TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS

*Tallinn Manual 2.0* expands on the highly influential first edition by extending its coverage of the international law governing cyber warfare to peacetime legal regimes. The product of a four-year follow-on project by a new group of 19 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 benefited from the unofficial input of many States and over 50 peer reviewers.

The Director of the Project, **Michael N. Schmitt**, is Chairman of the Stockton Center for the Study of International Law at the United States Naval War College and Professor of Public International Law at the University of Exeter. He is also Senior Fellow at the NATO Cooperative Cyber Defence Centre of Excellence.
TALLINN MANUAL 2.0
ON THE INTERNATIONAL
LAW APPLICABLE TO
CYBER OPERATIONS

Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence

General Editor
MICHAEL N. SCHMITT

Managing Editor
LIIS VIHUL
CONTENTS

Tallinn Manual 2.0 International Group of Experts and Other Participants xii
Tallinn Manual 1.0 International Group of Experts and Other Participants xix
Foreword by Toomas Hendrik Ilves, President of the Republic of Estonia xxiii
Foreword by Bert Koenders, Minister of Foreign Affairs of the Kingdom of the Netherlands xxv
Short form citations xxviii
Table of concordance xxxviii

Introduction 1

PART I General international law and cyberspace 9

1 Sovereignty 11
   Rule 1 – Sovereignty (general principle) 11
   Rule 2 – Internal sovereignty 13
   Rule 3 – External sovereignty 16
   Rule 4 – Violation of sovereignty 17
   Rule 5 – Sovereign immunity and inviolability 27

2 Due diligence 30
   Rule 6 – Due diligence (general principle) 30
   Rule 7 – Compliance with the due diligence principle 43

3 Jurisdiction 51
   Rule 8 – Jurisdiction (general principle) 51
   Rule 9 – Territorial jurisdiction 55
   Rule 10 – Extraterritorial prescriptive jurisdiction 60
   Rule 11 – Extraterritorial enforcement jurisdiction 66
   Rule 12 – Immunity of States from the exercise of jurisdiction 71
   Rule 13 – International cooperation in law enforcement 75
CONTENTS

4 Law of international responsibility 79
Section 1: Internationally wrongful acts by a State 79
  Rule 14 – Internationally wrongful cyber acts 84
  Rule 15 – Attribution of cyber operations by State organs 87
  Rule 16 – Attribution of cyber operations by organs of other States 93
  Rule 17 – Attribution of cyber operations by non-State actors 94
  Rule 18 – Responsibility in connection with cyber operations by other States 100
  Rule 19 – Circumstances precluding wrongfulness of cyber operations 104

Section 2: State countermeasures and necessity 111
  Rule 20 – Countermeasures (general principle) 111
  Rule 21 – Purpose of countermeasures 116
  Rule 22 – Limitations on countermeasures 122
  Rule 23 – Proportionality of countermeasures 127
  Rule 24 – States entitled to take countermeasures 130
  Rule 25 – Effect of countermeasures on third parties 133
  Rule 26 – Necessity 135

Section 3: Obligations of States for internationally wrongful acts 142
  Rule 27 – Cessation, assurances, and guarantees 142
  Rule 28 – Reparation (general principle) 144
  Rule 29 – Forms of reparation 148
  Rule 30 – Breach of obligations owed to the international community as a whole 152

Section 4: Responsibility of international organisations 153
  Rule 31 – General principle 157

5 Cyber operations not per se regulated by international law 168
  Rule 32 – Peacetime cyber espionage 168
  Rule 33 – Non-State actors 174

PART II Specialised regimes of international law and cyberspace 177

6 International human rights law 179
  Rule 34 – Applicability 182
CONTENTS

7 Diplomatic and consular law 209
   Rule 39 – Inviolability of premises in which cyber infrastructure is located 212
   Rule 40 – Duty to protect cyber infrastructure 217
   Rule 41 – Inviolability electronic archives, documents, and correspondence 219
   Rule 42 – Free communication 225
   Rule 43 – Use of premises and activities of officials 227
   Rule 44 – Privileges and immunities of diplomatic agents and consular officers 230

