AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

Engaging Cyber Communities

By

Yashua W. Gustafson, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisors: Mr. Roger Philipsek and Lt. Col. Paul L. Griffith, USAF

Maxwell Air Force Base, Alabama

Apr 2010

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Table of Contents

Abstract

There are 1.7 billion Internet users worldwide as of October, 2009 and growing.[1] The dramatic growth in online users in conjunction with the influence of social communities in cyberspace is having an effect in current and future international affairs.[2] Despite the growing amount of activity performed by social groups in cyberspace, the US military remains focused on technology centric operations such as computer network attack and computer network defense.[3] This leads to the question of whether the US military is missing an opportunity by not "focusing" on online social communities. This research performed a problem and solutions methodology to investigate this question. The research came up with the criteria of value and risk to analyze whether the US military should engage cyber communities. The results of this study suggest engaging online communities can augment the technology-centric solutions. Engaging online communities can help to degrade, deceive, and exploit adversaries operations in cyberspace. Engaging online communities can also influence and help respond to social groups' issues and concerns. Without responding or influencing these groups they are left to their own vagaries as well as negative and adversarial influence. There are risks associated with engaging online communities due to the ubiquitous reach of cyberspace. An ill-conceived comment, text, or video can be sent globally and have a negative impact to objectives and reputation. However, this study finds applying controls and rules of engagement in undertaking these operations can mitigate the risks. Thus, the US military needs to develop these capabilities and engage social communities in cyberspace.

INTRODUCTION

There are 1.7 billion Internet users worldwide as of October, 2009 and growing.[4] The dramatic growth in online users in conjunction with the influence of social communities in cyberspace is having an effect in current and future international affairs.[5] The 2009 Iranian presidential elections provide an example of the impact. According to a Washington Times editorial, "The mass protests followed a weekend of street demonstrations, rioting and other expressions of discontent. These events were brought to the world in real time through social-media networks and online video."[6] Another example is terrorists' use of cyberspace. According to Libicki, "terrorists use the Internet for three related purposes: recruiting adherents, distributing instructional materials, and exercising direct command and control."[7] Despite the growing amount of activity performed by social groups in cyberspace, the US military remains focused on technology centric operations such as computer network attack (CNA) and computer network defense (CND).[8] Both capabilities are vital, but the one-sided strategy relies too much on technology resulting in little to no social interaction with foreign actors. The small amount of interaction the US military does provide is one-way information to online communities as described below:

> DoD sponsors a number of information and online news Web sites. Some sites, such as ones maintained by U.S. Central Command, produce information relevant to some of the most difficult issues, particularly the war in Iraq. Others, such as the southeast Europeans Times (produced in nine languages) and Magharebia (produced in three languages), provide "regional news," and "in-depth analysis" for their respective areas.[9]

However, according to Kramer and Wentz,[10] the information provided is for mass audiences and does not provide two-way communication required for focused influence. This leads to the question of whether the US military is missing an opportunity by not "focusing" on online social communities. History has already shown that operations centered on technology without

contextual consideration have failed until changes in strategy were made. An example is the Vietnam War. The US proved unsuccessful even as the US maintained superior military technology.[11] Another example is the improved stability in OPERATION IRAQI FREEDOM (OIF) resulting in part from empowering local communities through the Sons of Iraq and less on technology centric operations inherent in conventional forces. Per a US General Accounting Office report, "In March 2008, DOD reported that the Sons of Iraq program has helped to improve security at the local level by involving local citizens in the security of their communities."[12] The result was arguably a major turning point for the US.

Cyberspace is a domain consisting of technology; however people ultimately operate and cooperate through the cyber domain. If the US military is not engaged with online communities then a reasonable assumption is communities will be influenced by other actors. While the US is currently waging warfare in cyberspace through technical means (CNA and CND), the cyber domain is ultimately controlled by humans,[13] and the US military should engage in social web interaction as a factor in cyberwar. To analyze this statement, this research uses the problem/solution methodology.

The structure supporting this study follows. The first section in this paper covers the background and defines the problem surrounding warfare in cyberspace and the US military's historical over-reliance of technology-centric solutions. The second section provides criteria to analyze an alternate to technology-only solutions and whether the technology-centric solution is adequate. The third section discusses the alternatives to technology-centric solutions. The fourth section analyzes the current and alternative strategy based on the developed criteria. The fifth section concludes by selecting whether or not social online communities should be engaged. Section six provides recommendations on how to engage social communities in cyberspace.

