Book Review

BUCHAN, RUSSELL. CYBER ESPIONAGE AND INTERNATIONAL LAW. OXFORD: HART PUBLISHING, 2019.

Gills Vilar Lopes [*]
André Lucas Alcântara da Silva [**]

In *Cyber Espionage and International Law*, Russell Buchan seeks to understand not only the Cyber Espionage limits but also its real scope in international relations. It consists of a brief introduction, eight chapters and a conclusion, which summarize his position on how Cyber Espionage activities should be interpreted in the light of the existing set of norms in force within the scope of international society.

The author is an International Law lecturer at University of Sheffield School of Law, England, and supervises research in the areas of International Security and Peace, Public International Law and Cybersecurity, in addition to composing the editorial board of the *Force Employment in International Law* journal.

At an international level, how can one legally limit an ancient activity (GONÇALVES, 2018) such as Espionage, and, more specifically, its cyber version, which has existed for decades (BESSA, 2014, p. 49)? This is certainly a problem addressed by current lawyers and researchers, especially after the impacts of the revelations on the digital information capture system carried out by a consortium of English-speaking countries (AFP, 2016).

If, currently, there is no international treaty on the subject - and apparently this state of affairs will remain ceteris paribus — there have been many attempts to standardize or apply legal analogies to strategic activities in cyberspace, such as the famous *Tallinn Manual 2.0*.

In the first chapter, Buchan defines the concept of Cyber Espionage as a non-consensual cyber operation designed to break into computers or systems to copy confidential data under the control of another actor. Then, he details the parts that make up such a definition, seeking to delimit the main object of his work. In other words, in the scope of the Cyber Espionage activity, there is no need to talk about (i) public, (ii) confidential and consensual or (iii) outside the cyberspace data collection. At this point, the difference between a Cyber Espionage action and a cyber-attack is highlighted. While the first seeks exclusively to collect or copy the protected data — in the Intelligence

* Professor de Relações Internacionais da Universidade da Força Aérea (UNIFA). Doutor em Ciência Política pela UFPE. Pesquisador da Rede CTIDC/Pró-Defesa IV (Capes)

** Oficial Engenheiro da Força Aérea Brasileira (FAB). Mestrado em Ciências Aeroespaciais pela Universidade da Força Aérea (UNIFA). Pesquisador da RedeCTIDC/Pró-Defesa IV (Capes/MD).

jargon, access to denied data —, the later affects the availability and integrity of the information accessed.

Also, Buchan describes two types of cyber espionage throughout his work: political and economic. From a historical point of view — and, to a certain extent, from a theoretical and realistic analysis of international politics — the author seeks to understand the role played by States in the current world order, which seek to protect national security information and, at the same time, monitor the actions of their potential enemies. When this monitoring consists of the collection of confidential information of a political, strategic and / or military nature, through cyber resources, then it is characterized as Political Cyber Espionage.

With the intensification of the globalization process in the post-Cold War period, States started to assume the economic sector as an integral part of national security (BUZAN; WÆVER; WILDE, 1998). In this scenario, States begin to monitor foreign companies in order to obtain secret commercial information and pass it on to national organizations. Such action, when performed in cyberspace, characterizes Economic Cyber Espionage. Buchan recognizes that both types of espionage are currently practiced by States, private institutions, independent organizations and even individuals. However, his work is dedicated exclusively to cyber espionage activities carried out by States in times of peace, analyzing the legality of such actions according to the framework of international law.

Chapter two assesses the influence of cyber espionage on the process of maintaining international peace and security. From the Political Espionage point of view, we can say that several thinkers already justify this practice, based on the realistic theory of Thomas Hobbes, that is, for them, in view of the existing international anarchy, stability is only achieved if there is a balance of power between the States to be provided also by the Intelligence Activity, in which the States would be able to obtain information from each other. For these thinkers, the restriction or prohibition of the activity of Political Espionage would be harmful to the promotion of the world order. According to Buchan, international society opposes defenders of Political Espionage, stating that such thinking has not been able to avoid conflicts throughout history. From the perspective of international society, the practice of this type of espionage inhibits cooperation between States and directly threatens world stability. In the case of Economic Espionage, the view of the international society is that such practice generates costs for the harmed countries, increasing unfair competition between them. Furthermore, such a practice would be a direct assault on the fundamental values defended by the international community. Therefore, the author shows that the increasing use of cyberspace enhances the practices of Political and Economic Espionage, making it urgent to develop standards — even if soft law — capable of restricting or even prohibiting such actions.

