International Journal of Cyber Warfare and Terrorism
Volume 7 • Issue 3 • July-September 2017

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

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 co-exist. 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

that has enjoined friend and foe, alike. The removal of many of the geographic separators have come about due to advancements in computing and information technologies that we applaud as they provide conveniences and advance our quality of life. The common thread (commerce) that has linked together entities that have been philosophically at odds on many different fronts for centuries has been facilitated by these technological advancements. The demand and dependence on trade and commerce has forced relationships that have not overcome the longstanding mistrust and cynicism that have plagued 'constructive' engagement in the past. It has been extremely difficult to move beyond the fundamental beliefs and doctrines that are so inherently different in many cultures. As such, it is prudent to focus on the less favorable potential of technology, i.e., its possible use within an 'arms race' which reinforces the impact of cyber. The use of technology in the invention and advancement of conventional weapons surely is nothing new. History, well documents how firearms, missiles, bombs, etc. have evolved. However, the development and evolution of new types of weapons and the design processes that enable them have taken a dramatic turn in their ability to exist as an enormous threat (Greenberg, 2014).

The role of technology also should not be understated in terms of how it has changed the dynamics of engagement between the haves and the have-nots. The cyber domain presents a different series of challenges that require a new view and approach to conflicts that can escalate to the level of war. As noted earlier, the role of technology in the formalism of weapons is not new. In the earliest stages, there were early developments and applications of new forms of weapons in aviation, navy and chemical warfare. The first widespread deployment of machine guns, artillery and the introduction of the lumbering armored tank occurred in World War I (Nash, 2015). The world is now more balanced in terms of those who can be viable threats, especially in the context of cyber-attacks. Society has witnessed a lot of advancements over past decades with the advent and progress of several different technologies and their applicability in warfighting, including: wearable solar panels to power battlefield displays and other equipment; a joint multirole technology demonstrator to enable soldiers to fly farther and faster with greater efficiency; a new fleet of aerial reconnaissance aircraft; the development of a new set of devices that can transfer energy to the soldier; and an augmented reality (AR) sand table that can more accurately model terrains (Curthoys, 2015). Along with the progress witnessed due to these technology advancements has been the transition of the United States (and most of the industrialized nations) from a geographically-focused regional view to a more global perspective. As a result, we find it necessary to examine the influence of cultural differences on how different communities co-exist and engage. Again, it is important to note that the scope is focused only on the cultural differences between the public, private, and government sectors.

Culture (and the Role It Plays in Cyber Conflicts)

A look at the approach by the military in dealing with conflict is very important to consider because in conventional or traditional warfighting campaigns, its methods have generally been unchallenged by other communities within society. The military is guided by a culture that is very rules-based and tradition-centered. Again, very little debate has taken place in terms of questioning how the military goes about its role and responsibility of protecting citizens and their interests. It is even driven home more succinctly when we look at the identification of two of the fundamental pillars of society, confidence and security (The Summit: Geneva, 2003; The Summit: Tunis, 2003). People want to feel safe and that they have the ability to evolve and prosper within society. Hence, the U.S. military, universally recognized by its prowess and ingenuity in terms of defending the interests of its citizens and allies, has been a very welcomed force (and largely gone unchallenged in its methods) not only within the United States but in other countries who rely and depend upon its strength and record of success in achieving desired outcomes in conventional campaigns.

The court of public opinion is still alive, active and formidable (Youssef, 2015)! In cyberspace, we are dealing with different kinds of conflict that have raised for one of the few times in history a challenge to the methods used by the military in addressing these types of conflicts. We are now

looking at conflicts in the cyber domain that do not have the graphic horrors often associated with conventional warfare in terms of kinetic damages which have significantly swayed public opinion in the past. We also have the difference in cyber on the 'turf' with which campaigns are waged. The public and private sectors, along with the government, in general and the military in particular, now are direct targets of perpetrators and feel compelled, understandably in some cases, to be able to weigh in on responses. Now, much closer scrutiny and evaluation of the methods used to address the conflicts have led to conflicts between cultures (communities) in terms of which methods are appropriate to be used and how they should be employed to resolve conflicts. The public and private sectors have recently expressed their displeasure in how cyber conflicts are being approached by the military. Again, we see that culture, as well as, trust between the communities as being major impediments to progress in addressing cyber threats. Trust, or the lack thereof, has been a huge challenge that must be overcome.