8 Law of the sea 232
   Rule 45 – Cyber operations on the high seas 233
   Rule 46 – The right of visit and cyber operations 235
   Rule 47 – Cyber operations in the exclusive economic zone 239
   Rule 48 – Cyber operations in the territorial sea 241
   Rule 49 – Cyber operations in the territorial sea during armed conflict 245
   Rule 50 – Exercise of jurisdiction in relation to foreign vessels in the territorial sea 246
   Rule 51 – Cyber operations in the contiguous zone 248
   Rule 52 – Cyber operations in international straits 249
   Rule 53 – Cyber operations in archipelagic waters 251
   Rule 54 – Submarine communication cables 252

9 Air law 259
   Rule 55 – Control of aircraft conducting cyber operations in national airspace 261
   Rule 56 – Cyber operations in international airspace 265
   Rule 57 – Cyber operations jeopardising the safety of international civil aviation 268

10 Space law 270
   Rule 58 – Peaceful purposes and uses of force 273
   Rule 59 – Respect for space activities 277
   Rule 60 – Supervision, responsibility, and liability 279
## CONTENTS

11 **International telecommunication law** 284
   - Rule 61 – Duty to establish, maintain, and safeguard international telecommunication infrastructure 288
   - Rule 62 – Suspension or stoppage of cyber communications 291
   - Rule 63 – Harmful interference 294
   - Rule 64 – Exemption of military radio installations 298

### PART III International peace and security and cyber activities 301

12 **Peaceful settlement** 303
   - Rule 65 – Peaceful settlement of disputes 303

13 **Prohibition of intervention** 312
   - Rule 66 – Intervention by States 312
   - Rule 67 – Intervention by the United Nations 325

14 **The use of force** 328
   - **Section 1: Prohibition of the use of force** 329
     - Rule 68 – Prohibition of threat or use of force 329
     - Rule 69 – Definition of use of force 330
     - Rule 70 – Definition of threat of force 338
   - **Section 2: Self-defence** 339
     - Rule 71 – Self-defence against armed attack 339
     - Rule 72 – Necessity and proportionality 348
     - Rule 73 – Imminence and immediacy 350
     - Rule 74 – Collective self-defence 354
     - Rule 75 – Reporting measures of self-defence 355

15 **Collective security** 357
   - Rule 76 – United Nations Security Council 357
   - Rule 77 – Regional organisations 360
   - Rule 78 – Peace operations 361
   - Rule 79 – Peace operations personnel, installations, materiel, units, and vehicles 368

### PART IV The law of cyber armed conflict 373

16 **The law of armed conflict generally** 375
   - Rule 80 – Applicability of the law of armed conflict 375
   - Rule 81 – Geographical limitations 378
17 Conduct of hostilities 401

Section 1: Participation in armed conflict 401

Rule 86 – Participation generally 401
Rule 87 – Members of the armed forces 402
Rule 88 – Levée en masse 408
Rule 89 – Spies 409
Rule 90 – Mercenaries 412
Rule 91 – Civilians 413

Section 2: Attacks generally 414

Rule 92 – Definition of cyber attack 415
Rule 93 – Distinction 420

Section 3: Attacks against persons 422

Rule 94 – Prohibition of attacking civilians 422
Rule 95 – Doubt as to status of persons 424
Rule 96 – Persons as lawful objects of attack 425
Rule 97 – Civilian direct participants in hostilities 428
Rule 98 – Terror attacks 433

Section 4: Attacks against objects 434

Rule 99 – Prohibition of attacking civilian objects 434
Rule 100 – Civilian objects and military objectives 435
Rule 101 – Objects used for civilian and military purposes 445
Rule 102 – Doubt as to status of objects 448

Section 5: Means and methods of warfare 451

Rule 103 – Definitions of means and methods of warfare 452
Rule 104 – Superfluous injury or unnecessary suffering 453
Rule 105 – Indiscriminate means or methods 455
Rule 106 – Cyber booby traps 457
Rule 107 – Starvation 459
Rule 108 – Belligerent reprisals 460
X CONTENTS

