O Ciberataque como Guerra de Guerrilha

O Caso dos Ataques DDOS à Estónia, Geórgia e ao Google - China

Pedro José Bentes Graça

Abstract

My main concerns and objectives lies within the computer security and information warfare . My goal is prevention and early detection of cyber attacks. Indeed, they present a complexity and increasing diversity that makes today impossible to ensure complete safety to a given system. My purposes are focused on scientific multydisciplinarity : That is, look in other branches of science - strategy , history of conflicts, political science, common patterns of behavior comparable with the nature of cyber attacks. Cyber attacks are acts of war? If the answer is yes, what kind of war are they? What forms they may have? What are the minimum necessary conditions for their appearance ? Which sectors of social organization can affect? I believe that will be useful to use the strategic and political teachings of guerrilla which is a quite old reality already studied in depth, and try to apply them to the new reality of cyber attacks . It is within this parallelism that this study may be of value , contributing to attempt to identify common and reproducible patterns, between the realities of guerrilla warfare and a particular type of cyber attack, or cyber attacks

This study aims to contribute to a more accurate perception of similarities between guerrilla warfare and the reality of cyber attacks. Also, if possible, to create a conceptual model of analysis between the attacks of guerrilla warfare since the early twentieth century to the present , and particular type of cyber attacks . This is done by identifying a common pattern among conventional guerrilla attacks , their methods , goals and targets, and cyber attacks , even leading me to wonder if this new phenomenon in the context of conflict , will be just another type of attack to add to the scope of the guerrillas , bringing it to the virtual, and so updating it and complementing it . Clearly , we are in the field of strategy, as it is defined by Admiral Silva Ribeiro " ... as the science and art of building , and employ available means of coercion in a given context, to materialize the policy objectives , overcoming obstacles and exploring contingencies in a disagreement environment "

The methodology is based on collecting a significant and diverse set of reports of past guerrilla war, which cover a wide range of situations and targets. Next, I compared them with a set of attacks and checked whether there similarities between the conduct of guerrilla warfare and cyber attack.

identified the variables common to both. I made an identification and conceptualization of similarities and differences. Then I tried to evaluate the potential preventive / reactive planning of lessons learned from conventional guerrilla attacks and apply them to the specific nature of cyber attacks, to identify patterns that may contribute to combat them.