Cyberspace: The New Battlefield - An Approach via the Analytics Hierarchy Process

John S. Hurley, National Defense University, College of Information and Cyberspace (CIC), Washington, DC, USA

ABSTRACT

The transition of the warfare mentality from the conventional domains of engagement (air, land, maritime, and space) to the cyberspace domain has not been an easy one for established organizations and institutions. The battlefield, in which now speed and stealth instead of size and budget are the determining factors that provide an edge have not well for many, especially those in the military. Now they do not clearly dictate who amongst combatants have the ‘upper hand’ and represent a significant paradigm shift from factors that were very good predictors of a potential outcome of military conflicts. The battles of the past were largely over territories and resources (Landscape Metrics, 2015). We see outcomes now being influenced by a broader range of factors, including politics, culture, economy, religion, and ethnicity. These new ‘pivot points’ for conflict require a very different understanding and approach to achieve desired outcomes. Technology continues to be the main enabler that has transformed the battlefield and the rules of engagement from the conventional domains to cyberspace. The issue of attribution has been a huge differentiator and looms very large in cyberspace conflicts because it is very difficult to determine within a sufficient timeframe the source of an attack and to be able to respond to or prevent attacks. Now conflicts have expanded in such a way that combatants now cross all prospective levels of society from targets to attackers or perpetrators. The low cost required to provide significant damage to a desired target environment in cyberspace has been a game changer. As a result, the rules of engagement which were much clearer in conventional domains on military fronts are much more blurred due to the new realm of combatants, and as such, has changed many of the approaches and methodologies that were standard practices in traditional campaigns. In this paper, we focus on cyber conflicts and how the cultural differences of these three communities have plagued the ability to achieve a simple and coherent response against attackers and perpetrators. We pursue the relevance of trust and deterrence and their influence on ‘warfare’ tactics in the cyberspace domain. We also look at culture and the ‘new norm’ and how they have required consideration of new and unconventional approaches. We see how data can better inform decision makers and those responsible for designing and implementing campaigns in this new era of conflict. Our results indicate the need for a different model to work through the differences in culture if better are to be obtained by the combatants. In addition, we see that an approach that includes cyber deterrence framed in the context of active defense provides optimism on future outcomes.

KEYWORDS

Actors, Conventional Battlefields, Cyberwarfare, Extremists, Strategic Weapons

DOI: 10.4018/IJCWT.2017070101

Copyright © 2017, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
INTRODUCTION

The world has changed dramatically and so have the interests and business priorities of the U.S. Unfortunately, the global transformation has also placed the United States’ interests in regions that are volatile with large anti-American sentiments, as well as brought persons with these mindsets to the United States. As a result, American allies and partners within these regions require the United States to rely much more on diplomacy and consensus rather than on the exercise of its military strength because the partners have their own interests to protect relative to neighbors with whom they must coexist. This new world order, which now includes China, India, and non-nation states, as new players, has dramatically altered the strategies that must be used to maneuver successfully through the maze of challenges, as well as, opportunities, that can present themselves. Such re-positioning requires that we examine a wide range of options. Traditional and historical strategies on conflict and engagement may serve us well in terms of how we are able to survive and flourish in this ‘New World’ order.

The role of the United States (U.S.) military is to protect and defend its citizens and interests of its allies around the world. Undeniably, the levels of engagement by the military in conventional warfare have placed a distinct fingerprint on the levels of engagement in the cyber domain. It is very important to understand how this new warfront must be addressed given the new wave of diverse and well-armed adversaries and perpetrators (from individuals to well organized non-nation states, to well-resourced and committed criminal enterprises) that must be engaged. This new battlefield requires a much broader and diverse approach because the adversaries have no rules by which they are constrained to engage and their motivations, expertise, and backgrounds are as diverse and varied as their resources and commitment to engage. In this paper, we search for ways to recognize and pursue the ‘new normal’ while holding firm to our norms and values.

BACKGROUND

What History Tells Us

Carl von Clausewitz, a Prussian general and influential military theorist, defined war as ‘a duel on a larger scale’; an act of force to compel an enemy to do the will of the adversary or target (Clausewitz, 1976). In his book, ‘On War’, Clausewitz focuses on the importance of information, in his ‘intention to provide a thinking man with a frame of reference, rather than to serve as a guide, which at the moment of action lays down precisely the path he must take’ (Clausewitz, 1976).

Sun Tzu promoted the notion that the operation environment must be thoroughly understood (Chen, 1994). Sun Tzu also warned that a commander must exhaustively and dispassionately analyze all information. He would study his enemies and proceed very humbly before engaging in offensive capabilities (Geers, 2011).

Jomini (trans. 2011) focused on the information aspects of a campaign in terms of geometry, especially in areas such as logistics and seapower. He felt that the amount of force that one deployed should be kept to a minimum in order to lower causalities. He viewed, however, that war was not an exact science. He focused on the need of regulation by fixed laws for strategy.

Machiavelli (2015) promoted the value of force and fraud in war. In the ‘Prince’, he counseled how to act towards one’s enemies, i.e., the use of force and fraud were encouraged. He valued information as a valuable source of power that was necessary to win wars.

All of the eminent strategists noted here considered war within a political framework, recognizing the significance of numbers as a practical dimension of war. Sun Tzu and Machiavelli saw war as an integral part of the political order—a tool of power (desaxx, 2010).

The ‘New World’ Order

Major differences in religion, culture, and ethnicity that were comfortably hidden by geographic borders in the past have given way to a ‘new world’ order that relies heavily on a global economy
Human Factor Role for Cyber Threats Resilience
www.igi-global.com/chapter/human-factor-role-for-cyber-threats-resilience/140530?camid=4v1a