BACKGROUND

Cyber communities or social websites on the Internet consists of varying groups meeting for social reasons. Edward Skoudis states, "online community refers to social setting in cyberspace such as MySpace, LinkedIn, and Orkut, where consumers with common interests communicate and share personal profiles, business contacts, and so forth. Such sites have flourished recently; MySpace had over 300 Million accounts for users around the world as of 2007."[14] Another form of online community is the blog where writers provide opinions on a range of topics and also provides an avenue for feedback from readers. The blogs are written by anybody from an individual blogging on their free time about personal events to news media and other professional news personalities writing about the latest political topic. Skoudis states the blog "is an online diary where a writer shares information and commentary about politics, hobbies, or other interest communities…some blogs have become quite popular and have helped shape political debates and news stories." A third type of online community according to Skoudis "involves integrated supply chains, in which a given manufacturer relies on a host of suppliers, who in turn rely on their own suppliers, and distributed in countries around the world, the controlled through cyberspace."[15] The forth online community is consumer commerce. Skoudis states, "consumer commerce, such as Amazon.com and eBay…created a lively interchange of buyers and sellers, with complex ranking, preference, and voting systems for products and providers."[16]

Another form of online community and arguably a player in international politics is activists, hacktivists, and cyberterrorists. According to Dorothy Denning cyber activity by activists consists of "normal, nondisruptive use of the Internet in support of an agenda or cause.

Operations in this area include browsing the web for information, constructing web sites and posting materials on them, transmitting electronic publications and letters through email and using the Net to discuss issues, form coalitions, and plan and coordinate activities." The second online community in cyberspace with intentions to influence political thinking is hacktivists. Dorothy Denning states, "hacktivism refers to the marriage of hacking and activism. It covers operations that use hacking techniques against a target's Internet site with the intent of disrupting normal operations but not causing serious damage. Examples are web sit-ins, and virtual blockades, automated email bombs, web hacks, computer break-ins, and computer viruses and worms."[17] A third type of political actor in cyberspace is the cyberterrorist. Denning states, "cyberterrorism refers to the convergence of cyberspace and terrorism. It covers politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage. An example would be penetrating an air traffic control system and causing two planes to collide."[18] Other disruptive entities in cyberspace include white and black hat hackers of all sorts as well as state sponsored hackers.

Social groups in cyberspace have international influence. As discussed above social groups protesting in Iran were enabled by the power of unity through online collaboration tools as well as influencing the international populace through stories and pictures of events happening on the ground in Iran. Attempts by the Iranian government to censure the flow of information did not stop the flow of information. An earlier example of social Cyberpower is the Kosovo conflict from 1998-1999. Social groups in cyberspace engaged international audiences to affect the war's outcome. Denning states,

> Just how much impact did the Internet have on foreign policy decisions relating to the war? It clearly had a part in the political discourse taking place, and it was exploited by activists seeking to alter foreign policy decisions. It also affected military decisions. While NATO targeted Serb media outlets carrying

> Milosevic's propaganda, it intentionally did not bomb Internet service providers or shut down the satellite links bringing the Internet to Yugoslavia.[19]

While cyber communities are organizing and influential as detailed above, the US military continues to focus on technical aspects of cyberwar through computer network attack, computer network defense (CND), and computer network exploitation (CNE) as described in Joint Publication (JP) 3-13, "CNO [computer network operations], along with EW [electronic warfare], is used to attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure. For the purpose of military operations, CNO are divided into CNA, CND, and computer network exploitation (CNE) enabling operations."[20] There is no mention of engaging cyberspace communities through dialogue or non-technical means. JP 3-13 does discuss psychological operations (PSYOP) as a peer capability to CNO, and lists PSYOP support to CNO as only "convincing enemy not to do something by describing effects of a CNA if they take undesirable action,"[21] and from a defensive stance in CND, "providing information about non-military threat to computers in the area of operations."[22] While CNA and CND provide the vital foundation for warfare in cyberspace, people ultimately dictate and influence how governments act. Kramer and Wentz discuss the historical importance of engaging communities by stating, "every battle commander in these irregular wars soon finds out that the communication battle is critical—because the center of gravity for success is the population. But all too often, our commanders have to learn this on the ground."[23]

