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

Harry Brown III, Norwich University, Northfield, VT, 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.

KEYWORDS

Cyber-policy, Cyber-relations, Cybersecurity, Cyber-threats, 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 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 carry out 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 is important to recall that the attributes are specific to the UNCA as we have defined it. While there may be other attack goals, those of the UNCA are focused on Level-1 attack and causing disruption as an exercise of power to effect political outcomes. This creates the environment that allows and facilitates cyber-interaction between actors in the international political system.

Relevance of UNCAs

It is possible that a UNCA would perpetrate a cyber-attack against a state for the purposes of demonstrating power and pursuing interests in the same ways that states have historically demonstrated power, such as in Russia’s efforts to demonstrate its power in the Russia-Ukraine Natural Gas Dispute of 2009, where Russia perceived it in its interests to stop the flow of natural gas to Ukraine (Brown, Harry, 2010). This may also be observed in North Korea’s ballistic missile tests (James Martin Center for Nonproliferation Studies, 2014), and Pakistan’s posturing and show of nuclear capability.
Related Content

World War III: The Cyber War
[www.igi-global.com/article/world-war-iii/69772?camid=4v1a](www.igi-global.com/article/world-war-iii/69772?camid=4v1a)

A Learning-based Neural Network Model for the Detection and Classification of SQL Injection Attacks

Information Technology and Emergency Management
[www.igi-global.com/chapter/information-technology-emergency-management/38376?camid=4v1a](www.igi-global.com/chapter/information-technology-emergency-management/38376?camid=4v1a)
Application of Information Technology in Disaster and Emergency Management
www.igi-global.com/article/application-of-information-technology-in-disaster-and-emergency-management/90837?camid=4v1a