ASSER PRESS

Yearbook of International Humanitarian Law

2012

Springer

Yearbook of International Humanitarian Law

Volume 15

For further volumes:
http://www.springer.com/series/8912

Terry D. Gill
General Editor

Yearbook of International Humanitarian Law Volume 15, 2012

ASSER PRESS CAMBRIDGE UNIVERSITY PRESS Springer

General Editor
Terry D. Gill
Professor of Military Law
University of Amsterdam and Netherlands Defence Academy
Amsterdam/Breda
The Netherlands

Cover Photo: © William Belcher, U.S. Air Force

ISBN 978-90-6704-923-8 ISBN 978-90-6704-924-5 (eBook)
DOI 10.1007/978-90-6704-924-5

This Volume is also available as a journal product through Cambridge University Press. In addition to the electronic version published on www.springerlink, the Yearbook is also available online through the Cambridge Journals Online service.
Published by T.M.C. ASSER PRESS, The Hague, The Netherlands www.asserpress.nl
Produced and distributed for T.M.C. ASSER PRESS by Springer-Verlag Berlin Heidelberg

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Contents

Part III Other Articles

In order to make the *Correspondents' Reports* immediately and widely accessible, they are now available online at

www.asser.nl/YIHL/correspondentsreports.

This brings the added benefit of making them fully searchable, thereby more easily serving the needs of scholars and practitioners.

Part I
The Tallinn Manual on the International Law Applicable to Cyber Warfare

Chapter 1
The Tallinn Manual and International Cyber Security Law

Wolff Heintschel von Heinegg

Contents

1.1 Introduction

In 2009, the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn, Estonia, established an "International Group of Experts" to conduct the first comprehensive examination of the international law governing cyber warfare. The group consisted of twenty international law scholars and practitioners, including senior military officers responsible for legal advice on cyber operations. Three organizations provided observers to the process: the International Committee of the Red Cross, NATO's Allied Command Transformation, and the

The author is Charles H. Stockton Professor of International Law, U.S. Naval War College; Professor of International Law, Europa-Universität Viadrina, Frankfurt (Oder).

W. Heintschel von Heinegg (✉)
U.S. Naval War College, Newport, RI, USA
e-mail: wolff.vonheinegg.de@usnwc.edu

T. D. Gill et al. (eds.), *Yearbook of International Humanitarian Law 2012*,
Yearbook of International Humanitarian Law 15, DOI: 10.1007/978-90-6704-924-5_1,

United States Cyber Command. A team of technical experts provided advice throughout the process. The resulting product of the three-year process was the *Tallinn Manual on the International Law Applicable to Cyber Warfare*.[1]

The authority of the International Group of Experts is not to be exaggerated. All members participated in their personal capacity. Moreover, no attempt was made to ensure geographical representation. Instead, participants were selected based on their mastery of the relevant law or their sensitivity to the cyber contexts in which that law would be applied, or both. Although a number of States took the opportunity to informally provide feedback on drafts of the *Tallinn Manual*, this was always done in an unofficial, non-attributable, and non-binding manner. Other international experts served as peer reviewers of the product, providing advice on revisions and corrections. Ultimately, all members of the International Group of Experts agreed with the formulation of the so-called "Rules" set forth in the Manual. They also agreed that the accompanying Commentary fairly explained how each rule was meant to be interpreted and applied, and fully captured any differences of opinion in that regard. Ultimately, the *Tallinn Manual* should be characterized as a consensus academic work by an international group of experts who devoted three years to identifying the *lex lata* applicable to cyber warfare.

In terms of scope, the *Tallinn Manual* addresses the *jus ad bellum, jus in bello,* and, to a lesser extent, the law of neutrality. It was felt that despite the malleability of the *jus ad bellum* in the cyber context, users of the Manual would be forced to consider both bodies of law, often in tandem, in order to evaluate most cyber situations. Indeed, as the project unfolded, it became clear that to fully understand the legal context of cyber warfare, some examination of sovereignty and State responsibility was also required.

While the *Tallinn Manual* addresses those cyber operations that are most severe, it must be acknowledged that the vast majority of cyber operations directed at a State (or entities on its territory) will not rise to the level of a use of force under the *jus ad bellum* or an armed conflict under the *jus in bello*. Accordingly, the CCD COE has commissioned a follow-up three-year project to examine State responses to cyber operations falling short of the use of force and armed conflict thresholds. Combined, the two products will address the full range of international cyber security law in a coherent fashion. This is essential, for until the latter is produced there may be a tendency to inappropriately view many cyber operations through the *Tallinn Manual*'s prism. After all, when one only has a hammer, most problems look like nails.

[1] Schmitt 2013.

