REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
30-04-2018	Master's of Military Studies	SEP 2017 - APR 2018

4. TITLE AND SUBTITLE
Unconventional Thinking: How the Cyberwarfare Domain Needs an Unconventional Force

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Bell, Charles F. III, Lieutenant Commander, USN

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)
Dr. Eric Shibuya

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

President Trump recently directed that CYBERCOM be elevated to the status of unified combatant command, no longer subordinate to U.S. Strategic Command. To date, operations in the cyber domain have been approached conventionally by the Department of Defense. Conventional and unconventional techniques must be used in the newest domain. The approach to building an unconventional force should exemplify techniques developed in other domains such as land, air, and sea and incorporate certain aspects of military source operations. The unconventional force could use techniques prescribed by Saul Alinsky in "Rules for Radicals" to develop communities to protect U.S. systems and carry out attacks on enemy state and non-state actors.

15. SUBJECT TERMS

Unconventional Warfare; Cyberwarfare Domain; Saul Alinsky; Cadre; U.S. Cyber Command; CYBERCOM; Intelligence; Human Intelligence

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
					19b. TELEPHONE NUMBER *(Include area code)*
Unclass	Unclass	Unclass	UU	42	(703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTERS OF MILITARY STUDIES

TITLE: Unconventional Thinking: How the Cyberwarfare Domain Needs an Unconventional Force

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR: LIEUTENANT COMMANDER CHARLES F. BELL, III, USN

AY 17-18

Mentor and Oral Defense Committee Member: Eric Y. Shibuya, PhD
Approved: [signature]
Date: 1 May 2018

Oral Defense Committee Member: Francis H. Marlo
Approved: [signature]
Date: 1 May 2018

Introduction

"The challenges [in cyberspace] are so broad...it is going to take a true partnership between the private sector, the government, and academia to address [them]."
- ADM Michael S. Rogers, Commander, U.S. Cyber Command and NSA Director

Recognizing that United States cyber networks must be guarded against state and non-state entities in 2009, United States Cyber Command (CYBERCOM) was formed as a sub-unified command under U.S. Strategic Command.[1] Headquartered at Fort George G. Meade, MD and collocated with the National Security Agency (NSA), NSA and CYBERCOM are currently headed by the Director of the NSA, ADM Michael Rogers. CYBERCOM's mission is to "plan, coordinate, integrate, synchronize and conduct activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."[2] Creation of CYBERCOM acknowledges that there is a new domain to warfighting. The joint force must be able to fill the ranks of the military with warriors who can fight, win, protect, and dominate in cyber using a Range of Military Options (ROMO).

President Trump recently directed that CYBERCOM be elevated to the status of unified combatant command, no longer subordinate to U.S. Strategic Command. In his August 2017 statement, President Trump said, "The elevation of United States Cyber Command demonstrates our increased resolve against cyberspace threats and will help reassure our allies and partners and deter our adversaries."[3] Increased resolve requires professionals who are capable of winning the online domain. In addition to what is already occurring to man, train, and equip the cyber force, DoD and CYBERCOM should take a holistic approach to use every lever to its advantage. Most Importantly, CYBERCOM should build a relatively small cadre of Unconventional Warfare

(UW) professionals modeled after US Special Operations Command (SOCOM), but residing in and belonging to CYBERCOM, to create an online movement that protects U.S. systems, infiltrates subversive groups, and thwarts attacks. This small cadre should also be prepared to conduct a wide range of UW tactics in the cyber domain.

This paper will discuss a brief history of UW in the United States, and how there is a precedent already for UW in the other warfighting domains. The paper will then discuss current approaches to fighting in the cyber domain, and will then transition to how and why building a small cadre of cyber-professionals acts as a force multiplier. The paper will discuss how these warriors should use UW, community organizing and Human Intelligence (HUMINT) recruiting tactics to organize online communities to build a force capable of UW military options. Finally, it will conclude with implications for the future of this emerging warfighting domain. While not comprehensive in tactics techniques and procedures due to classification and space restrictions, the paper will hopefully spur unconventional thinking for this unconventional domain.

Unconventional Warfare History

The history of unconventional warfare (UW) in the United States is long and storied. During the French and Indian War, Cherokee Indians inspired the likes of Francis "Swamp Fox" Marion to use the land to their advantage to thwart the British, "they concealed themselves in the Carolina backwoods and mounted devastating ambushes. Two decades later, Marion would apply these tactics against the British [during the American Revolution]."[4] In World War II, General William "Wild Bill" Donovan formed the Office of Strategic Studies (OSS), which originally formed as an intelligence fusion outfit for the President, and quickly morphed into a UW mechanism of the U.S. government. Using men recruited out of the Ivy League particularly sports players, "Donovan likewise believed in the brilliant amateur, the Ivy League athlete who,

without a great deal of preparation, could become a secret agent or commando dropped behind enemy lines."[5]

