Applied Computing and Informatics (2015) **11**, 144–157

Saudi Computer Society, King Saud University

Applied Computing and Informatics

(http://computer.org.sa)
www.ksu.edu.sa
www.sciencedirect.com

ORIGINAL ARTICLE

Clear and present danger: Interventive and retaliatory approaches to cyber threats

Danilo V. Bernardo *

Db2P Research Institute, Bathurst Street, Sydney, NSW 2000, Australia

Received 3 May 2014; revised 14 September 2014; accepted 23 November 2014
Available online 4 December 2014

KEYWORDS

Cybersecurity;
Cyber warfare;
Cyberattacks;
Interventive;
Retaliatory;
Intelligence sharing

Abstract Organizations, including governments, have been attempting to address cyber threats for years by deploying technologies (e.g., security perimeter defences). These technologies are overarching policies and regulations designed to encourage resilient cybersecurity strategies that safeguard not only data, but also properties and human lives. Implementing these technologies is one thing, but ensuring their effectiveness is another. Lack of effectiveness and inability to satisfy existing government requirements and approaches in dealing with cyber threats and attacks are likely to continue until better approaches are employed. These approaches may emanate from effective regulations, intelligence gathering and sharing, and good security practices to workable alliances and interactions with other communities. This work is proposing approaches based on the premise that cybersecurity strategies must adhere to and be guided by the effectiveness criteria: that is, intervention and retaliatory approaches should be employed and utilized on the basis of their empirically demonstrated effectiveness to combat cyber threats.

* Tel.: +61 475 195 839.
E-mail address: bernardan@gmail.com.
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.aci.2014.11.002

1. Introduction

In achieving effective cybersecurity (http://belfercenter.ksg.harvard.edu/events/6230/intelligence_in_the_private_sector.html, 2014), as in employing effective cyber warfare preparation and governance, the importance of quickly recognizing cyber threats concerns the most basic elements of their identification, recognition, and employment of appropriate courses of action.

It is a challenge for policy makers and practitioners to effectively determine potential threats as early as possible. Hence, when cyber strategies (http://belfercenter.ksg.harvard.edu/events/6230/intelligence_in_the_private_sector.html, 2014; Bernardo and Chua, 2013) are examined, there is an ideal opportunity to observe the means through which organizations, governments in particular, become challenged in adjusting to the expectations of their stakeholders under the conditions of alliances, cooperativeness, socio-demographic values, and other practical influences.

In these conditions, the opportunity must be explored to develop processes and approaches that are survivable long-term. These conditions, however, do not reflect effective governance and, most of all, effective strategies in dealing with cyber threats, because these conditions are: firstly, influenced by practitioners' lack of effective interventive approach that falls short of compliance with the regulations and exercise of better security mechanisms; and secondly, found to be lacking comprehensive and effective retaliatory approach to launch mitigation strategies (e.g., counterattacks, etc.).

Attaining viable strategies to address cyber threats and attacks remains a challenge (http://belfercenter.ksg.harvard.edu/events/6230/intelligence_in_the_private_sector.html, 2014; Bernardo and Chua, 2013) due to lack of concentration on tailoring approaches to address appropriate actions to cyber threats: (a) key but uninformed practitioners are too conservative in meeting their agenda to carry out their own strategies on dealing with cyber threats; (b) another is the slowness of legitimate governments to move beyond mere identification of cyber threats by introducing enforceable regulation and actions, and viable solutions to curb and address them, and to fully recognize the importance of alliances with industries and other governments to have unified and effective approaches to combat cyber threats.

Central to the process of this phenomenon is the general perception that trivializes cyber threats and cyber security practices and the kind of impact that led to the lack of effective approaches. Consequently, practitioners become more reluctant to stably carry out their responsibilities and raise their level of awareness in order to minimize threats.

Theory and research into cyber security should therefore shift across various perspectives, and not be limited to: (1) retaliatory and interventive approaches, (2) compliance to existing regulations, (3) multi-way process and contemporary view of cybersecurity as fundamentally an emergent necessity of interaction and