-rf.html.
23. Сили АТО відбили наступ ворога на Донецькому напрямку. URL: http://www.mil.gov.ua/news/2016/12/18/sili-ato-vidbili-nastup-voroga-na-doneczkomu-napryamku/.

Стаття надійшла 15.09.2020 р.

В. В. Музика, аспірантка
Національний університет «Одеська юридична академія»
Кафедра міжнародного та європейського права
Фонтанська дорога, 23, Одеса, 65009, Україна
e-mail: viktoriiamuzyka@gmail.com

АНАЛІЗ КІБЕРАТАК ПРОТИ СИСТЕМ ЕНЕРГОПОСТАЧАННЯ УКРАЇНИ В КОНТЕКСТІ ЗБРОЙНОГО КОНФЛІКТУ НА ДОНБАСІ

Резюме

Стаття містить аналіз кібератак 2015 та 2016 рр. проти систем енергопостачання України в контексті збройного конфлікту на території Донбасу. Робиться висновок про їх зв'язок зі збройним конфліктом та здійснення цих атак з ціллю дестабілізації ситуації на території України і зміни військових позицій урядових сил. Підставою для такого висновку є фактичний контекст, який враховує військові дії на території Сходу України, їх активізацію до та в момент здійснення кібератак. При цьому, використовувались як урядові дані, що знаходяться у відкритому доступі, так і відомості моніторингової місії ОБСЄ.

В статті підкреслюється важливість атрибуції кібератак проти об'єктів критичної інфраструктури, які відіграють ключову роль у забезпеченні функціонування суспільства та держави в цілому. Завдання шкоди таким об'єктам може призвести до негативних наслідків – гуманітарної кризи, серйозних порушень прав людини тощо, які особливо гостро постають в ході збройного конфлікту. У зв'язку з цим наголошується на необхідності створення незалежного міжнародного органу, який би здійснював технічну атрибуцію кібератак. Така пропозиція обумовлена тим, що наявна практика централізованої та децентралізованої атрибуцій кібератак не може вирішити проблему притягнення держав до відповідальності на основі тесту ефективного контролю.

Автор використовує приклад України для того, щоб показати реальну загрозу кібератак для систем енергопостачання та об'єктів критичної інфраструктури в цілому, а також можливі кінетичні наслідки, що матимуть місце при ігноруванні проблеми здійснення атрибуції.

Ключові слова: кібератака; атрибуція; атаки проти систем електропостачання України; промислові системи; критична інфраструктура.

В. В. Музыка, аспирантка
Национальный университет «Одесская юридическая академия»
Кафедра международного и европейского права
Фонтанская дорога, 23, Одесса, 65009, Украина
e-mail: viktoriiamuzyka@gmail.com

АНАЛИЗ КИБЕРАТАК ПРОТИВ СИСТЕМ ЭНЕРГОСНАБЖЕНИЯ УКРАИНЫ В КОНТЕКСТЕ ВООРУЖЕННОГО КОНФЛИКТА НА ДОНБАССЕ

Резюме

Статья содержит анализ кибератак 2015 и 2016 гг. против систем энергоснабжения Украины в контексте вооруженного конфликта на территории Донбасса. Делается вывод об их потенциальной роли в дестабилизации ситуации на территории Украины и попытке изменить военные позиции правительственных сил. Подчеркивается важность осуществления атрибуции кибератак против объектов критической инфраструктуры – особенно в ходе вооруженного конфликта, а также необходимости создания независимого международного органа, который бы осуществлял техническую атрибуцию.

Ключевые слова: кибератака; атрибуция; атаки против систем электроснабжения Украины; промышленные системы; критическая инфраструктура.