General Marion only had to fight in one domain, Land. Likewise, General Donovan had to consider three domains: land, air, and sea. Today's warrior must consider five domains: land, air, sea, space and cyber. Unlike land, air, sea, and space where fighting is primarily in the physical realm, fighting within the cyber domain is complicated by the physical, cognitive, and digital realms. UW tactics can be utilized to achieve great effects in the protection of U.S. networks, and the disruption of enemy capacity to attack U.S. interests. According to Joint Publication 3-05, "UW operations are a national strategic option, which uses fewer resources than conventional operations, while still mitigating an adversary's typical anti-access capabilities. UW operations' objectives include supporting the insurgency/resistance movement so that it can influence, coerce, disrupt, or foster a change in governing authority."[6] First, a look at UW phases employed by the United States today.

Fighting in the Cyber Domain

Traditional warfighting strategy and tactics are currently employed by the DoD in the cyber-warfare domain. For example, according to *Joint Publication 3-12 Cyberspace Operations* (JP 3-12), the definition of Fires is, "Depending on the objective, cyberspace fires can be offensive or defensive, supporting or supported. Like all forms of power projection, fires in and through cyberspace should be included in the joint planning and execution processes from inception in order to facilitate synchronization and unity of effort."[7] As this method of warfare evolves, exclusively using traditional methods in a non-traditional domain will not work in all situations. Instead, a holistic approach should be used. The US is engaging in a war with state and non-state adversaries to keep US networks safe and rendering competitor nations and

adversaries impotent. Some situations call for traditional targeting, fires, and battle damage assessments; other situations require unconventional measures. The DoD should approach cyber-warfare from a comprehensive, holistic approach, which includes employing UW tactics online. It should also consider employing community organizing strategies such as those laid out by Saul Alinsky in his *Rules for Radicals*, and bring to bear skills already available to act as a force multiplier and achieve online success.

Cyber operations can be broken down into two essential categories: Offensive and Defensive. Offensive Cyber Operations (OCO) are "intended to project power by the application of force in and through cyberspace. OCO will be authorized like offensive operations in the physical domains, via an execute order"[8] Defensive Cyber Operations are "intended to defend DOD or other friendly cyberspace [domains]. Specifically, they are passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems."[9] Both categories require highly trained professionals. Both disciplines require years of training and experience. Currently, they have to be able to get a clearance before they can be allowed to access and defend their industry or country's most sensitive networks.

In December 2017, President Trump released the *2017 National Security Strategy*, and it states, "We face simultaneous threats from different actors across multiple arenas—all accelerated by technology. The United States must develop new concepts and capabilities to protect our homeland, advance our prosperity, and preserve peace."[10] The defensive side must be attuned to all threats continually bombarding their networks, and those threats rapidly evolve. These disciplines require the defensive cyber-professional to remain on the cutting edge of both

hardware and software and to train and collaborate with their community. They must be able to preempt an attack or react swiftly should penetration of the networks occur and shut it down.

The offensive cyber-professional must be one step better than the enemy's best defensive measures. They have to know how to write code to exploit the limitations of the networks and systems they are trying to attack. They must know how to thwart defensive measures designed to keep them out. They must be able to work independently, but also in teams to take down a network or to perform espionage to gain an advantage. The offensive cyber professional requires extensive training and hands-on experience and a protected sandbox in the cyber realm with which to test new and novel techniques to be used against an adversary.

Unconventional Warfare in the Cyber Domain

Offensive cyber operations by DoD must operate under "statutory authorities that apply to DoD include Title 10, United States Code (USC), Armed Forces; Title 50, USC, War and National Defense; and Title 32, USC, National Guard."[11] Authorities to act in the cyber domain reside with the Secretary of Defense. Titles 10 and 50 encompass DoD and will be used to accomplish the missions, but according to JP 3-12, lawful military operations illustrates how the U.S. top-down approach to operating in the cyber environment needs further discussion, "Military attacks will be directed only at military targets. Only a military target is a lawful object of direct attack. By their nature, location, purpose, or use, military targets are those objects whose total or partial destruction, capture, or neutralization offers a direct and concrete military advantage."[12] However, in the cyber-domain defining "military" targets are not always possible. Further discussion and policy decisions are needed to strike a balance between effectiveness and oversight to ensure there is no overreach. All of these discussions should be included in the hybrid approach to operating in the cyber environment.

