POSIZIONE ITALIANA SULL'APPLICABILITA' DEL DIRITTO INTERNAZIONALE ALLO SPAZIO CIBERNETICO

BIBLIOGRAFIA DI RIFERIMENTO

1. A. Berkes, "Human Rights Obligations of the Territorial State in the Cyberspace of Areas Outside Its Effective Control", in *Israel Law Review*, 2019, pp. 197 ss.
2. A. Bonfanti, "Attacchi cibernetici in tempo di pace: le intrusioni nelle elezioni presidenziali statunitensi del 2016 alla luce del diritto internazionale", in *Rivista di diritto internazionale*, 2019, pp. 694 ss.
3. J.K. Canfil, "Honing Cyber Attribution: A Framework for Assessing Foreign State Complicity", in *Journal of International Affairs*, 2016, pp. 217 ss.
4. W. Chan, "The Need for a Shared Responsibility Regime between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware", in *Brooklyn Journal of International Law*, 2019, pp. 795 ss.
5. F. Delerue, *Cyber Operations and International Law*, Springer, 2020.
6. K. Giles, *Prospects for the Rule of Law in Cyberspace*, Strategic Studies Institute, U.S. Army War College Commandant, 2017.
7. K. Kittichaisaree, *Public International Law of Cyberspace*, Springer, 2017.
8. A. Payne, L. Finlay, "Addressing obstacles to cyber-attribution: model based on state response to cyber-attack", in *George Washington International Law Review*, 2017, pp. 535 ss.
9. M. Roscini, *Cyber Operations and the Use of Force in International Law*, OUP, 2014.
10. H. Lahmann, *Unilateral Remedies to Cyber Operations*, CUP, 2020.
11. A. Sardu, "L'*international cybersecurity law*: lo stato dell'arte", in *La Comunità Internazionale*, 2020, pp. 5 ss.
12. M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, CUP, 2017 (2° ed.).
13. A. Tanzi, *Introduzione al diritto internazionale contemporaneo*, CEDAM, 2019 (6° ed.).