1.2 The Tallinn Manual and the Security Dimension of Cyberspace

As noted, the *Tallinn Manual*'s focus on public international law, and therefore inter-State relations, does not accurately reflect the realities of cyberspace. This is especially so in light of its almost exclusive analysis of the *jus ad bellum* and the *jus in bello*. Indeed, in view of the centrality of cyberspace in modern life, current challenges to cyber security that affect the private sphere, business, and civil society would appear to have been riper for examination than the rules and principles of international law regarding the use of force or armed conflict. For the average person, for instance, cybercrime is of far greater concern than the 'high politics' of international relations. Moreover, the economic benefits derived from digital information and communications infrastructure are growing at an unparalleled rate. Despite these realities, recent events such as the Stuxnet incident illustrate the importance of the security dimension that underlies the *Tallinn Manual*.

1.2.1 The Private, Economic and Social Dimension

Although unforeseen by its creators, today cyberspace (the globally-interconnected digital information and communications infrastructure) has become a "backbone of economic growth" and a "critical resource that all economic sectors rely upon."[2] There are virtually no economic activities in modern societies that are not dependent on cyberspace.[3] In some cases, the dependence is total, as with the financial and banking industries. Dependency, of course, creates vulnerability, a particular concern with respect to critical infrastructure such as that associated with the energy (electricity and water) and transport sectors. Moreover, in many States the seamless functioning of cyberspace has become a precondition to social intercourse and the exercise of democratic rights.

The rapid development of digital information and communications infrastructure can be attributed to the fact that it offers business opportunities and private

[2] EU 2013, p. 2. See also U.S. President 2011, p. 3: "Digital infrastructure is increasingly the backbone of prosperous economies, vigorous research communities, strong militaries, transparent governments, and free societies." Cyberspace has been defined as "the interdependent network of information technology infrastructures, [which] includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries." See National Security Presidential Directive 54/Homeland Security Directive 23 (NSPD-54/HSD-23).

[3] DoD July 2011, p. 1: "U.S. and international businesses trade goods and services in cyberspace, moving assets across the globe in seconds. In addition to facilitating trade in other sectors, cyberspace itself is a key sector of the global economy. Cyberspace has become an incubator for new forms of entrepreneurship, advances in technology, the spread of free speech, and new social networks that drive our economy and reflect our principles."

amenities that the global community has widely embraced. In view of the profits involved, the creation of "digital infrastructure's architecture was driven more by considerations of interoperability and efficiency than of security."[4] The resulting openness, interoperability and ubiquity created dangerous vulnerabilities. As the European Union has noted, "Cybersecurity incidents, be it intentional or accidental, are increasing at an alarming pace and could disrupt the supply of essential services we take for granted such as water, healthcare, electricity or mobile services."[5] In light of the vulnerabilities, cybercrime[6] is an especially grave threat.[7]

In view of both the criticality of cyberspace to economic and social well-being and the pervasive threat of cybercrime, it is unsurprising that cyber security strategies tend to concentrate on preserving fundamental freedoms, privacy, information flow, and economic viability[8] by defending (critical) cyber infrastructure against malicious and criminal activities. Their shared goals include global interoperability, network stability, reliable access, multi-stakeholder governance, and cybersecurity due diligence.[9] The means to achieve these goals include network protection, law enforcement (including cyber forensics), and Internet governance.[10]

Despite its military roots, the Internet has become a venue for private commercial and other non-governmental entities, such as internet service providers (ISP's), the Internet Corporation for Assigned Names and Numbers (ICANN), cyber security providers, and even individuals. Information and communications networks are largely owned and operated by the private sector, both nationally and internationally. This being so, the private sector plays "a leading role"[11] in the field of cyber security.

---

[4] Cyberspace Policy Review 2009, p. iii.

[5] EU 2013, p. 3. See also DoD July 2011, p. 4: "Cyber threats to U.S. national security go well beyond military targets and affect all aspects of society. Hackers and foreign governments are increasingly able to launch sophisticated intrusions into the networks and systems that control critical civilian infrastructure. Given the integrated nature of cyberspace, computer-induced failures of power grids, transportation networks, or financial systems could cause massive physical damage and economic disruption."

[6] 'Cybercrime' refers to "a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware)." See EU 2013, p. 3.

[7] See U.S. President 2011, p. 13: "In the case of criminals and other non-state actors who would threaten our national and economic security, domestic deterrence requires all states have processes that permit them to investigate, apprehend and prosecute those who intrude or disrupt networks at home or abroad. … all key tenets of the Budapest Convention on Cybercrime." See also Cyberspace Policy Review 2009, p. 1.

[8] U.S. President 2011, p. 5.

[9] Ibid., p. 10.

[10] Ibid., p. 17 *et seq*.

[11] EU 2013, p. 2.

In this environment, the role of States has often been to foster cooperation with and among these private actors. Although States do engage in regulatory activities, both national and international, they tend to assiduously avoid interference with the economy and social cyber actors, who are often motivated by a desire to minimize governmental regulation and control.

