Last name, first name, patronymic (if available)	Habib Hasan Al-Badawi
Organization	Lebanese University
Address	Beirut
Position (*course, group - for student, graduate student)	
Academic degree and (or) academic title	Ph.D – Professor
Contact phone	009613202997
Number (be sure to specify the area code)	
E-mail	Habib.badawi@ul.edu.lb

Tallinn Manual as a Legal Approach towards Cyber Warfare

*"The **Tallinn Manual** examines the international law governing **cyber warfare**. As a general matter, it encompasses both the jus ad bellum, the international law governing the resort to force by States as an instrument of their national policy, and the jus in bello, the international law regulating the conduct of armed conflict (also labelled the law of war, the law of armed conflict, or international humanitarian law). Related bodies of international law, such as the law of State responsibility and the law of the sea, are dealt with in the context of these topics."*

The Tallinn Manual[1] on the International Law Applicable to Cyber Warfare was published by the International Group of Experts at the invitation of the North Atlantic Treaty Organization NATO. It is an academic, non-binding study on how international law applies to cyber conflicts and cyber warfare. The manual was revised in 2017 and published by Cambridge University Press as a book titled Tallinn Manual 2.0[2].

Keywords: National Security – State Sovereignty - Cyberespionage - International Law - Tallinn Manual.

Cyberespionage under International Law

Cyberespionage is a form of cyberattack that aims to steal confidential, sensitive, or intellectual property data to gain an advantage over a rival government company or entity, espionage is "using spies to obtain important information about plans and activities of a foreign government or a rival company[3]".

In the world of the Internet, spies are armies of infiltrators from all over the world who use war and electronic means for economic, political, or military gain. These high-value cybercriminals have the knowledge and technical capacity to penetrate government infrastructure, financial and real estate systems, or utility resources such as airports, ports, etc., and have been able to influence the outcome

---

[1] *TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE*. (n.d.). Центр стратегических оценок и прогнозов. https://csef.ru/media/articles/3990/3990.pdf (accessed: 10. 12. 2021).

[2] Schmitt M., Vihul L. Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge: Cambridge University Press, 2018.

[3] "Espionage, according to Merriam-Webster, is "the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company."
What is Cyber Espionage | VMware Glossary [online] // VMware. 2021. URL: https://www.vmware.com/topics/glossary/content/cyber-espionage (accessed: 10. 12. 2021).

of political elections in several countries (accusing the United States of Russia of interfering in the election results that led to Trump's victory), creating international chaos, and helping companies succeed or fail[4]. Many of these attackers use Advanced Persistent Threats[5] as modus to sneak into corporate and state networks or systems and stay undetected for years.

Article 29[6] of the Hague Convention of 1907[7] stipulates that an individual can only be considered a spy for a particular State if he or she obtains information in the enemy's area of operations by acting secretly and intending to inform the hostile party, and therefore undetected soldiers who enter the area of operations of an army hostile to obtain military or intelligence information are not considered spies, nor are spies of soldiers or civilians of a particular State who carry out their duties in public or are Mandated to deliver letters addressed either to their army or to the enemy army.

Article 46 (2) of the First Additional Protocol of 1977 of the Geneva Convention stipulates that it is not engaged in espionage by members of the armed forces of a party to a particular conflict and is mandated by that party and in an[8] adversary-controlled territory to collect information or attempt to collect it in the uniform of its country's armed forces[9].