History has shown the over-use of technological solutions can fail due to the lack of appropriate doctrine or faulty assumptions. An example is the Air Force's role in Vietnam and Korea. Tami Biddle states,

> The Air Force's response to criticism implying that it had not lived up to public expectations was not to try to modify those expectations but rather to insist that bombing could be decisive—if only it could be freed from political restraints… but two important observations are worth noting here. First, there were few

> important targets in Korea and Vietnam that were not hit hard by bombers (often multiple times). Even when heavy pressure can be brought to bear on enemy economies and societies, they can prove resilient and robust. In the economies realm, industry can be dispersed, repairs can be made, and resources can be obtained externally. In the social realm, civilians can move out of the way of bombs, they can become acclimated to their effects over time, or they can choose to accept high levels of discomfort and sacrifice. Motivated and mobilized civilians backed by determined governments can sustain vey high pain thresholds. In addition, discontented civilians may simply lack the mechanisms to convey their discontent into political leverage against the national leadership.[24]

This quote on airpower is not to take-away from the large contribution and success in past conflicts, but to point out an example of technological limitations in warfare.

OIF produced another example of relying on technology too much. The US Army success bringing down the government of Iraq was quickly overshadowed by the challenge to create a stable environment. According to Nigel Aylwin-Foster, "despite its own multi-cultural nature, the Army was not culturally attuned to the environment. U.S. Army personnel instinctively turned to technology to solve problems. Similarly, their instinct was to seek means, including technology, to minimize frequent close contact with the local population, in order to enhance force protection, but this served further to alienate the troops from the population."[25]

An important aspect to understanding cyberspace is humans ultimately control cyberspace. Rattray states, that "cyberspace is a manmade environment, unlike land, sea, air, or space. States, corporations, and other actors utilizing cyberspace can and do make choices about ownership, control, and operations of these key cyberspace features."[26] Rattray further states, "cyberspace is actually a physical environment: it is created by the connection of physical systems and networks, managed by rules set in software and communications protocols."[27] Another way of looking at cyberspace is to see the physical environment as the air, land, and sea of cyberspace and the exploitation and exchange of information as the activity of the living on earth. As mentioned above, the Department of Defense (DoD) appears to have a strategy toward

the hardware, software, and information aspects. This is like saying manipulating the geographic landscape is all that is needed in warfare. Albeit, a powerful force, not acknowledging and engaging social aspects, which "may" have the ability to curtail costly effects of CNA and other attacks on a state is equivalent to ignoring diplomacy. The point is the military's lack of focus on engaging and influencing social communities is under-developed.

CRITERIA

The main question of this research is whether or not the current US strategy in Cyberspace is missing an opportunity by not engaging online social communities. Thus, this research looks into a binary equation. The equation is either the US is missing an opportunity or the US is not missing an opportunity. If the US is missing an opportunity then there must be some value that is missing. According to the Merriam-Webster dictionary "value" can be thought of as the "relative worth, utility, or importance"[28] of some entity. The value in a military sense can be thought of as the capability it provides.

The second criteria deals with the risk involved. If the US is missing an opportunity by not engaging online communities then the action must also be worth the risk of implementing. Therefore, this study performs a risk analysis of the capability. An example is a risks analysis of launching a nuclear weapon. The US currently possesses a nuclear weapon capability. Using the capability in the current wars in Afghanistan and Iraq would provide a decisive capability, but the risk to international standing and huge loss of life is not worth the risk. Therefore, the risk criterion provides a counter-weight to the criterion of value. If the US is missing an opportunity then the value must be worth the risk.

The Merriam-Webster dictionary defines risk as the "possibility of loss or injury."[29] In the context of this research a great capability may exist, but is it worth the risk? Like the nuclear weapons analogy discussed above, a capability like nuclear weapons are still valuable, but the deployment or use of nuclear weapons and its risk is mitigated. US President Truman's statement about the risk of nuclear weapons follows:

> I don't think we ought to use this thing unless we absolutely have to. It is a terrible thing to order the use of something that is so terribly destructive beyond anything we have ever had. You have got to understand this isn't a military weapon. It is used to wipe out women, children and unarmed people, and not for military use. So we have to treat this differently from rifles and cannon and ordinary things like that.[30]

