Introduction

In 2009, the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), an international military organization based in Tallinn, Estonia, and accredited in 2008 by NATO as a 'Centre of Excellence', invited an independent 'International Group of Experts' to produce a manual on the law governing cyber warfare.[1] In doing so, it followed in the footsteps of earlier efforts, such as those resulting in the International Institute of Humanitarian Law's *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*[2] and the Harvard Program on Humanitarian Policy and Conflict Research's *Manual on International Law Applicable to Air and Missile Warfare*.[3] The project brought together distinguished international law practitioners and scholars in an effort to examine how extant legal norms applied to this 'new' form of warfare. Like its predecessors, the *Manual on the International Law Applicable to Cyber Warfare*, or '*Tallinn Manual*', results from an expert-driven process designed to produce a non-binding document applying existing law to cyber warfare.

Cyber operations began to draw the attention of the international legal community in the late 1990s. Most significantly, in 1999 the United States Naval War College convened the first major legal conference on the subject.[4] In the aftermath of the attacks of 11 September 2001, transnational terrorism and the ensuing armed conflicts diverted attention from the topic until the massive cyber operations by 'hacktivists'

[1] The NATO CCD COE is neither part of NATO's command or force structure, nor funded by NATO. However, it is part of a wider framework supporting NATO Command Arrangements. Located in Tallinn, its present Sponsoring Nations are Estonia, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, and the United States.

[2] San Remo Manual. [3] AMW Manual.

[4] The proceedings were published as Computer Network Attack and International Law, 76 Naval War College International Law Studies (Michael N. Schmitt and Brian T. O'Donnell eds., 2002).

against Estonia in 2007 and against Georgia during its war with the Russian Federation in 2008, as well as cyber incidents like the targeting of the Iranian nuclear facilities with the Stuxnet worm in 2010.

These and other events have focused the attention of States on the subject. For instance, in its 2010 *National Security Strategy* the United Kingdom characterized 'cyber attack, including by other States, and by organised crime and terrorists' as one of four 'Tier One' threats to British national security, the others being international terrorism, international military crises between States, and a major accident or natural hazard.[5] The United States' 2010 *National Security Strategy* likewise cited cyber threats as 'one of the most serious national security, public safety, and economic challenges we face as a nation'[6] and in 2011 the US Department of Defense issued its *Strategy for Operating in Cyberspace*, which designates cyberspace as an operational domain.[7] In response to the threat, the United States has now established US Cyber Command to conduct cyber operations.

During the same period, Canada launched *Canada's Cyber Security Strategy*,[8] the United Kingdom issued *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digitized World,*[9] and Russia published its cyber concept for the armed forces in *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Information Space*.[10] NATO acknowledged the new threat in its 2010 *Strategic Concept*, wherein it committed itself to 'develop further our ability to prevent, detect, defend against and recover from cyber attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations'.[11]

[5] HM Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* 11 (2010).
[6] The White House, *National Security Strategy* 27 (2010).
[7] Department of Defense, *Strategy for Operating in Cyberspace* (2011).
[8] Government of Canada, *Canada's Cyber Security Strategy* (October 2010).
[9] HM Government, *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digitized World* (2011).
[10] Russian Federation, *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Information Space* (2011).
[11] NATO, *Active Defence, Modern Engagement: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization: Active Engagement, Modern Defence* 16–17 (2010).

One of the challenges States face in the cyber environment is that the scope and manner of international law's applicability to cyber operations, whether in offence or defence, has remained unsettled since their advent. After all, at the time the current international legal norms (whether customary or treaty-based) emerged, cyber technology was not on the horizon. Consequently, there is a risk that cyber practice may quickly outdistance agreed understandings as to its governing legal regime.

The threshold questions are whether the existing law applies to cyber issues at all, and, if so, how. Views on the subject range from a full application of the law of armed conflict, along the lines of the International Court of Justice's pronouncement that it applies to 'any use of force, regardless of the weapons employed',[12] to strict application of the Permanent Court of International Justice's pronouncement that acts not forbidden in international law are generally permitted.[13] Of course, the fact that States lack definitive guidance on the subject does not relieve them of their obligation to comply with applicable international law in their cyber operations.[14]

The community of nations is understandably concerned about this normative ambiguity. In 2011, the United States set forth its position on the matter in the *International Strategy for Cyberspace*: 'The development of norms for State conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding State behavior – in times of peace and conflict – also apply in cyberspace.'[15] Nevertheless, the document acknowledged that the 'unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them'.[16]

This project was launched in the hope of bringing some degree of clarity to the complex legal issues surrounding cyber operations, with

[12] *Nuclear Weapons* Advisory Opinion, para. 39.