1.2.2 The Public and Military Dimension

It would be inaccurate to conclude that States play no role in cyber security. On the one hand, States can facilitate private efforts to enhance cyber security. Moreover, States have the power and legitimacy to "safeguard access and openness, to respect and protect fundamental rights online and to maintain the reliability of the Internet."[12] On the other hand, States use, and will continue to use, cyberspace for genuinely governmental purposes, including military purposes. Thus, they have a vested interest in dealing with cyber vulnerabilities.

Conflict between States will soon be reflected in cyberspace.[13] It has become evident that "governments are seeking to exercise traditional national power through cyberspace"[14] and that a "growing array of state and non-state actors are compromising, stealing, changing, or destroying information and could cause critical disruptions."[15] Today, "both state and non-state actors possess the capability and intent to conduct cyber espionage and, potentially, cyber attacks …, with possible severe effects."[16] The United States Cyberspace Policy Review summarized the threat as consisting of "continued exploitation of information networks and the compromise of sensitive data, especially by nations, leave the United States vulnerable to the loss of economic competitiveness and the loss of the military's technological advantages. As the Director of National Intelligence (DNI) recently testified before Congress, 'the growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures.' The Intelligence Community assesses that a number of nations already have the technical capability to conduct such attacks."[17]

---

[12] Ibid.

[13] U.S. President 2011, p. 4.

[14] Ibid., p. 9.

[15] Cyberspace Policy Review 2009, p. iii.

[16] White House 2012, p. 3.

[17] Cyberspace Policy Review 2009, p. 2, referring to: Director of National Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee*, Statement for the Record, March 10, 2009, p. 39.

State-based cyber threats have generated efforts to increase the resiliency of critical cyber infrastructure. They have also led to the consideration of State-to-State responses. Perhaps most notably, President Obama has announced that the United States has "the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests."[18] Therefore, the U.S. armed forces are taking steps to ensure they "have all necessary capabilities in cyberspace to defend the United States and its interests," including the ability to respond militarily in cyberspace.[19] Self-defense against cyber operations may also be conducted through resort to conventional armed force. It must be emphasized that exercise of the right of self-defense is not limited to actual cyber attacks that cause death, injury, destruction or damage. Any State attempting "to prevent the President from exercising traditional national security options by threatening or implying the launch of a crippling cyber attack against the United States … would be taking a grave risk."[20] For the United States, the right of self-defense matures whenever there is a hostile act, or demonstration of hostile intent, of sufficient gravity. Such acts "may include significant cyber attacks directed against the U.S. economy, government or military."[21] Similarly, a "particularly serious cyber incident or attack could constitute sufficient ground for a Member State [of the European Union] to invoke the EU Solidarity Clause (Article 222 of the Treaty on the Functioning of the European Union)."[22]

There is a genuinely military dimension to cyberspace. Information and communications technology has both opened new possibilities for military actions, while presenting the armed forces with difficult challenges. It is no exaggeration to observe, "national security is being redefined by cyberspace" because contemporary military operations "depend upon cyberspace for mission success."[23]

Today, advanced armed forces use cyberspace "to enable … military, intelligence, and business operations, including the movement of personnel and material and the command and control of the full spectrum of military operations."[24] The ability "to use cyberspace for rapid communication and information sharing in support of operations is a critical enabler."[25] In response, the United States will

[18] U.S. President 2011, p. 14.

[19] DoD November 2011, p. 2. See also White House 2012, p. 4.

[20] DoD November 2011, p. 3.

[21] Ibid., p. 4.

[22] EU 2013, p. 19. Interestingly, the Draft Strategy does not refer to Article 42(7) of the Treaty on European Union, although that would have benn the provision of first choice with regard to a "particularly serious cyber attack".

[23] DoD July 2011, p. 13. See also Lynn 2010, p. 101.

[24] DoD July 2011, p. 1.

[25] Ibid., p. 2. See also White House 2012, p. 5: "Modern armed forces cannot conduct high-tempo, effective operations without reliable information and communication networks and assured access to cyberspace and space."

"invest in the capabilities critical to … prevailing in all domains, including cyber."[26] Cyberspace has become a 'fifth domain/dimension' of warfare.[27]

The use of, and dependence on, digital information and communications infrastructure creates a degree of vulnerability that forces the military to take measures to ensure the resiliency of their cyber infrastructure.[28] For instance, the establishment of the U.S. Cyber Command (USCYBERCOM) was in part an effort to manage cyberspace risk.[29] Effective cyber defense not only requires knowledge of the offensive cyber capabilities of potential adversaries, but also the capability of deterring attack through the possession of offensive capabilities. It is therefore unsurprising that the U.S. Department of Defense asserts it possesses "the capability to conduct offensive operations in cyberspace to defend our Nation, Allies and interests."[30]

1.2.3 The Tallinn Manual's Approach

For a period of roughly ten years, there was a widely-held view that cyberspace "is not a physical place—it defies measurement in any physical dimension or time space continuum. It is a shorthand term that refers to the environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the World Wide Web."[31] Some commentators concluded that cyberspace eluded the traditional rules and principles of international law and that therefore an urgent need existed for new rules specifically designed for State conduct in the 'fifth domain.'