One method of risk analysis is found in Air Force Instruction 90-901. The instruction states, "potential benefits should be compared to all potential costs. The process of weighing risks against opportunities and benefits helps to maximize unit capability. Even high risk endeavors may be undertaken when there is a well founded basis to believe that the sum of the benefits exceeds the sum of the costs."[31]

The focus of this study is whether there is value in engaging online communities or not. The "value" criterion is selected as a factor because there is no use incorporating additional resources to a task that provides no value. Value in this study is associated with its ability to improve information operations. Information operations are the umbrella military missions in cyberspace fall under.[32] If there is an alternate to the current US strategy in cyberspace the alternative would likely meet one of the information operations mission areas. According to JP 3-13, information operations have eleven capabilities. In order for the alternate to have value it must meet at least one of the capabilities listed and defined below. These capabilities are:

> 1. Destroy: To damage a system or entity so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt.
> 2. Disrupt: To break or interrupt the flow of information.

3. Degrade: To reduce the effectiveness or efficiency of adversary C2 or communications systems, and information collection efforts or means. IO can also degrade the morale of a unit, reduce the target's worth or value, or reduce the quality of adversary decisions and actions.
4. Deny: To prevent the adversary from accessing and using critical information, systems, and services.
5. Deceive: To cause a person to believe what is not true. MILDEC seeks to mislead adversary decision makers by manipulating their perception of reality.
6. Exploit: To gain access to adversary C2 systems to collect information or to plant false or misleading information.
7. Influence: To cause others to behave in a manner favorable to US forces.
8. Protect: To take action to guard against espionage or capture of sensitive equipment and information.
9. Detect: To discover or discern the existence, presence, or fact of an intrusion into information systems.
10. Restore: To bring information and information systems back to their original state.
11. Respond: To react quickly to an adversary's or others' IO attack or intrusion.[33]

ALTERNATIVE SOLUTION

The alternate to the current US military strategy (CNA, CND, and CNE) is a people or social centric solution. People socialize in communities outside of cyberspace and inside of cyberspace. Cyber communities interact and develop like-minded ideas based on influences. Skoudis, states, "some blogs have become quite popular and have helped shape political debates and news stories."[34] If the US military is not engaged in some effort to understand or affect their beliefs then the group as a whole stands to be influenced by others. The US Counterinsurgency Guide provides another weakness in not engaging communities. "Influence activities (actions and messages) can be proactive or reactive. Being proactive gives a significant influence advantage, since the first impression or report of an event that reaches a population will often receive the widest exposure and will subsequently be most resistant to alternative accounts."[35] Thus, if the DoD is not engaging then hackers, hacktivists, and other online groups and cyber

communities are left to be influenced by others. The other options are to either engage after an impression is established as discussed above or not to engage at all. If the influence of social communities is important then at least an understanding or capability to effectively respond should be available.

Terrorist groups such as Al Qaeda incorporate cyberspace operations into their overall strategy. While Al Qaeda engages in devastating human and material destruction in one part of the world their power is generated through its ability to reach the minds of global populations. Cori Dauber states, terrorists "fight a battle to shape the perceptions and attitudes of the public—a battle over the public's very will to continue fighting, whether that is the indigenous public insurgents seek[ing] to intimidate or the domestic American public they seek to influence so as to force counterinsurgents to withdraw from the battlefield prematurely. And in the modern world, this will, of necessity, be a battle to shape media coverage."[36] Cyberspace provides a medium for terrorists to post messages and videos to recruit as well as terrorize the global population. Al Qaeda posts videos of attacks, makes claims against the US and allies that technology based solutions cannot address. The US may be able to defend and attack using current CNO in a technical matter, but the battle is more in the minds of people. An example is terrorists posting videos showing deadly attack against US forces or claims of US fratricide. It is documented that world news media broadcasts these videos to global populations with the message the terrorists provide. Dauber states,

> Terrorists (and, again, insurgents using terrorist methods) no longer depend upon the professional media to communicate with their own constituents and no longer depend upon the professional media to communicate with the outside world. (In fact, to an unprecedented degree, the professional media have become dependent upon *them*.) Technological developments permit any terrorist cell to film, edit, and upload their actions virtually in real time whether Western media are there to serve witness or not.[37]

Meanwhile, the US military does not have a bomb, network attack, or some other method to quickly react or proactively pursue. The US's strategy in cyberspace is technology based CNO.