[13] The Permanent Court of International Justice famously asserted that 'The rules of law binding upon States … emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims.' *Lotus* case at 18.

[14] For the view that the law of armed conflict applies to cyber warfare, see International Committee of the Red Cross, *International Humanitarian Law and Challenges of Contemporary Armed Conflicts*, ICRC Doc. 31IC/11/5.1.2 36–7 (October 2011).

[15] *White House Cyber Strategy* at 9.

[16] *White House Cyber Strategy* at 9.

particular attention paid to those involving the *jus ad bellum* and the *jus in bello*. The result is this '*Tallinn Manual*'.

Scope

The *Tallinn Manual* examines the international law governing 'cyber warfare'.[17] As a general matter, it encompasses both the *jus ad bellum*, the international law governing the resort to force by States as an instrument of their national policy, and the *jus in bello*, the international law regulating the conduct of armed conflict (also labelled the law of war, the law of armed conflict, or international humanitarian law). Related bodies of international law, such as the law of State responsibility and the law of the sea, are dealt with in the context of these topics.

Cyber activities that occur below the level of a 'use of force' (as this term is understood in the *jus ad bellum)*, like cyber criminality, have not been addressed in any detail. Nor have any prohibitions on specific cyber actions, except with regard to an 'armed conflict' to which the *jus in bello* applies. For instance, the Manual is without prejudice to other applicable fields of international law, such as international human rights or telecommunications law. The legality of cyber intelligence activities is examined only as they relate to the *jus ad bellum* notions of 'use of force' and 'armed attack', or as relevant in the context of an armed conflict governed by the *jus in bello*. Although individual States and those subject to their jurisdiction must comply with applicable national law, domestic legislation and regulations have likewise not been considered. Finally, the Manual does not delve into the issue of individual criminal liability under either domestic or international law.

In short, this is not a manual on 'cyber security' as that term is understood in common usage. Cyber espionage, theft of intellectual property, and a wide variety of criminal activities in cyberspace pose real and serious threats to all States, as well as to corporations and private individuals. An adequate response to them requires national and international measures. However, the Manual does not address such matters because application of the international law on uses of force and armed conflict plays little or no role in doing so. Such law is no more applicable to these threats in the cyber domain than it is in the physical world.

[17] The term 'cyber warfare' is used here in a purely descriptive, non-normative sense.

The *Tallinn Manual*'s emphasis is on cyber-to-cyber operations, *sensu stricto*. Examples include the launch of a cyber operation against a State's critical infrastructure, or a cyber attack targeting enemy command and control systems. The Manual is not intended for use in considering the legal issues surrounding kinetic-to-cyber operations, such as an aerial attack employing bombs against a cyber control centre. It likewise does not address traditional electronic warfare attacks, like jamming. These operations are already well understood under the law of armed conflict.

Finally, the Manual addresses both international and non-international armed conflict. The Commentary indicates when a particular Rule is applicable in both categories of conflict, limited to international armed conflict, or of uncertain application in non-international armed conflict. It should be noted in this regard that the international law applicable to international armed conflict served as the starting point for the legal analysis. An assessment was subsequently made as to whether the particular Rule applies in non-international armed conflict.

The Rules

There are no treaty provisions that directly deal with 'cyber warfare'. Similarly, because State cyber practice and publicly available expressions of *opinio juris* are sparse, it is sometimes difficult to definitively conclude that any cyber-specific customary international law norm exists. This being so, any claim that every assertion in the Manual represents an incontrovertible restatement of international law would be an exaggeration.

This uncertainty does not mean cyber operations exist in a normative void. The International Group of Experts was unanimous in its estimation that both the *jus ad bellum* and *jus in bello* apply to cyber operations. Its task was to determine how such law applied, and to identify any cyber-unique aspects thereof. The Rules set forth in the *Tallinn Manual* accordingly reflect consensus among the Experts as to the applicable *lex lata*, that is, the law currently governing cyber conflict. It does not set forth *lex ferenda,* best practice, or preferred policy.

When treaty law directly on point or sufficient State practice and *opinio juris* from which to discern precise customary international law norms was lacking, the International Group of Experts crafted the Rules broadly. In these cases, the Experts agreed that the relevant principle of

law extended into the cyber realm, but were hesitant to draw conclusions as to its exact scope and application in that context. Where different positions as to scope and application existed, they are reflected in the accompanying Commentary.