Rule 109 – Reprisals under Additional Protocol I 463
Rule 110 – Weapons review 464

Section 6: Conduct of attacks 467
Rule 111 – Indiscriminate attacks 467
Rule 112 – Clearly separated and distinct military objectives 469
Rule 113 – Proportionality 470

Section 7: Precautions 476
Rule 114 – Constant care 476
Rule 115 – Verification of targets 478
Rule 116 – Choice of means or methods 479
Rule 117 – Precautions as to proportionality 481
Rule 118 – Choice of targets 481
Rule 119 – Cancellation or suspension of attack 483
Rule 120 – Warnings 484
Rule 121 – Precautions against the effects of cyber attacks 487

Section 8: Perfidy and improper use 491
Rule 122 – Perfidy 491
Rule 123 – Ruses 495
Rule 124 – Improper use of the protective indicators 496
Rule 125 – Improper use of United Nations emblem 499
Rule 126 – Improper use of enemy indicators 499
Rule 127 – Improper use of neutral indicators 503

Section 9: Blockades and zones 504
Rule 128 – Maintenance and enforcement of blockades 508
Rule 129 – Effect of blockades on neutral activities 509
Rule 130 – Zones 510

18 Certain persons, objects, and activities 512
Section 1: Medical and religious personnel and medical units, transports, and material 513
Rule 131 – Medical and religious personnel, medical units and transports 513
Rule 132 – Medical computers, computer networks, and data 515
Rule 133 – Identification 515
Rule 134 – Loss of protection and warnings 517

Section 2: Detained persons 519
Rule 135 – Protection of detained persons 520
CONTENTS

Rule 136 – Correspondence of detained persons 522
Rule 137 – Compelled participation in military activities 523

Section 3: Children 524
Rule 138 – Protection of children 524

Section 4: Journalists 526
Rule 139 – Protection of journalists 526

Section 5: Installations containing dangerous forces 529
Rule 140 – Duty of care during attacks on dams, dykes, and nuclear electrical generating stations 529

Section 6: Objects indispensable to the survival of the civilian population 531
Rule 141 – Protection of objects indispensable to survival 531

Section 7: Cultural property 534
Rule 142 – Respect for and protection of cultural property 534

Section 8: The natural environment 537
Rule 143 – Protection of the natural environment 537

Section 9: Collective punishment 539
Rule 144 – Collective punishment 539

Section 10: Humanitarian assistance 540
Rule 145 – Humanitarian assistance 540

19 Occupation 543
Rule 146 – Respect for protected persons in occupied territory 544
Rule 147 – Public order and safety in occupied territory 546
Rule 148 – Security of the Occupying Power 548
Rule 149 – Confiscation and requisition of property 549

20 Neutrality 553
Rule 150 – Protection of neutral cyber infrastructure 555
Rule 151 – Cyber operations in neutral territory 556
Rule 152 – Neutral obligations 558
Rule 153 – Response by parties to the conflict to violations 560
Rule 154 – Neutrality and Security Council actions 562

Glossary 563
Index 569
TALLINN MANUAL 2.0 INTERNATIONAL
GROUP OF EXPERTS AND OTHER PARTICIPANTS

International Group of Experts

Director and General Editor

Professor Michael N. Schmitt*
United States Naval War College
University of Exeter

Managing Editor

Liis Vihul*
NATO Cooperative Cyber Defence Centre of Excellence

Legal Experts

Professor Dapo Akande
University of Oxford

Colonel (retired, United States Air Force) Gary D. Brown*
Marine Corps University

Professor (Brigadier General) Paul Ducheine
University of Amsterdam
Netherlands Defence Academy

Professor Terry D. Gill*
University of Amsterdam
Netherlands Defence Academy

Professor Wolff Heintschel von Heinegg*
Europa-Universität Viadrina

1 Affiliations during participation in the project.
* Individuals who contributed draft text for consideration by the International Group of Experts are marked with an asterisk.