The US could use online social means by reacting to the video/message with a response so as to limit or stop the negative influence. The lack of US engagement to the videos and web posts combined with the global reach of propaganda can have dramatic effect. Dauber states,

> New information and communication technologies are being used to great synergistic effect by the enemy: the military has to understand how this works and be prepared to make use of such technologies to counter enemy messaging to the extent possible, as quickly as possible. This cannot, by definition, be left to the PAO [Public Affairs Officer] community, but must be understood by, and participated in, the entire military to have a chance at success.[38]

While Dauber supports a military role in engagement there is also an argument against use of military forces engaging people in cyberspace.

An argument against engaging and influencing cyber communities is the difficulty, resources, and potential that engagement could be seen as meddling or worse an act of aggression and subversion to the group. According to Kramer and Wentz, "the first shortcoming is that the necessary expertise does not exist in sufficient capacity or at high enough levels in either the State Department or DoD."[39] "The second shortcoming is that we do not make good use of the capacities we do have. In a wartime situation, the military undertakes to do the best it can in terms of influence operations."[40] Another example provided by Kramer and Wentz is "the assumption is that, in a war, the impact of combat generally will overwhelm the use of words."[41] Another important aspect according to Kramer and Wentz is that, "information campaigns cannot rely simply on 'increasing the flow' to spread the information effectively."[42] Resources, situational characteristics, and the strategy of simply spreading information may hamper an attempt to influence communities in cyberspace. But, this does not mean the US military should not engage.

RESULTS OF COMPARISON

This study looks at whether the US military is missing an opportunity by not engaging communities in cyberspace. The first criterion for comparison is whether engaging cyber communities provides any value. The values are based on IO capabilities listed in Joint Publication 3-13. The following table below displays the results from analyzing whether engaging cyber communities can perform any IO capabilities.

Table 1: Engaging Cyber Communities vs. Value

Value (IO Capability, JP 3-13)	Criteria Met (Yes/No)	Rationale:
Destroy	No	Engaging cyber communities cannot directly damage hardware.
Disrupt	No	Engaging cyber communities cannot directly interrupt information flow.
Degrade	**Yes**	**Engaging cyber communities has the possibility to degrade the morale of a unit or reduce the quality of adversary decisions and actions.**
Deny	No	Engaging cyber communities cannot directly deny or prevent the adversary from accessing critical information.
Deceive	**Yes**	**Engaging cyber communities can deceive a person to believe what is not true.**
Exploit	**Yes**	**Engaging cyber communities has the possibility of gaining access to adversary C2 systems to collect information or to plant false or misleading information.**
Influence	**Yes**	**Engaging cyber communities has the possibility of causing others to behave in a manner favorable to US forces.**
Protect	No	Engaging cyber communities cannot directly guard against espionage or capture of sensitive equipment and information.
Detect	No	Engaging cyber communities cannot directly discover or discern the existence, presence, or fact of an intrusion into information systems.
Restore	No	Engaging cyber communities cannot bring information and information systems back to their original state.
Respond	**Yes**	**Engaging cyber communities has the ability to react quickly to an adversary's or others' IO attack or intrusion.**

The results indicate engaging cyber communities satisfy 5 of the 11 areas of value. The areas of value met are degrade, deceive, exploit, influence, and respond. Engaging cyber

communities satisfies the degrade capability because it has the ability to lower or effect the morale of adversaries. An example is a message or video sent to adversaries showing their failures or other negative aspects of their actions. The deceive capability is possible by sending information to an adversary or releasing information in a way that deceives others into thinking the opposite is true. The third IO capability satisfied is exploit. The exploit capability can be achieved by engaging cyber communities through gaining access to adversary C2 systems, to collect information, or to plant false or misleading information. This can be accomplished through social engineering or other methods to get information from system users. The fourth capability met is influence. The influence capability is achieved through causing others to behave in a manor favorable to the US military. Messages and videos can provide influence to online communities manipulating their thoughts and actions. The fifth and final IO capability satisfied is respond. Engaging cyber communities provides a method of responding to events or countering information negative toward the US.

The next step in this study is risk analysis. The risk analysis compares IO capabilities associated with engaging cyber communities with the risk involved in executing. The first step is to determine the risk for each capability. The next step assesses whether the risk can be mitigated. The overall assessment as well the rationale behind mitigating the risks can be seen in Table 2.

