The Law Applicable to Countermeasures against Low-Intensity Cyber Operations

Nicholas Tsagourias*

Contents
1. Introduction
2. Genealogy of Countermeasures
3. Attribution in Low-Intensity Cyber Operations
4. Proportionality in Countermeasures
5. Countermeasures by Third States and Countermeasures Affecting Third States
6. Conclusion

1. Introduction

Cyber threats appear in different forms and present different levels of seriousness. Whereas a cyber-attack amounting to armed attack is perhaps the most serious threat emanating from cyberspace, the probability of such an attack happening is quite low. Yet, legal commentators have focused their attention almost exclusively on such attacks and discussed how the rules on the use of force found in the United Nations (UN) Charter and in customary law apply to such attacks.¹ Although low-intensity cyber operations are more frequent, the legal framework that applies to them has not been fully explored.² Low-intensity cyber operations refer to cyber operations amounting to a use of force below the threshold of an armed attack as well as to cyber operations below the use of force threshold. Whether low-intensity cyber operations constitute uses of force depends on the harm they cause in the sense of material damage, human injury and loss or loss of functionality.³

This article will focus on countermeasures as acceptable responses to low level cyber operations and examine the legal framework within which countermeasures operate.

* Professor of International Law, University of Sheffield. Email: Nicholas.Tsagourias@sheffield.ac.uk.
The article proceeds thus as follows. Part 2 will provide an account of the genealogy of countermeasures and explain the legal regime within which they operate. This is very important because, although the term countermeasures is a recent invention having specific legal connotations, the normative and legal history of countermeasures is quite rich and instructive. Identifying the target of countermeasures is critical not only for the effectiveness but also for the lawfulness of countermeasures, therefore Part 3 will examine the standards according to which low level cyber operations can be attributed to a State or to a non-State actor. Part 4 will explore the scope of the principle of proportionality in the context of countermeasures whereas Part 5 will examine the availability of third party countermeasures against low-intensity cyber operations and consider the legal effects of countermeasures on third parties.

2. Genealogy of Countermeasures
Countermeasures are unilateral and decentralised mechanisms of enforcing international law in view of the latter’s weak enforcement mechanisms.4 Their legality is premised on three factors: (i) the existence of a prior wrongful act; (ii) the inability or unwillingness of the wrong-doer to redress the situation; (iii) the proportionality of the measure.5

Countermeasures are the modern incarnation of reprisals which as a concept and activity has a long pedigree.6 As it was said, reprisals “existed well before law, needless to say international law. The paradox of international law as a legal order is that it allowed reprisals into the legal system itself.”7 The locus classicus of the law of reprisals is the Naulilaa arbitration of 1928. The case concerned forcible action against Portuguese forts and posts in Angola, following the killing and wounding of German officers by Portuguese soldiers.8 Reprisals were defined there as “an act of self-help on the part of the injured states, responding after an unsatisfied demand to an act contrary to international law on the part of the offending State … They would be illegal if a previous act contrary to international law had not furnished the reason for them. They aim to impose on the offending State reparation for the offense or the return to legality in avoidance of new offenses.”9

---


8 *Naulilaa Incident Arbitration Decision (Port. v. Ger)* 2 RIAA (1928) p. 1011.