Chapter 9
Anonymity, Actual Incidents, Cyber Attacks, and Digital Immobilization

Pauline C. Reich
Waseda University, Japan

Stuart Weinstein
University of Hertfordshire, UK

Charles Wild
University of Hertfordshire, UK

Allan S. Cabanlong
Philippines National Police, Philippines

1. UNITED KINGDOM

The issue of foreign states and terrorist groups attacking UK Internet based computer resources has perplexed Lord West of Spithead who served from June 2007 to May 2010 as Parliamentary Under-Secretary of State at the British Home Office with responsibility for Security and a Security Advisor to then Prime Minister Gordon Brown. In drawing the lines between what is an act of war and what is not in the cyber world, Lord West opined that if a foreign nation would bomb the UK's electronic grid, this would be clearly an act of war. In the same vein, Lord West believes that people are coming to realize that if the same country would use sophisticated computers to knock out the UK's electricity grid, this would also be an act of war (Sydney Morning Herald, 2010). He notes that there have been many significant attacks on UK core computer networks and communications systems (Guardian, 2010). In fact, Lord West contemplates that some state players have managed to use cyber espionage to illegally obtain large amounts of materials under intellectual copyright and designs for aero engines. West notes that the problem here is attribution: "The moment you mention a particular state, they will deny it. The problem with cyberspace is that attribution is extremely difficult. It's almost impossible to do it in terms of evidence that would be necessary in a court of law" (Guardian, 2010).

The UK's Government Communications Headquarters' Cyber Security Operations Centre (CSOC) has warned of the catastrophic problem

DOI: 10.4018/978-1-61520-831-9.ch009

that could be caused as a result of a successful cyber attack (Williams, 2010). CSOC monitors UK Internet security by producing intelligence on botnets, Denial of Service attacks and other digital threats to national security (Williams, 2010). Unfortunately, an elusive definition of what constitutes "cyber warfare" – with some countries making use of hired "hacktivists" to carry out deniable cyber attacks – remains a significant issue of concern here (Williams, 2010).

2. UNITED STATES

2.1 The United States Cyber Command: Inability to Adopt Terms of Engagement for Cyberwarfare

The 24th US Air Force was created in recognition of cyberspace becoming a military domain. It is an operational war fighting organization that establishes, operates, maintains and defends Air Force networks and conducts full-spectrum operations in cyberspace to protect same. Even if the US Air Force has created its newest numbered air force (as of 18 August 2009), one would be mistaken to suggest that the "historic constructs of war—force, offense, defense, deterrence—can be applied to cyberspace with little modification" (Libicki, 2009a).

2.2 Martin Libicki

Martin Libicki offers the following maxims for the cyber world (Libicki, 2009a, Libicki, 2007, Libicki, 1995):

Cyberspace is its own medium with its own rules.

Cyber attacks, for instance, are enabled not through the generation of force but by the exploitation of the enemy's vulnerabilities.

Permanent effects are hard to produce.

The medium is fraught with ambiguities about who attacked and why, about what they achieved and whether they can do so again.

Something that works today may not work tomorrow (indeed, precisely because it did work today).

Deterrence and war fighting tenets established in other media do not necessarily translate reliably into cyberspace.

Libicki (2009) offers that what constitutes an act of war can be defined in three ways: universally, multilaterally, and unilaterally.

2.2.1 Universal Definition

A universal definition is just what it says it is - every state accepts it such as when the United Nations says it is an act of war. The next-closest analog is if enough nations have signed a treaty that says as much. Of course, in the cyber world, no such United Nations dictum exists, and no treaty says as much (Libicki, 2009b).

2.2.2 Multilateral Definition

A cyberattack (with specified characteristics) can be seen as an act of war if a set of states has so defined it as such. The most obvious example is NATO and the failure to declare the 2007 cyber attack on Estonia an event requiring implementation of NATO's collective-defense clauses. The problem of attribution however made it impossible for NATO to undertake a response on behalf of Estonia (Libicki, 2009b).

2.2.3 Unilateral Definition

A state can unilaterally declare a cyber attack an act of war. The problem here is that "potential attackers may or may not take such a declaration seriously" (Libicki, 2009b). And then there is the issue of an appropriate response: "If the state