Chapter 9
SPCTA:
An Analytical Framework for Analyzing Cyber Threats by Non-State Actors

Harry Brown III
Norwich University, USA

ABSTRACT

The field of cybersecurity crosses multiple domains as it has risen to affect state governance. The Internet has enabled aspects of connectedness and capabilities that have the potential to effect state power. Such conditions affect the standing of nation-states within the international political system and their relation to other states. This is a matter of cyber-relations, where the behavior of states towards each other is based on the comparative cyber-capability of the state. Emerging conditions include the ability of non-state actors to wield similar cyber-power and affect state governance, and affect state operations and its contract with its constituents (contract alluding to the provisions for the public good). This research addresses the notion of non-state actors within this context, specifically, proposing and analytical framework for analyzing cyber threats from non-state actors.

While the initial thesis also posed a theoretical foundation for the Social Process for Cyber-threat Analysis (SPCTA), this article will focus on the proposition of a new methodology for analyzing cyber-threats between international actors, and providing a methodology that assists in formulating effective policy. To a great extent, the threats posted by UNCAs will be based on current data of attempted and actual cyber-incursions. Data for these activities are often classified, thus, data for a more expansive analysis are extremely limited. However, we seek to overcome this barrier using known attacks against states or their agencies from unknown perpetrators. The proposed framework is used to identify potential threats posed to states by Unsanctioned Non-state Cyber Actors (UNCA), and it explains the underlying causes that compel the cyber attack.

In this research, we are primarily addressing a range of cyber-attacks that might result in major disruption of critical infrastructure, government agencies, military operations, or private sector resources that have substantial economic, social, and political impact. These kinds of cyber-attacks might be

DOI: 10.4018/978-1-5225-7909-0.ch009

Figure 1. Threat levels for cyber-attacks (types of cyber-attacks)

Threat Level	Attack Description
1	Major Disruption of critical infrastructure, public services, governmental operations, military operations.
2	Disruption of organizational operations, long-term outages or effects, dissemination of confidential or classified data, large impact on public services.
3	Short-term prevention use of computing resources, compromised access / authentication failures, collection of confidential information / trade secrets.
4	Cyber-surveillance, information gathering, unauthorized access to information resources.
5	Scanning. monitoring

equivalent to the cyber-attack on Estonia, which will be referred to throughout our analysis. Such cyber-attacks would be referred to as Level-1 cyber-attacks. Figure 1 identifies the level of cyber-attacks and the fallout from those attacks.

The threat level and type of attack is primarily determined by what it accomplishes, and the resulting damages from the attack. Figure 1 will be reintroduced towards the end of the analysis where we establish a threat level using SPCTA.

Defining Non-State Actors

UNCAs may be motivated to attack a nation-state using cyber technology. As such, these UNCAs are unsanctioned by any recognized state. The original thesis presented discourse on the various types of non-state cyber-actors; however, for the purposes of this article, we only mention them briefly with the assumption that the reader has some knowledge of cyber-actors. Literature on non-state cyber actors present a variety of non-state cyber-actors (Andress, Winterfeld, Steve., 2013; Rattray & Healey, 2011) that are motivated to perpetrate cyber-attacks for various reasons. Classes include individuals, corporations or organizations, organized crime, terrorists, autonomous agents, and UNCAs as they are defined in this research.

Figure 2 identifies the attributes of a UNCA. The environmental attribute suggests the requirements of the technological infrastructure necessary to carryout an attack. We also assert that the major attack goal is to perpetrate a Level-1 for the purpose of influencing or coercing the state for political or economic reasons. As we established earlier, the UNCA seeks to target nation-states or state agencies. The ability to carry out a cyber-attack on a target also assumes that the target sustains the technological infrastructure to support the attack vector, and operates within a nation-state that sustains a cyber-infrastructure necessary to organize and support a cyber-attack. Upon review of Figure 2, it important to recall that the