The solutions in the discussion above are predicated on the DoD and its military services thinking conventionally to answer an unconventional problem. The holistic approach which includes conventional and unconventional tactics to man, train, and equip the force will serve the needs of the DoD better. Cybersecurity and attack in the age of the internet of things will grow. The military's dependence on networks and networked systems will grow. Dependence on systems, handling threats, and providing "offensive effects" in a nascent domain will produce a revolution in military affairs where the United States must act to maintain a decisive advantage. Conventional thinking to address the challenges faced by the US will not work in this domain. The Deep Net is essentially all of the rest of the internet that conventional search engines such as Google and Yahoo cannot reach due to the sheer volume of information and websites. The Dark Net uses Tor networks which are, "A collection of secret websites (ending in .onion) that require special software to access them. People use Tor so that their Web activity cannot be traced -- it runs on a relay system that bounces signals among different Tor-enabled computers around the world,"[13] where hackers write and publish their code, plot their next 'attack,' and share in the glory of their latest takedown. It is also where weapons proliferators ply their trade and circumvent traditional means of tracking.[14] UW in traditional warfighting domains is accomplished in eight phases, and some of these phases can occur simultaneously and the cyber domain is no exception.

Phases

According to U.S. public law, UW is defined as "activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area."[15] A denied area is "an area that is operationally unsuitable for conventional forces due to

political, tactical, environmental, or geographical reasons. It is a primary area for special operations forces."[16] While the scope of this discussion is not necessarily to overthrow foreign governments using resistance movements online, specific techniques within UW doctrine can be used to form and build a network of operatives who can conduct operations to deny enemies both governmental and non-governmental, the ability to operate and attack U.S. systems. There are eight phases of UW: Phase 0 – Steady State, Phase I – Preparation, Phase II – Initial Contact, Phase III – Infiltration, Phase IV – Organization, Phase V – Buildup, Phase VI – Employment, and Phase VII – Transition.

This paper will focus on Phase 1 and Phase IV because the online cadre built by DoD will initially operate in these phases to build their networks. The question is whether to build a small cadre of officers and enlisted within the DoD that run relatively small, tightly controlled online networks, or for the cadre to build larger more extended networks that turn into movements to affect political change. Both can be true depending on the goals of the program. The difference in which network to build, large or small controlled by the small cadre, depends on the outcomes desired. There are parallels to how the U.S. Army conducts Human Intelligence (HUMINT) and source handling operations which are discussed later in this paper.

According to Army Field Manual 3-05, "The preparation phase for unconventional warfare begins with the approval of the President and Secretary of Defense to execute an unconventional warfare campaign. The primary purpose of this phase is to ensure that the insurgency, resistance, and the population are "prepared" to conduct and support an unconventional warfare campaign."[17] During Phase 1, UW forces prepare the environment to form a resistance. In this state, the online cadre will mainly perform day-to-day operations to include: spotting and assessing of assets to include online communities, placement and access of

potential targets and/or assets, threat analysis enabled by the intelligence community, operational environment requirements to include activities to legitimize the narrative to support U.S. Interests and Potential resistance movements, setting the conditions to, once approved, executing the planned campaign or activity.[18]

Phase IV is defined as the organization phase.[19] In this phase, the online cadre will begin to coagulate the resistance or insurgency by:

> Link[ing] up with resistance leadership, their objective is to determine and agree upon a plan to organize the resistance for expanded operations. In addition to physical preparations, this entails a confirmation of mutual objectives and prior agreements. This requires a period of rapport-building to develop trust and confidence, as well as a period of discussion of expectations from both sides.[20]

These objectives can be accomplished by activating certain cells online that have been assembled by the cadre in the various communities that have been cultivated to achieve the desired effects. It will be imperative that the cadre will: develop campaign plans, establish operational and intel infrastructure, and enhance force protection and counterintelligence capabilities. It will be up to the cadre to determine the strength of his or her network that has been developed and whether that network can achieve its goals because "Unconventional warfare requires centralized direction and decentralized execution under conditions that place great demands on the resistance organization and its leadership."[21] Furthermore, some communities that have taken months or years to be refined by the cadre may, by their nature, should be considered "one-time use," and this must be carefully considered before employment or activation.

Cyber-HUMINT operations

In Phase 0, during the steady state, and before active offensive UW operations are initiated, the cadre must build a network amongst the online communities that will benefit fu;ture operations. These networks of potential sources will inherently be humans, and therefore HUMINT collection and source handling techniques must be utilized. The UW cadre will be using HUMINT techniques for recruitment to carry out online UW activities, intelligence gathering, and spotting and assessing operations. Source handling operations in the cyber realm should mirror those in the physical realm and in accordance with Army Field Manual 2-22.3. Cyber HUMINT and network building should enable "Cross-cue from an almost endless variety of potential sources including friendly forces, civilians, detainees, and source-related documents."[22]

In the model proposed, CYBERCOM will need to develop a new J-code, similar to a J2X, to handle the coordination efforts of online activities including offensive, defensive, and intelligence activities. For this paper, it will be called J2Z. The J2Z will be responsible for source and cadre deconfliction, source validation, targeting packages, and operating areas. Cyber HUMINT and UW activities will necessarily overlap, and authorities will need to be written to allow the cyber cadre to operate with a certain amount of freedom to achieve the desired effects of the campaign. Conducting HUMINT support to cyber operations must be guided by "…to minimize the time between when friendly forces encounter potential sources (detainees, refugees, and local civilians) and when a HUMINT collector screens them."[23] Currently, authorities exist to conduct UW and HUMINT operations in the physical domains, and they are more nebulous when operating in the cyber domain. The campaigns proposed by the cadre will need to be limited in scope to ensure that cases of overreach can be reined in and controlled.