Such conclusions often characterize new technologies. However, only in rare cases are they justified. Wide-spread agreement now exists that the "same laws and norms that apply in other areas of our day-to-day lives apply also in the cyber domain."[32] In their cyber activities, States must therefore abide by the existing rules and principles of international law. While the unique characteristics of the digital information and communications infrastructure may require certain adaptations and modifications, the "development of norms for state conduct in

---

[26] White House, 2012.

[27] DoD July 2011, p. 5: "…treating cyberspace as a domain is a critical organizing concept for DoD's national security missions. … DoD must ensure that it has the necessary capabilities to operate effectively in all domains—air, land, maritime, space, and cyberspace." See also White House 2012, p. 8, stressing the determination "to ensure the United States, its allies, and partners are capable of operating in A2/AD, cyber, and other contested operating environments." 'A2/AD' stands for Anti-Access Area-Denial (A2AD) in military domains and in cyberspace.

[28] DoD July 2011, p. 6 *et seq*.

[29] Ibid., p. 5.

[30] DoD November 2011a, b, p. 5.

[31] Wingfield 2000, p. 17.

[32] EU 2013, p. 3.

cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete."[33] This position is in accord with the International Court of Justice's Advisory Opinion on the Legality of Nuclear Weapons,[34] which held that the *jus ad bellum* applies "to any use of force, regardless of the weapons employed"[35] and that the conduct of armed hostilities is governed by international humanitarian law as soon as there exists an (international) armed conflict.[36]

It is incontestable that the law of self-defense applies to certain cyber operations. Similarly, there is no doubt as to the full applicability of international humanitarian law to cyber operations,[37] if they either rise to the level of an armed conflict or they are taken in the course of an armed conflict and qualify as 'attacks' under that law, and if they are conducted by members of the armed forces, members of organized armed groups or civilians directly participating in hostilities. These axioms do not resolve whether particular cyber operations constitute a use of force or an armed attack. Nor do they provide the complete guidance to members of armed forces who are actively engaged in an armed conflict involving cyber operations.

At times, cyber strategies and practice will deviate from the strict boundaries of international law. For instance, it would be naïve to believe that States will refrain from conducting cyber operations merely because the issue of attributability has not been definitively resolved in a manner that would satisfy a domestic or international court. The so-called Stuxnet incident demonstrates that governments may sometimes take advantage of the opportunities presented by cyber technology even when the operation in question might qualify as a prohibited use of force. Clearly, there is a need for sober and in-depth analysis of international law in general, the *jus ad bellum* and the *jus in bello* in particular, to provide States the guidance they need when pursuing national and international security interests in or through cyberspace. The *Tallinn Manual* seeks to offer just such an analysis.

---

[33] U.S. President 2011, p. 9. See also EU 2013, p. 15: "The EU does not call for the creation of new international legal instruments for cyber issues."

[34] International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I.C.J. Rep., 226 (July 8, 1996).

[35] Ibid., para 39.

[36] Ibid., paras 74 *et seq*.

[37] DoD November 2011, p. 5: If directed by the President, DoD will conduct offensive cyber operations in a manner consistent with the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict." EU 2013, p. 16: "If armed conflicts extend to cyberspace, International Humanitarian Law and, as appropriate, Human Rights law will apply to the case at hand." See also: DoD November 2011, p. 1: "[C]yberspace operations are … governed by all applicable domestic and international legal frameworks, including the protection of civil liberties and the law of armed conflict."

1.3 The Tallinn Manual and International Cyber Security Law

The *Tallinn Manual* does not claim to be the blueprint for an international convention on the use of force in or through cyberspace. But is there a body of law that deserves to be characterized as "international cyber security law" and, if so, how does the *Tallinn Manual* contribute to it?

1.3.1 The Tallinn Manual: A "Subsidiary Means for the Determination of Rules of Law"?

In view of the composition of the International Group of Experts and of the drafting process, the *Tallinn Manual* might qualify as a "subsidiary means for the determination of rules of law" in the sense of the International Court of Justice Statute's Article 38 (1) (d). It is, after all, a publication of what the expert participants agreed to by consensus with regard to the rules and principles of international law applicable to cyberspace. However, the label should not be attached too readily.