Table 2: Engaging Cyber Communities Risk Analysis

Value (IO Capability, JP 3-13)	Capability Description	Risk	Mitigate (Yes/No)	Rationale
Degrade	Engaging cyber communities has the possibility to degrade the morale of a unit or reduce the quality of adversary decisions and actions.	Political fallout from being caught and counter-reaction of perceived US meddling.	Yes	Mitigation in a domain with the global reach of cyberspace will have to be very controlled to not expand beyond its intent. Military operations already include PSYOPS and pursuits of PSYOPS in cyberspace and are assumed no different than in any other medium.
Deceive	Engaging cyber communities can deceive a person to believe what is not true.	Loosing Foreign and/or Domestic Trust in Military.	Yes	Mitigation in a domain with the global reach of cyberspace will have to be very controlled to not expand beyond its intent. Will also have to guard against breaking US laws by accidentally deceiving domestic audiences.
Exploit	Engaging cyber communities has the possibility of gaining access to adversary C2 systems to collect information or to plant false or misleading information.	Political fallout from being caught.	Yes	Intelligence collection and deception operations are already performed in military operations and it is assumed no different than in any other medium.
Influence	Engaging cyber communities has the possibility of causing others to behave in a manner favorable to US forces.	Counter-reaction of perceived US meddling.	Yes	Mitigation in a domain with the global reach of cyberspace will have to be very controlled to not expand beyond its intent. Will also have to guard against breaking US laws by accidentally influencing domestic audiences.
Respond	Engaging cyber communities has the ability to react quickly to an adversary's or others' IO attack or intrusion.	Disjointed US response or wrong response w/strategic implications.	Yes	Develop rules of engagement (ROE) similar to ROEs typical in military operations on what can be said and steps to quickly elevate a response with global/strategic implications.

The overall results suggest all five capabilities have risks and all can be mitigated. The reality is most risks in any situation can be mitigated and this analysis provides information on the risk as well as possibilities of mitigation. Nonetheless, the actual implementation of each social engagement in cyberspace will ultimately fall back on the implementers. The results from

this risk analysis indicate the "degrade" factor can be mitigated. It is assumed that the risk posed by degrading morale through PSYOPS is the same in all mediums and can be mitigated. Mitigating the "deceive" capability through false or misleading information is assumed to have similar risks in all mediums and can be mitigated through controlled and targeted actions. A fundamental assumption is deception operations in cyberspace are not too different from any other medium and since the military already performs these operations mitigation can be achieved. The "exploit" capability is based on intelligence operations and is assumed to take the same secretive or clandestine nature to mitigate the risks involved. Intelligence gathering in an open source medium such as the Internet is characterized as low risk as there are no breaches in sovereignty or broken foreign laws. The "influence" capability appears unique in cyberspace because of its pervasive reach to influence beyond an intended audience. An attempt to influence in one particular area of the world may have an influential affect somewhere else in a negative or positive way. Additionally, US laws dictate active military units are not allowed to perform operations on the US domestic population.[43] Therefore, influence operations should be structured and controlled to limit influence to un-intended audiences and the US population. The structure and control of these operations is the mitigating method. The "respond" capability runs the risk of sending a disjointed message not synchronous with an official US stance or a message that causes un-intended impacts. The disjointed message can be mitigated through developed rules of engagement (ROE) directing steps and actions to take given a certain situation. The un-intended impacts of an errant or poorly drafted message can follow a similar method of control and include methods to quickly elevate to an appropriated level of authority for direction.

CONCLUSION

The dramatic growth in the number of Internet users around the world and social websites is enabling people to form online communities in cyberspace.[44] These social groups are having an influence on international relations through organizing and pursuing political ends.[45] However, the US military is attacking cyber threats through technological ways of CNA and CND.[46] History has shown technology-centric solutions can fail when social or human aspects are not engaged as seen in the Vietnam War and OIF.[47][48] The results of this study suggest engaging online communities can augment the technology-centric solutions. Engaging online communities can help to degrade, deceive, and exploit adversaries operations in cyberspace. Engaging online communities can also influence and help respond to social groups' issues and concerns. Without responding or influencing these groups they are left to their own vagaries as well as negative and adversarial influence. There are risks associated with engaging online communities due to the ubiquitous reach of cyberspace. An ill-conceived comment, text, or video can be sent globally and have a negative impact to objectives and reputation. However, this study finds applying controls and rules of engagement in undertaking these operations can mitigate the risks. Thus, the US military needs to develop these capabilities and engage online communities in cyberspace. Not engaging cyber communities will ensure influence from other sources, which could ultimately create an un-checked sanctuary for anti-US propaganda and coordinated attack of all forms against the US and its interests.