xii
INTERNATIONAL GROUP OF EXPERTS AND PARTICIPANTS

Dr Gleider I Hernández*
Durham University School of Law

Deborah Housen-Couriel*
University of Haifa Faculty of Law
Tel Aviv University Interdisciplinary Cyber Research Center

Professor Zhixiong Huang
Wuhan University Institute of International Law

Professor Eric Talbot Jensen*
Brigham Young University Law School

Professor Kriangsak Kittichaisaree
Member of the International Law Commission of the United Nations

Associate Professor Andrey L. Kozik
International Law and Arbitration Association (BILA Association)
KIMEP University

Professor Claus Kreß
University of Cologne

Professor Tim McCormack
University of Melbourne
University of Tasmania

Professor Kazuhiro Nakatani
University of Tokyo

Gabor Rona*
Visiting Professor of Law, Cardozo School of Law
Formerly International Legal Director, Human Rights First

Phillip Spector*
Formerly Senior Adviser to the Legal Adviser, United States Department of State

Professor Sean Watts*
Creighton University School of Law

Technical Expert

Bernhards Blumbergs
NATO Cooperative Cyber Defence Centre of Excellence

Non-Voting Observer

Steven Hill
North Atlantic Treaty Organization
xiv  International Group of Experts and Participants

Other Participants

Contributors

Air Commodore (Retired) William H. Boothby*
Formerly Deputy Director of Legal Services, Royal Air Force (UK)

Professor Michel Bourbonnière*
Royal Military College of Canada

Dr Robert Heinsch*
Leiden University

Professor Stephan Hobe*
University of Cologne

Colonel Darren Huskisson*
United States Air Force

Professor Jann K. Kleffner*
Swedish Defence University

Professor James Kraska*
United States Naval War College

Dr Rob McLaughlin*
Australian National University

Lieutenant Colonel Jan Stinissen
Army Legal Service, the Netherlands

Legal Peer Reviewers

Squadron Leader Thomas Allan
Royal Air Force (UK)

Dr Louise Arimatsu
London School of Economics

Evelyn Mary Aswad
University of Oklahoma College of Law

Wing Commander Duncan Blake
Royal Australian Air Force

Professor Gabriella Blum
Harvard Law School

Dr Tare Brisibe
Formerly Chair, Legal Subcommittee of the United Nations Committee on the Peaceful Uses of Outer Space
INTERNATIONAL GROUP OF EXPERTS AND PARTICIPANTS

Dr Russell Buchan
University of Sheffield

Major-General Blaise Cathcart
Canadian Armed Forces

Colonel Gary P. Corn
United States Army

Professor Ashley Deeks
University of Virginia Law School

Eileen Denza
Formerly Legal Counsellor, Foreign and Commonwealth Office
Visiting Professor, University College London

Professor Alison Duxbury
University of Melbourne

Dr Dieter Fleck
Formerly Director, International Agreements and Policy, German Ministry of Defence

Daniel B. Garrie
Journal of Law & Cyber Warfare
Law & Forensics LLC

Professor Robin Geiß
University of Glasgow

Lieutenant Commander David Goddard
Royal Navy (UK)

Jason A. Greene
United States Naval Postgraduate School

Professor Juan Pablo González Jansana
Faculty of Law, Universidad Diego Portales

Dr Douglas Guilfoyle
Faculty of Law, Monash University

Dr Heather A. Harrison Dinniss
Swedish Defence University

Dr Sarah Heathcote
Australian National University

Group Captain Ian Henderson
Royal Australian Air Force
University of Adelaide

Professor Duncan B. Hollis
Temple University School of Law
xvi  INTERNATIONAL GROUP OF EXPERTS AND PARTICIPANTS

Colonel Rob Holman
Canadian Armed Forces

Dr Jiefang Huang
International Civil Aviation Organization

Lieutenant Colonel Robert Jarman
United States Air Force

Professor David Kaye
University of California, Irvine

Major Israel D. King
United States Air Force

Lieutenant Colonel Matthew King
United States Air Force

Commander Jude Klena
United States Navy

Professor Dino Kritsiotis
University of Nottingham

Associate Professor David Letts
Australian National University

Dr Catherine Lotrionte
Georgetown University

Dr Kubo Mačák
University of Exeter

Dr Marko Milanovic
University of Nottingham

Naz K. Modirzadeh
Harvard Law School Program on International Law and Armed Conflict