Each cadre member should spot and assess potential sources using all of the means available to HUMINT collectors that exist in the physical world. Once a network has been vetted and approved, techniques articulated by Saul Alinsky, which are discussed later, should be used to coalesce the community around a cause should be used. Spotting and assessing potential targets and sources will accomplish two objectives for the cadre in the future. First, the pool of potential talent to draw from in the future will be identified and growing ever larger. Second, one-time sources will be more accessible when they realize they are not being targeted for collection, prosecution, or removal.

Using Organizing Techniques Online

The virtual forums all over the Internet are primarily communities. These communities congregate according to their interests and attract hackers and potential hackers from all over the world. These communities are unregulated, but the US Government also underutilizes them due to their sensitive and often illegal nature. If the US is trying to grow their cyber offensive and defensive ranks, and the unprecedented nature of cyber offense and defense requires unconventional thinking, then it is time to think of an alternative plan that does not require directly hiring individuals into the service. Instead, the DoD should build a relatively small cadre of "online community organizers" to explore building an online movement and harness the power of the many offensive and defensive cyber personnel who may not be able, or even want, to meet the requirements laid out by the DoD.

Saul Alinsky "founded what is known today as the Alinsky ideology and Alinsky concepts of mass organization."[24] This ideology promotes the concepts of Information Operations, enthusiastic leaders, and fighting for a cause that appeals to the broadest swath of individuals within a community. Within the cyber domain is a robust collection of communities

that the US should organize and use for its ends to counter rival state and non-state actors aiming to foment cyber terror and attacks on US DoD, infrastructure, and industry.

Alinsky believed the ends justify the means and states, "Life and how you live it is the story of means and ends."[25] He later wrote, "He [the man of action] asks of ends only whether they are achievable and worth the cost; of means, only whether they will work."[26] This view of the world, though cynical, is very true in the online community. Tactics used to attempt to sway elections, introduce ransomware such as the WannaCry virus, or online espionage are all utilized by foreign countries to influence the US and Western Democracies for strategic political gains of state and non-state actors.[27] To throw the lone superpower into political chaos creates propaganda wins and substantial strategic advantages for the regimes in those countries. According to the National Security Strategy, " Over the years, rivals have used sophisticated means to weaken our businesses and our economy as facets of cyber-enabled economic warfare and other malicious activities."[28] It allows time and space for maneuvers in the physical and cyber domain while the US is distracted by infighting and finger-pointing.

The power of organizing online communities to work on behalf of the United States is in that these communities can do things like stop ransomware attacks as happened in 2017 with the WannaCry attack. During this attack, WannaCry ransomware was spreading all over the globe and shutting down commerce, industry, infrastructure, and more. One 22-year-old IT professional recognized what was happening and shut it down out of his sense of morality, but had this person been working in a community organized and curated by a DoD organizer; perhaps he/she could have recognized it and gotten the word out to his community and shut it down even sooner. The self-taught individual "took just a few hours to stop the breach…He is believed to have stopped the attack from a small bedroom in his parents' house."[29] This

individual is not unique in the online world. He/she is self-taught, young, attends hacker conferences, and probably does not want to join the military. By having military UW cadre "organizers" aggregating witting or unwitting actors into like-minded online communities, the US will have force multipliers throughout the online community.

How to Organize

Every individual has an issue or series of issues that are central to who they are. Community organizing in the virtual world is no different online than it is in the physical world. The online organizer must find the critical issue that the people he/she is trying to organize care most about and relate to them on their level. Alinsky says "The organizer recognizes that each person or bloc has a hierarchy of values."[30] Each person has one thing that they care about the most, very similar to Maslow's hierarchy of needs.

The online organizer must determine what is most important to his community and use it to their advantage. A person will only passionately care about a national issue if it translates into social transgressions that affect them directly. To use Alinsky's example, neighbors in a neighborhood have very different concerns: one man is worried about property values because his entire life savings are tied up in the house, his neighbor is worried about drug use in the neighborhood influencing her children, and still another neighbor is worried about rising food costs. The organizer must take all of these issues and translate them into a relatable menu of issues that every actor perceives as the root cause of the problem. The community being organized must have a variety of issues that can be rallied around because, "A single- or even dual-issue organization condemn you to a small organization, it is axiomatic that a single-issue organization will not last. An organization needs action as an individual needs oxygen."[31] This means that the organization needs always to be roused about something, and only having one or

two issues will quickly stagnate and kill the organization. The same is true for online communities.