The next chapter deals with the practice of cyber espionage under the perspective of the principles of international law of

territorial sovereignty, non-intervention and the prohibition of the use of force — all of which, moreover, are confirmed in articles 1 and 4 of the *Federal Constitution of Brazil*. Territorial sovereignty gives States the right to control the flow of entry and exit into their territory and the right to exercise their own governmental functions. For many, such a right could not be applied within the scope of actions in cyberspace since the data and information that is shared therein are not delimited by a territory. In the author's view, cyberspace cannot be interpreted as something disconnected from the physical world; it is, therefore, the object of analysis for the application of international law. For Buchan, States exercise territorial sovereignty over the entire cyber infrastructure present in their territory. Given this perspective, the practice of cyber espionage that targets an infrastructure located outside the domains of its Country violates the territorial sovereignty of the affected Country. However, if a Country stores its data in an infrastructure residing in another nation, it cannot claim the principle of territorial sovereignty, if its data is collected by the nation that stores it. Regarding the right to exercise government functions, the understanding is that Cyber Espionage does not violate it, but this position has changed, especially after the disclosures made by Edward Snowden in 2013. At that time, for example, target countries, including Brazil, positioned themselves saying that such action influenced their governmental actions and, therefore, would violate the principle of territorial sovereignty. Buchan concludes the chapter by pointing out that Cyber Espionage cannot characterize a violation of the principle of nonintervention (due to the absence of the coercive factor), as well as the principle of the prohibition of the use of force (since Cyber Espionage is dedicated only to collect data and does not produce physical damage).

In chapter four, the author assesses the application of consular and diplomatic laws within the scope of Cyber Espionage activities. The devices referenced by Buchan are those described in the Vienna Convention on Diplomatic Relations (VCDR), 1961, and the Vienna Convention on Consular Relations (VCCR), 1963. Even though they were created decades ago, and obviously do not include actions in the cyberspace, the author believes in the possibility of evaluating cyber espionage based on some important points of the conventions themselves. One of them is the principle of the inviolability of facilities, properties, files, documents, and correspondence related to the diplomatic mission. While the State that receives diplomatic missions from another nation pledges to guarantee such inviolability, the State that sends its representatives pledges not to use them as a means for espionage actions (Articles 22 of the VCDR and 31 of the VCCR). In Buchan's view, this concept can be extended to the actions of Cyber Espionage, protecting both States from possible damage caused by improper access to confidential information. As it turns out, there is a specific situation in which the principle of diplomatic inviolability could be breached: armed attack, according to Article 51 from the Charter of the United Nations, practiced by the consular mission. Such a situation would allow the receiving State to take

necessary actions to stop the attack, including cyber espionage activities. This is a topic that is debated in the specialized literature. But, in the void of international law on specific rules for the case, here we bring this externalized concern from Buchan by a document from the French Ministry of Defense, which states that the country "reserves the right to respond to any cyber operation that constitutes a violation of the international law in which they are victim" (FRANCE, [2019], p. 6, free translation). As can be seen, in the silence of international treaties on cyber operations, the government of a Country states that a cyber attack, depending on its damage, can be considered not only a transgression of an international law, but, as such, deserving military retaliation. An interesting point to be considered later, would be to know to what extent an action of Cyber Espionage, as defined in the inaugural chapter of the work under review, can, even if not intentionally, cause a cyber attack.

The fifth chapter introduces the discussion around cyber espionage against individuals and how such actions can violate international human rights law. The author delimits his analysis under the scope of the International Covenant on Civil and Political Rights (ICCPR), 1966, and the European Convention on Human Rights (ECHR), 1950. As for the right to privacy, both documents are forceful about the subject matter. The interpretation is that the cyber privacy of individuals must be preserved and therefore protected from Political or Economic Cyber Espionage. Buchan stresses that the right to privacy, like any right, is not absolute and, in legally exceptional situations, could be violated by the state. In addition, cyber espionage actions in these cases must be proportionate to the desired objective, generating the least possible impact on individual rights.

Then, the author assesses how the World Trade Organization (WTO) can collaborate in the fight against Economic Cyber Espionage. The WTO has a set of rules and treaties that subordinate its signatory countries. Among them, Buchan highlights two instruments that, *a priori*, could be useful in the process of restricting / prohibiting the practices of Economic Espionage. The first is Article 10 *bis* from the 1967 Paris Convention, which prohibits any act that constitutes unfair competition. The second would be Article 39.2 from the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), 1994, which seeks to protect confidential information from the acquisition, disclosure, and unauthorized use of intellectual property. However, the application of such rules in the context of the central theme of the work hereby analyzed is not a consensus among scholars, and international law remains, even if in analogy, vague in relation to Cyber Espionage.

