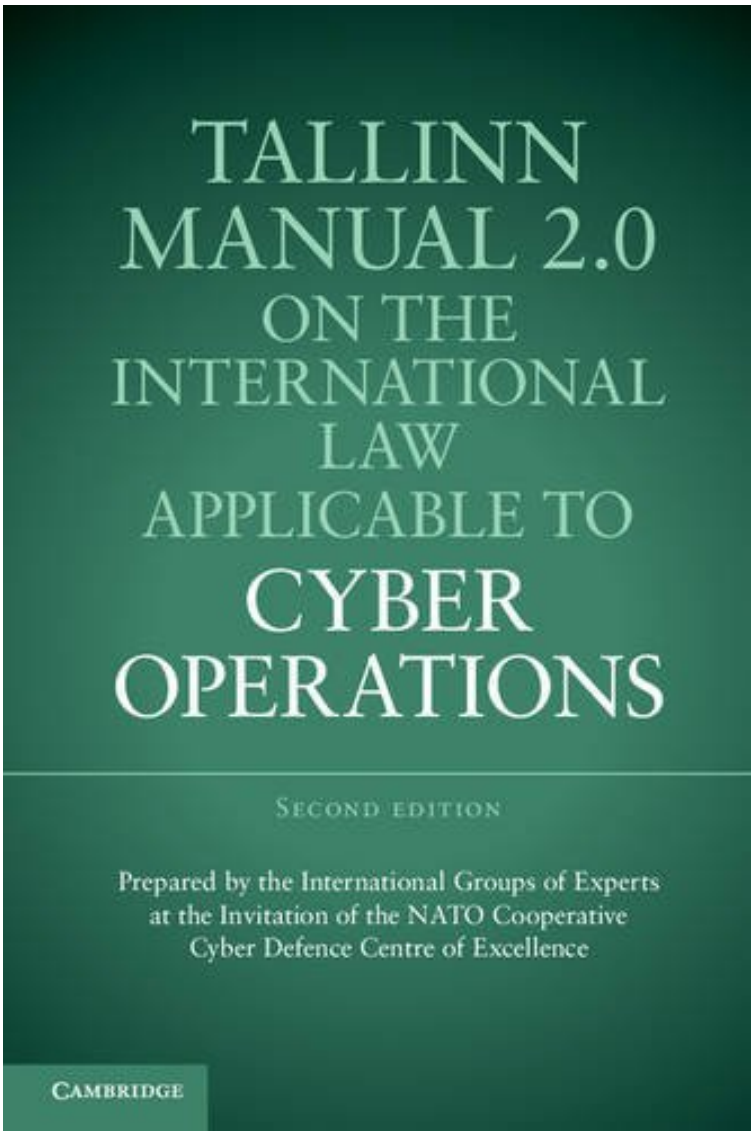
Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

From CAMBRIDGE UNIVERSITY PRESS
*DOC | *audiobook | ebooks | Download PDF | ePub*



#270255 in Books CAMBRIDGE UNIVERSITY PRESS 2017-02-02Original language:English 8.98 x 1.30 x 5.98l, #File Name: 1316630374638 pagesCAMBRIDGE UNIVERSITY PRESS | File size: 26.Mb

From CAMBRIDGE UNIVERSITY PRESS : Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations before purchasing it in order to gage whether or not it would be worth my time, and all praised Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations:

0 of 0 people found the following review helpful. Worthy UpdateBy GoddessofcodeThis is a very worthy update to its predecessor...I now own both and have no plans of getting rid of the original. Honestly having the historical version to

look back on is interesting as we learn more about cybersecurity threats and cyberwarfare in general.0 of 0 people found the following review helpful. A Very Informative Repository of InformationBy Bryce MullinsThe Tallinn Manual 2.0 is an extension of the first book, which covered Cyber Warfare. In the off-chance that you need to find something out such as whether it's legal to hack medical personnel on a belligerent airplane, you need to consult this book. It does contain the answer.If you plan to read this book while exercising, which I do, you may want to consider buying the hardcover.0 of 0 people found the following review helpful. Five StarsBy Alexandru DeacExcellent synopsis of international cyber operations legal framework.

Tallinn Manual 2.0 expands on the highly influential first edition by extending its coverage of the international law governing cyber operations to peacetime legal regimes. The product of a three-year follow-on project by a new group of twenty renowned international law experts, it addresses such topics as sovereignty, state responsibility, human rights, and the law of air, space, and the sea. Tallinn Manual 2.0 identifies 154 'black letter' rules governing cyber operations and provides extensive commentary on each rule. Although Tallinn Manual 2.0 represents the views of the experts in their personal capacity, the project benefitted from the unofficial input of many states and over fifty peer reviewers.

'Appropriately named Tallinn Manual 2.0: International Law Applicable to Cyber Operations, the new book offers a fascinating look at how far the cyber threat landscape has evolved in the less than half decade since the first version's release in 2013, shifting the focus from conventional state-authorized and operated cyber warfare to the small-bore deniable cyber activities that form the majority of day-to-day cyber attacks today.' Kalev Leetaru, Forbes (www.forbes.com)About the AuthorMichael N. Schmitt is Chairman and Charles H. Stockton Professor at the Stockton Center for the Study of International Law, United States Naval War College, Newport, Rhode Island; Professor of Public International Law at the University of Exeter; Senior Fellow of the NATO Cooperative Cyber Defence Centre of Excellence; Francis Lieber Distinguished Scholar at the Lieber Institute, United States Military Academy, West Point; Fellow of the Harvard Law School Program on International Law and Armed Conflict; a Member of the Secretary of State's Advisory Committee of International Law; and General Editor of International Law Studies. A member of the Council on Foreign Relations and a Fellow of the Royal Society of Arts, he sits on many advisory and editorial boards in the field of international law.