Introduction

Michael Schmitt

Since the digital revolution, the exponential growth of information and communication technology has created a complex web of networked systems. This is the new and vibrant environment that we know as cyberspace. More specifically, cyberspace is the 'global domain within the information environment consisting of the interdependent network of information technology infrastructure, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers'.[1]

Over the course of the last three decades, cyberspace has been 'woven into the fabric of daily life'[2] and now permeates all aspects of modern society. Millions of people, organisations, governmental and public institutions, corporations and businesses use cyberspace every day to communicate, gather or exchange information, bank, shop, do business, distribute energy, govern and exert influence. By December 2013, 39 per cent of the world population used the internet (with usage in Europe being 68.6 per cent and in North America 84.9 per cent), an increase of 676.3 per cent since 2000.[3]

Notwithstanding the enormous benefits and advantages it offers, cyberspace has also become a repository for various threats, vulnerabilities and insecurities. They may originate from governments, organised groups, individuals, or businesses, be intentional or accidental and have financial, military, political or other aims. For instance, conventional crime is metastasising to the cyber domain with criminals using networks and cyber tools. Cyber theft, cyber fraud, the sale of illegal products, blackmail, pornography and copyright and intellectual property theft are common occurrences that can generate deleterious financial, personal, and even political consequences.[4] State security can be compromised by military-like and non-military-like cyber attacks targeting critical national infrastructure and other essential assets and activities.

[1] Joint Chiefs of Staff, Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms* (8 November 2010) (as amended through 15 June 2014) 64. The International Telecommunications Union describes cyberspace as 'systems and services connected either directly or indirectly to the internet, telecommunications and computer networks'; ITU, *ITU National Strategy Guide* (Geneva: ITU, 2011) 5, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf accessed 13 October 2014.

[2] 69th Session of the UN General Assembly A/69/112 (30 June 2014) 4, foreword by the UN Secretary-General, http://undocs.org/A/69/112 accessed 13 October 2014.

[3] Internet World Stats: Usage and Population Statistics (26 September 2014), http://www.internetworldstats.com/stats.htm accessed 13 October 2014.

[4] In the UK, the cost of cybercrime to the UK has been estimated to be around £27bn per annum of which £3.1 is the cost to citizens, £2.2 the cost to government and £21bn to business; UK Cabinet Office and Detica, *The Cost of Cyber Crime: A Detica Report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office* (Guildford, Surrey: Detica Limited, 2011), 18–24.

Terrorists may begin to use cyberspace to perpetuate terrorist acts; they already use it for recruitment, training, propaganda and funding purposes.[5]

The unique characteristics of cyberspace magnify both its potential benefits and risks. At its core, cyberspace is a virtual environment; it is not subject to a time-space continuum and is thus unconstrained by the limitations that these characteristics impose. In this virtual environment, no physical action takes place. Instead, information is transferred instantly through interconnected networks that transcend physical, legal or political borders. In cyberspace actors can often maintain their anonymity. For instance, efforts to trace cyber attacks encounter serious legal and technical obstacles because they may operate through different networks.

Its unique characteristics make cyberspace a challenging environment for legal regulation. Important questions arise about the role and efficacy of law, particularly international law, in regulating cyber activities and cyberspace. In the immediate years that followed the advent of cyber activities, some legal commentators claimed that existing legal frameworks – whether it be national, regional or international law – are inapplicable to cyberspace.[6] The argument was that existing legal frameworks were designed to regulate physical, geographically defined territories. In contrast, cyberspace is a virtual domain that is global in scope but technically borderless. It was thus proposed that cyberspace should be governed by a *sui generis* regulatory framework, one devised and shaped by its users according to the specific features and needs of this new domain. What they anticipated was the emergence of a subject-specific 'law of cyberspace'.

In recent years, states have made it clear that existing legal frameworks continue to apply to cyberspace. For example, the UN Group of Governmental Experts established by the UN Secretary-General to review existing and potential threats from cyberspace stated in its 2013 report that '[i]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment' and that 'State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory'.[7] Similarly, in 2014 NATO's heads of state agreed '[o]ur policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace'.[8]

This is not to say however that the application of these legal frameworks is uncontested or unproblematic. Indeed, this is particularly the case with international

---

[5] See generally UN Office on Drugs and Crime: The Use of the Internet for Terrorist Purposes (2012), http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf accessed 13 October 2014.

[6] D Johnson and D Post, 'Law and borders – The rise of law in cyberspace' (1996) 48 *Stanford Law Review* 1367.

