STRATHMORE LAW JOURNAL

VOLUME 2, NUMBER 1, AUGUST 2016

Strathmore University Press

Strathmore Law School
Madaraka Estate, Ole Sangale Road
P.O. Box 59857 00200
Nairobi - KENYA
Tel. +254-703-034601
editor.sup@strathmore.edu
www.press.strathmore.edu
www.law.strathmore.edu
Twitter: @strathmorelaw

Book Reviews

Cyber-attacks and the exploitable imperfections of international law

By Yaroslav Radziwill
Brill Nijhoff, Leiden, 2015

Reviewed by Ivan Sang[*]

George Orwell's prescient *1984*,[1] which was published in 1949, is a modern classic that is often said to have predicted many of the things that are common features of life today. Startling parallels can be found between the current wars, the frightening extent of surveillance, the shocking use of torture and the key events described in the book. The omnipresent 'Big Brother', with his all-seeing eye, may now be a suitable metonymy for the extraordinary extent to which our society is inter-connected through cyberspace. This was implicitly foretold in *Neuromancer*, a 1984 cyber-punk novel published at the incubation of our digital age.[2] It described cyberspace as a 'consensual hallucination experienced daily by billions of legitimate operators, in every nation'[3] and also conjured 'Operation Screaming Fist', a cyber-attack mission to remotely hack into and disrupt the Union of Soviet Socialist Republics' computer systems. These two fictional dystopian futures mirror our present. And nowhere was this clearer than in the wake of cyber-attacks against Tallinn, the highly-networked capital of Estonia,[4] and the 2013 Snowden revelations of the intrusive scope of

1 Orwell G, *1984*, Secker & Warburg, London, 1949.
2 Gibson W, *Neuromancer*, Ace, New York, 1984.
3 Gibson, *Neuromancer*, 69.
4 Tikk E, Kaska K &Vihul L, *International cyber incidents: Legal considerations*, CCD COE, Tallinn, 2010, 18-24.

* Consultant @ILabAfrica, Strathmore University.

electronic espionage by the major military powers.[5] The logic is now undeniable that we are back to the future of cyber warfare.

More recently, reports of cyber intrusions bordering on crime have been frequent at the domestic level in various jurisdictions.[6] But it is international cyber-incidents, involving inter-state operations, which have attracted much attention as an area of key concern.[7] The fact that the global economy is highly dependent on cyberspace presents as much an opportunity for expanding trade and industry as it does for frightful cyber-attacks and other cyber-unique vulnerabilities.[8] As might be expected, the current law struggles to rein in on an emergent and evolving threat whose adverse capabilities could not have been envisaged when the law was adopted, which implies both problems and prospects. However, it is now widely accepted that despite not being covered by positive rules of international law, cyberspace is regulated by existing international legal norms.[9] This is also the basic premise of Yaroslav Radziwill's *Cyber-attack and the exploitable imperfections of international law*. He focuses, however, on the current gaps in the legal framework and how states can use the deficiencies of the law to their advantage.

The starting point of Radziwill's constructive critique of the extent to which the existing international law can address the challenges posed by cyber-attack is a careful analysis of the *jus ad bellum* (norms on the legality of recourse to force) and *jus in bello* (norms regulating permissible conduct in war). At the outset, Radziwill takes the view that current international law governs cyber operations defectively, and his central thesis is that international law has a substantial amount of significant imperfections that can be exploited in cyber-warfare. He elaborates this by explaining that although institutional and technical tools can usefully expand the regulatory scope of current international law over cyber

5 Milanovic M 'Human rights treaties and foreign surveillance: Privacy in the digital age' *Harvard International Law Journal* (2015), 81.

6 Koch R, Stelte Band Golling M, 'Attack trends in present computer networks' in Czosseck C, Ottis R and KZiolkowskiK (eds), *2012 4th international conference on cyber conflict*, CCD COE, Tallinn, 2012, 272.

7 Schmitt MN, *Tallinn Manual on the international law applicable to cyber warfare*, Cambridge University Press, Cambridge, 2013, 1-2 referring to 'the massive cyber operations by "hacktivists" 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 [as having] focused the attention of States on the subject.'

8 Clarke RA and Knake R, *Cyber war: The next threat to national security and what to do about it*, Harper Collins, New York, 2010, 220; Denning DE, 'Terror's web: How the internet is transforming terrorism' in Jewkes Y and Yar M (eds), *Handbook of internet crime*, Wilan, London, 2010, 198.

9 Roscini M, *Cyber operations and the use of force in international law*, Oxford University Press, London, 2014, 40: '[I]t should be clear that existing primary and secondary rules of international law, including the law of state responsibility, the *jus ad bellum* and the *jus in bello*, do apply to cyber operations.'

operations, uncertainties and gaps still remain that can cynically be used to justify politically motivated action. In response, systematic effort is made throughout his analysis to clearly explain aspects of international law which are insufficient to contain the threat of cyber-attacks and to offer practical remedies that can eliminate them. This advances the existing debate significantly.

