CHAPTER 17

MASSIVE CONVENTIONAL TERRORIST ATTACK AS A THREAT TO CRITICAL INFRASTRUCTURE SECURITY

EKATERINA STEPANOVA

Dr. Ekaterina Stepanova is Senior Fellow and Programme Leader of the Armed Conflict and Conflict Management Programme at the Stockholm International Peace Research Institute (SIPRI), Stockholm, Sweden.

1. Introduction

The main focus of this chapter is the interface between terrorism and the security of the technological and economic systems vital for the functioning of society and the economy – the so-called critical infrastructures (CIs). When it comes to this subject, there is a certain disconnect between experts on technology, weapons and infrastructure security, on the one hand, and academic experts on terrorism, on the other. While technicians and managers prioritise the vulnerabilities of infrastructure and risks in terms of what is technologically possible, terrorism experts focus on the motivations and organisational forms of groups that employ terrorist means. They also highlight the specifics of terrorism as a form of political violence, compared to other forms of armed violence.

Terrorism is the most asymmetrical form of political violence, as it is designed in such a way that its broader destabilising political and psychological effects (human effects) go far beyond its actual damage to human lives or infrastructure. When it comes to terrorism, the sheer number of casualties, incidents, metres of pipeline or the number and size of buildings destroyed is of less critical importance than terrorists' *ability to affect politics* through the use of or threat to use violence against civilians or infrastructure *in an asymmetrical way,* that is, by causing a disproportionately high impact with relatively limited means. This ability depends on the political context, the timing, the type of society that is under attack or the broader disruption that an attack on a physical object can cause. A terrorist incident