[7] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security UN Doc, A/68/98 (24 June 2013) paras 19–20, http://www.mofa.go.jp/files/000016407.pdf accessed 13 October 2014.

[8] Wales Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales (5 September 2014), para 72, http://www.nato.int/cps/en/natohq/official_texts_112964.htm accessed 13 October 2014.

law because it very much adopts a state-based structure that is preoccupied with notions of territory. With this in mind, the objective of this research handbook is to map out the international rules and regulatory frameworks that apply to cyberspace in general and to specific activities in cyberspace in particular. For this reason it brings together leading international law scholars and practitioners to critically assess the application of various international law principles and regimes to cyberspace.

Before I proceed to provide an overview of the contents of the book, allow me to offer a few words about the originality and importance of this project. As a result of the widespread media attention dedicated to the topic of cyber war, a great deal of scholarly attention has been directed towards examining whether and how international law applies to cyber attacks that is, military-like attacks on states by other states or non-state actors. The *Tallinn Manual on the International Law applicable to Cyber Warfare*, for example, has made a significant contribution to clarifying the application of international laws relating to cyber uses of force and armed conflict involving cyber operations.[9] The present collection builds upon that research with chapters addressing both the *jus ad bellum* and *jus in bello*.

However, much less attention has been focused upon the role of international law in addressing other threats in and from cyberspace, such as cyber terrorism, cyber crime and cyber espionage. The present research handbook responds to such a need. The handbook also assesses the cyber security policies of a number of international organisations, such those of the EU, NATO, and the UN, and assesses Asian approaches to achieving and maintaining cyber security. This research handbook thus makes a very important contribution in the field of cyber security by assessing the application of international law to these different types of cyber threats.

The normative scope of the handbook is likewise broad. It examines the status as well as the governance structures that apply to cyberspace. Accordingly, it contains chapters on the legal character of cyberspace and the application of general principles of international law to cyberspace, such as the law of state responsibility, international human rights law, international criminal law and intellectual property law.

The result is a handbook that for the first time provides a comprehensive account of the international legal rules that apply to cyberspace, engages in a systematic analysis of how they do so, and provides an assessment of their suitability and effectiveness. Moreover, where the regulatory functions performed by international law in cyberspace are found lacking, this handbook offers suggestions for new regulatory regimes or interpretations of existing rules that can deal more effectively with cyber activities. In sum, the present research handbook contributes to the creation of a common base of knowledge in this field.

As such, it is essential reading for policy makers, lawyers, political scientists, the military and police, technologists, researchers or students who want or need to know, understand or apply the international regulatory framework governing cyberspace and cyber activities. I heartily congratulate the individual authors and both editors for their efforts in bringing this important project to successful completion. It is a work that will influence and shape this complex, but increasingly central, facet of international law.

---

[9] M Schmitt (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare (CUP, 2013).

OVERVIEW OF THE CHAPTERS

The first part of the handbook comprises five chapters that focus upon the application of general principles of international law to cyberspace. In the opening chapter, Nicholas Tsagourias examines the legal status of cyberspace under international law. He challenges the position that because state sovereignty has been historically associated with control over physical territory, and that because cyberspace is a domain that states cannot subject to territorial claims, states cannot therefore exercise sovereignty in cyberspace. Tsagourias disentangles sovereignty from territory. In doing so, he argues that states are able to exercise sovereignty and thus jurisdiction over persons, objects and actions in cyberspace. He then explores the question of whether cyberspace can itself be sovereign and goes on to consider the legal implications of treating cyberspace as a global commons. Tsagourias concludes by suggesting a global treaty to regulate cyberspace, albeit explaining that one is not possible at this stage.

In Chapter 2 Uta Kohl assesses the conditions under which states can exercise jurisdiction in cyberspace. Kohl argues that state practice indicates that states exercise jurisdiction in cyberspace on the basis of the objective territoriality principle, meaning that a state will assert jurisdiction over online activity if the effects of that activity are felt on its territory. Although Kohl concedes that this is a common-sense approach, she nevertheless concludes that the approach is likely to artificially fragment the internet, an inherently global domain, into a web of national cyberspaces. The impact, Kohl concludes, is that this may jeopardise the enjoyment of fundamental human rights such as freedom of expression in cyberspace and may, more broadly, endanger the potential for economic, political, social and cultural exchange.

