MERKOURIOS
Utrecht Journal of International and European Law
ISSN 0927-460X

Georg Kerschischnig
Cyberthreats and International Law

Eleven International Publishing (2012) ISBN-13: 978-9490947644

Arno R Lodder[*]

I. Introduction

We all experience daily the benefits the internet brings us, but in cyberspace, as in life, along with the good comes the bad. Some users are insulted on social media, others are swindled in online marketplaces, and spam, viruses and worms exist in large numbers. The latter are commonly headed under the term 'threats', and where the internet is used as the medium, they are labelled 'cyberthreats'.

Both the internet's infrastructure and applications have vulnerabilities as it was not developed to be secure. Ironically, what began as a military network did not contain any security measures—they were not needed back then, because the internet was meant to serve as a closed system. This historical background must be kept in mind when discussing cyberthreats, which are inherent features of the internet.

One of the infrastructural inconveniences of threats is the identification of internet users. While surfing the web, individuals cannot be identified; only the computers used which are part of the network can. Basically, in locating the source of these threats it might be clear which computers were used, but not who used these computers. In addition, there are many ways to hide one's identity or to mislead those who want to identify computers or their users. Attribution is the term used for linking acts on the internet to individuals, and the term mostly arises in the context of *the problem* of attribution.

Threats are a good starting point to address insecurity in cyberspace. From a legal point of view, however, it is often difficult to determine the appropriate response to threats and who should exercise this response. The legal system is not very fit for this task. Namely, certain legal actors respond to the acts of certain individuals and, as was just indicated, it is usually not clear who is acting. For instance, if the threat comes from a criminal, the police and prosecutor are typically called on to act whereas if the threat comes from another country, the army may be called into action. But what if it is not clear who is behind the threat? Who should react then? This problem asks for a different approach. The existing legal framework should be disregarded and states should form response teams with competences that are currently spread out among the various governmental parties, such as the police, the army and the secret service.

[*] Arno R Lodder is a Professor of Internet Governance and Regulation in the Department of Transnational Legal Studies at VU University in Amsterdam.

Merk*ourios* 2013 – Volume 29/Issue 76, Book Review, pp. 106-108.
URN:NBN:NL:UI:10-1-112867
ISSN: 0927-460X
URL: www.merkourios.org
Publisher: Igitur publishing

Cyberthreats and International Law walks on existing paths. It is a good thing that threats have a central position in the book, but the application of the existing legal framework does not sufficiently add what is needed in addressing the threat. Numerous articles and books on how to apply international law to activities on the internet have already been published and this book is just the next in the series. The book, however, does offer a good overview for those who are not familiar with the field of cyberthreats and international law. Let me first address the structure of the book that, as such, reveals some shortcomings, and follow with some analysis.

II. Structure

The book consists of 25 chapters, which is in itself quite a large number for 300 pages. The book is, moreover, divided into five parts:

1. Conceptualization of cyberthreats (pp 5-80);
2. Interstate cyberthreats (pp 83-218);
3. Non-state actor cyberthreats (pp 221-257);
4. Jurisdiction and cyberspace (pp 261-278);
5. A new approach toward cyberthreats (pp 281-311).

It seems that several chapters were added at a later stage, probably after a first version was sent to the publisher. The result is unbalanced. Six of the chapters only contain two pages, *viz* chapters 4, 6, 7, 13, 20, 22, while four chapters only contain three pages, *viz* chapters 11, 17, 19, 25. The core of the book, Part 2, addresses the least interesting subject: Cyberwar and the *jus ad bellum* and the *jus in bello*. Many people have already discussed the application of *jus ad bellum* and *jus in bello* to cyberthreats. One of the early and most often referenced publications in this context is Michael Schmitt's 1999 article,[1] which was further developed by Wingfield in 2000.[2] However, even over 15 years ago the topic was already addressed by Aldrich.[3] Kerschischnig is right in stating (p 132): '[C]yber attacks do not fit into traditional categories (...) armed force or economic coercion (...) lie somewhere in between.'[4]

Unfortunately, instead of coming up with a new angle or interesting proposals, he sticks to the already explored paths (p 132): '[A]s long as the international community is not willing to pronounce itself specifically on the issue, it has to be placed within the traditional prescriptive system.' In doing so, he provides an interesting overview of the issues, but for those familiar with the literature this is not very interesting since it does not include positions not taken before.

