Chapter 20
Due Diligence in Cyberspace

Joanna Kulesza
University of Lodz, Poland

ABSTRACT

Within the chapter, the author discusses the possibility of introducing an international due diligence standard for Internet Service Providers (ISPs). She analyzes the due diligence standard in public international law as the common element of two accountability regimes binding upon states: the regime of state responsibility for the breach of an international obligation and international risk-liability for transboundary harm. They are both aimed at preventing transboundary harm originating from state territory. Such harm may presently be inflicted also with the use of cross-border electronic networks. Since the Internet is considered a global resource, the analysis provided is based upon international environmental law doctrine with its detailed due diligence standard and principle of prevention. The author goes on to propose their application to cyber-security. The idea argued within the chapter is for the development of an international cyberspace-specific due diligence standard and possibly a liability mechanism, as based on the multistakeholder principle recognized within Internet governance. The author aims to answer the question of whether a due diligence standard for cyberspace may and if so ought to be introduced through particular obligations laid upon Internet Service Providers, in particular Critical Internet Resources operators and introduction of an international ISP liability fund.

INTRODUCTION

Internet creates significant risk of transboundary harm. Insufficient security of its components, such as root-servers and other Critical Internet Resources (further herein: CIRs) (COE, 2012), faulted by Internet Service Providers, may cause damage to international and state security or cause significant transboundary harm. Presently international law lays upon states no particular obligation relating to cybersecurity directly or indirectly aimed at preventing that risk and minimizing the threatening damage. It does however contain a generally recognized due diligence standard in transboundary harm prevention where lack of due diligence of state organs in preventing significant

DOI: 10.4018/978-1-4666-4979-8.ch020

transboundary harm may bring international responsibility to that state. Existing international treaties on international environmental law transfer significant part of that risk liability onto businesses benefiting from the created risk. Although the international due diligence standard cannot be directly applied to private parties, states are under international obligation to introduce national laws aimed at preventing significant transboundary harm binding private actors. The contents of those laws are funded upon the international due diligence standard, which allows to identify obligations resting upon states. This chapter is an attempt at applying those general due diligence obligations to prevention of transboundary harm in the cyber-realm. The practical application of such seemingly academic exercise comes to foreground in the context of prevention of international terrorist acts conducted or initiated online. International community recently directed its attention towards legal possibilities of holding states "sponsoring" cyberterrorism accountable for their omissions in preventing such attacks initiated from their territories or conducted with infrastructure located therein. Identifiable international obligations of states in preventing transboundary harm affected through cyberthreats is soon to be transposed into national obligation of companies operating CIRs. Since international law offers models for private liability schemes, they are likely to be applied also towards cybersecurity and cyberterrorism prevention.

Usually listed among asymmetric threats, the term cyberterrorism covers threats to international peace and security originated with the use of devices connected to the global computer network and relying upon the Internet Protocol (TCP/IP) and protocols compatible with it. A Draft Convention on Cyber Crime and Terrorism from the U.S. Hoover Institute described this activity as "intentional use or threat of use (…) of violence, disruption or interference against cyber systems, when it is likely that such use would result in death or injury of a person or persons, substantial damage to physical property, civil disorder, or significant economic harm" (Sofaer, 2012). In particular damage attempted or done to the functioning of "critical infrastructures" or CIRs constitutes international cyberterrorism[1]. The cited document defines "critical infrastructure" as "interconnected networks of physical devices, pathways, people and computers that provide for timely delivery of government services; medical care; protection of the general population by law enforcement; firefighting; food; water; transportation services, including travel of persons and transport of goods by air, water, rail or road; supply of energy, including electricity, petroleum, oil and gas products; financial and banking services and transactions; and information and communications services"[2]. Therefore diligent administering of those resources and their protection against harmful unauthorized interference is the necessary condition for preventing significant transboundary harm. For entities administering such systems any legal obligations to act diligently may originate solely from national laws. Those however are being shaped by international consensus and international obligations of states. States are obliged to show due diligence in preventingok transboundary harm and to introduce national laws meeting that standard. For that reason the background of the existing due diligence standard in international law must be considered when ISP risk-liability is to be discussed.

STATE RESPONSIBILITY VS. INTERNATIONAL LIABILITY IN INTERNATIONAL LAW

Contemporary international law, as recapitulated by the International Law Commission (further herein: ILC), foresees for two seemingly separate regimes: that of state responsibility for internationally wrongful acts and that on international liability