In Chapter 3 Constantine Antonopoulos suggests that although the rules relating to the responsibility of states for internationally wrongful acts apply to state conduct in cyberspace, such applicability is fraught with difficulties because this legal framework is premised upon the assumption that internationally wrongful acts are capable of attribution to states. As Antonopoulos explains, this is problematic in the context of cyberspace because of its unique characteristics, such as the anonymity that cyberspace affords. In light of this, he argues that the best solution is to subject states to a duty of due diligence to prevent computer systems that are subject to their jurisdiction from being used to commit acts that are injurious to other states.

Chapter 4 assesses the extent to which international law protects intellectual property rights in cyberspace. This is an important question since cyberspace can act as a venue for intellectual property rights, while the protection of such rights may be technically difficult. Andreas Rahmatian contrasts cyberspace with the territorial scope of intellectual property rights. He then goes on to examine copyright law as applied to cyberspace, patent protection of computer-implemented inventions, and trade mark/domain name protection. He asserts that the standardisation of international property rights by international conventions, and especially the TRIPS Agreement, has loosened the territoriality principle. For him, any future international convention for the regulation of cyberspace would have to address the problem of the territoriality of intellectual property rights and perhaps consider the establishment of an international organisation for the monitoring and policing of such a convention.

In Chapter 5, David Fidler addresses the relationship between cyberspace and human rights. For him, cyberspace challenges certain principles of international law central to the protection of human rights, such as the principle of sovereignty and jurisdiction. For instance, it raises questions as to whether internet access is a human right and how the concept of, and debate over, the extraterritoriality of human rights law applies in the cyber context. The cyberspace-human rights relationship also evokes questions as to national and international policies on internet governance and cyber security, an important issue given Edward Snowden's revelations concerning the United States National Security Agency's massive cyber surveillance campaign. Fidler concludes that cyberspace is subject to international politics that have historically affected human rights protection. Examples include the resilience of sovereignty, national security concerns and shifting balances of power. He concludes that this means the potential of cyberspace to significantly enhance the enjoyment of fundamental human rights may never be fully realised.

In Chapter 6 Kai Ambos considers the question of whether the commission of cyber attacks can give rise to individual criminal responsibility, with particular reference to the provisions of the Rome Statute. Ambos examines the conditions by which individuals may be held criminally responsible for war crimes and crimes against humanity and applies them in the cyber context. He also asks whether cyber aggression can fall within the definition of the crime of aggression under the Rome Statute and whether criminal jurisdiction can be exercised over cyber aggression.

Part II of the handbook assesses the extent to which international law adequately deters and suppresses threats that emerge in and from cyberspace. In Chapter 7 Ben Saul and Kathleen Heath evaluate whether international terrorism conventions apply to cyber terrorism. Although they conclude that certain terrorism conventions can be interpreted in such a manner, they assert that gaps remain in legal regulation, not the least of which is that there is no definition of terrorism (and, for that matter, of cyber terrorism). They query whether cyber terrorism would be better addressed through the negotiation and conclusion of a direct and specific international treaty on cyber terrorism.

In Chapter 8 Russell Buchan assesses the permissibility of cyber espionage under international law. Buchan argues that accessing and collecting confidential information resident in cyberspace that falls under the sovereignty of another state is an intrinsically pernicious practice that breeds distrust and hostility between states. This reality is exemplified by the international response to the Snowden revelations. Buchan asserts that in such an environment states are unable to act in a collaborative and coordinated manner to address issues that threaten international peace and security, such as international terrorism, environmental degradation and human rights abuses. Buchan thus concludes that cyber espionage represents a threat to international peace and security. Moreover, he argues that because states exercise sovereignty in cyberspace, when a state accesses and copies (without authorisation) confidential information falling under the jurisdiction of another state such conduct constitutes an unlawful intervention in that state's sovereign authority and is therefore violative of international law.

Chapter 9 focuses upon cyber crime and the role of national, regional and international law in combating this activity. Philipp Kastner and Frédéric Mégret argue

that many crimes committed in cyberspace are regulated by domestic criminal legal systems. They illustrate this by reference to specific crimes committed in cyberspace. The application of domestic criminal law notwithstanding, Kastner and Mégret suggest that in order to achieve adequate criminal law enforcement multilateral initiatives such as the Council of Europe's Convention on Cyber Crime are essential, for they lay the foundations for greater cooperation between states. Indeed, they conclude that a multilateral treaty achieving global cooperation, beyond state or regional boundaries, and across the state/non-state divide, is needed to deal with many forms of cyber crime

In Part III, the relationship between hostile cyber operations and the *jus ad bellum* is examined. To provide background, Paul Ducheine explores the notion of cyber operations in Chapter 10. He argues that, at the state level, there are broadly five distinct paradigms that can be used to describe cyber operations: governance, protection, law enforcement, intelligence and military operations. Ducheine asserts that it is the last paradigm that constitutes the most far-reaching framework for governmental action and therefore suggests that the proliferation of concepts such as cyber attacks, cyber targeting and cyber war are indicative of the growing militarisation of cyberspace.