Trust as an Obstacle

There has been an inherent love-hate relationship between the federal government and the private sector that has been at issue for decades. It is important that the relationships be given more attention because in many different cases, most of the resources, management skills, and best practices are primarily in the domain of the business sector. However, the private sector cannot deploy them fast enough without the appropriate support from the federal government for government organizations have the appropriate frameworks in place needed to ensure success. As a result, it is critical that the federal government and the private sector work collectively to make sure that certain outcomes are achieved. The mistrust of government is not limited to the private sector. In a recent survey taken by the Edelman public relations firm, it was found that mistrust in the United States (U.S.) and Europe were at very depressing levels (Cartmell, 2012). For instance, in the U.S., there was a dramatic drop in political trust, 16 percentage points, to 37%. In Europe, there was a similar precipitous fall, especially within France which saw a drop 17 percentage points to 32% of those who trusted government. Numerous reasons have been given, including in the U.S., the revelations of widespread access by the National Security Agency (NSA) to information and the "challenged' start of Obamacare via the immense website difficulties. In France, however, the inability of former President Francois Hollande and his government to reinvigorate France's economy has been cited as critical factors to the challenges to trust between government and other sectors of society.

It is interesting that the survey also showed that little solace should be taken by industry because of the eight groups monitored, even though the overall level of trust in the commercial sector held steady at 58%, the survey showed that only government officials were less trusted than Chief Executive Officers (CEOs). The survey also emphasized that business should not view the results as a mandate to push for more deregulation because concerns over business' ability to self-regulate have been renewed by a number of very expensive outcomes that have come front-and-center to the public. In particular, the $13 billion record fine levied against JP Morgan Chase, Latin America's largest-ever bankruptcy, and the failure of Elke Batista's EBX deep-water oil drilling firm, and unfortunately, a number of other events have played out very poorly and in public view. A number of these and similar events have been attributed at least in the perception of many in the public as being the primary sources for many of the significant financial debacles around the world (Pylas, 2014). It is also of interest that the consequences to the mistrust between the different sectors have ramifications across the board, i.e., from areas that are quite obvious, like privacy, to those that deal with the environment (Everett, 2010).

As the cultural differences are examined between the organizations of interest (federal government vs other communities), two models are employed to highlight the cultures and their differences. In addition, the impact that current and new technologies can have on helping organizations meet their mission and performance objectives are considered. Also, one of the most important issues that has divided the two entities in terms of challenges-- the issue of trust, is addressed. There are huge differences between the communities in terms of perspectives and approaches to resolving conflicts

and challenges. It is important to work toward a solution of resolving the differences in a way that is mutually beneficial.

In the cyber domain, because borders and lines of separation are increasingly blurred there are also issues at a grander level that are relevant in this discussion, i.e., the need to build trust between nations. The candidates, of note, are two familiar nations that seem to consistently take different positions and have entrenched cultural and philosophical differences, the United States and China. To the surprise of many, there is actually a reason for optimism for cultural differences to be overcome as shown by an agreement between the U.S. and China in the area of cybersecurity. The collaboration targets the growing problem of spam. In 2011, a bilateral agreement was signed that sought to build trust between the nations while addressing the problem of spamming (Rauscher & Yonglin, 2011). The noted bilateral agreement was the result of a commitment by former President Barack Obama and President Hu Jintao, respectively of the U.S. and China. This effort represented the first attempt by the two nations to work together to address a major cybersecurity challenge. Spamming has been identified as a largely underestimated huge problem in which several hundred billion messages are transmitted across networks every day. Spamming accounts for almost 90% of all email messages and is a much more serious threat than many acknowledge, publicly. Spam is responsible for much of the malicious behavior on the Internet, in which it can infect hosts via web browsers and viruses. A lot of malicious code is carried by spam, which is also the source of botnet operations to achieve some form of financial gain. This is also a huge problem because email is the primary mechanism by which much of the modern world does business--it is truly indispensable (Rauscher & Yonglin, 2011). On a larger scale that it is important for nations to mitigate conflict, especially in the case of cyberattacks because of the concern for bigger problems.

Cultural differences should not be taken lightly for cultures are deep rooted and personal to communities. They can be tied to many aspects of the community that have evolved and been cemented for decades (in some cases hundreds of years). Inherent within the differences is the fundamental idea of mistrust, a harbinger of ill will and discomfort that can truly derail the hopes of achieving common goals. It is good, however, that there is some room for optimism, i.e., the bilateral agreement between the U.S. and China to address the common issue of spamming.

Models (Competing Values Framework and Schein Model)

The two models that will be the focus of attention for this study are the:

- Competing Values Framework (Quinn & and Rohrbaugh, 1981; Quinn & Rohrbaugh, 1983); and
- The Schein Model (Schein, 1990).

Competing Values Framework (CVF)

The Competing Values Framework (CVF) provides a basis for predicting organizational effectiveness. The CVF maps a distinct set of organizational and individual factors into four quadrants. The quadrants represent a distinct set of organizational and individual factors which map into four core values, which can represent opposite or competing assumptions. As such the competing values in the quadrants are responsible for the designation as a competing values framework (Cameron, 2015). The horizontal axis maps whether or not the organization is focusing either internally or externally. The vertical dimension maps who makes the decisions, where in the upper region, employees are empowered to make decisions. In the lower region, control rests with management. Also, in the upper half of the map, the focus is on flexibility and discretion. On the left-hand vertical region, the emphasis is on internal focus and integration. At the lower half of the map, the emphasis is on stability and control. Lastly, on the right side of the map, vertically, the emphasis is on external focus and differentiation. In Figure 1, the four quadrants that are seen to be related to hierarchies.