The online community has needs, wants, and desires the same as a physical community. While these may or may not manifest themselves in physical reality, they still produce real and raw emotions in the user and even the community as a whole. According to Alinsky, "Before men can act, an issue must be polarized. Men will act when they are convinced that their cause is 100 percent on the side of the angels and that the opposition are 100 percent on the side of the devil."[32] The online organizer must be able to rally his community around action and an issue that mobilizes the individual to act. An example of a mobilized community that highlights organizing in action, is the net neutrality debate. There is a large community of people, as well as tech companies like Etsy and Kickstarter that have organized to fight it.[33] The communities have lobbied Congress and have gained bipartisan support to pass a bill reinstating Net Neutrality. According to Evan Greer:

> The [Congressional Review Act] CRA is by far the most likely path to restoring net neutrality protections nationally, as it only requires a simple majority in the Senate and House. With 50 senators, including Republican Susan Collins, already publicly supporting - only need one more Republican to win any Senate vote on it, and there are more than half a dozen GOP senators who have strongly indicated they're considering it.[34]

Highlighting Net Neutrality shows there are many online communities fighting to keep it, and the power of communities to affect an issue both in the cyber and the physical domain. If an entity could organize the disparate groups into a bloc, then the power of that bloc could be used to influence even more lawmakers. This is one example of the power of organizing. Imagine if

the cadre of cyberwarriors working for the government could tap into a passion of a community and use that passion to ward off cyber attacks, or other forms of defense. The same would be true if the government dispatched community organizers around the web to enlist the help of the online community to fight for their "cause." By making issues relatable to the community that the organizer represents and presenting the facts in a way that seems to encroach on the rights of the participants, the organizer can mobilize the community to fight for the cause.

Small Cadre – Multiple Networks

A hybrid of Military Source Operations (MSO) and UW techniques will be required to build online villages to secure U.S. networks and attack adversaries. In JP 3-05, MSO refers to

> The collection, from, by, and/or via humans, of foreign and military and military-related intelligence. HUMINT sources serve as "eyes and ears" to track adversary activity. Sources include walk-ins, developed sources, unwitting persons, and protected sources. HUMINT collection personnel may develop information through the elicitation of sources. Establishing a reliable source network is an effective collection method.[35]

Using a small cadre of professionals to build multiple networks using techniques online that resemble special operations will fill a void currently in the cyber domain by U.S. forces. Developing source networks will enable Joint Intelligence Preparation of the Operational Environment which will enable the cadre to target specific areas where the enemy can be exploited and mitigate areas where friendly forces are vulnerable.

Command and control (C2) of source operations online will require the J2Z to match resources to requirements and needs of the service. In cyber, the technical aspects of C2 will be

more critical than in any other warfighting domain. According to to FM 2-22.3, "The success of the HUMINT collection effort depends on a complex interrelationship between command and control (C2) elements, requirements, technical control and support, and collection assets."[36] During operational campaign planning, transition from C2 of MSO to UW operations online requires careful vetting and validation procedures that should be well established prior to employment of the network. J2Z will be required to deconflict multiple source networks to ensure they are not working at cross-purposes. J2Z will also need to ensure that control is exerted over the networks have been developed and see to it that the individuals within the network do not "go rogue" and execute operations without proper guidance and approvals. Authorities do not currently exist that include cyber domain operations of this type and will need to be written and implemented.

Organizing Online Communities

During the 1960's and 70's, the U.S. government sponsored the VISTA program which is now an arm of AmeriCorps. VISTA was a program whereby "volunteers who engage in community organizing and advocacy … challenge officials to address poverty and inequality at state and local levels…VISTA identifies five program emphasis areas for new projects: health, education and manpower, economic development, community planning, and general services."[37] A program similar to VISTA could be established to organize online communities by appealing to a sense of pride in protecting U.S. networks; people who work ostensibly for the organizer, but ultimately for the government. The cadre could either be using witting or unwitting sources in accordance with JP 3-05, whatever the situation dictates.[38]

The cyber domain is similar to the physical domain in that there are virtual territories, websites, meeting sites, and social media platforms. Each of these areas has its own unique

"community" of users. Whether openly or clandestinely, DoD should endeavor to operate in all of these areas and a technique for organizing them is described below using Alinsky's techniques Developing a small cadre of individuals who are willing to operate in these communities to protect U.S. networks and possibly attack state and non-state enemies will be a force multiplier. They must, however, be able to drive a narrative amongst the community that the members can rally behind. Driving the narrative is as important as the narrative itself. Before that though, the organizer that the DoD should hire should have the following qualities:

1. Political relativity or the ability to relate to political passions of the individual or group being recruited
2. A free and open mind
3. Curiosity
4. A sense of humor
5. Distrust of dogma
6. An understanding of irrational human behavior and the nature of irrationality
7. A flexible personality with the ability to evolve
8. A charismatic individual who is capable of efficiently communicating with the members of the community and can sway the community to act [39]

In addition to the abilities listed above, technical acumen will also be a critical characteristic needed for the cadre operator. Hackers generally hack because they want to be recognized by their peers. The charismatic cadre leader has to have technical acumen and the ability to discuss the various "victories" that hackers have accomplished in order to play to the ego of the hacker and convince them to join the community being built by the cadre. These characteristics are what the DoD should be looking for when seeking out a cyber professional who is looking to

lead an online cause; with the cause being the security of US networks. These individuals must be adept in their craft of either offensive or defensive cyber but must have the ability to lead large groups of disparate individuals towards a common goal to ensure United States networks are safe and enemy networks are vulnerable to attack.