Lieutenant Colonel Sarah Mountin
United States Strategic Command

Dr Alexander Orakhelashvili
University of Birmingham

Dr Bruce ‘Ossie’ Oswald
Asia Pacific Centre for Military Law, University of Melbourne

Commander Ian Park
Royal Navy (UK)

University of Oxford

Professor Ki Gab Park
Korea University School of Law
INTERNATIONAL GROUP OF EXPERTS AND PARTICIPANTS  xvii

Professor Nohyoung Park
Korea University School of Law

Professor Bimal N. Patel
Gujarat National Law University
Member, 21st Law Commission of India

Major General Jeff Rockwell
United States Air Force

Professor Marco Roscini
University of Westminster

Professor Scott J. Shackelford
Indiana University
Harvard University

David A. Simon
Sidley Austin LLP

Dr Dale Stephens
University of Adelaide

Professor Christian J. Tams
University of Glasgow
Matrix Chambers (London)

Major Susan Trepuczynski
United States Air Force

Professor Nicholas Tsagourias
University of Sheffield

Dr Antonios Tzanakopoulos
University of Oxford

Professor Ian Walden
Centre for Commercial Law Studies, Queen Mary University of London

Commander (Retired, United States Navy) Paul Walker
American University

Dr Chanaka Wickremasinghe
Foreign and Commonwealth Office of the United Kingdom

Colonel Philip T. Wold
United States Air Force

Em. Professor Rüdiger Wolfrum
Max Planck Institute for Comparative Public and International Law

Dr Marten Zwanenburg
Ministry of Foreign Affairs, the Netherlands
xviii INTERNATIONAL GROUP OF EXPERTS AND PARTICIPANTS

Technical Peer Reviewers

Jeffrey Carr
Taia Global, Inc.
Ragnar Rattas
NATO Cooperative Cyber Defence Centre of Excellence

Legal Research

Harvard Law School

Molly Doggett
Jiawei He
Ariane Moss

University of Amsterdam

Nicolò Bussolati

United States Army

Lieutenant Allyson Hauptman

University of Tartu

Carel Kivimaa
Liis Semjonov
Aleksander Tsuiman

Cardozo School of Law

Barry Dynkin

Fletcher School of Diplomacy

Mark Duarte

NATO Cooperative Cyber Defence Centre of Excellence

Nicolas Jupillat

Emory University School of Law

Kiana Arakawa
Ryan Light
Tariq Mohideen
Christopher Pitts
Daniel Rubin
TALLINN MANUAL 1.0 INTERNATIONAL
GROUP OF EXPERTS AND OTHER
PARTICIPANTS

International Group of Experts

Director

Professor Michael N. Schmitt
United States Naval War College

Editorial Committee

Air Commodore (Retired) William H. Boothby
Formerly Deputy Director of Legal Services, Royal Air Force (UK)

Bruno Demeyere
Catholic University of Leuven

Professor Wolff Heintschel von Heinegg
Europa-Universität Viadrina

Professor James Bret Michael
United States Naval Postgraduate School

Professor Thomas Wingfield
George C. Marshall European Center for Security Studies

Legal Group Facilitators

Professor Eric Talbot Jensen
Brigham Young University Law School

Professor Sean Watts
Creighton University Law School

2 Affiliations during participation in the project.

xix
INTERNATIONAL GROUP OF EXPERTS AND PARTICIPANTS

Legal Experts

Dr Louise Arimatsu
Chatham House

Captain (Navy) Geneviève Bernatchez
Office of the Judge Advocate General, Canadian Forces

Colonel Penny Cumming
Australian Defence Force

Professor Robin Geiß
University of Potsdam

Professor Terry D. Gill
University of Amsterdam, Netherlands Defence Academy, and Utrecht University