Figure 1. Competing Values Framework (CVF)

For clans, the organization is often flat with people and teams acting more autonomously. Their organizations are more focused on flexibility and less on structure and control.

In an adhocracy, there is a rapidly changing business environment in which there is greater independence and flexibility than the clan. The adhocracy will be more inclined to use prototyping and experimenting. Its leaders are generally visionaries and innovation-focused with a view on making significant gains though there may be calculated risks.

The hierarchical view is a basic and common element seen in many organizations and characterized by well-defined policies and processes. In this view, there is a strong emphasis on control and structure—a concerted top-down approach.

Lastly, the market organization's view is controlled and externally-focused in a market context. The market view is very competitive, outward looking and very driven by results (Changing Minds, 2015).

Schein Model

The Schein model focuses on the view that an organization's culture (or belief that values and beliefs of an organization) is based largely on the use of experiences and the external environment to solve problems and meet objectives (Schein, 2015). The focus is on the following three levels of organizational cultures:

- **Artifacts:** Objects made by a human being, typically an item of cultural or historical interest;
- **Values:** Modalities of selective orientation (Pepper, 1958). Speaks to relative worth, utility, or importance;
- **Underlying Assumptions:** Facts or statements (as a proposition, axiom, postulate, or notion) taken for granted evident only on close inspection.

Above, brief background was provided on the two models that will form the basis for comparison of the organization cultures of the federal government (a special emphasis is place on the military), public and private sectors. The fact that there are indeed other models for organizational structure that could be used is noted. However, two of the most well utilized models are the ones that have

been selected here. Later there is a discussion of the models and their relevance to the communities in the results and discussion section.

Deterrence

Over time, the discussion of warfighting has been expanded beyond the traditional land and maritime domains to now embrace additional domains such as: air, space, and cyberspace. As the scope, breadth, and depth of warfighting has changed from the times of Hemocrates and Sun Tzu, so have the strategic plans necessary to address the threats of today. It is still the purview of the military to engage in or deter from war in support of national objectives (Joint Operations, 2011). Though most of the emphasis has been placed on the engagement in warfighting, many efforts largely dedicated to how to deter warfighting are noted. There are additional documents such as the National Security Strategy (The White House, 2015), National Military Strategy for the United States: The United States Military's Contribution to National Security (The Joint Staff, 2015), the DoD Strategy for Operating in Cyberspace (U.S. Department of Defense) and the International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (The White House, 2011) which reinforce the value of focusing on deterrence.

The prominence of deterrence as a critical part of strategic thought is linked to the need to deter adversaries while developing opportunities to meet mission objectives. It is important to be reminded that the notion of deterrence is not a new one. Hemocrates, a Syracusan statesman and general, during the Athenian' Sicilian Expedition, in the midst of the Peloponnesian War, over 2400 years ago, noted that 'no one is driven into war by ignorance, and no one who thinks he will gain anything from it is deterred by fear' (Thucyidides, 431 B.C.E.). Sun Tzu, a Chinese military general, strategist, and philosopher, of 6th century BC, noted that 'for to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill' (Tzu, 1963). The philosophies of these prominent members of history were relevant to the land and maritime domains many centuries ago. It is worth noting the value of deterrence as a viable and necessary component of strategic thought, especially with respect to conventional military operations in most of the domains. However, as we look at deterrence in the context of cyberspace, we see limitations due to restrictions imposed by a lack of credibility, attribution, and signaling (Trujillo, 2014). Deterrence, defined by Joint Doctrine, is the prevention of action by either the belief that the cost of action outweighs the perceived benefits or the existence of a credible threat of unacceptable counteraction (Joint Staff, 2011).

Cyber Deterrence Case Study

The cyberspace domain can lead to a form of war that is just as destructive as traditional warfighting. In the book, *Cyber War* (Clarke & Knake, 2010), many of the details of this destruction are highlighted. Suffice it to say that the world would be better off if the ugliness of cyber war remained a text-book description and not reality. The solution to cyber deterrence centers on active defense work done by Watkins et. al. The authors focus on two major cyber threats that threaten our critical infrastructure, specifically the banking industry, many aspects of our government, and online ecommerce and business-to-business industries. These threats are the Zeus (Banking Trojan) and Dirt Jumper (Distributed Denial of Service (DDoS)) botnets which have contributed to the almost $575 billion in global hacking damage according to (Riley, 2014).