To the extent the Rules accurately articulate customary international law, they are binding on all States, subject to the possible existence of an exception for persistent objectors. At times, the text of a Rule closely resembles that of an existing treaty norm. For instance, Rule 38 regarding military objectives is nearly identical to the text of Article 52(2) of Additional Protocol I. In such cases, the International Group of Experts concluded that the treaty text represented a reliable and accurate restatement of customary international law. Users of this Manual are cautioned that States may be subject to additional norms set forth in treaties to which they are Party.

The Rules were adopted employing the principle of consensus within the International Group of Experts. All participating experts agreed that, as formulated, the Rules replicate customary international law, unless expressly noted otherwise. It must be acknowledged that at times members of the Group argued for a more restrictive or permissive standard than that eventually agreed upon. The Rule that emerged from these deliberations contains text regarding which it was possible to achieve consensus.

Although the observers (see below) participated in all discussions, the unanimity that was required for adoption of a Rule was limited to the International Group of Experts. Therefore, no conclusions can be drawn as to the position of any entity represented by an Observer with regard to the Rules.

The Commentary

The Commentary accompanying each Rule is intended to identify its legal basis, explain its normative content, address practical implications in the cyber context, and set forth differing positions as to scope or interpretation. Of particular note, the International Group of Experts assiduously sought to capture all reasonable positions for inclusion in the *Tallinn Manual*'s Commentary. As neither treaty application nor State practice is well developed in this field, the Group considered it of the utmost importance to articulate all competing views fully and fairly for consideration by users of the Manual.

Since the Commentary includes a variety of perspectives, users should not conclude that individual members of the International Group of Experts supported any particular position set forth therein. All that should be concluded is that every reasonable position that arose during Group proceedings – as well as those offered by observers, States, and outside experts – is included in the Commentary. For instance, although all members of the International Group of Experts agreed that launching cyber attacks against civilians or civilian objects is unlawful (Rules 32 and 37), views differed as to which operations qualify as 'attacks', as that term is used in the law of armed conflict.

Terminology posed a particular obstacle to the drafting of the *Tallinn Manual*. Many words and phrases have common usage, but also have specific military or legal meanings. For instance, the word 'attack' is commonly used to refer to a cyber operation against a particular object or entity, and in the military sense it usually indicates a military operation targeting a particular person or object. However, attack in the *jus ad bellum* sense, qualified by the word 'armed', refers to a cyber operation that justifies a response in self-defence (Rule 13), whereas the term as used in the *jus in bello* indicates a particular type of military operation that involves the use of violence, whether in offence or defence (Rule 30). Similarly, a 'military objective' in common military usage refers to the goal of a military operation. Yet, as employed in the *jus in bello* the term refers to objects that may be made the lawful object of 'attack', subject to other rules of the law of armed conflict (Rule 38). Users of this Manual are cautioned it employs most terminology in its international law sense, subject to particular meanings set forth in the Glossary.

Significance of sources, citations, and evidence in support of the Rules

Numerous sources were drawn on to develop the Rules and Commentary. Of course, treaty law is cited throughout for the propositions set forth. Customary law posed a greater challenge. In this regard, three sources were of particular importance. The Manual draws heavily on the ICRC Customary IHL Study, as it is a valuable repository of evidence and analysis regarding customary law in both international and non-international armed conflict. The AMW Manual also proved especially valuable because it addresses customary law in both international and non-international law. Finally, the International Group of Experts frequently considered the NIAC Manual when assessing whether a

particular Rule applies during non-international armed conflict. With the exception of treaty law, all of the aforementioned sources were persuasive, but not dispositive, evidence of a norm's status as customary international law. Ultimately, the professional knowledge, experience, and expertise of the Experts form the basis for the *Tallinn Manual*'s conclusions as to the customary status of a Rule or its extension into non-international armed conflict.

The International Group of Experts regularly referenced the military manuals of four States – Canada, Germany, the United Kingdom, and the United States. The international legal community generally considers these four manuals to be especially useful during legal research and analysis with respect to conflict issues, although their use should not be interpreted as a comment on the quality of any other such manuals. Moreover, the International Group of Experts included members who participated in the drafting of each of the four manuals. These members were able to provide invaluable insight into the genesis, basis, and meaning of specific provisions. Finally, unlike many other military manuals, these four are all publicly available.

Among the manuals, the US Commander's Handbook served an additional purpose. Unlike Canada, Germany, and the United Kingdom, the United States is not a Party to either of the 1977 Additional Protocols to the 1949 Geneva Conventions, two key sources relied on during the project. The International Group of Experts took the position that the appearance of an Additional Protocol norm in the Handbook was an indication (but not more) of its customary nature. Of course, in doing so they were very sensitive to the fact that the Handbook is a military manual, not a legal treatise, and as such also reflects operational and policy considerations. At the same time, the Experts equally acknowledged that the fact that a State is party to the Additional Protocols does not mean that a provision of its own military manual is reflective only of treaty law.

