The Nascent Law of Cyber Blockades and Zones

Ana Lenard*

1 Introduction

Technology has allowed humans to conduct war and intervene in the affairs of other states in every realm possible. In addition to fostering human expansion into new realms (from land, to sea and air), technology has provided for the development of new means and methods by which warfare and intervention can be conducted. With the creation of the cyber realm, cyber warfare and intervention using cyber tactics have become possible, and indeed, commonplace. Each realm of expansion has raised difficult legal questions that states have often dealt with by relying on existing international law, with appropriate adjustments to accommodate the unique attributes of each realm. Many international lawyers have also approached the task of ascertaining the law of cyber warfare and intervention in this way, seeking appropriate analogies in existing international law.

Following this method, this article seeks to add to the scholarship on cyber warfare and intervention by considering whether the law of conventional blockades and zones can apply to the same cyber tactics, and if not, what the law of cyber blockades and zones otherwise ought to be. This is an area where there is not yet much scholarship, although international lawyers have touched on it. For example, in the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, released on 8 February 2017, cyber blockades and zones receive a passing mention.1

There are two reasons why ascertaining the law of cyber blockades and zones is important. First, in the late 2000s, cyber operations appearing to be cyber blockades were conducted against Estonia and Georgia.2 This confirms that such tactics exist and can be used against states. Secondly, it is foreseeable that tactics such as cyber blockades and zones will become more prevalent in the future as states look for low-risk, low-cost ways to conduct or support war efforts, or intervene in the affairs of other states.

* LLB(Hons)/BSc. Associate at Gilbert Walker. I would like to thank Dr Caroline Foster and Jack Oliver-Hood for their support and guidance in writing this article.


2 See Section 4.2.1 below.
This article canvasses the topic of cyber blockades and zones in three parts. Part 2 is about blockades and details what they are, their purpose, the law, and the function that blockade law serves – or the “mischief” to which it is directed. Part 3 will follow the same structure in respect of exclusion zones, with a focus on no-fly zones in particular. Part 4 involves a discussion of cyber blockades and zones, their purpose, the mischief inherent in such cyber tactics that requires regulation by law, and whether the law of blockades and zones can be the basis of the law regulating the same cyber tactics.

2 Blockades

2.1 What is a Blockade?
A blockade is a method of warfare involving “the blocking of the approach to the enemy coast, or a part of it, for the purpose of preventing ingress and egress of vessels or aircraft of all States”. Aerial blockades became possible with the expansion of warfare into air space. An aerial blockade is defined as “a belligerent operation to prevent aircraft ... from entering or exiting specified airfields or coastal areas belonging to, occupied by, or under the control of the enemy.” A blockade might be close or distant, partial or total, porous or tight, and limited or unlimited. Traditionally, warships would organise themselves into a cordon around the enemy coastline, but in modern times, distant blockades have become possible with developments in technology such as


