DOI 10.34054/bdc003

OPINION: «LEGAL ASYMMETRY» IN THE CONTEXT OF LIABILITY OF THE STATE AND STATE SPONSORED CYBER-ATTACKS ACTORS

Bulda Oksana
IT Lawyer

Promote Ukraine

Conference proceeding

Behind the Digital Curtain. Civil Society vs State Sponsored Cyber Attacks

Brussels - 25/06/2019

DOI 10.34054/bdc000

The globalized world is more and more confronted with the phenomenon of “hybrid war”, which poses a new type of threat based on a combination of military and non-military means such as cyber-attacks, mass disinformation campaigns and many others.

Cyber-attacks are particularly dangerous as they can hit the country’s strategic infrastructure, interrupt political processes and influence economic development. Therefore, hybrid war can destabilize and undermine entire societies. The increasingly widespread use of these new tactics, especially in combination, raises concerns about the adequacy of existing legal norms.

The legal framework for cyber security measures still has no definition of “hybrid war” and there is no unified legislation on the matter as well. However, the common understanding is that the main feature of this phenomenon is “legal asymmetry”, as hybrid adversaries, as a rule, deny their responsibility for hybrid operations and try to avoid legal consequences for their actions.

Despite the complexity of “hybrid war”, hybrid adversaries do not operate in a legal vacuum and that relevant domestic and international law norms must be applicable to their actions, although the question of attribution and hence accountability may raise difficulties. If, in the framework of “hybrid war”, a state resorts to the use of force against another state, the latter state is allowed to invoke the right to self-defense but in practice, hybrid adversaries avoid manifest use of force that would reach the required threshold for triggering application of the above norms, thereby creating a legal grey area.

The «legal asymmetry» problem arises from the fact that international law does not generally hold states responsible for the actions of non-state actors as in most cases of cyber-attacks, states don’t generally operate through formal state bodies. Instead, they use non-state actors who are less visible, more removed and offer plausible deniability. Thus, the liability will only be acknowledged if the

state either recognizes and adopts the conduct of the non-state actor as its own, which is unlikely to happen, or the state directs or controls the non-state actor. As a result, the chances that a state will ever be held publicly accountable for cyber-attacks under existing legal framework are quite low.

The delay in the enactment of laws, outdated legal norms, rapid technologies development, collision of legislation, limited scope of the law applicability and cybersecurity low awareness - all together make it much difficult to incorporate the sufficient legislation in order to bring to justice not only the state sponsored cyber-attacks actors but also to hold the state accountable for such actions.

Various considerations determine the creation of laws in different countries, so their promulgation depends on a multiplicity of factors; for example, political issues or other issues affecting local initiatives, or adherence to international agreements encouraging the same level of development for cross-border collaboration.

However, it is on account of these very conditions and characteristics that legislation is often postponed. The Budapest Convention has been in the ratification process for more than a decade.

Also, the evolution of technologyshould be considered; the development of standards may, therefore, fall far behind technological advances. Just as organizations continuously update their standards in response to evolving risks and new technologies, the law must be at the forefront when it comes to responding to present and emergent issues which may need to be regulated.

Perhaps the way to rectify this disparity between technological innovation and the enactment of appropriate legal measures, is to focus on regulating human behaviors, especially since technologies can become obsolete in a relatively short period. This may prove to be the most reliable way for

The «legal asymmetry» problem arises from the fact that international law does not generally hold states responsible for the actions of non-state actors

regulation to be effective, but it is also important to note that this could lead to rising tensions in the future. An example of this might be trying to regulate the use of social networks, which are not supported by legislative enactment.

Similarly, the absence of legislation or agreements on specific aspects of certain issues can undermine international collaboration, even within the same territory. Public and private sectors face a challenge when it comes to access the information for investigations, with implications for security, the right to privacy, and commercial interests, mainly of tech companies.

The aim is therefore to have legal measures in place for protection at various levels and in various spheres. To this end, legislators have also started to consider

the requirements necessary for security in their countries, including their capacity to respond to large-scale incidents, the protection of their critical infrastructure, their ability to collaborate with other countries, and even to consider the development of a security culture which can be implemented in society.

Considering all above mentioned, in order to make the legislation truly effective, there is a need to define the unified common rules based on international, regional or national agreements and cross-border countries cooperation considering not only the legal side of the problem but the technical as well.

Bibliography:

1. Council of Europe. (26 April 2018). Legal challenges related to the hybrid war and human rights obligations. Resolution 2217, Parliamentary Assembly, Committee on Legal Affairs and Human Rights. Available at https://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-EN.asp?FileID=24762&lang=EN

2. Payne, C., Finlay, L. (2019). International law cannot keep up with cyber-criminals. World Economic Forum. Available at https://www.weforum.org/agenda/2019/02/why-international-law-is-failing-to-keep-pace-with-technology-in-preventing-cyber-attacks/

3. Calam, M., Chinn, D., Porter, J. F., Noble, J. (2018). Asking the right questions to define government's role in cybersecurity. McKinsey&Company. Available at https://www.mckinsey.com/industries/public-sector/our-insights/asking-the-right-questions-to-define-governments-role-in-cybersecurity

4. Rikk, R. (2018). National Cyber Security Index 2018. e-Governance Academy. Available at https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf

5. Mendoza, M. A. (2017). Challenges and implications of cybersecurity legislation, Miguel Angel Mendoza. WeLiveSecurity. Available at https://www.welivesecurity.com/2017/03/13/challenges-implications-cybersecurity-legislation/

promoteukraine
promoteukraine
promoteukraine

Web: www.promoteukraine.org
Contact: info@promoteukraine.org

Promote Ukraine is a non-profit start-up. It is a politically and governmentally independent organization situated in Belgium. It consists of a thriving team of professionals who on pro bono basis seek to give voice to Ukrainian civil society in Europe and, in particular, throughout Belgium. We believe in European values such as civil rights, good governance and equal opportunities. Through connecting EU businesses and politicians with Ukrainian stakeholders, we facilitate the sharing of best practices between EU and Ukrainian partners with the goal to bring Ukraine closer to EU norms and values from a bottom-up perspective.