Tallinn Manual[10]

A group of legal and military experts published a guide known as the Tallinn Guide, a non-binding document for States, to which the International Committee of

---

[4] Justice, J. W., & Bricker, B. J. (2019). Hacked: Defining the 2016 Presidential Election in the Liberal Media. *Rhetoric and Public Affairs*, *22*(3), 389–420. https://doi.org/10.14321/rhetpublaffa.22.3.0389 *(accessed: 12. 12. 2021).*

[5] *What is APT (Advanced Persistent Threat) | APT Security | Imperva [online] // Learning Center. 2021. URL: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/ (accessed: 12. 12. 2021).*

[6] *Treaties, States parties, and Commentaries - Hague Convention (IV) on War on Land and its Annexed Regulations, 1907 - Regulations: Art. 29 - [online] // Ihl-databases.icrc.org. 2021. URL: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=090BE405E194CECBC12563CD005167C8 (accessed: 12. 12. 2021).*

[7] *Treaties, States parties, and Commentaries - Hague Convention (IV) on War on Land and its Annexed Regulations, 1907 [online] // Ihl-databases.icrc.org. 2021. URL: https://ihl-databases.icrc.org/ihl/INTRO/195 (accessed: 12. 12. 2021).*

[8] *Treaties, States parties, and Commentaries - Additional Protocol (I) to the Geneva Conventions, 1977 - 46 - Spies [online] // Ihl-databases.icrc.org. 2021. URL: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/ART/470-750056?OpenDocument (accessed: 12. 12. 2021).*

[9] Customary IHL - Practice Relating to Rule 107. Spies [online] // Ihl-databases.icrc.org. 2021. URL: https://ihl-databases.icrc.org/customary-ihl/rus/docindex/v2_rul_rule107 (accessed: 12. 12. 2021).

[10] The Tallinn Manual [online] // Ccdcoe.org. 2021. URL: https://ccdcoe.org/research/tallinn-manual/ (accessed: 18. 14. 2021).

the Red Cross ICRC[11] contributed as an observer. This document indicates that international humanitarian law applies to cyber warfare as with conventional wars and determines the role that the rules of international humanitarian law will play in this area[12], despite many negative observations[13].

For legal advisers, policymakers, and military leaders interested in international law as it relates to electronic weapons, the Tallinn Guide is an important starting point for analyzing how international humanitarian law applies to cyber operations and weapons. Tallinn's 2017 guide addresses the issue of cyber weapons review, as well as many other vital issues related to this area in nearly 600 pages of rules and instructions related to public international law.

In 2009, the NATO Cooperative Cyber Defence Centre of Excellence[14], a renowned online defense research and training institution in Tallinn, Estonia, invited a group of independent cyber experts to prepare a guide on international law that should govern electronic activities during wars like traditional activities. The legality associated with electronic warfare and its clarification. In 2013, the first version of the Tallinn Guide to International Law was published and became the only reference in this area and because of the success of the first guide, CCD COE began a follow-up project to expand coverage with an updated and developed guide to international law governing electronic activities during peacetime[15].

In February 2017, the second group of more diverse cyber experts participated, and their work led to the creation and dissemination of the second updated version of the Tallinn Guide. The extensive guide included material from the Tallinn I manual and another to cover the legal frameworks of forces involved in cyber activities and incidents in peacetime. It contained 154 rules, the most important of which was Rule 110 on the arms review process under international humanitarian law. The detailed commentary of each rule provides some important ideas regarding the legal basis and justification of the rules and their context, as

---

[11] *Mandate and mission [online] // International Committee of the Red Cross. 2021. URL: https://www.icrc.org/en/who-we-are/mandate (accessed: 14. 12. 2021).*

[12] Jensen E. The Tallinn Manual 2.0: Highlights and Insights [online] // Ssrn.com. 2021. URL: https://ssrn.com/abstract=2932110 (accessed: 14. 12. 2021).

[13] *A Warning About Tallinn 2.0 … Whatever It Says [online] // Lawfare. 2021. URL: https://www.lawfareblog.com/warning-about-tallinn-20-%E2%80%A6-whatever-it-says (accessed: 18. 12. 2021).*

[14] CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise. About us [online] // Ccdcoe.org. 2021. URL: https://ccdcoe.org/about-us/ (accessed: 14. 12. 2021).