In the second part of the book, some pages deal with the interesting topic of cyber espionage, but unfortunately these are two of the extremely short chapters. Also, this short part suffers from the same problems as much of the literature on international law, in that it tries to qualify what happens in cyberspace as involving the *use of force* (p 172):

> '[S]tealing those data undermines their value, which could indicate destruction of property if the loss of data's exclusivity can be equalled to destruction, which again could potentially subject cyberespionage under the prohibition of the use of force.'

How could loss of value by itself ever cause the destruction of something? This is a results-based argument; it reasons backwards from the conclusion. Currently, international law measures the effects of the use of force in terms of personal damages (including death) and damage to objects. So, destruction is a relevant notion for the use of force. However, when data are copied and subsequently deleted, this does not qualify as destruction since the original data is preserved through copying.

The fourth part is for several reasons a misfit. First, jurisdiction and cyberspace is one of the most crucial topics of internet governance. An early contribution to this debate was the Johnson & Post 1996 article,[5] which was taken up and continued by

[1] M Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 Columbia Journal of Transnational Law. The layout and overview of the literature by Kerschischnig is a bit messy, but it seems as if this publication is not included in the overview. The author does, however, refer to this work, eg p 133.

[2] T Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace* (North Falls Church: Aegis Research Corporation 2000).

[3] R Aldrich, 'The International Legal Implications of Information Warfare' (1996) Airpower Journal 99-110.

[4] See also A Lodder, 'There is more to cyberwar than death and destruction' (25 January 2013) presentation <http://bit.ly/WUvMLv> accessed 29 January 2013.

[5] D Johnson and D Post, 'Law And Borders: The Rise of Law in Cyberspace' (1996), 48 Stanford Law Review, 1367.

many others such as Goldsmith & Wu's *Who controls the internet*[6] in an on-going and unsettled debate. The positions taken are that geography does matter on the internet (*cf.* Goldsmith & Wu), that the internet is borderless (Post),[7] while others stand somewhere between these positions. Jurisdiction and, in particular, sovereignty are relevant for cyberwar, for a country is allowed to take certain actions or not depending on the position adopted. This issue of jurisdiction should not be cursorily discussed in only fifteen pages of a book on cyberthreats.

III. Analysis

To fully understand law on the internet one requires knowledge of the internet itself. The author has therefore done right in spending the first part of his book to a technical introduction and background.

The references to the literature are at some points outdated. To give just two examples from the opening paragraph on p 291:

- "not enough so far" with reference to two 2002 publications;
- "at a time of increasing importance of cyberspace" with reference to a 1998 publication.

An interesting observation that deserves further thought is the relation between the quality of a State's cyber defence and the decision to 'potentially or actually cause physical damage or loss of life.' (p 130). Should it matter how good the State's defence is? Is it more legitimate for a technologically inferior State to carry out a physical attack after a cyber attack? The consequence would be that countries with an inferior cyber defence would be legitimised in reacting after a weak attack, and countries with a superior defence might never be legitimised to react.

Another good point is the inclusion of non-state actors in the discussion. Because of the problems relating to attribution, it is important to analyse the role of non-state actors. The discussion on cyberterrorism is helpful in this respect. The addition of hacktivism and webtivism is in itself interesting, for it adds to the discussion on non-state actors, but in only seven pages not much can be said about it.

An excellent observation can be found on p 273: '[A] violation of a state's law may not go unpunished just because the potential offender crosses an imaginary line into a safe zone.' This is actually what happens when enforcement agencies stop following someone once he enters the physical infrastructure of another country. I agree with the author that this is not a good development. The internet is a network of computers in the first place and for this network to function it should not matter where a computer is located. Why should we be prevented from taking action against someone for attacking the Dutch parliament only because he moved his laptop to Paris? The physical location of the offender should not matter under these circumstances.

IV. Conclusion

This book could serve as an introduction to the topic of cyberthreats and international law. The list of references in this book is impressive and includes, *inter alia*, scholarly work, policy documents, and popular media. The layout does not particularly help the reader to browse quickly through the references, but it at least forces the reader to go through it carefully. The last chapter, *Outlook* (p 309-311), includes some interesting observations. In particular, the author states that there is still a lot of work to be done in this field, a notion with which I could not agree more. ■

[6] J Goldsmith and T Wu, *Who Controls the Internet?: Illusions of a Borderless World* (Oxford University Press 2008).

[7] D Post, *In Search of Jefferson's Moose: Notes on the State of Cyberspace* (Oxford University Press 2009).