Professor Derek Jinks
University of Texas School of Law

Professor Jann Kleffner
Swedish National Defence College

Dr Nils Melzer
Geneva Centre for Security Policy

Brigadier General (Retired, Canadian Forces) Kenneth Watkin
United States Naval War College

Technical Experts

Dr Kenneth Geers
NATO Cooperative Cyber Defence Centre of Excellence

Dr Rain Ottis
NATO Cooperative Cyber Defence Centre of Excellence

Observers

Colonel Gary D. Brown, United States Air Force
United States Cyber Command

Dr Cordula Droegen
International Committee of the Red Cross

Dr Jean-François Quéguiner
International Committee of the Red Cross

Ulf Häußler
Headquarters, Supreme Allied Commander Transformation, NATO
Other Participants

Peer Reviewers

Professor Geoffrey Corn
South Texas College of Law

Professor Ashley Deeks
University of Virginia

Dr Heather A. Harrison Dinniss
Swedish National Defence College

Commander Clive Dow
Royal Navy (UK)

Professor Charles Garraway
Human Rights Centre, University of Essex

Group Captain Ian Henderson
Royal Australian Air Force

Dr Gleider Hernandez
Durham University

Professor Chris Jenks
Southern Methodist University School of Law

Dr Noam Lubell
University of Essex

Sasha Radin
University of Melbourne Law School

Commander Paul Walker
United States Navy

Colonel David Wallace, United States Army
United States Military Academy

Dr Katharina Ziolkowski
NATO Cooperative Cyber Defence Centre of Excellence

Project Coordinator

Dr Eneken Tikk
NATO Cooperative Cyber Defence Centre of Excellence
INTERNATIONAL GROUP OF EXPERTS AND PARTICIPANTS

Project Manager

Liis Vihul
NATO Cooperative Cyber Defence Centre of Excellence

Rapporteurs

Jean Callaghan
George C. Marshall European Center for Security Studies
Dr James Sweeney
Durham University

Legal Research

Creighton University Law School

Jennifer Arbaugh
Nicole Bohe
Christopher Jackman
Christine Schaad

Emory University Law School

Anand Shah

Chatham House

Hemi Mistry
FOREWORD

TOOMAS HENDRIK ILVES
President of the Republic of Estonia

In 2007, several Estonian private and public e-services fell victim to an onslaught of malicious cyber operations. These coordinated attacks focused the international community’s attention on the severe risks posed by the increasing reliance of States and their populations on cyberspace. In retrospect, these were fairly mild and simple DDoS attacks, far less damaging than what has followed. Yet it was the first time one could apply the Clausewitzean dictum: War is the continuation of policy by other means.

The attacks also sped up the establishment of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) in Tallinn. Estonia is honoured to host and contribute to this world-class think tank and training institution that is a valued partner for NATO, Allies, and the international community. Among the NATO CCD COE’s first activities was to commission a major study on cyber warfare conducted by an international group of legal experts. The experts examined how international law governs the use of cyber force by States and the employment of cyber operations during an armed conflict. The resulting Tallinn Manual has become a guidebook for governments around the world as they assess the application of international law in such situations.

Upon publication of the Tallinn Manual in 2013, the NATO CCD COE launched a follow-on research effort to expand the Manual to encompass the international law governing cyber activities occurring in peacetime. The outcome is by far one of the most comprehensive analyses of international law applicable to cyber operations. The publication you are holding covers topics ranging from space law and jurisdiction to international human rights law, as well as an analysis of conflict law from the first Tallinn Manual.

The fact that international law is often dismissed as window-dressing on realpolitik is misleading. Such an approach understates the importance of international agreements in maintaining peace and security. For liberal democracies that respect the rule of law, international law
undoubtedly shapes and bounds governments’ activities. At a time when the actions of unscrupulous States and violent extremist groups continue to threaten peace and security internationally, it is even more important that such actions are countered with a strong commitment to existing international law and the values that it represents.

On the diplomatic level, governments should continue to interact in order to foster a better understanding of how international law regulates their cyber conduct. That said, these initiatives have proven to be slow and laborious, sometimes hobbled by narrow national interest and perspectives. The creation of the second Tallinn Manual has been unconstrained by politics and the book will serve as a road-map for governments as they seek greater clarity regarding their rights and obligations in cyberspace. The book will also be useful to the international community while struggling with the complexity of identifying extant cyber norms and promulgating new ones.

