Chapter 24
Surveillance, Privacy, and Due Diligence in Cybersecurity:
An International Law Perspective

Joanna Kulesza
University of Lodz, Poland

ABSTRACT

The chapter covers the international law due diligence principle as applied to the prevention of transboundary cyberthreats. The analysis is based on the work of the International Law Commission referring to state responsibility and international liability as applicable to the challenge of international cybersecurity. The first attempts of this application by European international organizations are discussed. This is done in the light of the current political challenge of engaging all states in the discussion on the appropriate standard of cyberthreats prevention. Reaching to the no harm principle of international law, the author argues that all states need to take all necessary measures in order to prevent significant transboundary damage originated by online activities of individuals within their jurisdiction, power, or control. Should they fail to show due diligence they may be held internationally responsible for an omission contrary to their obligation of preventing harm to other states, foreigners, or shared resources.

INTRODUCTION

The chapter covers the due diligence standard for preventing cyberthreats according to international law standards. The author describes details of a cyberspace specific due diligence requirement of online service providers and information infrastructure operators in the light of international customary and contractual legal practice. While international law obligations rest directly upon states, they are being implemented through acts of national law, binding upon information services and infrastructure operators within each state jurisdiction. Unlike with other media, the unique transboundary character of the Internet requires a uniform, international standard of due care in preserving the network's resiliency and stability for both: practical and technical reasons. Such an international cybersecurity due diligence standard allows for simultaneously securing all elements of the network at an equal level and makes it easier for intentional companies, operating in various ju-

DOI: 10.4018/978-1-4666-6324-4.ch024

risdictions, to meet professional security standards required according to national laws. The analysis provided within the chapter is derived from rich international law jurisprudence and includes an up-to-date application of the due diligence principle to the challenges posed by transboundary online interactions, in particular to significant transboundary harm inflicted through online activities. The chapter is based on a thorough analysis of due diligence in public international law as the common element of two accountability regimes: the regime of state responsibility for the breach of an international obligation and international risk-liability for transboundary harm. The presented research devolves from the doctrine of international environmental law with its detailed due diligence standard and principle of prevention for the purpose of applying it to cyber-security. It also includes the crucial human rights perspective, calling for a flexible equilibrium between international online security and individual privacy or freedom of speech.

According to the work of the International Law Commission (ILC) significant transboundary damage may result in so-called risk liability. International liability is bound not to state actions, but to its omissions – failures to prevent or at least minimize the risk of significant transboundary harm by inadequately controlling entities causing risk of such harm within state territory, jurisdiction or control. A mechanism designated to aid states in preventing such harm resolves to state monopoly in authorizing private entities for running risk generating enterprises. In order to assess whether a state met its prevention and risk-assessment obligations, the due diligence standard is revoked on a case-by-case basis.

The non-exhaustive list of state authorized monopolies does not explicitly include IT-based services. Yet with the rise of asymmetric threats to international peace and security, especially so-called "cyberterrorism," a question whether it should, is being raised forever more frequently, in particular with reference to the definition of "critical infrastructure." The principle of prevention originating from international environmental law may be applied to cyberthreats originating from one state territory causing significant transboundary harm outside it. Should that be the case a state might be held liable for its failure to supervise activities conducted by the IT service providers within its territory. States willing to mitigate liability for such failure create forever more strenuous national laws obliging IT professionals to show due diligence. So far however no international due diligence standard for cybersecurity is being directly named, leaving companies operating in numerous jurisdictions one their own when dealing with varying national regulations.

The idea presented within the chapter covers an international cyberspace-specific due diligence standard and a possible liability mechanism, based on the multistakeholder principle recognized within Internet governance. The author answers the question whether a due diligence standard for cyberspace may and if so - ought to be introduced through particular obligations laid upon Internet service providers and critical infrastructure operators. Recognition of such a standard on the international level would set IT companies free from having to invest in costly legal counseling in each and every jurisdiction they enable their services in.

BACKGROUND

"Transboundary harm" is a significant term in the 21th century international law doctrine and jurisprudence. It is the focal criteria of the ongoing discussions aimed at tracing the limits of state responsibility and international liability for damage caused by private parties acting within state jurisdiction. Transboundary harm may appear when their activities cause detrimental results within the jurisdiction of other states or shared spaces, like the Open Sea or the Antarctic. State responsibility for transboundary harm grew in