Chapter 8
To Define or Not to Define:
Law and Policy Conundrums for the Cybercrime, National Security, International Law and Military Law Communities

Pauline C. Reich
Waseda University, Japan

ABSTRACT

There have been three stages of Internet use: the happy days of e-commerce and optimistic sharing in military and academic circles; the growing awareness of Cybercrime issues to be addressed by law; and recent concerns about cyber attacks and national security issues and the paucity of national and international legal means to address them. This and the following two chapters analyze actual incidents and the applicability and inapplicability of law and policy; attempts to define terms that are thrown about in the media and by legislatures; such conundrums as attribution and anonymity, the lack of precedents and metaphors to guide legislators and policy makers; privacy and civil liberties issues; proposed legal and policy measures at national and international levels.

1. INTRODUCTION

1.1 The Third Stage of the Internet, Law, and Policy Relationship

In the present third stage, there are both criminal elements and different players whose purposes are not financial but involve national security or extreme violence for political, religious and other purposes. Some nations have been in the third stage of Internet/IT development for a much longer time, others are beginning to be concerned about it or affected by it, and some are not yet preparing for it because they do not think about it or know how it will affect them.

Terminology is being bandied about to describe some of the new forms of attack (ProjectCyW-D, n.d., Lawson, 2010). The same attacks, for example

DOI: 10.4018/978-1-61520-831-9.ch008

those against Estonia in 2007, have been described as "cyberattacks", "cyber war" and "cyber riots". That terminology has significant consequences in terms of decision-making at the national and regional and international levels about whether new forms of war will ensue, or whether new forms of legal responses coupled with technology and policy will emerge over time.

In order for individual countries to plan their own national legislation, clarification of the terms is important. Why? At this point, if countries are able to trace individuals who have engaged in Stage 3 activities (so-called non-state actors or state actors – see below), the lack of common national law terminology is a hindrance to prosecuting them under national law as well as the ability to respond to another country which might have detected such individuals, given the notion that both countries are acting in good faith and are opposed to such cross-border activities, although that may not be the case between states or groups with longstanding difficult relations (e.g. India-Pakistan, Palestinian-Israeli, the Russian Federation and former member states of the Soviet Union, China, North Korea and other countries).

The advantage of having a convention is that there is harmonization of the laws and consistency, however, as mentioned previously, not all the countries worldwide have been willing, for example, to sign and ratify the Council of Europe Convention on Cybercrime or other Council of Europe initiatives, and there are various alternative suggestions of ways in which the United Nations could play a role in cybersecurity as it has in the nuclear issues that have arisen since that form of aggression has been developed and then subjected to monitoring and other actions by the United Nations rather than between states.

As some have pointed out, any United Nations initiatives are slow to develop given the need for consensus; in the interim, the various nations with cyber capacity and reliance on cyber technology need to develop common terms and rules through which to arrive at the standards by which they should operate in globally connected networks.

One purpose of this chapter is to examine the terminologies and concepts being utilized in Stage 3, to enable those within the various circles developing national, regional and international policies and laws not to talk at cross purposes, but to develop common terminologies and understandings over the long term.

Another objective is to describe areas in which law does not work when applied to the phenomena being experienced, in which technology does or does not work, and in which policy needs to be developed that bridges the law and tech communities or the tech and other communities within the context of law and policy.

The nature of law is to make order out of chaos, i.e. to take a set of facts, organize them, present them to a judge to see if or how the law applies to them. There are many problems in doing so when there are cyber issues, as will be discussed below. First of all, some countries do not have laws to cover the situations we are seeing that affect national security. Secondly, the terminology is so varied that the same phenomena are called by different names or may not be addressed at all in domestic laws or bilateral/multilateral treaties. This presents a problem when there are cross-border attacks, for example, if one country has a law, the other doesn't, and the two countries are not in a legal relationship such as a multilateral assistance treaty (MLAT) or parties to a convention which would form a basis for a similar terminology and concept of what is and is not legal. Even worse, much more work needs to be done about identifying the sources of attacks; botnets and zombie computers are the scourge of the law enforcement, national security and military communities. Thus, law in its traditional modes may not be useful in punishing those who attack critical information infrastructures (Brunner & Suter, 2008).[1]