The book comprises nine chapters that are sequentially organised to build upon the arguments of the previous chapters and, ultimately, to make the case for overcoming the gaps that currently exist in the law to advance state interests in cyberspace. In Chapter 1, Radziwill outlines the book's objectives and research questions, identifies the relevant literature on the subject of inquiry and points out their deficiencies, and explains how the research fits in and adds to the existing body of work. It is here that Radziwill shows his independent thoughts and also reveals a rigorous methodology that characterises the book's tenor in the remaining chapters. The point is clearly made in this chapter that, presently there is insufficient evidence to suggest any imminent threat of cyber-attack that can cause death, injury or destruction on a scale comparable to kinetic operations. But this point is arguable in the light of some recent reports of thwarted cyber-attacks that had the potential to cause widespread damage.[10]

Radziwill also laments the fact that most authors on the subject overlook crucial legal aspects, including cyber-terrorism and peacekeeping in the virtual domain. This is bold because it offers readers a basis on which to evaluate how the author delivers in terms of gap-filling. Another noteworthy aspect of Chapter 1 is its explanation of the meaning of certain key words, including 'cyber-attack' and 'cyber-space', and why they are to be preferred over other terms as used in other sources. Radziwill's brief defence of the word 'cyber-space' is well reasoned, but even more convincing is the fact that, unlike other alternatives, it is 'short, clear, reasonably comprehensive and well-established'.

Chapter 2 discusses in detail the underlying theoretical framework of the book. Its main thrust is that governments do not usually ignore regulatory norms of the international legal process, but deliberately press for interpretations of those norms which best favour their state-centric interests. His argument recognises the central place that governments hold in the current state-centred politico-legal system of the United Nations (UN). And it is on this basis that he

[10] 'David E Sanger: US indicts 7 Iranians for cyber-attacks on banks and a dam' *New York Times*, 24 March 2016 http://www.nytimes.com/2016/03/25/world/middleeast/us-indicts-iranians-in-cyberattacks-on-banks-and-a-dam.html?_r=0 on 24 August 2016.

argues convincingly that since the major powers have a pivotal role in developing the rules of engagement for military cyber operations, it is highly likely that they would want to press for interpretations of certain norms in ways that best suit their interests. An important illustration that is used throughout this book is the persistent rejection by the Western-allied military powers (led by the United States) of proposals by members of the Russian-led Shanghai Cooperation Organisation on the need to agree on special written norms to govern cyber operations. That most of the technical experts drawn from the Western states participated in a parallel process that resulted in the adoption of the Tallinn Manual, without involving nations such as China or Russia, amply supports the argument made by Radziwill.[11]

Chapter 3 seeks to refute many of the exaggerated claims of cyber military capabilities, which the author argues have the capacity to diminish the seriousness of the issue and to hinder efforts to secure a comprehensive international legal framework. The position taken by Radziwill in this chapter is: instead of uninformed scaremongering, which creates the false perception that law cannot catch up with cyber-technological advances, the better approach is to show by way of technical analysis that cyber operations can partially be accommodated by existing law. Another objective of this chapter is to offer a convincing basis for arguing that minimal, rather than revolutionary, reforms to current international law can address most of the seemingly futuristic challenges that presently confront it.

From the perspective of law meets technology, Chapter 4 makes for an enlightening read since it re-imagines certain foundational principles of international law in the context of cyberspace, a non-physical yet very real domain where virtual warfare can be conducted. Using the concepts of sovereignty, territoriality and jurisdiction, Radziwill unpacks the very ideas that have long formed the basis of international relations and casts them in a new light, making it possible to articulate a clear conceptual framework within which cyber-attacks may be accommodated. Given his stated aim to find imperfections in the law, it is unsurprising that he finds quite a number. This does not, however, cast any doubt on the methodology used. Instead, in comparison with what other scholars have argued, it illustrates the variety of views on an emerging subject.

[11] Liivoja R and McCormack T, 'Law in the virtual battlespace: The Tallinn Manual and the *jus in bello*' *Yearbook of International Humanitarian Law* (2012), 45.

The next two chapters, Chapter 5 and 6, take up the task of rigorously analysing the doctrine of *jus ad bellum* (international law governing the use of force) and *jus in bello* (international law governing armed conflict). While acknowledging the application of both regimes to cyber operations, its principal focus is on the chinks in their armour, the imperfections that can be lawfully exploited by states confronted with cyber threats or other unwanted intrusions. Radziwill argues in Chapter 5 that there is no clear position in current international law regarding the question whether cyber-strikes mounted by independent individuals or non-state groups can reach the threshold of 'armed attack' within the meaning of Article 51 of the UN Charter.[12] Also, he argues that it is less clear at what point such cyber operations may activate the right to exercise self-defence.

