REVIEWS AND ANNOTATIONS

Jozef Valuch, Daniel Bednár. Armed Conflicts and Cyber Threats as Challenges for International Law in the 21st Century. Bratislava: Wolters Kluwer SR, 2022, 268 p.

International security faces currently challenges that are more complex than ever before. Recently, security enviroment is rapidly changing. These changes occur in many fields of security environment. Specifically, their impact on security sphere perception is not only quantitative but mainly qualitative.

Firstly, with ongoing international and non-international armed conflicts in various parts of the world, new possible military alliances (or blocs) of states emerge. Due to the ongoing changes in international security, major superpowers seek at least informal allies from less developed countries. The balance of power within the international sphere faces therefore new developments, which have the possibility to shift with the current understanding of international security.

Secondly, new actors within the security environment have emerged. These subjects represent not only ongoing changes within the security sphere but also pose threats to national and international security. In particular, these new types of actors are by their nature usually not affiliated directly with the state. Indeed, they can be characterized as non-state actors. In this regard, of particular importance are private military and security companies (hereafter also as "PMSCs"), which emerged on the international scene approximately in the 1960s. Currently, these actors are of utmost importance for states and other subjects due to their role in ensuring security.

Thirdly, changes in security are connected to rapid technological development and in particular to the development of artificial intelligence. This is reflected for instance by new types of weapons, specifically by autonomous weapons. What is unique is that this type of weapon could potentially apply deadly force without human intervention in the decision-making process. As a result, in regard to international law, it raises numerous questions which should but also must be answered.

Lastly, international security can be viewed through the prism of various fields. Times when armed conflicts were fought only through ground, air or naval operations are gone. Currently, strategies to overcome adversaries rely also on cyber and even on space-related activities. Particularly, cyber threats can be regarded as serious security risks, because they have the potential to harm critical infrastructure within a state.

These issues demonstrate how vulnerable states and other actors are on the international scene when faced with the newest forms of security threats. However, from a legal point of view, international law has to address these challenges and cannot ignore them.

The presented publication deals with these issues and elaborates broadly on them. As the authors point out in the preface of the publication, international law in general seems not ready to address these social and technological developments. Frankly, these developments seem to occur too fast. On the other hand, there is a moral, social and legal need to apply already existing norms of international law. Nevertheless, this is not always the case. The authors of the reviewed publication have therefore appropriately chosen the topic. By highlighting these security-related issues, these topics will come to the fore for discussion. Although intellectually challenging, these topics have to be discussed not only among academics but especially among policymakers who have real decision-making authority.

The publication is logically divided into two parts. The first part of the publication deals with *Armed conflicts*. This part is also structured into three chapters. The first chapter deals with "Definition of terms".

Particularly, it clarifies "security" and related terms, such as international, collective or cyber security. It is important to mention that clarification of these terms is necessary to have a better under-

standing of the publication as such. For instance, this is reflected in the explanation of the difference between "international security" and "collective security" and according to the authors, the latter term is narrower than the former. Subsequently, threats to international security are analyzed. The authors rightly point out that international security is an interconnected system and therefore it is necessary to respond to them at the global, regional, and national level.

The second chapter within the first part of the publication deals with armed conflicts. Specifically, it covers an important phenomenon, namely the privatization of armed conflicts. Following that, authors devote their attention to private military and security companies. Thus, they critically examine this developing actor on the international scene. Importantly, there is an analysis related to the legal status of PMSC employees. Clearly, this analysis is directly related to International Humanitarian Law (hereafter also as "IHL"), since PMSC employees are mostly contracted for tasks within an area where an armed conflict occurs or possibly where it already occurred (post-conflict area). The authors correctly assume that from an IHL perspective, these persons will be mostly civilians. Besides, in some particular cases, they could legally be qualified as civilians accompanying armed forces. However, the situation concerning their legal qualification can become more blurred once these persons directly participate in hostilities. Their legal status has to be therefore determined on a case-by-case basis, depending upon the nature of their activities, as the authors of the publication state.

The third chapter of the first part deals with peacekeeping operations and its legal implications. As the authors correctly state, the idea of peacekeeping remains relevant in the 21st century. Nevertheless, peacekeeping in its current form faces various challenges. Specifically, according to the authors, current peacekeeping operations require qualitatively different armed forces. These should consist of interoperable units and individuals qualified in joint operations. Peacekeeping in its current form seems to need a considerable change. This change should be qualitative and should be based on past successes and failures. As the authors point out, peacekeeping operations achieve often small "victories", such as preventing day-to-day violence. Nevertheless, many times these operations only assisted in preserving already long-lasting conflicts. Consequently, the emphasis should not only be primarily put on peacekeeping but also on peacebuilding, since long-lasting peace requires much more than just prevention of conflict. It requires cooperation and capacity-building.