RECOMMENDATIONS

The US military should improve its efforts in computer network operations by engaging online communities. The US should particularly focus on a two-way engagement capability with influential online groups. According to Wentz and Kramer, "the downside of mass messages is that they are in transmission mode…virtually no communication is received without the audience being involved in creating meanings. Moreover, the meanings created will importantly reflect the target's cultures. Thus, the issue that arises for the United States is what is often described as *segmentation*, dividing the mass audience to focus on specific receiver needs. Creating segmentation in a real world of multiple, overlapping audiences is a difficult, though not impossible, proposition."[49] It is hard to believe every one-way transmission will always be received correctly for every individual receiving the message. Thus, two-way exchange on the message provides an avenue to not only address any clarification or misunderstanding, but also receive feedback on the affects in the community. The two-way exchange provides the hope to obtain situational awareness or influence or gain subsequent information to affect online communities.

The US military should also take a page out of Al Qaeda's book of media and become a source of videos and messages. The US has a tremendous amount of intelligence platforms that produce a tremendous amount of video. These videos could be used to attract media and adversaries as well as populations to see ground truth. The videos do not have to be real-time but post-mission with the intent of sending a message and informing. The objective is to pro-actively present the information by having audiences come to you versus react to the negative information posted by others. A web-site centralizing these operations may provide a place

where people within the target audience will know and respond in either a public or private manner. This places the US military in a position to proactively engage and keep abreast of online communities and their issues.

These recommendations may appear aggressive in nature, but these kinds of operations are already being performed by adversaries. The US must be better organized and able to act quicker and engage to win in the realm of cyberspace. The US already performs operations in the technical realm of cyberspace through computer network operations. The US military should now engage in the social side and update joint doctrine for guidance.

Future research should pursue a better understanding of how the US should engage online communities and the advantages and disadvantages of doing such operations. The risk of engaging online communities should be further developed. The challenges engaging cyber communities through degrade, deceive, exploit, influence, and respond may have unique risks not fully explored nor understood in the realm of cyberspace.

ENDNOTES

[1] Miniwatts Marketing Group, *World Internet Usage and Populations Stats*, http://www.internetworldstats.com/stats.htm.
[2] Lui Hebron and John F. Stack, Jr., *Globalization: Debunking the Myths*, 61.
[3] US Department of Defense, *Information Operations*, JP 3-13, II-4 to II-5.
[4] Miniwatts Marketing Group, *World Internet Usage and Populations Stats*, http://www.internetworldstats.com/stats.htm.
[5] Lui Hebron and John F. Stack, Jr., *Globalization: Debunking the Myths*, 61.
[6] Washington Times, *Iran's Twitter Revolution.*
[7] Martin Libicki, *Conquest in Cyberspace*, 46.
[8] US Department of Defense, *Information Operations*, JP 3-13, II-4 to II-5.
[9] Dr. Franklin Kramer and Mr. Larry Wentz, *Cyber Power and National Security, 351.*
[10] Ibid, *351.*
[11] Barry Watts, *Doctrine, Technology, and War*
[12] US Government Accountability Office, *Securing, Stabilizing, and Rebuilding Iraq*, 21.
[13] Gregory Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security*, Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, 273.
[14] Edward Skoudis, "Evolutionary Trends in Cyberspace ," in *Cyberpower and National Security*, Kramer, Franklin D., Stuart H. Starr and Larry K. Wentz, 168.
[15] Ibid, 169.
[16] Ibid, 169.
[17] Dorothy Denning, Activism, "Hakctivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in *Networks and Netwars: The Future of Terror, Crime, and Militancy,*.John Arquilla and David Ronfeldt, 241.
[18] Ibid, 241.
[19] Ibid, 240.
[20] US Department of Defense, *Information Operations*, JP 3-13, II-4 to II-5.
[21] Ibid, B-3.
[22] Ibid, B-3.
[23]Franklin Kramer and Larry Wentz, *Cyber Power and National Security, 361.*
[24] Tami Biddle, *Rhetoric and Reality in Air Warfare*, 299
[25] Nigel Aylwin-Foster, "Changing the Army for Counterinsurgency Operations," in *Military Review*, November-December 2005 Issue, 6
[26] Gregory Rattray"An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security*, Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, 268-269.
[27] Ibid, 254.
[28] Http://www.merriam-webster.com/dictionary/value
[29] Http://www.merriam-webster.com/dictionary/risk
[30] Lillienthal, *The Atomic Energy Years*, 391
[31] US Air Force, AFI 90-901, 2.
[32] US Department of Defense, *Information Operations*, JP 3-13, I-1
[33] US Department of Defense, *Information Operations*, JP 3-13, I-9to I-10.