Chapter 11 considers whether cyber attacks constitute an unlawful use of force under Article 2(4) UN Charter. Marco Roscini argues that force within the meaning of Article 2(4) requires the use of a weapons accompanied by a coercive intention and effects. Roscini concludes that in the context of cyber attacks this occurs when the attack against computer systems results in physical damage to property or loss of life or injury to people, as in the case of an attack against computer systems that subsequently causes planes to crash. He also advocates a reading of Article 2(4) that extends to cyber attacks that, whilst not manifesting real-world damage, nevertheless render ineffective or unusable computer systems that sustain critical infrastructures and thus cause significant disruption to the delivery of essential services.

Following on from this assessment of Article 2(4), in Chapter 12 Carlo Focarelli examines the circumstances by which a cyber attack can amount to an armed attack pursuant to Article 51 of the UN Charter and thus trigger a state's right to use force in self-defence. In particular, and with reference to state practice and recent literature, Focarelli debates whether an armed attack can only be said to occur where the cyber attack produces sufficiently serious physical damage or instead whether its application extends to sufficiently serious non-physical damage. An attack that affects the functionality of computer systems sustaining critical national infrastructure illustrates the latter. In addition, Focarelli considers how the principles of necessity and proportionality apply to cyber uses of force that are committed in accordance with to Article 51 UN Charter.

States may seek to protect their cyber infrastructure against military threats from cyberspace by recourse to the language of cyber deterrence by asserting that it will respond to cyber attacks with a devastating cyber attack of its own. In Chapter 13 Eric Myjer compares deterrent strategies in the nuclear realm with deterrence in the cyber arena. He argues that because of the unique features of cyberspace, cyber deterrence is not comparable with nuclear deterrence and that therefore cyber deterrence is unlikely to be effective. Perhaps more importantly, Myjer concludes that deterrence by the threat

of cyber retaliation would be contrary to certain basic principles of international law, such as necessity and proportionality.

Part IV focuses upon the use of cyber technology during times of armed conflict and in particular the application of international humanitarian law to cyber weapons and to hostilities conducted in cyberspace. In Chapter 14 Neil Rowe identifies various important ethical concerns unique to the use of cyber weapons. These include attribution, product tampering, unreliability, damage repair and collateral damage. He concludes that many of these concerns are intractable. As a result, he encourages the development of international treaties to restrict and regulate their use.

In Chapter 15 Louise Arimatsu addresses how cyber conflicts should be classified under international humanitarian law and, most notably, whether cyber conflicts give rise to an international or a non-international armed conflict. This inquiry involves consideration of whether cyber attacks satisfy the requirement of 'international', 'armed' and 'attack' for the purpose of international armed conflict. In relation to non-international armed conflict, the key questions are whether cyber groups can be regarded as 'organised' and whether cyber conflict can be ever of sufficient intensity to trigger international humanitarian law.

In Chapter 16 Karine Bannelier-Christakis assesses whether the principle of distinction is still relevant to hostilities conducted in cyberspace. Bannelier-Christakis explains that the principle of distinction applies only to conduct that amounts to an attack under international humanitarian law, which conventionally requires the use of violence that produces physical damage. Bannelier-Christakis criticises this conclusion given that in the contemporary era states place heavy reliance upon cyberspace and thus conduct that affects the functionality of computer systems can be extremely damaging even if it does not cause physical damage. As a result, she argues that the better approach is to subject all military operations (including those in cyberspace) to the principle of distinction regardless of the damage they cause. Customary international law, at least according to Bannelier-Christakis, supports such an approach. She also stresses the difficulty of distinguishing between military and civilian objects in cyberspace given its inherent interconnectivity and also explores how the concept of direct participation in hostilities applies to individuals involved in devising, maintaining and implementing cyber operations during times of armed conflict.

