CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

The Tallinn Manual 2.0, published by Cambridge University Press, is the most comprehensive analysis of how existing international law applies to cyber operations. Authored by nineteen international law experts, the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, is the updated and considerably expanded second edition of the 2013 *Tallinn Manual on the International Law Applicable to Cyber Warfare*, an influential resource for legal advisers around the world. The drafting of the Tallinn Manual 2.0 was facilitated and led by the NATO Cooperative Cyber Defence Centre of Excellence.

The Tallinn Manual 2.0 analysis rests on the understanding that the 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.

The focus of the original Tallinn Manual was on the most severe cyber operations, those that violate the prohibition of the use of force in international relations, entitle states to exercise the right of self-defence, and/or occur during armed conflict. Tallinn Manual 2.0 adds a legal analysis of the more common cyber incidents that states encounter on a day-to-day basis, and that fall below the thresholds of the use of force or armed conflict.

As such, the 2017 edition covers a full spectrum of international law as applicable to cyber operations, ranging from peacetime legal regimes to the law of armed conflict. The analysis of a wide array of international law principles and regimes that regulate events in cyber space includes principles of general international law, such as the sovereignty and the various bases for the exercise of jurisdiction. The law of state responsibility, which includes the legal standards for attribution, is examined at length. Additionally, numerous specialised regimes of international law, including human rights law, air and space law, the law of the sea, and diplomatic and consular law are examined within the context of cyber operations.

Professor Michael Schmitt, a Senior Fellow at the Centre and Professor at the United States Naval War College and the University of Exeter, directed the Tallinn 2.0 initiative. Liis Vihul of the NATO CCD COE served as Managing Editor. Additionally, a team of legal and IT experts from the Centre supported the effort. The expanded edition of

the Tallinn Manual, like its predecessor, represents only the views of its authors, and not those of NATO, the NATO CCD COE, its Sponsoring Nations, or any other State or organisation.

More information is available online at https://ccdcoe.org/tallinn-manual.html.

NATO Cooperative Cyber Defence Centre of Excellence

The NATO Cooperative Centre Cyber Defence Centre of Excellence is a NATO-accredited knowledge hub, research institution, and training and exercise facility. The Tallinn-based international military organisation focuses on interdisciplinary applied research, consultations, trainings and exercises in the field of cyber security.

NATO CCD COE is the home of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. The Centre organises the world's largest and most complex international technical cyber defence exercise Locked Shields and the annual conference on cyber conflict, CyCon.

The Centre is a multinational and interdisciplinary hub of cyber defence expertise, uniting practitioners from 20 nations. The heart of the Centre is a diverse group of experts: researchers, analysts, trainers, educators. The mix of military, government and industry backgrounds means the NATO CCD COE provides a unique 360-degree approach to cyber defence. The organization supports its member nations and NATO with cyber defence expertise in the fields of technology, strategy, operations, and law.

As of 2017, Belgium, the Czech Republic, Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, Turkey, the United Kingdom and the United States are Sponsoring Nations of the NATO Cooperative Cyber Defence Centre of Excellence. Austria and Finland have become Contributing Participants, and Sweden is well on its way to following suit. The Centre is staffed and financed by member nations and, as such, is not part of NATO's military command or force structure.

Many of the Centre's publications and databases, as well as further information, can be found at www.ccdcoe.org.