[34] Edward Skoudis, *Cyberpower and National Security*, 168.
[35] US Government, *U.S. Government Counterinsurgency Guide*, 21.
[36] Cori Dauber, *Youtube War: Fighting in a World of Cameras Within Every Cell Phone and Photoshop on Every Computer*, 2.
[37] Ibid, 5
[38] Ibid, 92
[39] Dr. Franklin Kramer and Mr. Larry Wentz, *Cyber Power and National Security, 359.*
[40] Ibid, *359.*
[41] Ibid, *355.*
[42] Ibid, *354.*
[43] United States of America, *The Posse Comitatus Act*, 18 US Code, Section 1385.
[44] Lui Hebron and John F. Stack, Jr., *Globalization: Debunking the Myths*, 61.
[45] Washington Times, *Iran's Twitter Revolution*
[46] US Department of Defense, *Information Operations*, JP 3-13, II-4 to II-5.
[47] Barry Watts, *Doctrine, Technology, and War*
[48] Dr. Franklin Kramer and Mr. Larry Wentz, *Cyber Power and National Security, 351*
[49] Ibid, *351.*

BIBLIOGRAPHY

Aylwin-Foster, Brigadier Nigel. "Changing the Army for Counterinsurgency Operations." *Military Review* (November-December 2005): 2-15.

Arquilla John and Ronfeldt David, *Networks and Netwars,* RAND: National Defense Research Institute, 2001

Biddle, Tami Davis. *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945.* Princeton, NJ: Princeton University, Press, 2002.

Dauber, Cori E. *You Tube War: Fighting in a World of Cameras in Every Cell Phone and Photoshop on Every Computer*, Strategic Studies Institute, 16 November, 2009. http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=951

Hebron, Lui, and John F. Stack, Jr. *Globalization: Debunking the Myths.* Upper Saddle River, NJ: Pearson-Prentice Hall, 2009.

Herbert H. Hyman and Paul B. Sheatsley, *Some Reasons Why Information Campaigns Fail*, The public Opinion Quarterly 11, no 3 (Autumn 1947), 412-423

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. *Cyberpower and National Security*, Potomac Books, Inc., Washington, DC, 2009.

Libicki, Martin A., *National Security and Information Warfare*. Cambridge University Press, New York, NY, 2007

Lillienthal, David, *The Journals of David E. Lillienthal,* vol. II, *The Atomic Energy Years 1945-1950*, New York. Harper and Row, 1964,

Merriam Webster, Inc. *Merriam Webster Online Dictionary*, 1 April, 2019. http://www.merriam-webster.com.

Miniwatts Marketing Group. *World Internet Usage and Populations Stats*, 7 December, 2009. http://www.internetworldstats.com/stats.htm.

United States Air Force, *Operational Risk Assessment*, Air Force Instruction 90-901, Washington, DC. 1 April, 2000.

United States of America, *The Posse Comitatus Act*, 18 US Code, Section 1385, June 1878.

US Department of Defense, *Information Operations*, Joint Publication 3-13, Washington, DC. 13 Feb, 2006.

US General Accounting Office. *Securing, Stabilizing, and Rebuilding Iraq.* US GAO Report GAO-08-837, Washington, DC. June 2008.

US Government. *US Government Counterinsurgency Guide*. Washington, DC. January 2009.

Washington Times. *Editorial: Iran's Twitter Revolution.* Washington Times, 16 June, 2009. http://www.washingtontimes.com/news/2009/jun/16/irans-twitter-revolution/

Watts, Barry D. *Doctrine, Technology, and War*, Air and Space Power Journal, 30 April-1 May, 1996. http://www.airpower.au.af.mil/airchronicles/cc/watts.html