Each of the experts was hand-selected and most had worked intensively in the area of (cyber) security law. Moreover, they hailed from "various nations." The fact that they came from predominantly Western countries (the "North") and therefore did not represent the world's various legal cultures is not necessarily an obstacle to an application of Article 38 (1) (d). As has been noted, "one must admit that, as unfortunate as it is, the main doctrinal 'production' still comes from the North and more particularly from a handful of countries where international law has gained a rather high degree of sophistication."[38]

Still, the *Tallinn Manual* is not, and does not claim to be, a "subsidiary means for the determination of rules of law." This is not because the International Court of Justice has only rarely relied upon the "teachings of publicists", nor because the Manual's value is open to question.[39] Rather, the *Tallinn Manual* does not meet the requirements of Article 38 (1) (d) because its object and purpose is not to establish the existence of (new) rules of customary international law or to contribute to the progressive development of international law. The majority of rules and principles identified and analyzed were already recognized as belonging to customary international law. Hence, there was no need for in-depth scrutiny, evaluation, and classification of State practice. The few rules that the experts did not consider to be customary in nature were so identified and they have been

[38] Pellet 2006, p. 792 (MN 323).

[39] In the *Lotus* Case, the Permanent Court of International Justice seems to have had doubts "as to what their value may be from the point of view of establishing the existence of a rule of customary law". The SS Lotus, PCIJ, Ser. A, No. 10, p. 26.

limited in their scope of applicability to the Parties to the respective treaties from which they derive.

The *Tallinn Manual* is instead a restatement and analysis of the *lex lata*—no more, no less. Its unique feature is the application of the *lex lata* to a relatively new technological environment. The experts have merely identified possible State conduct in and through cyberspace, interpreted the applicable rules of international law, and provided solutions based upon a methodologically sound procedure. As with any interpretive endeavor, the findings of the experts can be challenged. States may even reject them as contrary to either their national and international security interests or their understanding of the law.

In that the Manual was produced through consensus by a group of experts, its black letter rules are an appropriate tool for States to employ in shaping their conduct in and through cyberspace. Moreover, it offers States normative options because the Commentary accompanying each rule clearly identifies those issues on which the experts were divided with respect to interpretation and application. In a sense, the *Tallinn Manual* is akin to the *San Remo Manual*[40] on the law of naval warfare and of the *AMW Manual*[41] on the law of air and missile warfare. Like those works, it intentionally examined issues about which States are concerned and for which they seek solutions. For instance, the U.S. Department of Defense identified the "issue of third-party sovereignty to determine what to do when the U.S. military is attacked, or U.S. military operations and forces are at risk in some other respect, by actions taking place on or through computer or other infrastructure located in a neutral country". Similarly, it highlighted the "issue of the legality of transporting cyber 'weapons' across the Internet through the infrastructure owned and/or located in neutral third countries without obtaining the equivalent of 'overflight right'."[42] These are matters that are dealt with extensively in the *Tallinn Manual*'s section on neutrality. Similarly, uncertainty exists as to the precise applicability of international humanitarian law to military operations in cyberspace, as well as to what cyber operations qualify as a use "use of force" under the *jus ad bellum*.[43] The existence of such uncertainty highlights the value of the *Tallinn Manual*.

1.3.2 The Tallinn Manual as Part of "International Cyber Security Law"?

It is obvious that the *Tallinn Manual* deals with important international law aspects of cyber security. Whether it can be considered as forming part of international

[40] Doswald-Beck 1995.

[41] HPCR 2009.

[42] DoD November 2011, p. 8.

[43] Ibid., p. 9.

cyber security law depends upon the definition of the term "international cyber security law." Fashioning the definition necessitates a brief look at the meaning of the terms "cyber security" and "cyber security policy."

"Cyber Security" refers to "the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein."[44] "Cyber security policy" includes "strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure."[45] Rules and principles of international law that contribute to the aims of 'cyber security policy' accordingly comprise "international cyber security law."

It would be premature to suggest that "international cyber security law" has become a distinct branch of international law. Moreover, "cyber security in general, and cyber operations in particular, fit into a wide range of paradigms, ranging from (internet) governance to warfare."[46] The assorted cyber security strategies demonstrate the impossibility of drawing clear dividing lines between the economic and social aspects of cyberspace on the one hand and the policy and military aspects on the other. The necessity of a multi-stakeholder approach and public–private-partnership vis-à-vis cyber security has blurred the traditional distinction between the public and a purely private spheres. Activities and operations in cyberspace are therefore subject to a wide range of international law rules that derive from neither the *jus ad bellum strictu* sensu nor of the *jus in bello*. For instance, State responses to cyber-attacks may have to be evaluated in the light of international telecommunications law, international trade law,[47] space law, international finance law, and international human rights law.[48] Consequently, "international cyber security law" is a collective term that encompasses rules and principles derived from multiple branches of international law.

