mgr Przemysław Roguski

Summary of the doctoral thesis "Cyber operations in international law"

written under the direction of:
dr hab. Brygida Kuźniak

The aim of the doctoral dissertation "*Cyberoperations in the light of international law*" is to identify the standards of behaviour of States in cyberspace. The subject under consideration is the interpretation of the fundamental rights and obligations of States, resulting *inter alia* from the United Nations Charter and rules concerning international responsibility of states, in the specific conditions of cyberspace, understood as a space for processing and exchanging information created by ICT systems, along with links between them and relations with users. The main research problem is to determine whether the current norms of international law are sufficient to set the legal framework for actions of States in cyberspace, or whether there is a need to create a new catalogue of rights and obligations specific to cyberspace.

The indicated objective has been implemented by analizing the practice and *opinion iuris* of States, set out primarily in strategic documents and declarations of representatives of States given at an international level, as well as in documents and statements of international and intergovernmental organizations. Additionally, the analysis included the views of theoreticians international law and international courts and tribunals, with particular reference to the case law of the International Court of Justice.

The work is divided into four main parts. The first part of the work is devoted to defining key concepts for the research problem: cyberspace, cyber operations and cyber attacks. To better illustrate the presented technical aspects, current examples of cyberoperations are being discussed; the presented examples form at the same time the facts underlying the legal analysis made in subsequent chapters.

The second chapter deals with the problem of the application of international law in cyberspace. This issue is of fundamental importance for the further course of the dissertation, as it determines its normative framework: if the study showed that the cyberspace is perceived by the international community as a new, previously unregulated international space, then State operations in cyberspace would be covered by full freedom of action, up to the limit of explicitly prohibitive norms. However, the analysis of the practice and *opinio iuris* of States showed that states agree that international law is applicable in cyberspace without the need to create a separate legal instrument. The key to reaching agreement on this matter were the work of the Government Expert Group held in 2012-2013 and 2014-2015 under the aegis of the UN. The agreement, which was widely accepted among States, includes the application of the principles of the United Nations Charter in cyberspace, including in particular the prohibition of the use of force, the prohibition of intervention in internal affairs and the respect for States' territorial sovereignty, as well as the principles of international responsibility of States.

In the third part, the author discusses the legal qualification of cyber operations. This analysis concerns three main norms included in the United Nations Charter and international custom: the prohibition of the use of force, the prohibition of intervention in internal affairs, and the requirement to respect the territorial sovereignty of States. The first subsection is devoted to the determination whether cyber operations can constitute a use of force within the meaning of

art. 2(4) UN Charter. Furthermore, the discussion centers around the criteria which should be adopted in order to qualify a particular cyber operation as tantamount to the use of force. The second and third subchapter concern, respectively, the prohibition of intervention in internal affairs and the requirement to respect territorial sovereignty of States. Particular attention was paid to the question whether the territorial sovereignty of the State is merely a principle of international law from (which specific prohibitory rules, such as the prohibition of the use of force, arise), or whether the violation of territorial sovereignty is also regulated by a primary norm which prohibits the exercise of State authority within the territory of another State. Additionally, the legal qualification of *de minimis* violations as well as cyber-espionage are being analysed in the light of the above-mentioned standards.

The fourth chapter deals with the responsibility of States for internationally wrongful acts in cyberspace, including the responsibility for operations of non-state actors operating from the territory of a State. Particular attention is devoted to the problem of attributing cyber operations to a State in the light of the anonymity of cyberspace and the related technical difficulties in identifying the author of a given cyber operation. The author analyses whether there has developed a *lex specialis* in the field of cyber responsibility and whether modifying the applicable attribution rules and the standards of proof could be a viable solution to the so-called "attribution problem" as a postulate *de lege ferenda*.

The study closes with a summary and final evaluation of the research problem in light of the findings in the previous chapters. The author presents his conclusions as well as an assessment of the need to take further steps to clarify the interpretation of UN Charter norms and principles of responsibility of States in the context of cyberspace.

Przemysław Roguski

11.06.2018