[15] *"Defend Forward" and Sovereignty*. (n.d.). Hoover Institution.URL: https://www.hoover.org/sites/default/files/research/docs/goldsmith-loomis_webreadypdf.pdf (accessed: 18. 12. 2021).

well as justifying the effects of the application of the rules in the cyber context in terms of the field results and legal consequences of the weapon. This level of access to detail is particularly useful for legal advisers and academics. In addition to that, there is an explanation of experts' justifications for explaining legal rules and their positions on them when reaching an agreement. Also, they are unable to reach a consensus on a particular issue, as well as highlighting the reasons for incompatibility to understand the legal context of consensus or not[16].

The Tallinn analysis states that pre-cyber era international law applies to cyber operations, both conducted by, and directed against, states. This means that cyber events do not occur in a legal vacuum and thus states have both rights and bear obligations under international law[17].

Rule 110 of Tallinn Manual

All States are required to ensure that the electronic warfare methods they obtain, or use comply with binding rules of armed conflict law.

States parties to Protocol I are required to examine the means and methods of electronic warfare to determine whether their use, in some or all circumstances, is prohibited under that Protocol or any other rule of international law.

There are at least six points to be illuminated concerning Rule 110:

1. Rule 110 of the Tallinn Guide must be read from the perspective of the Advisory Opinion of the International Court of Justice on Nuclear-Weapons[18], which confirmed the idea that international humanitarian law applies to new weapons as old as they are. Although cyber weapons were invented after the emergence of most of the principles and rules of international humanitarian law, it would be wrong to conclude that international humanitarian law did not apply to them, and as noted by the International Court of Justice, it would be incompatible with the fundamental humanitarian nature of the legal principles of international

---

[16] *ALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS*. (n.d.). // Assets.cambridge.org. 2021. URL:https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf (accessed: 18. 12. 2021), p. 467.

[17] *Cyber operations and international humanitarian law: five key points - Humanitarian Law & Policy Blog [online] // Humanitarian Law & Policy Blog. 2021. URL: https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/ (accessed: 18. 12. 2021).*

[18] *Legality of the threat or use of nuclear weapons | International Court of Justice*. (n.d.). Cour internationale de Justice - International Court of Justice | International Court of Justice. https://www.icj-cij.org/en/case/95 *(accessed: 18. 12. 2021).*

humanitarian law to believe that this law does not apply to new weapons. As a result, international humanitarian law applies to all forms of electronic or conventional warfare and to all types of weapons that exist past and present and can be invented in the future.

2. To reinforce the point above, the classification of any equipment used in war or peace as an electronic weapon also means that such a weapon must at any time comply with international humanitarian law.

Subparagraph (a) reflects customary international law and stems from a general duty to comply with international humanitarian law. Subparagraph (b) is derived from Article 36, the obligations outlined in this paragraph are not limited to international humanitarian law but extend to the entire international law, they are much broader and more comprehensive than those in subparagraph (a).

Subparagraph (b) does not specify or require a specific methodology for conducting a review of cyber weapons, so States are not obliged to make their weapons reviews public, and this is particularly relevant in the context of cyberweapons because of the highly secretive nature of such weapons. As in all arms under international humanitarian law, the legality of a cyber weapon must be determined by reference to its natural and expected use at the time of assessment.

5. If one State receives an electronic weapon from another for use in its future cyber operations, the fact that the arms supplier has conducted a review does not exempt the possessing State from its obligations about that cyber weapon. The acquired State may consider the review conducted by the supplier State and must fulfill its obligations under international humanitarian law.

6. Regarding what needs to be reviewed, for States parties to Protocol I, to answer the question of what specifically constitutes weapons, means, or electronic methods, it can be said that all States, regardless of whether they have ratified The First Additional Protocol, are required to systematically assess the legitimacy of their new weapons, means, and methods. This obligation logically stems from the common public duty to comply with international humanitarian law and the fact that States are prohibited from using illegal weapons, means, or methods of war and are contrary to the Bill of Human Rights.