KSU Proceedings on Cybersecurity Education, Research and Practice

2021 KSU Conference on Cybersecurity Education, Research and Practice

Oct 30th, 9:00 AM - 9:30 AM

A Taxonomy of Cyberattacks against Critical Infrastructure

Miloslava Plachkinova
Kennesaw State University, mplachki@kennesaw.edu

Ace Vo
Loyola Marymount University, ace.vo@lmu.edu

Abstract

The current study proposes a taxonomy to organize existing knowledge on cybercrimes against critical infrastructure such as power plants, water treatment facilities, dams, and nuclear facilities. Routine Activity Theory is used to inform a three-dimensional taxonomy with the following dimensions: hacker motivation (likely offender), cyber, physical, and cyber-physical components of any cyber-physical system (suitable target), and security (capable guardian). The focus of the study is to develop and evaluate the classification tool using Design Science Research (DSR) methodology. Publicly available data was used to evaluate the utility and usability of the proposed artifact by exploring three possible scenarios – Stuxnet, the Ukrainian power grid shut down, and ransomware attacks. While similar taxonomies exist, none of them have been verified due to the sensitive nature of the data and this would be one of the first empirically validated frameworks to explore cyberattacks against critical infrastructure. By better understanding these attacks, we can be better prepared to prevent and respond to incidents.

Location

Online Zoom Session

Disciplines

Information Security | Management Information Systems

EXTENDED ABSTRACT

Cybercrime is a problem of growing significance in society. When it comes to critical infrastructure such as power plants, nuclear facilities, electric grid, dams, they are especially vulnerable to attacks because they were built predominantly before today's cybersecurity standards. These growing opportunities combined with the increased motivation and resources that hackers have, make our society an easy target of cybercrimes. Specifically, cyberterrorism and information warfare demonstrate in practice the massive impact of malicious attacks. Such attacks are often state-funded and categorized as Advanced Persistent Threats (APT). Thus, it is vital to focus on this growing threat to national security and consider new approaches to better protect individuals and government structures and identify means to respond to incidents.

Identifying the hackers who commit cybercrimes is challenging. The growing use of technology and the easier access to exploits on the Darknet make it easier even for someone with limited technical skills to commit crimes. And while technology is rapidly developing, our legislature on cybercrimes and cyberterrorism is lagging behind. Part of this is due to the complexity of the topic and the lack of understanding among policy makers. In addition, many still do not believe that entire critical infrastructures can be compromised with little effort. The lack of adequate incident response guidelines is another important aspect of this problem.

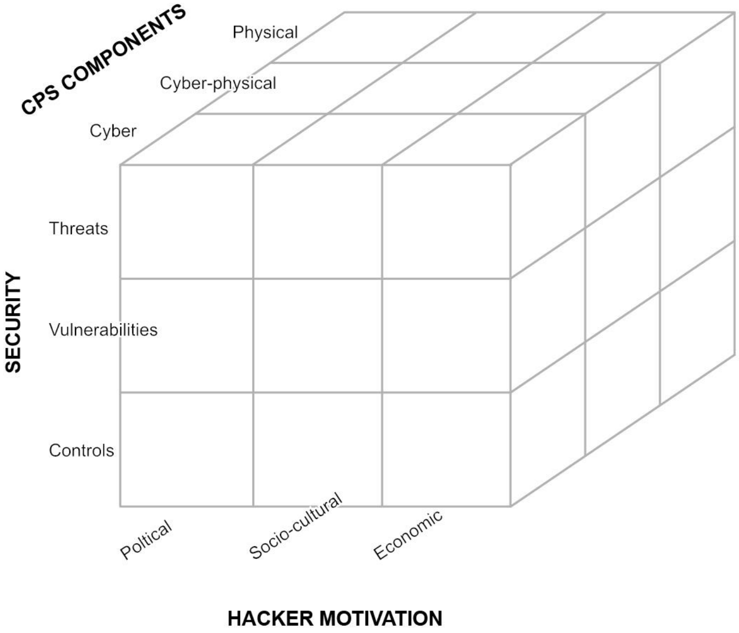
A significant first step in this direction would be to analyze the hacker culture and understand why these individuals commit cybercrimes in the first place. Attacking the root cause of the problem is the only viable solution to reduce cybercrimes in the future. While some hackers may be motivated by financial gain, others commit crimes for social or political reasons. By focusing on these different types of offenders, we can propose more adequate solutions to policy makers because one single policy may not be able to adequately resolve all these problems.

The current study is the first attempt not only to create but empirically validate a taxonomy of cyberattacks against critical infrastructure. The goal is to assist practitioners and scholars in improving the guardianship of such facilities of national security and improve the existing incident detection and response practices. This is a crucial step to strengthen the overall security posture of our country.

The current study offers a comprehensive classification of cyberterrorism attacks with consideration of the hackers' motivation. With regards to policy recommendations, our focus is on the guardianship aspect of Routine Activity Theory (RAT) and how the government can better protect the legacy SCADA systems and improve the security posture of these facilities.

The first dimension, hacker motivation, is related to the offenders which could be politically, socio-culturally, and/or economically motivated. The second dimension represents the cyber, physical, and cyber-physical components of any cyber-physical system (CPS) and is a differentiation of the various aspects of the suitable target. The third dimension, security, is related to the threats, vulnerabilities, and controls that represent the lack of the capable guardian. These different dimensions are conceptualized and depicted in Figure 1.

Figure 1. *Proposed Taxonomy*


CPS COMPONENTS
Physical
Cyber-physical
Cyber
SECURITY
Threats
Vulnerabilities
Controls
Poltical
Socio-cultural
Economic
HACKER MOTIVATION