Although the term "international cyber security law" denotes a cross-sectional area of international law, the *Tallinn Manual*'s rules belong to the panoply of norms encompassed by the label "international cyber security law."

---

[44] EU 2013, p. 3, fn 4.

[45] Cyberspace Policy Review 2009, p. 2.

[46] Ducheine et al. 2012, p. 110 *et seq*.

[47] Interference with foreign service providers may violate obligations under the GATS.

[48] See also EU 2013, p. 3: "The same laws and norms that apply in other areas of our day-to-day lives apply also in the cyber domain." See also Ducheine et al. 2012, p. 111 *et seq*.

1.3.3 The Potential Impact of the Tallinn Manual on International Cyber Security Law

Like-minded States agree that the "establishment of international cyberspace norms will … serve to strengthen cyberspace for the benefit of all."[49] They are determined "to work internationally to forge consensus regarding how norms of behavior apply to cyberspace, with the understanding that an important first step in such efforts is applying the broad expectations of peaceful and just interstate conduct to cyberspace."[50] By clarifying the scope of applicability of existing norms of international law governing the use of force, both prior to and during an (international) armed conflict, the *Tallinn Manual* fosters those efforts. Thus, a first fundamental contribution to the emergence and development of international cyber security law as a distinct branch of international law has been taken. At the very least, the Manual will serve as a basis for discussion in the process of achieving international consensus on the *jus ad bellum* and *jus in bello* applicable to State conduct in and through cyberspace.

An evaluation of the *Tallinn Manual* from a more cynical perspective could, however, give rise to concerns. Cyberspace is a highly complex domain in which the traditional distinction between the public and the private spheres no longer appears tenable. The very architecture of the globally-interconnected digital information and communications infrastructure, and the fact that modern societies have become so dependent on highly vulnerable critical infrastructure (including energy, banking and finance, transportation, communication, and the Defense Industrial Base[51])—seems to auger against the sectorial (and selective) approach to cyber security that underlies the *Tallinn Manual*. In other words, with its focus on the *jus ad bellum* and the *jus in bello,* the Manual might contribute to the fragmentation of 'international cyber security law' as a new branch of law.

Of particular note is the fact that both State and non-State actors—including organized criminals, terrorists, politically-motivated hackers, and others—possess the capabilities and intent to conduct cyber operations that could severely affect a State's economy and its water, healthcare, electricity, communications, and supply services.[52] Since such threats can no longer be clearly separated from each other, the only viable and sustainable solution is a holistic and coherent legal approach devoid of the traditional borders between rules applicable to the conduct of States and non-State actors. International law is far from the relatively coherent international legal order it was until the 1970's. The rapid progressive development of international law through treaty law has generated a multitude of international legal regimes that, to a certain extent, enjoy a life of their own. International trade

[49] DoD July 2011, p. 2.

[50] U.S. President 2011, p. 9.

[51] DoD July 2011, p. 1.

[52] EU 2013, p. 3.

law and international environmental law are but two examples for the said diversification and expansion of international law.[53] Rules of a highly technical nature, special treaty organs, and specialized international organizations increasingly seem disconnected from general international law. In particular, specialized institutions function through, *inter alia*, new mechanisms, sometimes with disregard for other applicable rules and principles of international law. Although international cyber security law, if it develops into a distinct branch of international law, may contribute to a further fragmentation of international law, a coherent legal approach would at least prevent sub-fragmentation. The international rules and principles agreed upon to counter cybercrime could then serve as guidelines for a new branch of international law that would deserve to be characterized "international cyber security law."

The fragmentation of international law is a phenomenon that reflects the desire of States to cleanly regulate particular aspects of their international relations. This trend will continue. It is therefore highly probable that in view of the urgency felt by governments regarding cyber issues, cyber security law will soon become a distinct branch of international law. The like-minded States are already determined to "work internationally to forge consensus regarding how norms of behavior apply to cyberspace."[54] Convinced that "international cyberspace norms will enhance the stability and predictability of State conduct in cyberspace," States are pursuing "bilateral and multilateral engagements to develop further norms that increase openness, interoperability, security, and reliability."[55]

It is doubtful that the sectorial/selective approach adopted in the *Tallinn Manual* will indelibly fragment (a prospective) "international cyber security law." States see the on-going efforts to clarify the *jus ad bellum* and the *jus in bello* as merely "an important first step"[56] in the overall process of international cyber security norm creation. It is unquestionable that the *Tallinn Manual*'s findings on various matters will eventually be supplemented by additional rules that will facilitate coherent legal approach. Coherence implies that international cyber security law would form a unified whole that enables States to preserve and enhance cyber security against all identified threats. It is typical that States initially concentrate on select, usually fundamental, rules and principles that are subsequently refined and supplemented to address a given issue in its entirety.