The current business and political climate is such that there has been huge outrage and many have been very vocal in favor of suspending the restrictive Computer Abuse and Fraud Act which prevents businesses from retaliating and "Hacking Back" against criminals. Despite the legalities, some companies have taken matters into their own hands and retaliated anyway. The researchers recount a poll taken at the Black Hat conference of 2012 where the company nCircle polled 181 of the conference attendees and determined that 36% of them had engaged in retaliatory hacking at least once (Watkins, 2015). In fact, in 2015 "Hacking Back" was a $78 billion-dollar business (Riley, 2014).

Although attribution remains an issue, we believe a step in the right direction is to endorse active defenses as a response to cyber threats. Watkins et. al demonstrated the feasibility of active defenses due to the inherent vulnerabilities in the command and control (C&C) of the Zeus (Watkins, 2014) and Dirt Jumper (Watkins, 2015) botnets. This work and others like it suggest that a policy of holding perpetrators of cybercrimes, like DDoS, data exfiltration, and financial fraud, responsible for their action and hacking back is a viable and responsible option. The suggestion is not nearly as far-fetched as it may sound given former President Obama's recent statement that "Hacking Back" for such reasons are warranted (Riley, 2014). This policy is likely effective against both nation state and black hat hackers. In both cases, there is likely an organized effort to take something valuable away from the government or industry. Since, an active defense results in consequences for cyber-attacks, the attackers are either forced to get ready to battle or be deterred from further attacks. The consequences could range from a rigorous campaign of surveillance to prosecutions to being subjected to the same kind of cyber-attacks perpetuated. The intent of the '*Arms Race'* is essentially to step back and review one's position, consider negotiation, when the reality sits in that one side believes that their resources or arsenal of cyber-tools are superior to the other side. Once the two sides are reasonably convinced that the outcome is not nearly as secured, then cyber-deterrence can more likely lead to the desired outcomes.

RESULTS AND DISCUSSION

Refer to Figure 2, Figure 3, and Figure 4. Using the CVF, it is possible to see how the Military, Public and Private Sectors break down in terms of primary (1), secondary (2), and other hierarchies (3 and 4). As noted in the earlier discussion, we see the military is seen to be very much about control and structure with a focus on the internal aspects and integration. On the private sector, the focus is on the market and is more externally driven and emphasizes differentiation. On the public sector, there is more of a focus on the clan side with a greater emphasis on flexibility. The public sector by the model appears to be more internally focused and emphasizing integration.

In the Table 1, there is a breakdown of the organizational cultures of the three segments of society and how they fit within the Schein model. The comparisons of cultures through the two models reveal

Figure 2. CVF (Military)

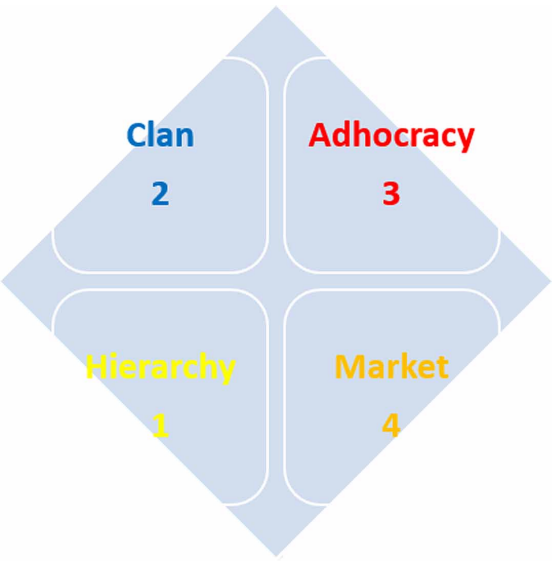

Figure 3. CVF (Private Sector)

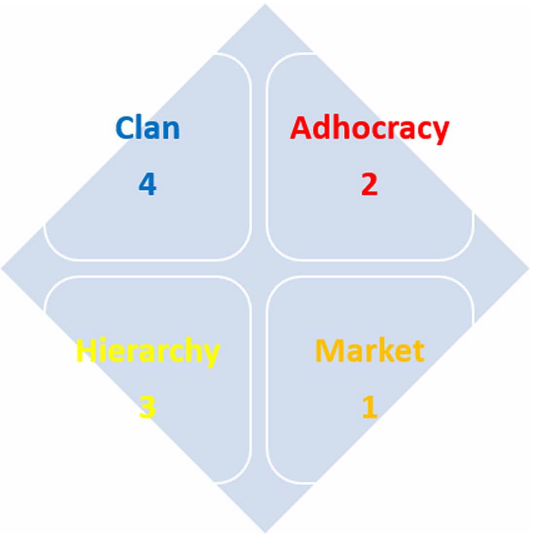

Figure 4. CVF (Public Sector)