Political relativity speaks to the 'ends' portion of the relationship between the organizer and the community. If the end is to secure the safety of US networks, then the relative portion is how to achieve it. If, for instance, the community is largely anti-American, but the community sees services provided by US networks as a net positive, then the organizer must seize on those desires and capitalize on the community's wants. Alinsky says "In a mass organization, you can't go outside of people's actual experience."[40] One has to go after an issue by relating to the desires of the individual. It is all well and good for everyone to want 'Net Neutrality,' but that is abstract. Instead, the organizer has to be able to delve into the inner sanctum of the individual and illustrate the threat to that individual. If the individual is threatened by the loss of their online access, then the organizer must seize on that and illustrate how the collective community is threatened, and thereby the individual must act by the community to ensure that *all* rights to free access of the internet are assured.

The cadre could use cyber industry leaders to affect defense of United States systems because it is in their interest to have secure networks as well. An example of how this works can be seen in Sweden where the Swedish government is implementing a "Fortress Sweden" concept that incorporates the whole population in their war plan to deter aggressive actions from entities such as Russia and state and non-state actors abroad.[41] In Sweden, the cyber industry has a vested interest in helping the government secure the national cyber architecture. According to Erik Brattberg, a fellow at the Carnegie Endowment for International Peace, "the domestic cyber industry won't raise objections to working on new security standards or assisting the government

with emergency preparations."[42] Sweden is currently incorporating cyber-defense into their Fortress Sweden concept, "As a result...the commission has suggested the government work to craft new coordination on cybersecurity issues with private sector companies, as well as driving toward greater investment in military cyber capabilities."[43] Sweden may attempt to emulate their neighbor, Finland, who is also attempting to secure their networks using their organic citizenry. Finnish Defence Policy Director-General Janne Kuusela said, "…we benefit a lot from having people who worked in this [cyber] domain, in their civilian lives, so they are reservists and bring a lot of additional knowledge and interaction for the defense goals for us. It's a good way of dealing with this."[44] In the United States, the cadre could manage a large network or community of cyber professionals who work to secure U.S. systems by organizing willing professionals whose expertise in cyber defense could be harnessed. The professionals could act in an almost reservist capacity where they have a civilian job but are activated when needed to address specific problems that relate to their expertise. Each community could be organized into Teams of Interest (TOI) to aggregate the knowledge of the village that is led by the cadre. Each TOI could be organized functionally (i.e. software development) or they could be organized into teams that have representation across the cyber operational domain. However the cadre chooses to organize their TOI's, the key will be to convince the civilian population to willingly

Alinsky says "a threat or action becomes the precondition to communication."[45] He is saying that no crisis should go to waste. Here is where the agility of the organizer with the ability to evolve can help the online organizer. By seizing on a particular threat, the skilled organizer can rally the community to ensure that the threat to the network is neutralized. Herein lies the power of the community as a force multiplier. Within the DoD, there is a hierarchy often called the chain of command. The chain of command can sometimes be cumbersome, and decisions to act are rarely timely, but with communities organized to act decisions can be made

at a rapid pace. Those quick decisions can be the difference between service denial and threat avoidance.

The organizer begins the mission by appearing as a natural and charismatic leader in the community. He/she must take charge, be credible, and make decisions that not only drive the community to achieve the stated ends but must also *appear* to be making progress toward those ends. By establishing his/her credibility and relatability to the community, the organizer proves that he/she belongs and has the best interests of the community at heart. After this credibility has been established, the organizer can then begin to delegate authority to faithful lieutenants to carry out the plan of the day to either secure a network or threaten another. Building the community builds support for the cause, and this is why the organizer must be conversant on a wide range of issues. If he/she can win people over to his/her side, then the community grows and the security of the network is more assured.

If the organizer is cunning enough, he/she can convince the people working for him to take the same level of pride in taking down would be threats, as those who present those threats are when they are successful. Among the online hacker community, people who are successful in hacking hard-targets such as large corporations, banks, and U.S. government websites become legendary amongst their peers. Having a community of so-called "white hat" hackers to thwart the black hat hackers and naming their operations for the online community to see could be helpful in recruiting and retention to join the U.S. side.