The second part of the book focuses on *Cyber threats*. It has four chapters, which introduce the topic in a logical structure.

The first chapter aims to define terms important to cybersecurity. It generally introduces various forms of cyber threats. The authors stress that cyber threats have often different origins. They can come from simpler subjects, such as hackers, but also from criminal and terrorist organizations and even from states *per se*. The multiplicity of actors thus often causes complex problems, and it is for instance often hard to distinguish between hackers and foreign intelligence services, which from an international law point of view constitute organs of the state *par excellence*. Moreover, the authors mention the term cyberspace and provide doctrinal, governmental and institutional definitions. Importantly, cyberspace differs from "the previously known and used levels of space". Its global dimension blurs the borders between states and operates regardless of the political system. Following that, another basic term introduced is the "cyber attack". This term has an important international legal implications, since it has relevance to IHL as well as to the international law regulating use of force in international relations. Briefly, a cyber attack can be characterized as a cyber operation with negative and destructive consequences. The authors also mention an important point, mainly that not all cyber operations have to be considered as cyber attacks. The distinguishing feature lies in the use of violence against a target.

The next chapter concerns cyberspace and international law. By showing practical examples, the authors demonstrate that international law does apply in cyberspace. Despite that, the main issue is how to apply international law within the given sphere. The authors mention that general rules of international law are particularly relevant. However, they also highlight some more specific concepts, such as the concept of due diligence, or the duty of vigilance. They refer for instance to the famous

Corfu Chanel case and apply the conclusions of the court to the given topic. The principle of due dilligence can therefore be inferred from rules of general international law as well as case law of international judicial institutions, yet its application is highly relevant for the assessment of cybersecurity law issues. Besides, an important part of the given chapter analyses use of force in cyberspace. Importantly, a highly relevant issue in this matter concerns the situation when cyber-operation (cyber attack) reaches the threshold of an *armed attack*. If it does, it constitutes the use of force, which is generally prohibited under international law. Subsequently, if there is an armed attack, the attacked subject has a legal right to stop or avert the attack, namely by exercising the right of self-defense. The complexities of these issues are broadly discussed within the given chapter, which gives the reader a fundamental understanding of the issues at hand.

Another issue analyzed within the publication is cyber espionage. Following the rapid advancement of technology, the multiplicity of actors capable of cyber operations and the current state of international politics, this is a highly relevant topic. Interestingly, as the authors state, cyber espionage *per se* does not violate the general rules of international law. Nevertheless, the manner in which it is carried out may amount to such violation. Moreover, cyber espionage differs from traditional methods of espionage, as the authors observe. It can be distinguished on the basis of the speed and the volume of the obtained information. In addition, there is no need for physical presence of the spy to carry out an act of cyber espionage in the given area. Everything can be done remotely and thus from a safe distance. Besides, the authors are particularly concerned with the issue of the attribution of cyber operations. This is a particularly problematic and sensitive issue. However, as the authors demonstrate, there are few important initiatives, which address this issue. For instance, Microsoft came out with an idea of creating an *International Cyberattack Attribution Organization*. Subsequently, the authors introduce further proposals and critically examine them. At the end of the given chapter, they assume that given the specifics of cyberspace, sooner or later the international community will witness the creation of an entity entrusted with coordination of individual states at the international level with the aim of preventing disputes related to cyberspace between states.

The last two chapters of the second part concern cases of misuse of cyberspace and measures of selected organizations. Briefly, these two chapters are based on empirical understanding. They analyze cases of some selected cyber operations. Based on the analyzed situations, the authors make an important conclusion. Cyber operations can happen in support of an ongoing armed conflict. This also means that IHL (in such cases) does apply to cyber operations.

The last chapter specifically relates to the practice of two regional international organizations, mainly the North Atlantic Treaty Organization (hereafter as "NATO") and the Organization for Security and Cooperation in Europe. The authors analyze selected activities and efforts of these organizations. Particularly, worth mentioning are the conclusions of the NATO Wales Summit in 2014, where NATO recognized that international law does apply in cyberspace. Subsequently, cyberspace was declared an operational domain by NATO. As a result, cyber defense currently constitutes for NATO a core collective defense mission.

To conclude, the authors provide a well and logically-structured book, which allows readers to follow a step-by-step approach as they familiarize themselves with the content of the publication. The publication is aimed for the scientific community, but it will be particularly meaningful to legal professionals, especially those working in governmental or institutional environments. The publication has a solid theoretical basis, which is supplemented with practical examples. The publication is also appropriately timed since many important changes in the security environment are ongoing. In fact, it is a book worth reading, if one wants to know more about current challenging times.

František Tóth*

* JUDr. František Tóth, PhD. Candidate, Faculty of Law, Palacký University in Olomouc, Czech Republic. ORCID: 0009-0005-6123-8500.