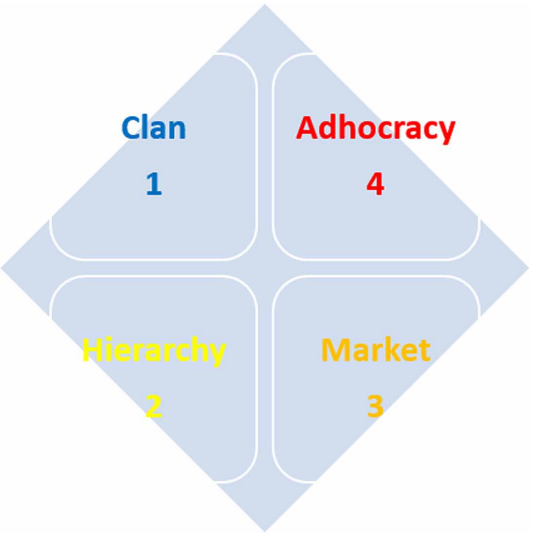

Table 1. Schein model

	Military	Private Sector	Public Sector
Artifacts	Uniforms Patches/Insignia	Brand Logo/Trademark	Community Quality of Life
Values	Tradition Protocol	Market-driven Shareholder Interests	Flexibility Privacy
Underlying Assumptions	Structure is Important Lead from the top	Innovation drives success Government over-regulates	Government support Security

some of the reasons why there is such disconnect and mistrust between the three communities. One of the biggest challenges in Cyberspace noted above was the need to work between three communities (federal government, public and private sectors) that have historically been plagued by self-serving interests that have often been the source of major conflict between them. A number of surveys conducted by a number of groups bear out this point. For example, in a poll conducted by the East West Institute, a non-partisan think tank, found that more than 90 percent of the respondents across the three communities, rate cyber-attacks as serious threats. However, there is no consensus on who is doing enough to secure their networks.

Thirty-nine percent of the public-sector think government networks are not secure enough, while 79 percent of government officials think private-sector networks are not secure enough (Cyber-Security Survey Shows Distrust Between the Public and Private Sectors, 2010). Officials from the United States, China, Russia and India participated in a poll from April 19 to 26 in which 34 government officials and 103 business officials were anonymously surveyed. Most of the experts agreed that the public and private sectors are not coordinated well enough to avoid the barrage of sophisticated and complex cyberattacks being coordinated by perpetrators. The results reflect the urgent need to build trust between governments and businesses on a global level. In addition, a common platform for information sharing (which has been a main source of conflict between the three communities) continues to plague engagement. About sixty percent of the public-sector officials polled, as well as, nearly three out of four government officials felt uncomfortable using social media as a medium to share information. The private sectors' hesitance, however, is more linked to concerns about regulation, as well as, having the federal government serve as stewards of the information. The latter point concentrates on the competitive advantage that some businesses feel that they would lose if the federal government controls information and how it is shared.

Technology has played a very important role both in support of, and to the angst of some, a downside to how information is shared. However, in this era and time, millennials and many of the businesses that they control prefer the social media platform to share information. Social media allows the millennials to feel connected, an important factor for them. A Nielsen survey has revealed that millennials have selected technology use as the most defining characteristic of their generation, over other factors such as pop culture consumption and music (Naftulin, 2016). Hence, one of the first challenges is to work through the cultural differences in one of the most important aspects of society, communication, in which technology has had a major impact. Technology has also provided a dynamic in terms of the speed with which events occur. Now it is necessary to address events in real time and near real time which dramatically changes the ability to protect and defend against attacks against our information assets. This factor is very relevant in the context of cyber attacks because events occur so quickly and the issue of attribution presents such a major challenge (The Attribution Problem in Cyber Attacks, 2013). The sources of activities carried out through the Internet are extremely difficult, almost impossible, to define conclusively. In issues of national security and the responsibilities in conventional warfare, the law of war, requires that in order for a counterattack to be launched, the initial attack must be definitively attributed to some source(s). Active defense measures reflect the ability of one state to hold another state responsible for an attack. As noted earlier, this becomes even more challenging in the context of 'cyber warfare' because attribution is so difficult to know conclusively. In addition, the basis for an act of war (due to a cyberattack) is so poorly defined.