Conclusion

By adopting a hybrid "all of the above" approach to fighting in the cyber domain, the United States continues to address long and medium-term requirements, also look for new and novel ways to address short-term needs. Recommendations for this approach include:

- Sustain building an officer corps capable of leading cyber warriors in conventional areas.
- Use a mix of active duty, and reservists who work in their civilian capacity in the technology field to leverage knowledge gained by training in both government and civilian sectors.
- Create a small cadre of online community organizers to build communities to conduct UW and to defend friendly networks and infiltrate enemy, both state and non-state, networks and communities meant to do U.S. harm.
- Develop UW and Military Source Operations to address unconventional aspects of operating in the cyber domain.

Finally, by creating a UW capability that operates in the cyber domain, the DoD will be fully capable of operating across the Range of Military operations online and will present a formidable deterrent to actors seeking to do harm to the U.S. in any warfighting domain.

Notes

[1] United States Cyber Command Factsheet, accessed April 30, 2018, http://www.stratcom.mil/Portals/8/Documents/CYBERCOM_Fact_Sheet.pdf.
[2] Ibid.
[3] US President. "Statement by President Donald J. Trump on the Elevation of Cyber Command" *Statements and Releases,* (August 2017). Accessed April 30, 2018, https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/.
[4] Crawford, Amy. "The Swamp Fox," *Smithsonian.com.* (June 30, 2007). Accessed April 26, 2018, https://www.smithsonianmag.com/history/the-swamp-fox-157330429/.
[5] Thomas, Evan. "Spymaster General" *Vanity Fair*, (March 3, 2011). Accessed April 26, 2018 https://www.vanityfair.com/culture/2011/03/wild-bill-donovan201103.
[6] Joint Publication 3-05 *Special Operations* (16 July 2014), II-9.
[7] Joint Publication 3-12 *Cyberspace Operations* (05 February 2013), viii.
[8] Ibid. II-2.
[9] Ibid. II-2.
[10] Office of the President of the United States. *National Security Strategy*. (Washington, D.C.: White House, December 2017), 26.
[11] Joint Publication 3-12 *Cyberspace Operations* (05 February 2013), III-2.
[12] Ibid. III-10.
[13] Pagliery, Jose. "The Deep Web You Don't Know About" *CNN.com*, (March 10, 2014), Accessed April 23, 2018 http://money.cnn.com/2014/03/10/technology/deep-web/index.html.
[14] Ibid.
[15] Public Law 114-92 Sec. 1097, S.1356 — 114th Congress (2015-2016), National Defense Authorization Act for FY 2016.
[16] Army Field Manual 3-05 *Army Special Operations* (January 2014), 2-1.
[17] Ibid. 2-2.
[18] Unconventional Warfare, *Pocket Guide V1.0* (Fort Bragg, NC, April 5, 2016), 11.
[19] Ibid. 13.
[20] Ibid. 13-14.
[21] Army Field Manual 3-05, *Army Special Operations* (January 2014), 2-4.
[22] Army Field Manual 2-22.3, *Human Intelligence Collector Operations* (September 2006), 1-13.
[23] Ibid. 3-1.
[24] Alinsky, Saul D. *Rules for Radicals – A Pragmatic Primer for Realistic Radicals,* (New York: Vintage Books – Random House, 1971), 197.
[25] Ibid, 24.
[26] Ibid. 24.
[27] Chapell, Bill and Neuman, Scott "U.S. Says North Korea Directly Responsible for WannaCry Ransomware Attack" *NPR.* (December 19, 2017). Accessed April 14, 2018, https://www.npr.org/sections/thetwo-way/2017/12/19/571854614/u-s-says-north-korea-directly-responsible-for-wannacry-ransomware-attack.
[28] Office of the President of the United States. *National Security Strategy*. (Washington, D.C.: White House, December 2017), 21.
[29] Willgress, Lydia and Walker, Peter. "IT Expert Who Saved the World From Ransomware Virus is Working With GCHQ to Prevent Repeat" *The Telegraph.* (May 15, 2017). Accessed 25 April, 2018, http://www.telegraph.co.uk/news/2017/05/14/revealed-22-year-old-expert-saved-world-ransomware-virus-lives/.
[30] Alinsky, Saul D. *Rules for Radicals – A Pragmatic Primer for Realistic Radicals,* (New York: Vintage Books – Random House, 1971), 78.
[31] Ibid. 77-78.
[32] Ibid. 78.

