CERIAS

The Center for Education and Research in Information Assurance and Security

Canada's Cyber Warfare Capabilities

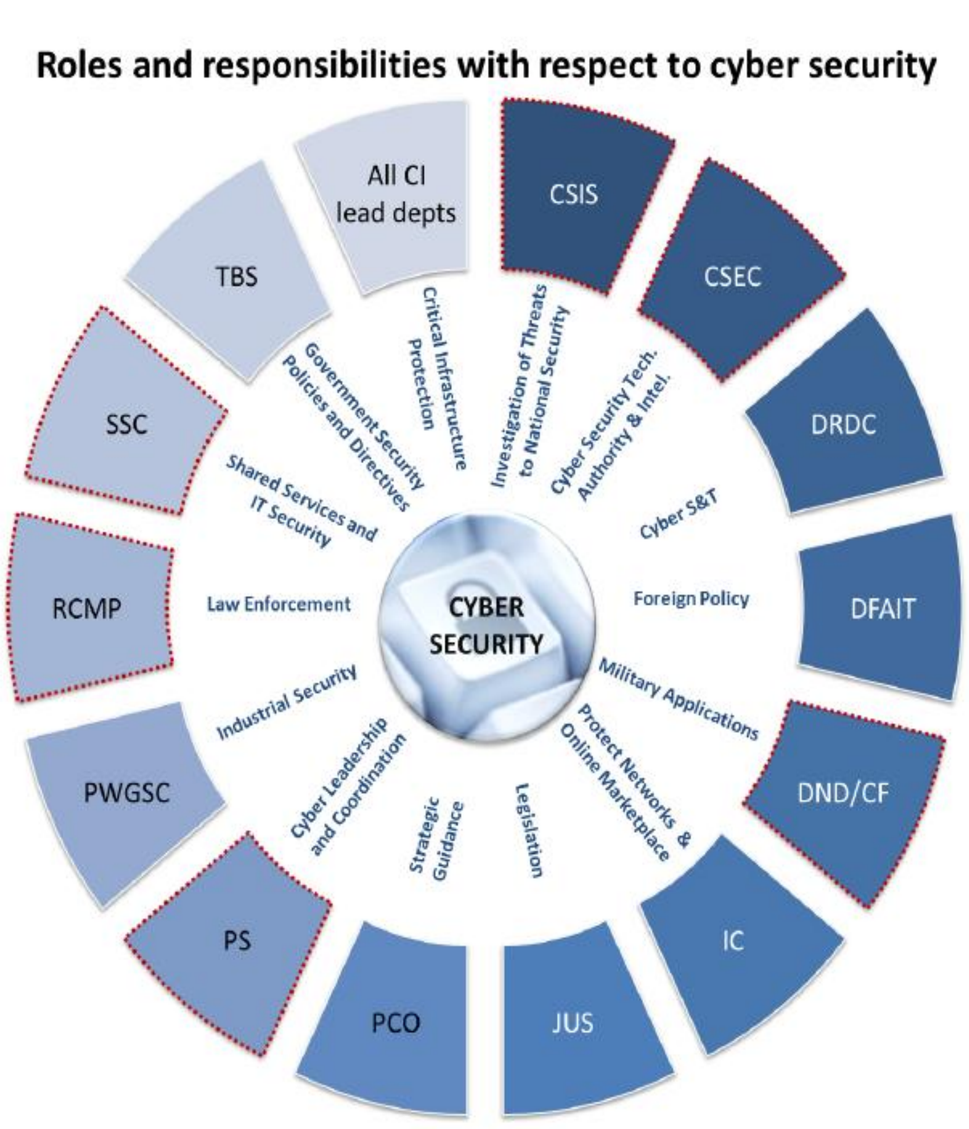
By: Bryan R. Lee and Dr. Sam Liles

Statement of Purpose

Current and relevant information is extremely important in the realm of transnational conflict. The field of intelligence and counter-intelligence has changed with the advent of the internet and the shift from using physical to digital media for much of the communication needed during a conflict. A nation's ability to control information that an enemy nation has access to, as well as the ability to gather information about an enemy nation is important to maintain the upper hand in a transnational conflict. It is important for the United States to understand what allies can bring to the table in transnational conflict. Canada is one of the United States' closest allies, both in terms of physical distance and strength of relations. Therefore, it is important to understand the cyber capabilities that Canada possesses in order to maintain a strong relationship and quickly and effectively communicate and coordinate intelligence gathering and analysis in times of conflict.

Abstract

This paper discusses Canada and its ability to wage cyber warfare. Several definitions of cyber warfare are presented and discussed, as well as the motives and potential actors behind a cyber attack. Several definitions of cyberspace are also discussed in order to provide a context for the domain of cyber warfare. A case is then made for why anyone should care about cyber warfare. Cyber attacks are a threat to a nation's security. Cyberspace must be considered a fourth domain of war, with the other three domains being land, air, and sea. There are many dangers within cyberspace that can affect individuals, corporations, and nation-states. Canada's cyber warfare capabilities are then examined. Both offensive and defensive capabilities are considered, with the focus of much of the research being on defensive capabilities. Canada recently released a cyber security strategy which is discussed in detail. Furthermore, capabilities of several government organizations are examined. Finally, a comparative assessment of Canada's capabilities within cyberspace is given. Canada's capabilities are found to be less than adequate to defend against a cyber engagement by an enemy nation-state. However, it is likely that many nation-states would be unable to defend against such an engagement from a knowledgeable and timely attacker.



Critique

-Responsibilities dispersed among multiple organizations
-Cyber security plan does not address attacks of nation-states – only smaller threats
-Canada has no central command for cyber operations
-Canadian CIRC only provides advice and monitors
-Canada ranked 3 ½ / 5 in cyber warfare preparedness
-Spain, UK, US ranked 4/5 and Israel and Sweden ranked 4 ½ / 5.
-Canada's cyber security plan is non-specific and leaves many potential issues unaddressed.
-No discussion of why cyberspace is important
-No discussion of what needs to be secured
-Shows a lack of understanding of the international nature of cyberspace

CERIAS

PURDUE UNIVERSITY