There have been attempts to improve relations between the three communities. A few years ago, former President Obama held a White House Summit on Cybersecurity and Consumer Protection at Stanford University. He assembled CEOs and government officials from across the country to discuss how to protect the growing digital economy. President Obama discussed support of net neutrality, student privacy rights and government cybersecurity measures. Of note was the Executive Order (EO) that he signed which framed a new era of cooperation between the three sectors. The EO, 'Promoting

Private Sector Cybersecurity Information Sharing', promotes the creation of information sharing and analysis organizations (ISAOs) around the country with government support. The plans include an effort to expand the reach of the National Cybersecurity and Communications Integration Center (Ntim, 2015). However, these plans though noble and well-intended, have fallen far short of having the desired impact because they are short on specifics and details. In particular, the EO does not discuss how and in what form cooperation between the private and public sector will work to enable the level of cybersecurity needed. The former President surely understood the challenges, especially the issue of mistrust, as reflected in an interview that he conducted shortly after the meeting at Stanford University. He noted the harm of the Snowden disclosures in escalating the mistrust between the government and the private sector. However, there is a growing consensus, as noted by some like Kenneth Chenault, former CEO, American Express, that there has to be a basis for trust in order to expect cooperation (Ntim, 2015). In cyberspace, it is important to consider a way to bring the three different communities together in order to enable the communities to meet their needs.

The Analytic Hierarchy Process (AHP) is used within this study because of its ability to incorporate diverse, and at times conflicting, priorities which is idea for the three communities of interest, i.e., public, private and government sectors. See Figure 5 and Table 2.

The AHP is used to establish the priority of the three communities in terms of the criteria of trust needed to lead and promote Cyberspace as the secure, safe and efficient information sharing environment.

Figure 5. Pairwise comparison

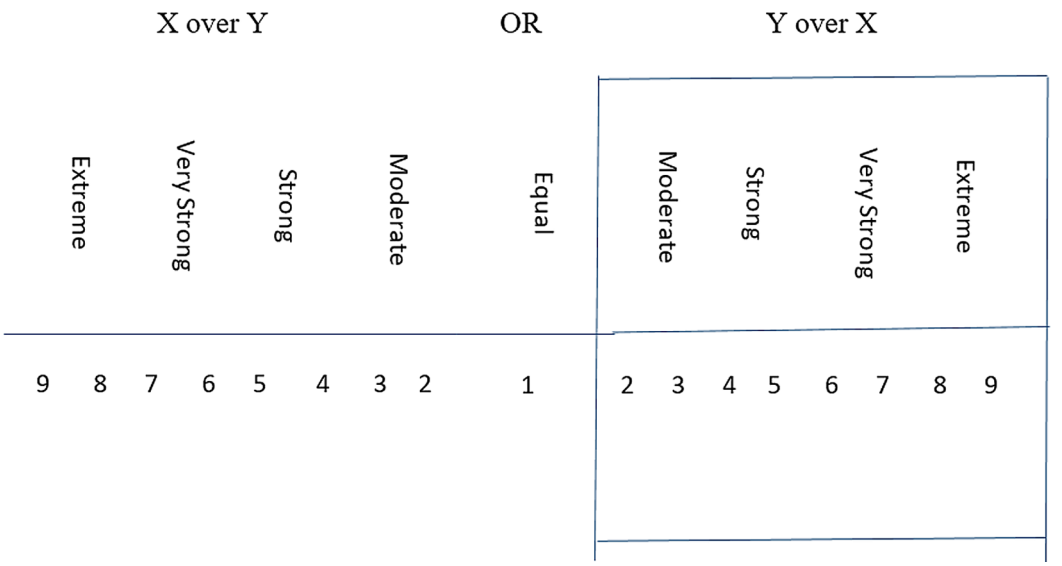

Table 2. AHP pairwise comparison

Trust	Government	Public Sector	Private Sector	Priorities
Government	1	4	8	.7
Public Sector	1/4	1	2	.2
Private Sector	1/8	1/2	1	.1

CONCLUSION

In this paper, the organizational culture of three segments of our society, i.e., the public, private, and government sectors were examined in order to determine how to better address the challenges and opportunities presented in the cyberspace domain. The impact that the historical presence from past decades and centuries have had on the military approach to defending and protecting the information assets in cyberspace is shared through the use of two models, the Competing Values Framework and Schein model. A breakdown of key tenets of each society segment and why there has been so little headway on some of the differences are also presented. The comparisons were good in illustrating the differences, but left with more questions than answers in terms of how to reconcile the cultural differences to better address cyber threats and vulnerabilities. As a result, a new model (the AHP) is proposed that might help better reconcile some of the differences.

Also, a case study was presented that explored the use of active defenses to deter cyber criminals and nation state hackers from engaging in cyber war against the government and industry. In addition, cyber deterrence is believed to be achievable as a national policy. In addition, the keys are to develop a rigorous attribution system and to provide consequences to hackers for their attackers. Attribution is a non-trivial task and is beyond the scope of this paper; however, the research that exists in the literature regarding active defenses are a sufficient place to start to begin to provide real consequences to hackers for cyber-attacks. A reasonable starting point could be to provide real consequences to perpetuators of DDoS and online financial fraud. This is within the purview of the government. The key here is that this policy of using active defenses as a response to cyber-attacks holds hackers accountable for their actions by providing consequences for hacking.