Chapter 7, on cyber-terrorism, considers a cumulative view of both *jus ad bellum* and *jus in bello* in the specific context of cyber-enabled terrorist attacks. It makes the case for the need, both as a matter of principle and institutional efficiency, to distinguish treaty-regulated aspects of terrorism from those governed more generally by customary international law. The reason for this, argues Radziwill, is that governments may deliberately conflate the two so as to conveniently designate as terrorism cyber operations that are essentially political, including hacktivism. Perhaps on this basis, the chapter eschews the debate on the criminalisation of cyber-terrorism at the domestic level, which Radziwill argues may give rise to fragmentary standards that can undermine the universality of terrorism offences. Conceding the difficulty of defining terrorism and taking account of its duality, this chapter views cyber-terrorism as a variable concept with different elements depending on which specific treaty is implicated and also that, depending on the actors, different elements of international law apply differently. The most notable aspect of this chapter is the systematic examination of the attempts adopted under the auspices of the UN to expand the scope of current law to accommodate the unique aspects of cyber operations.

Chapter 8 focuses on the institutional capacity and weaknesses of the collective security regime, which is premised on the UN Charter, to deal with cyber-related threats. In this chapter, Radziwill takes on a more critical view of the contemporary efforts to address the gaps in the international framework. Using the case studies of the UN and the North Atlantic Treaty Organisation, the author contends that the failure to properly respond to cyber threats can be explained by institutional aspects that hinder effective action. But he finds the majority

[12] Article 51, *Charter of the United Nations,* 24 October 1945, 1 UNTS XVI.

of these problems to be attributable to poor coordination, under-utilisation of available resources, institutional inertia, and political power plays. An illustrative example from the introduction is the mistrust between the United States and other emerging superpowers regarding persistent opposition of the former to the Chinese-supported Russian proposal[13] for a comprehensive treaty regulation of cyber-security aspects of sovereign state relations. To elaborate institutional defects in need of reform, Radziwill explains that because the collective security framework implies a reporting obligation to the UN Security Council, it can be anticipated that complaints will be raised among states of failure to report if, or when, attacks are launched in self-defence.

The main arguments advanced throughout the book and the reforms suggested as a way to fill the identified legal gaps are summarised in Chapter 9. It also analyses current and future implications of the research findings. Divided into two parts, this chapter uses the findings drawn from the various chapters to test the validity of the thesis statement and as a basis to map the way forward. The resulting findings confirm most of the logic on which Radziwill's study, and other comparable work, is based: that is, there has been no express agreement as to which principles of international law apply to cyber-attacks; the legal methodology to be used in approaching cyber-attacks; the state practice (if any) that is relevant; the institutions responsible for handling cyber-threats and how they are to coordinate action amongst each other. It concludes by making the case for starting a process leading to the adoption by a broader constituency of states of a comprehensive document that stipulates specific norms governing inter-state relations in cyberspace. In this regard, he supports both the development of evolutive readings of existing rules that were designed to govern kinetic operations and the adoption of new rules to make up for the exploitable deficiencies and uncertainties of current law.

On the whole, Radziwill's book contributes in a measured and constructive manner to the debate on the extent to which current law can accommodate and effectively address the challenges arising from inter-state interactions in cyberspace. Its greatest merit lies in the sober, concise and up-to-date analysis of international cyber-incidents and how they have an impact on the development of the substantive law of cyber warfare. It is also noteworthy that Radziwill wades into the choppy waters of doctrinal dispute over certain deeply disputed questions of international law, including the threshold of cyber-armed-attack, direct participa-

[13] Gady FS and Austin G, *Russia, the United States and cyber diplomacy: Opening the doors*, East West Institute, New York, 2010, 15.

tion in cyber-hostilities and the standard of attribution as a basis for state responsibility. The conclusions reached by the author are sound and uncontroversial, based as they are on a comparative critique of existing positions. However, there are certain omissions in the book. For instance, in his presentation of the residual gaps and deficiencies in the current law, the author overlooks some nascent if not contestable norms of customary international law. Following this omission, Radziwill's work can be criticised for focusing so much on what is not there that it ultimately ignores what is in the process of filling that gap. The significance of the evolving customary norms is not lost on other authors who argue that 'it cannot be excluded that customary international law rules specific to cyber operations might be in the process of forming and eventually ripen.'[14]

The above demerit, however, is remedied to a significant extent by the fact that the book adopts an infrequently broad multi-disciplinary approach to analysing existing problems and, ultimately, the validity of the conclusions reached. In particular, Radziwill adopts a positivist politico-legal framework through which the norms relating to the use of force and humanitarian law are examined. This is augmented by a discussion of inter-related rules, which bear secondary importance for the wider discourse. Unlike most of comparable literature on this point, it innovatively draws the elusive link between why states obey international law and how this influences the ordering of the state-centric matrix of international law. It recognises that attitudes of states are influenced by key aspects of natural law and that, while seemingly irrelevant, the violation of legal norms carries adverse political consequences.

[14] Roscini, *Cyber operations*, 25.