I am glad that the journey of the international group of experts began in my nation’s capital and the understanding of international law matures under Tallinn’s name. I congratulate the NATO CCD COE, the experts, and the many others scattered around the world who contributed to this trailblazing endeavour.
FOREWORD

BERT KOENDERS
Minister of Foreign Affairs of the Kingdom of the Netherlands

We find ourselves in an exciting age. Information technology has stirred innovation in an unprecedented fashion. The Internet has connected people in ways and numbers that were previously unimaginable. Knowledge and information have become public property as never before. This has proven especially true for the Netherlands, the European leader in responding to technological trends and effectively applying information and communication technologies and related skills.

All new technologies present new opportunities and challenges. As was the case, for instance, with gunpowder and the aeroplane, the same holds true with respect to digital technologies. For the Netherlands, and many other countries, our reliance on digital technology is both a boon and a bane. It fosters innovation, but increasingly also represents a point of vulnerability that can be exploited by malicious actors. In the face of this threat, we must develop capabilities to defend ourselves in a manner that preserves the international legal order. At the same time, it is the responsibility of the international community to ensure that peace, security, and stability are maintained, and that such capabilities are only used in accordance with international law.

In the past, *inter arma enim silent leges* – ‘In times of war, the law falls silent’ – was an oft-heard claim. More recently, some have argued that the law falls silent in the face of the challenges of the digital age. Neither assertion is correct. States have developed a body of law that regulates armed conflict, commonly known as international humanitarian law. They have also recognised that existing international law applies to the digital domain.

It is not always immediately evident how rules that were developed before a new technology existed should be applied to that technology. Yet, it is important to reach common understandings on such applications in order to promote an open, secure, stable, accessible, and peaceful ICT environment. This is something that States should debate.
among themselves. Academic experts have an important role to play in informing the debate.

In 2013, that role was clearly illustrated with the publication of the Tallinn Manual on the International Law Applicable to Cyber Warfare. The manual has made a valuable and significant contribution to promoting and informing the debate among States regarding the application of international law in the cyber domain.

The scope of the 2013 manual was limited to international law on the use of force and international humanitarian law. In practice, many questions concerning the application of international law fall outside of its scope. Fortunately, situations of armed conflict are the exception rather than the rule. Most cyber activities take place in times of peace.

The invitation that the NATO Cooperative Cyber Defence Centre of Excellence extended to the experts led by Professor Schmitt to update the manual and explore the application of peacetime international law was therefore a welcome initiative. It offered a unique opportunity for exchanges and engagement between academic experts and national legal advisors.

I am proud that the Netherlands was able to facilitate these exchanges by organising a series of consultation meetings between the authors of the new manual, Tallinn Manual 2.0, and States of diverse regional backgrounds. This ‘Hague Process’ offered the authors of the updated manual an opportunity to gain insight into State practices, and provided States with a forum for dialogue. My intention is for the Hague Process to continue, even after the publication of the new manual.

The Netherlands has long attached great importance to promoting the development of the international legal order. In fact, our constitution explicitly cites doing so as one of the government’s tasks. The international legal order provides a measure of stability, predictability, and accountability in States’ international relations and is of paramount importance in preventing conflict. I believe that the application of international law to State conduct in the digital domain can serve as a bedrock for peace and security, as it does in all other domains, because technological advances have no bearing on the underlying legal principles. By facilitating the Hague Process, I am convinced that The Hague is fulfilling its role as international city of peace, justice, and security.

I have no doubt that this Tallinn Manual 2.0, like the original version, will become an important resource for national legal advisors. This is in no small part due to the high quality of the experts involved and the rigorous drafting process employed.
I am also confident that the manual will continue to play an important role in the continuing dialogue regarding how international law applies to cyber activities. Its ultimate and most important role lies in helping States reach common understandings. After all, only by safeguarding the international order can we ensure security in an open and innovative digital domain. This must be our objective, and it is one that the Netherlands remains committed to achieving.
SHOR T FORM CITATIONS

Treaties

1884 Cable Convention: Convention for the Protection of Submarine Telegraph Cables, 14 March 1884, USTS 380.


Additional Protocol II: Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, 8 June 1977, 1125 UNTS 609.