As a result, there is some optimism in the future that efforts can be devoted to resolve differences between cultures to better address future cyber threats and vulnerabilities. We offer the U.S.-China bilateral agreement to combat spam as an example. In addition, the promise of how framing cyber deterrence using active defenses can also be a part of the solution to better protect information assets can play an essential role.

REFERENCES

Blechman, B. M., & Kaplan, S. S. (1978). *Force without War*. Washington, DC: The Brookings Institution.

Cameron, K. (2015, November). *An Introduction to the Competing Values Framework*. Retrieved from http://www.thercfgroup.com/files/resources/an_introduction_to_the_competing_values_framework.pdf

Cartmell, M. (2012, January 23). Edelman Trust Barometer Reveals Distrust of UK Government and Business. *PR Week*. Retrieved from http://www.prweek.com/article/1113501/edelman-trust-barometer-reveals-distrust-uk-government-business

Changing Minds. (2015, November). *The Competing Values Framework*. Retrieved from http://changingminds.org/explanations/culture/competing_values.htm

Chen, M. (1994). Sun Tzus Strategic Thinking and Contemporary Business. *Business Horizons*, *37*(2), 42–48. doi:10.1016/0007-6813(94)90031-0

Clarke, R. A., & Knake, R. K. (2010). *Cyber War*. New York: HarperCollins.

Clausewitz, C. v. (1976). *On War*. Princeton: Princeton University Press.

Curthoys, K. (2015, April 2). Five New Technologies for the Army Warfighter. *Army Times*. Retrieved from http://www.armytimes.com/story/military/tech/2015/04/01/army-ausa-technology-via/70774660/

de Jomini, A.-H. (2011). *The Art of War.* Princeton: Bottom of the Hill.

desaxx. (2010, September 8). *Discussion: Sun Tzu, Machiavelli, Clausewitz, and Jomini.* Retrieved from http://desaxx.blogspot.com/2010/09/discussion-sun-tzu-machiavelli.html

DoD Strategy for Operating in Cyberspace. (2015). Washington, DC: Pentagon.

Dunn, M. (1996, October). Levels of War: Just a Set of Labels? *Clausewitz*. Retrieved from http://www.clausewitz.com/readings/Dunn.htm

Dunnigan, J. F. (2003). How to Become an Effective Armchair General. In J. F. Dunnigan (Ed.), *How to Make War: A Comprehensive Guide to Modern Warfare in the 21st Century* (pp. 2–7). New York: Quill.

Everett, C. (2010, March 17). *Stigson Warns Mistrust between Business and Government is Hampering Low Carbon Economy*. Retrieved from Youris.com: http://worldblog.eu/2010/03/17/page/2/

Fearon, J. (1995). Rationalist Explanations for War. *International Organization*, *49*(3), 379–414. doi:10.1017/S0020818300033324

Geers, K. (2011). *Sun Tzu and Cyber War.* NCIS. Retrieved from https://media.blackhat.com/ad-12/Geers/bh-ad-12-art-of-cyberwar-geers-WP.pdf

Geers, K. (2015, October 15). *Sun Tzu and Cyber War.* NCIS. Retrieved from https://media.blackhat.com/ad-12/Geers/bh-ad-12-art-of-cyberwar-geers-WP.pdf

Government Technology. (2010, May 1). *Cyber-Security Survey Shows Distrust Between the Public and Private Sectors.* Retrieved from http://www.govtech.com/security/Cyber-Security-Survey-Shows-Distrust-Between-Public.html

Greenberg, A. (2014, May 5). How 3-D Printed Guns Evolved into Serious Weapons in Just One Year. *Wired*. Retrieved from http://www.wired.com/2014/05/3d-printed-guns/

INFOSEC Institute. (2013, February 1). *The Attribution Problem in Cyber Attacks.* Retrieved from http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/#gref

International Strategy for Cyberspace. (2011). Washington, DC: Executive Branch.

ITU.INT. (2003, December). *The Summit: Geneva.* Retrieved from http://www.itu.int/net/wsis/index.html

ITU.INT. (2005, December). *The World Summit on the Information Society.* Retrieved from http://www.itu.int/net/wsis/index.html

Jackson, M. O., & Massimo, M. (2009). The Reasons for Wars-an Updated Survey. In C. Coyne (Ed.), *Handbook on the Political Economy of War*. Elgar Publishing.

JP 3-0, Joint Operations. (2011). Washington, DC: The Joint Staff.