An important caveat exists. While the *Tallinn Manual* rules may become an integral part of a future "international cyber security law," they must not be allowed to replace concepts that distinguish between the private and the public spheres. In particular, any assimilation of State conduct to criminal conduct ought

---

[53] For some of the issues of the fragmentation of international law see International Law Commission, Report on the 57th session (2 May–3 June and 11 July–5 August 2005), Chapter XI, UNGA, Official Records, Sixtieth Session, Supplement No. 10 (UN Doc. A/60/10).

[54] U.S. President 2011, p. 9.

[55] DoD November 2011, p. 5 *et seq*.

[56] U.S. President 2011, p. 9.

to be avoided. The mere facts that both employ similar methods and means which may have similar effects does not justify abandoning this long-standing distinction. For instance, it would be a grave mistake if the military was subject to the same rules as private companies, individuals or non-State actors.

The decision by States to resort to the use of armed force remains an accepted "continuation of politics by other means"[57]—it is a fact of life. It would be naïve to believe that the contemporary United Nations system of collective security has been sufficiently developed to abolish the use of force in international relations. There are situations in which even the most peace-loving government may come to the conclusion that it must use its armed forces to achieve a given political goal. Such situations are not limited to the exercise of the inherent right of self-defense or to the enforcement of UN Security Council resolutions. The use of military force may also be the last resort when it comes to terminating gross and systematic violations of human rights[58] or to suppressing substantial organized crime. Governments will continue to make use of their armed forces for legitimate—and sometimes illegitimate—purposes. If, however, governments wish to preserve the military option, the operations of their (regular) armed forces must be judged on the basis of legal rules specifically designed for the conduct of States, i.e., the *jus ad bellum* and the *jus in bello*. If governments accepted the application of a unified body of international rules on cyber security that no longer distinguishes between State conduct on the one hand and the conduct of non-State actors on the other hand, the military option would simply be unavailable.

To reiterate, a coherent legal approach to cyber security is not jeopardized by the private–public distinction. Coherency does not exclude sub-systems or sub-regimes that have a limited and separate scope of applicability. In their entirety, the rules serve the same purpose—preserving and enhancing cyber security.

1.4 Concluding Remarks

The *Tallinn Manual*'s rules and interpretations may not be shared by everyone, but they represent the consensus view of a select group of scholars and practitioners who thoroughly analyzed the *lex lata*. As such, the *Tallinn Manual* will contribute to the legal discourse by serving as a basis upon which further scholarly work can build. Moreover, States should welcome the *Tallinn Manual* as a starting point in the process of forging agreement with other States on the applicability and scope of the rules and principles of international law governing the use of force and the conduct of hostilities in and through cyberspace.

---

[57] Clausewitz 1832/34.

[58] For the legality or illegality of humanitarian intervention see Byers and Chesterman 2003, pp. 177–203; Franck 2003, pp. 204–231. See also the statements on the Kosovo Campaign by Henkin et al. 1999, pp. 824–862.

Of course, the *Tallinn Manual* merely covers one, although highly relevant, facet of international cyber security law. This focus is adequate because a clarification of the applicability of the *jus ad bellum* and of the *jus in bello* to operations in and through cyberspace was overdue. Hence, the present contribution is far from criticizing the underlying approach. Any criticism by this author would in any event be quite odd since he actively and directly participated in the work of the Group of Experts and in the final drafting of the Manual. Still, much more needs to be done. International cyber security law is not a self-contained, established and highly-developed legal regime. For the time-being it is but a label for a legal cross-sectional area consisting of a panoply of rules and principles derived from most diverse fields of international law whose principal applicability to cyberspace and whose concurrence have not yet been fully analyzed. The same holds true for the role of the various stakeholders and for the critical issue of balancing democratic and economic freedoms on the one hand and security interests on the other hand.

References

Byers M, Chesterman S (2003) Changing the Rules about Rules? Unilateral Humanitarian Intervention and the Future of International Law. In: Holzgrefe J, Keohane R (eds.) (2003) Humanitarian Intervention, Cambridge University Press, Cambridge, pp 177–203.

Clausewitz C (1832/34) Vom Kriege, Book I, Section 24.

Cyberspace Policy Review (2009) Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf. Accessed 22 May 2013.

DoD (Department of Defense U.S) (July 2011)Strategy for Operating in Cyberspace http://www.defense.gov/news/d20110714cyber.pdf. Accessed 22 May 2013.

DoD (Department of Defense U.S) (November 2011) Cyberspace Policy Report - A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934 http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf. Accessed 22 May 2013.

Doswald-Beck L (ed.) (1995) San Remo Manual on International Law Applicable to Armed Conflicts at Sea. Cambridge University Press, Cambridge.

Ducheine P, Voetelink J, Stinissen J, Gill T (2012) Towards a Legal Framework for Military Cyber Operations. In: Ducheine P, Osinga F, Soeters J (ed) (2012) Cyber Warfare: Critical Perspectives. T.M.C. Asser Press, The Hague, pp 101–128.