[33] Greer, Evan. "Ajit Pai Tried to Kill Net Neutrality, But the Internet is Fighting Back" *NBC Think*, (March 6, 2018). Accessed 13 April, 2018 https://www.nbcnews.com/think/opinion/ajit-pai-tried-kill-net-neutrality-internet-fighting-back-ncna854151.
[34] Ibid.
[35] Joint Publication 3-05 *Special Operations* (16 July 2014), IV-3.
[36] Army Field Manual 2-22.3, *Human Intelligence Collector Operations* (September 2006), 2-1.
[37] "VISTA Timeline – Celebrating 50 Years of VISTA Service," *VISTA Campus.* Accessed April 21, 2018 https://www.vistacampus.gov/vista-timeline-celebrating-50-years-vista-service.
[38] Joint Publication 3-05 *Special Operations* (16 July 2014),IV-3. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_05.pdf?ver=2018-03-15-111255-653
[39] Alinsky, Saul D. *Rules for Radicals – A Pragmatic Primer for Realistic Radicals,* (New York: Vintage Books – Random House, 1971), 79.
[40] Ibid. 88.
[41] Mehta, Aaron. "Fortress Sweden: Inside the plan to mobilize Swedish society against Russia" *Defense News*, (March 14, 2018). Accessed April 19, 2018 https://www.defensenews.com/global/europe/2018/03/14/fortress-sweden-inside-the-plan-to-mobilize-swedish-society-against-russia/.
[42] Mehta, Aaron. "Sweden's Plan to Deter a Russian Digital Attack," *FifthDomain.com*, (March 14, 2018). Accessed online April 23, 2018 https://www.fifthdomain.com/international/2018/03/14/swedens-plan-to-deter-a-russian-digital-attack/.
[43] Ibid.
[44] Ibid.
[45] Alinsky, Saul D. *Rules for Radicals – A Pragmatic Primer for Realistic Radicals,* (New York: Vintage Books – Random House, 1971), 89.

Bibliography

United States Cyber Command Factsheet, accessed April 30, 2018, http://www.stratcom.mil/Portals/8/Documents/CYBERCOM_Fact_Sheet.pdf.

US President. "Statement by President Donald J. Trump on the Elevation of Cyber Command" *Statements and Releases,* August 2017. Accessed April 30, 2018, https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/.

Crawford, Amy. "The Swamp Fox," *Smithsonian.com,* June 30, 2007. Accessed April 26, 2018, https://www.smithsonianmag.com/history/the-swamp-fox-157330429/.

Thomas, Evan. "Spymaster General" *Vanity Fair,* March 3, 2011. Accessed April 26, 2018 https://www.vanityfair.com/culture/2011/03/wild-bill-donovan201103.

Joint Publication 3-05 *Special Operations* 16 July 2014.

Joint Publication 3-12 *Cyberspace Operations* 05 February 2013.

Office of the President of the United States. *National Security Strategy*, Washington, D.C.: White House, December 2017.

Pagliery, Jose. "The Deep Web You Don't Know About" *CNN.com*, March 10, 2014. Accessed April 23, 2018 http://money.cnn.com/2014/03/10/technology/deep-web/index.html.

Public Law 114-92 Sec. 1097, S.1356 — 114th Congress 2015-2016, National Defense Authorization Act for FY 2016.

Army Field Manual 3-05 *Army Special Operations,* January 2014.

Army Field Manual 2-22.3, *Human Intelligence Collector Operations,* September 2006.

Alinsky, Saul D. *Rules for Radicals – A Pragmatic Primer for Realistic Radicals*, New York: Vintage Books – Random House, 1971.

Chapell, Bill and Neuman, Scott "U.S. Says North Korea Directly Responsible for WannaCry Ransomware Attack" *NPR,* December 19, 2017. Accessed April 14, 2018, https://www.npr.org/sections/thetwo-way/2017/12/19/571854614/u-s-says-north-korea-directly-responsible-for-wannacry-ransomware-attack.

Willgress, Lydia and Walker, Peter. "IT Expert Who Saved the World From Ransomware Virus is Working With GCHQ to Prevent Repeat" *The Telegraph.* (May 15, 2017). Accessed 25 April, 2018, http://www.telegraph.co.uk/news/2017/05/14/revealed-22-year-old-expert-saved-world-ransomware-virus-lives/.

Greer, Evan. “Ajit Pai Tried to Kill Net Neutrality, But the Internet is Fighting Back“ *NBC Think*, March 6, 2018. Accessed 13 April, 2018 https://www.nbcnews.com/think/opinion/ajit-pai-tried-kill-net-neutrality-internet-fighting-back-ncna854151.

“VISTA Timeline – Celebrating 50 Years of VISTA Service,” *VISTA Campus.* Accessed April 21, 2018 https://www.vistacampus.gov/vista-timeline-celebrating-50-years-vista-service.

Mehta, Aaron. “Fortress Sweden: Inside the plan to mobilize Swedish society against Russia” *Defense News*, March 14, 2018. Accessed April 19, 2018 https://www.defensenews.com/global/europe/2018/03/14/fortress-sweden-inside-the-plan-to-mobilize-swedish-society-against-russia/.

Mehta, Aaron. “Sweden’s Plan to Deter a Russian Digital Attack,” *FifthDomain.com*, March 14, 2018. Accessed online April 23, 2018 https://www.fifthdomain.com/international/2018/03/14/swedens-plan-to-deter-a-russian-digital-attack/.