Chapter 17 examines the application of the principle of proportionality and the duty to take precautions in attack in relation to attacks carried out in the cyber domain. Terry Gill argues that a cyber attack would only qualify as an 'attack' for the purpose of international humanitarian law if it is committed in the context of a recognised armed conflict and is intended to or reasonably likely to cause appreciable danger of physical harm or damage. He concludes that while many cyber attacks would therefore not qualify as attacks, some would and, for those, international humanitarian law would be applicable by analogy in much the same way as it applies to attacks by kinetic weapons. Thus, cyber attacks against purely military installations or combatants, without any likely appreciable consequences to civilians or civilian objects, would fall outside the applicability of proportionality. Cyber attacks directed against military objectives or combatants that incidentally harm civilian objects or civilians are subject to the proportionality test and would be unlawful if the expected damage to the civilian

objects or civilians is likely to be excessive in relation to the anticipated military advantage.

In Chapter 18 David Turns assesses the application of the law of neutrality to cyberspace. Turns explains that this is a complicated process because the law of neutrality was devised more than a century ago and was therefore constructed with the intention of protecting the territorial sovereignty of neutral states, namely tangible constructs such as physical territory, territorial waters and territorial airspace. In contrast, cyberspace is an intangible and interconnected environment. This considerably enhances the potential for operations in cyberspace to implicate third parties. Turns concludes that the law of neutrality is still relevant to cyberspace by analogy and proceeds to examine how neutrality affects the conduct of cyber operations by neutrals and belligerents.

Part V reviews the approaches of various international organisations to regulating activities in cyberspace and in particular achieving and maintaining cyber security. In chapter 19 Ramses Wessel explains that over the past decade the EU has started to take its first steps in formulating and regulating cyberspace as a new policy area, especially since the adoption of its 2013 Cyber Security Strategy. In an exploratory fashion, Wessel's chapter evaluates both the EU's existing and emerging internal cyber security rules, as well as the EU's contribution to the development of a global regulatory framework for cyberspace.

In Chapter 20 Katharina Ziolkowski examines NATO's strategy for achieving cyber security. She explains that cyber defence entered NATO's agenda in 2002 after the cyber attacks against the Alliance's networks during the Kosovo crisis. Since 2002 NATO has begun to offer various cyber crisis management mechanisms and other assistance to its member states and partner nations so as to strengthen their national cyber defence capabilities. This being said, Ziolkowski argues that NATO has maintained a degree of strategic ambiguity in relation to the question of the circumstances under which malicious cyber activities constitute a situation pursuant to Article 5 of the North Atlantic Treaty and thereby engage its collective self-defence mechanism. This has been settled recently with NATO adopting the policy that a significant cyber attack on a member state implicates collective self-defence according to Article 5 of the North Atlantic Treaty.

Hitoshi Nasu and Helen Trezise explore Asia's approach to achieving cyber security in Chapter 21. The authors note that cyber security has become a key priority for many Asia-Pacific states, although they conclude that achieving cyber security in this region is likely to be a complex and difficult task because of the political, economic and socio-cultural diversity in the region. This chapter identifies cyber security policy initiatives adopted by institutions in the Asia-Pacific region, such as ASEAN and APEC. The authors assert that regional cyber security efforts have been somewhat frustrated by the traditional security challenges that confront many states in the region.

In Chapter 22 Christian Henderson reviews the role and recent activities of the UN in the cyber security context. He argues that although the UN has historically been sluggish in take on cyber security issues, it has, in the wake of the dramatic increase in cyber attacks since 2007, gradually begun to address this topic. In particular, activity can be seen in various committees of the UN General Assembly, including the achievement of consensus within several Groups of Governmental Experts on various

cyber issues. Additionally, issues of cyber security have surfaced in the UN Security Council, the Economic and Social Council and other subsidiary organs and specialised agencies. Henderson concludes that although the decision of these UN agencies to address cyber security is to be welcomed, the next challenge for these agencies is to cooperate more closely in order to ensure an integrated and concerted response to the maintenance of cyber security.

CONCLUSION

Although it is by now fairly well settled that international law applies to activities in cyberspace, the jury is still out on how to apply such law. This book engages that dialogue in a sophisticated and insightful manner. I admit to disagreeing with some of the reasoning and conclusions reached by individual contributors. Nevertheless, even in such cases, I find the analysis highly incisive and intellectually provocative. I again congratulate my friends Nicholas Tsagourias and Russell Buchan on bringing together such a talented group to so usefully examine one of the most complex topics being grappled with by the international law community.