The International Group of Experts accepted the position held by the International Court of Justice that the 1907 Hague Regulations reflect customary international law[18] and that most of the provisions of the 1949 Geneva Conventions have achieved the same status (a point of lesser significance in light of their universal ratification).[19] These instruments

[18] *Wall* Advisory Opinion, para. 89; *Nuclear Weapons* Advisory Opinion, para. 75. *See also Nuremburg* Tribunal judgment at 445.

[19] *Nuclear Weapons* Advisory Opinion, paras. 79, 82. *See also* Report of the Secretary-General Pursuant to Paragraph 2 of Security Council Resolution 808, UN SCOR, para. 35,

were accordingly particularly significant to the Experts in their deliberations regarding the customary status of a Rule.

Lastly, secondary sources, such as law review articles and books, are seldom cited. The International Group of Experts agreed that such citations are generally inappropriate in a manual. They accordingly appear only when particularly relevant on a certain point. Nevertheless, the Experts relied regularly on academic scholarship during their research.

Note that many sources are cited as support for the legal principles set forth in the *Tallinn Manual* (or their interpretation or application). This does not necessarily mean that the International Group of Experts viewed them as legal sources of the Rule or Commentary in question. For instance, the AMW Manual is often cited in order to draw attention to the acceptance of a particular principle in the context of air and missile warfare by the Experts involved in that project. However, the AMW Manual itself does not represent the legal source of any Rules or Commentary contained in the *Tallinn Manual*. Similarly, military manuals are not cited as a source of any particular Rule or Commentary, but rather for the purpose of alerting the reader to a State's acceptance of the general legal principle involved.

The International Group of Experts

Members of the International Group of Experts were carefully selected to include legal practitioners, academics, and technical experts. In particular, the Group's legal practitioners addressed, or had addressed, cyber issues in their professional positions, whereas the academics selected were recognized world-class experts on the *jus ad bellum* and *jus in bello*. This mix is crucial to the credibility of the final product. So too is the inclusion of technical experts who provided input to the discussions and the text to ensure the Manual was practically grounded and addressed key issues raised by actual or possible cyber operations.

Three organizations were invited to provide observers to the process. The observers participated fully in the discussions and drafting of the Manual, but their consent was not necessary to achieve the unanimity required for adoption of a Rule. NATO's Allied Command Transformation provided an observer to provide the perspective of a multinational

UN DOC. S/25704 (1993). The Security Council unanimously approved the statute to which the report referred. S.C. Res. 827, UN Doc. S/RES/827 (25 May 1993).

user of the Manual. The US Cyber Command's representative offered the perspective of a relevant operationally mature entity. Finally, the International Committee of the Red Cross was invited to observe and participate in the proceedings in view of the organization's special role *vis-à-vis* the law of armed conflict. Despite the invaluable active participation of the observers in the process, this Manual is not intended to reflect the legal positions or doctrine of any of these three organizations.

Drafting process

In September 2009, a small group met in Tallinn to consider the possible launch of a project to identify the relevant legal norms governing cyber warfare. The group quickly concluded such an effort was worthwhile and, therefore, went on to scope the project and draft a notional table of contents for a manual on the subject.

Based on that work, a larger International Group of Experts was invited to begin the drafting process. Initially, all members of the Group were tasked with researching and preparing proposed Rules on particular topics and an outline of the Commentary that might accompany them. The resulting inputs were combined into a first draft of the Manual.

The text of this draft was then split among three teams of Experts led by Group Facilitators. These teams were charged with refining the first draft. At subsequent meetings of the International Group of Experts, they presented their revised proposed Rules and accompanying Commentary. The meetings were designed to reach consensus on the precise text of the Rules and agreement that the Commentary reflected all reasonable views as to their meaning, scope, and application. At times, the resulting text was sent back into the teams for further consideration. In all, eight plenary meetings of three days each were held in Tallinn between 2010 and 2012.

Upon completion of the plenary sessions, an Editorial Committee drawn from among the International Group of Experts worked on the Manual to ensure the accuracy, thoroughness, and clarity of the Commentary. This team met twelve times in Tallinn or Berlin. The resulting draft was then divided among peer reviewers with deep expertise in the various subjects addressed by the Manual for comment. The Editorial Committee considered these comments and revised the Manual as appropriate. In July 2012, the International Group of Experts convened for a final time in Tallinn to consider the final draft, make any final changes, and approve both the Rules and the Commentary.