DDoS Cyber-Attacks from the Perspective of the Control over the Crime Theory in International Criminal Law: New Challenge, Established Solutions?

The subject of this project is the conduct involving **directing or launching distributed denial-of-service (hereinafter: "DDoS") cyber-attacks.** DDoS cyber-attacks are among the most prevalent forms of malicious operations on the Internet; they can be broadly defined as a collective and coordinated series of actions aimed at sending multiple communication requests to a target computer system or systems. It is important to note that, from the perspective of the substantive considerations planned for the second and third parts of the project, DDoS cyber-attacks are distinguished by the fact that they are carried out by multiple persons. In essence, the exercise of control over a "**botnet**" – an organised network of many unaware users – is a key element of the conduct in question, thereby enabling the effective execution of a cyber-attack.

Narrowing the scope of the study to DDoS cyber-attacks can be considered justified both in view of the legislative measures taken and the available statistical data. In 2011, the European Economic and Social Committee, in its opinion on the proposal for a directive of the European Parliament and of the Council on attacks against information systems, drew particular attention to cyber-attacks committed with the use of so-called botnets. As indicated in the recital 5 of the adopted Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems, there is evidence of a tendency towards increasingly dangerous and recurrent large-scale attacks and this tendency is accompanied by the development of increasingly sophisticated methods, such as the creation and use of so-called "botnets".

It should be noted that this position was included in the recitals of the directive adopted more than a decade ago, and since then there has been a clear and continuous upward trend in the occurrence of DDoS cyber-attacks. The latest statistics show that **in the first quarter of 2025, 20.5 million DDoS cyber-attacks were detected, representing an increase of 358% compared to the same period of the previous year** (Cloudflare, 2025).

It also seems obvious that the increase in cybercrime and the spread of DDoS cyber-attacks are influencing the way warfare is conducted in the 21st century. In this regard, it is worth quoting the position taken in the 2021 United Nations report, which states that **directing or launching cyber-attacks, for which a relevant *nexus* to a specific armed conflict can be established, may constitute acts prohibited under Article 8(2) of the Rome Statute of the International Criminal Court**, adopted in Rome on 17 July 1998 (hereinafter: "Rome Statute" or "Statute") (The Council of Advisers' Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare Prepared by the Permanent Mission of Liechtenstein to the United Nations, 2021; similarly Ambos, 2021; Freeman, 2023; Khan, 2023). A similar interpretation on this matter was presented in the latest document of the Office of the Prosecutor of the International Criminal Court of March 6, 2025 (Draft Policy on Cyber-Enabled Crimes Under the Rome Statute of March 6, 2025).

To clarify the area of the research, it should be emphasised that the study's main focus is not on all DDoS cyber-attacks, but **rather on those committed by multiple actors, reasonably expected to cause injury or death to persons, damage or destruction to objects, or serious disruptions to the functioning of critical infrastructure, used as part of international and internal armed conflicts.**

The significance of the project should be sought primarily in the fact that the implementation of the planned research tasks aims to fulfil two traditional functions of criminal law**: the preventive function and the retributive function.** The first of these looks to the future, justifying the research undertaken by the fact that clarifying the basis for criminal responsibility for the conduct involving directing or launching DDoS cyber-attacks is intended to have a preventive effect both on potential perpetrators of cyber-attacks and on the international community in general. Secondly, and equally crucial, is the necessity to put an end to impunity, whilst taking into account the legitimate expectations of victims of crime. The assumptions underlying both of these functions therefore reinforce the thesis that there is an urgent need **to establish precise grounds for criminal responsibility for participation in directing or launching DDoS cyber-attacks as part of international and internal armed conflicts (research objective of the project).**