EU (2013) Draft Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels.

Franck T (2003) Interpretation and Change in the Law of Humanitarian Intervention. In: Holzgrefe J, Keohane R (eds.) (2003) Humanitarian Intervention. Cambridge University Press, Cambridge pp 204–231.

HPCR (Harvard Program on Humanitarian Policy and Conflict Research) (2009) Manual on International Law Applicable to Air and Missile Warfare. Bern.

Henkin L, Wedgwood R, Charney J, Chinkin C, Falk R, Franck T, Reisman W (1999) 93 AJIL, pp 824–862.

Lynn W (2010) Defending an New Domain. 89 Foreign Affairs, pp 97–108.

Pellet A (2006) Article 38. In: Zimmermann A, Tomuschat C, Öllers-Frahm K (ed) The Statute of the International Court of Justice—A Commentary, Oxford University Press, pp 677–792

http://www.alainpellet.eu/Documents/PELLET%20%202006%20%20Article%2038%20of%20the%20Statute%20of%20the%20ICJ.pdf. Accessed 22 May 2013.

Schmitt M (2013) Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press, New York.

U.S. President (2011) International Strategy for Cyberspace. Washington, D.C.

White House (2012) Sustaining U.S. Global Leadership: Priorities for 21st Century Defense. http://www.defense.gov/news/defense_strategic_guidance.pdf. Accessed 22 May 2013.

Wingfield T (2000) The Law of Information Conflict: National Security Law in Cyberspace. Aegis Research Corp, Falls Church.

Chapter 2
The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II—The Use of Force

Nicholas Tsagourias

Contents

2.1 Introduction

Cyberspace and cyber technology are increasingly used by states and individuals for peaceful purposes, but they are also employed maliciously. Cyber attacks—that is, the use of cyber technology to attack a state's infrastructure—are perhaps one of the most serious threats currently facing states. Although not all cyber attacks are warlike, some of them may indeed be so, which immediately gives rise to the

The author is Professor of International Law, University of Sheffield.

N. Tsagourias (✉)
University of Sheffield, Sheffield, UK
e-mail: n.tsagourias@sheffield.ac.uk

T. D. Gill et al. (eds.), *Yearbook of International Humanitarian Law 2012*,
Yearbook of International Humanitarian Law 15, DOI: 10.1007/978-90-6704-924-5_2,

question of whether the current legal regulation of the use of force (*jus ad bellum*) applies to such attacks. *The 'Tallinn Manual' on the International Law Applicable to Cyber Warfare* responds to this question by mapping out the *jus ad bellum* and *jus in bello* rules that apply in such circumstances. The statement of the Rules is accompanied by a Commentary which clarifies the content of those rules, and explains their application in the specific context of cyber war.

In the following, I will present and critically comment on the *jus ad bellum* rules found in Chapter II of the *Tallinn Manual:* that is, Rules 10–19. The aim of this commentary is to draw attention to certain important but contested issues, identify jurisprudential ambiguities, and where possible offer alternative views.

2.2 The Rules

2.2.1 Rule 10: Prohibition of Threat or Use of Force

According to Rule 10, 'A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any state, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful.'

This rule is a reflection of Article 2(4) of the UN Charter, but also of customary international law.[1] Although the application of this rule to cyber war is in principle undisputed, its scope is subject to debate. According to the Manual, the prohibition of the threat or use of force binds members of the United Nations (UN) and, as a customary rule it also applies to states that are not members of the United Nations but does not apply to non-state actors unless their acts are attributable to a state, pursuant to the law of state responsibility.[2] In this respect, the Manual adopts a state-oriented approach as far as the prohibition of the threat or use of force is concerned but, as will be seen later, it accepts that a non-state actor can be the author of an armed attack and, consequently, the target of self-defence action. If an armed attack by a non-state actor is in fact a use of force, albeit a grave one, a non-state actor can also be the author of a less grave use force. Indeed, as the Report of the Secretary-General's High-level Panel on Threats, Challenges and Change acknowledged, non-state actors are able and willing to use force against states.[3] One could thus say that the prohibition of the threat or use of force should apply to

[1] For the application of Article 2(4) to cyber attacks see Waxman 2011, p. 421; Roscini 2010, pp. 102–109; Barkham 2001, pp. 57, 69–73, 79–80.

[2] Rule 10, para 5. See also Simma et al. 2012, pp. 213–4. For attribution see Rule 6 and accompanying text.

[3] As it was stated there: 'Al-Qaida is the first instance—not likely to be the last—of an armed non-state network with global reach and sophisticated capacity. Attacks against more than 10 Member States on four continents … have demonstrated that Al-Qaida and associated entities pose a universal threat to the membership of the United Nations and the United Nations itself.'