Landscape Metrics. (2015, September 22). Russia's territorial gains of oil and gas through the annexation of Crimea. Retrieved from http://www.landscapemetrics.com/blog/post/russias-territorial-gains-of-oil-and-gas-through-the-annexation-of-crimea

Landscape Metrics. (2015, September 22). Russia's Territorial Gains of Oil& Gas through the Annexation of Crimea. Retrieved from http://www.landscapemetrics.com/blog/post/russias-territorial-gains-of-oil-and-gas-through-the-annexation-of-crimea

Layton, J. (2015, September 01). How the Rules of War Work. *Howstuffworks*. Retrieved from http://people.howstuffworks.com/rules-of-war.htm

Machiavelli, N. (2015). The Prince (trans.). Florence. (originally published 1515)

Morris, E. (Director). (2003). *The Fog of War* [Motion Picture].

Naftulin, J. (2016, July 1). Here Are Some of the Strangest Ways that Millennials Use Technology. *Business Insider*. Retrieved from http://www.businessinsider.com/strangest-millennial-tech-trends-2016-7

Nash, T. (2015, November). Weapons Used in World War I. *The Finer Times*. Retrieved from http://www.thefinertimes.com/Weapons-of-War/weapons-used-in-world-war-i.html

National Military Strategy. (2015). Washington, DC: Executive Branch.

National Military Strategy. (2015, July). Retrieved from www.jcs.mil/.../2015_National_Military_Strategy.pdf

National Security Strategy. (2015). Washington, DC: Executive Branch.

Normand, T., & Poarch, J. (2015, September 03). *The Law of Armed Conflict (LOAC).* Retrieved from LOAC: http://loacblog.com/loac-basics/4-basic-principles/

Ntim, A. (2015, February 20). Cybersecurity in an Age of Distrust. *Stanford Political Journal*. Retrieved from https://stanfordpolitics.com/cybersecurity-in-an-age-of-distrust-1ea40d17b1b9#.vmz3x969e

PBS (Director). (2015). *The Aftermath of War* [Motion Picture]. Retrieved from PBS: http://www.pbs.org/kera/usmexicanwar/aftermath/war.html

Pepper, S. C. (1958). *The Sources of Value*. Berkeley: University of California Press.

Powers, R. (2015, September 03). Law of Armed Conflict (LOAC). *US Military*. Retrieved from About Careers: http://usmilitary.about.com/cs/wars/a/loac.htm

Pylas, P. (2014, January 20). Distrust in Government. *USA Today*. Retrieved from http://www.usatoday.com/story/news/world/2014/01/20/distrust-in-government-growing/4655111/

Pylas, P. (2014). Distrust in government growing, survey finds. Associated Press. Retrieved from http://www.usatoday.com/story/news/world/2014/01/20/distrust-in-government-growing/4655111/

Quinn, R., & Rohrbaugh, J. (1981). A Competing Values Approach to Organizational Effectiveness. *Public Productivity Review*, *5*(2), 122–140. doi:10.2307/3380029

Quinn, R., & Rohrbaugh, J. (1983). A Spatial Model of Effectiveness criteria: Towards a Competing Values Approach to Organizational Analysis. *Management Science*, *29*(3), 363–377. doi:10.1287/mnsc.29.3.363

Rauscher, K. F., & Yonglin, Z. (2011). *Fighting Spam to Build Trust*. New York, Beijing: East West Institute and The Internet Society of China.

Schein, E. (2015, November). Edgar Schein Model of Organization Culture. *Businessmate.org*. Retrieved from http://www.businessmate.org/Article.php?ArtikelId=36

Schein, E. H. (1990). Organizational Culture. *The American Psychologist*, *45*(2), 109–119. doi:10.1037/0003-066X.45.2.109

Stigson Warns Mistrust between Business and Government is Hampering Low Carbon Economy. (2010, March 17).

Sun-Tzu. (2011). *The Art of War* (trans.). Princeton: Bottom of the Hill.

The Finer Times. (2015, November). *Weapons of War.* Retrieved from http://www.thefinertimes.com/Weapons-of-War/weapons-used-in-world-war-i.html#sthash.ehRET5Bi.dpuf

Thucyidides. (431 B.C.E.). The History of the Peloponnesian War. *Classics.mit.edu*. Retrieved from http://classics.mit.edu/Thucydides/pelopwar.html

Trujillo, C. (2014). *The Limits of Cyberspace Deterrence*. Washington, DC: CJCS.

Tzu, S. (1963). *The Art of War (trans. S.B. Griffith)*. New York: Oxford University Press.

United Nations & International Telecommunications Union. (2003, December 12). WSIS. Geneva, Switzerland: United Nations and International Telecommunications Union.

Whitehouse.gov. (2015, February). *National Security Strategy.* Retrieved from www.whitehouse.gov/.../2015_national_security_strategy.pdf

Youssef, N. A. (2015, January 24). U.S. Won't Admit to Killing a Single Civilian in ISIS War. *The Daily Beast*. Retrieved from http://www.thedailybeast.com/articles/2015/01/24/u-s-won-t-admit-to-killing-a-single-civilian-in-the-isis-war.html