Chicago Convention: Convention on Civil Aviation, 7 December 1944, 15 UNTS 295.


xxviii
Conventional Weapons Convention: Convention on Prohibitions or Restrictions on
the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively
Injurious or to Have Indiscriminate Effects, 10 April 1981, 1342 UNTS 137.
CRC Optional Protocol: Optional Protocol to the Convention on the Rights of the
Child on the Involvement of Children in Armed Conflict, 25 May 2000, 2173
UNTS 222.
CRPD: Convention on the Rights of Persons with Disabilities, 30 March 2007, 2515
UNTS 3.
Property in the Event of Armed Conflict with Regulations for the Execution of the
Convention, 14 May 1954, 249 UNTS 240.
ECHR: European Convention for the Protection of Human Rights and Fundamental
 Freedoms, 4 November 1950, 213 UNTS 222.
Environmental Modification Convention: Convention on the Prohibition of Military
or Any Other Hostile Use of Environmental Modification Techniques (‘ENMOD’),
10 December 1976, 1108 UNTS 151.
Geneva Convention I: Convention (I) for the Amelioration of the Condition of the
Wounded and Sick in Armed Forces in the Field, 12 August 1949, 75
UNTS 31.
Geneva Convention II: Convention (II) for the Amelioration of the Condition of
Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, 12 August
1949, 75 UNTS 85.
Geneva Convention III: Convention (III) Relative to the Treatment of Prisoners of
War, 12 August 1949, 75 UNTS 135.
Geneva Convention IV: Convention (IV) Relative to the Protection of Civilian Persons
in Time of War, 12 August 1949, 75 UNTS 287.
9 December 1948, 78 UNTS 277.
Hague Convention IV: Convention (IV) Respecting the Laws and Customs of War on
Land, 18 October 1907, 36 Stat. 2277.
Hague Convention V: Convention (V) Respecting the Rights and Duties of Neutral
Powers and Persons in Case of War on Land, 18 October 1907, 36 Stat. 2310.
Hague Convention VIII: Convention (VIII) Relative to the Laying of Automatic
Submarine Contact Mines, 18 October 1907, 32 Stat. 2332.
Hague Convention XIII: Convention (XIII) Concerning the Rights and Duties of
Neutral Powers in Naval War, 18 October 1907, 36 Stat. 2415.
Hague Regulations: Convention (IV) Respecting the Laws and Customs of War on
Land and its annex: Regulations concerning the Laws and Customs of War on Land,
18 October 1907, 36 Stat. 2277.
ICCP: International Covenant on Civil and Political Rights, 16 December 1966, 999
UNTS 171.
XXX  SHORT FORM CITATIONS


Moon Agreement: Agreement Governing Activities of States on the Moon and Other Celestial Bodies, 5 December 1979, 1363 UNTS 3.


Registration Convention: Convention on Registration of Objects Launched into Outer Space, 12 November 1974, 1023 UNTS 15.


SHORT FORM CITATIONS

St Petersburg Declaration: Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, 29 November/11 December 1868, 18 Martens Nouveau Recueil (ser. 1) 474.


Case law

Aerial Incident judgment: Aerial Incident of 10 August 1999 (Pak. v. India) judgment on jurisdiction, 2000 ICJ 12 (22 June).


Archer Daniels arbitral award: Archer Daniels Midland Company v. Mexico, award, ICSID Case No. ARB(AF)/04/05 (21 November 2007).


Barcelona Traction judgment: Case Concerning the Barcelona Traction, Light and Power Company Limited (Second Phase) (Spain v. Belg.), judgment, 1970 ICJ 3 (5 February).


Enron v. Argentina award: Enron Co. v. Argentina, award, ICSID Case No. ARB/01/3 (22 May 2007).