Chapter seven assesses, within the scope of customary international law, the existence of exceptions that would allow the practice of political cyber espionage. Buchan explains that this Law is formed by general practices that are accepted as law, i.e., by custom. Therefore, international jurists understand that, even violating the principle of territorial sovereignty and

diplomatic agreements, the practice of this activity could be interpreted as legal, based on the custom of the States over the years. The author recognizes that Political Espionage is seen as an important national security resource for most States, which practice it even though they are aware of the restrictions imposed by international law. However, Buchan opposes the thought that the practice of espionage would be able to develop exceptions in customary international law, since it is exercised in secret.

In the eighth and final chapter of the book, the author devotes himself to analyzing Cyber Espionage from the perspective of the doctrines of Self-Defense and Necessity, since they are often used by States to justify their acts of espionage. The first is defined in Article 51 from United Nations Charter and can be used to justify cyber espionage in situations of current or imminent an armed attack threat. In addition, the spying action must be characterized as necessary (last resort) and proportional. The doctrine of Necessity, in turn, is established within the scope of customary international law and can justify espionage actions under the pretext that an essential state interest is threatened by grave danger.

Finally, the author concludes the work by reaffirming that the practices of Political and Economic Cyber Espionage are harmful to the maintenance of world peace and security, in addition to violating rules and principles of international law. Furthermore, he reinforces his opinion that society should endeavor to develop specific rules and laws capable of expressly prohibiting Espionage actions. Despite this need, the author recognizes that there are instruments in international law capable of limiting and inhibiting this practice from States, such as: the principle of territorial sovereignty; International Human Rights Law; diplomatic and consular conventions; and the treaties governing the commercial relations of WTO signatory States.

Buchan has a broad theoretical framework supported by works ranging from traditional to the most recent publications, such as the *Tallinn Manual 2.0*, written by almost 100 experts in international law and published by the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defense Centre of Excellence (CCDCOE, 2017). Cyber Espionage and International Law exemplifies the application of international laws in the scope of Espionage, as well as analyzes numerous facts, from the Cold War period to the present day.

Thus, Buchan's work is relevant today because Brazilian government has been making efforts, especially in the last decade, to guarantee its Sovereignty and national security in cyberspace. Within the Intelligence scope, Brazil points to espionage and cyber-attacks as two of the main current threats (BRAZIL, 2016), in addition, it views cyber espionage as a growing problem worldwide (BRAZIL, 2017). Therefore, recognizing how international laws address cyber espionage can collaborate in the maturity process of national laws, which seek to establish principles, guarantees and duties for users and providers of network services, such as the Civil Rights Framework for the Internet

in Brazil and the General Protection Law
Personal Data (LGPD).

References

AFP. UE e Estados Unidos lançam acordo para proteger a privacidade na internet. UOL, Bruxelas, 12 July 2016. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2016/07/12/ue-e-estados-unidos-lancam-acordo-para-proteger-a-privacidade-na-internet.htm. Acesso em: 27 July 2020.

BESSA, Jorge. *O escândalo da espionagem no Brasil*. Brasília: Thesaurus, 2014.

BRASIL. Decreto nº 8.793. Política Nacional de Inteligência. *Diário Oficial da União*, Brasília, DF, 30 de junho de 2016. Section 1, p. 5-7. Disponível em: http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=30/06/2016&jornal=1&pagina=5&totalArquivos=112. Acesso em: 4 July 2020.

_____ Decreto s/n, de 15 de dezembro de 2017. Aprova a Estratégia Nacional de Inteligência. *Diário Oficial da União*: seção 1, Brasília, DF, 18 dez. 2017. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=18/12/2017&jornal=515&pagina=36&totalArquivos=208. Acesso em: 31 Oct. 2020.

BUZAN, Barry; WÆVER, Ole; WILDE, Jaap de. *Security: a new framework for analysis*. Boulder: Lynne Rienner, 1998.

FRANÇA. Ministère des Armées. *Droit international appliqué aux opérations dans le cyberespace*. Paris: Délégation à l'information et à la communication de la défense, [2019].

CCDCOE. *Tallinn Manual 2.0*. Tallinn, 2017. Disponível em: https://ccdcoe.org/research/tallinn-manual. Acesso em: 31 Oct. 2020.

GONÇALVES, Joanisval B. *Atividade de Inteligência e legislação correlata*. 6. ed. Niterói: Impetus, 2018.

RESENHA - BUCHAN, RUSSELL. CYBER ESPIONAGE AND INTERNATIONAL LAW. OXFORD: HART PUBLISHING, 2019.

Resenha recebida em 30/07/2020
Aprovada em 27/10/2020