REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
29-04-2015	Master of Military Studies Research Paper	September 2014 - April 2015

4. TITLE AND SUBTITLE

Geeks in the Marine Corps: Bridging a Generational and Cultural Gap for the Cyber Workforce

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Mayoral, Joshua J., Major, USMC

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)

N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

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

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

N/A

14. ABSTRACT

A generational and cultural gap between Marine Corps Cyber leaders and future cyber warriors exists that stems from the rapid growth of technology and the Marine Corps force generation model failing to keep pace. Millennials have grown through rapid changes in technology, which has aided in their predisposition and intuitive understanding of that technology. Some of the millennials specifically sought to understand that technology intimately by pursuing hobbies and studies in science, technology, engineering, and mathematics and have immersed themselves in science fiction for diversion and inspiration. The resulting science fiction-based culture that penetrates and grows around them is geeky. Geeks do not typify a poster Marine, yet these future employees are leading the cyber industry. Millennial geeks are the future cyber professionals both in the commercial and military workforce. The Marine Corps needs the best cyber warriors to fight the future fight. The Marine Corps needs to adopt a force generation model that screens, assesses, and selects future candidates for cyber-operations. Those individuals, selected through assessment and undergraduate study, like that of naval aviators, should then undergo training that prepares them to execute warfighting and cyberspace operations in support of the Marine Corps.

15. SUBJECT TERMS

Cyber, Cyberspace, MARFORCYBER, Manpower, Culture, Generation

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Marine Corps University/Command a
Unclass	Unclass	Unclass	UU	45	**19b. TELEPHONE NUMBER** *(include area code)* (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

MASTER OF MILITARY STUDIES

TITLE: Geeks in the Marine Corps: Bridging a Generational and Cultural Gap for the Cyber Workforce

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

AUTHOR: Major Joshua Mayoral, USMC

AY 14-15

Mentor and Oral Defense Committee Member: Matthew Flynn

Approved: _____

Date: 4/24/15

Oral Defense Committee Member: Hugh Cartwright

Approved: _____

Date: 4/24/15

J.W. Barden

4/24/15

Executive Summary

Title: Geeks in the Marine Corps: Bridging a Generational and Cultural Gap for the Cyber Workforce

Author: Major Joshua Mayoral, USMC

Thesis: A generational and cultural gap between Marine Corps Cyber leaders and future cyber warriors exists that stems from the rapid growth of technology and the Marine Corps force generation model failing to keep pace.

Discussion: Millennials have grown through rapid changes in technology, especially cyberspace. Their daily use of that technology as they have grown up has aided in their predisposition and intuitive understanding of that technology. Some of the millennials specifically sought to understand that technology intimately by pursuing hobbies and studies in science, technology, engineering, and mathematics. In the process of doing so, many have immersed themselves in pastimes for diversion and inspiration: science fiction. The resulting science fiction-based culture that penetrates and grows around them is geeky and nerdy. Geeks and nerds do not typify a poster Marine, spit-polished and broad-shouldered, yet these future employees may be leading the cyber industry.

Conclusion: Millennial geeks are the future cyber professionals both in the commercial and military workforce. Those professionals will make the best cyber warriors. The Marine Corps needs the best cyber warriors to fight the future fight. The Marine Corps needs to adopt a force generation model that screens, assesses, and selects future candidates for cyber-operations. Those individuals, selected through assessment and undergraduate study, like that of naval aviators, should then undergo training that prepares them to execute warfighting and cyberspace operations in support of the Marine Corps.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Table of Contents

Preface

I conducted this study because I have been immersed in the geek and cyber culture throughout my life. For me, it is a passion, a hobby, an interest, and what I believe is an inextricable part of future generations. Much of the culture has been shaped, as I have, by the growth of technology and those who have speculated on its future abilities. Those individuals, like myself, have often found unconventional means by which we have expanded our own understanding of transistor-transistor logic circuitry to programming languages and beyond. Many individuals share not only a passion for this culture but also an understanding and empathy for a culture once shunned by society as passingly useful and socially inconvenient techies. That culture is a culture of artists and dreamers whose canvas is made up of electronics and code. Many of their dreams echo in science fiction novels and movies, and the advances, seen in commentary in *Popular Science, Popular Mechanics,* and *Wired,* for example, resonate within the geek community as challenges, touchstones, or discussion points. As such, these community artifacts inspire geeks of today and tomorrow. In other words, the science fiction of today is more than flights of passing fancy. Rather, good science fiction is made of three parts: science fiction, science theory, and science fact. The combination makes for not only a believable story, but for engineers and scientist to apply their current knowledge, hypothesize new possibilities, see new angles, or even shift accepted technological paradigms. Their dreams, however, are grounded firmly in computer science, engineering, mathematics, and logic. As a Marine, I choose to see the way to marry my interest with my work. This study offers a possible solution for geeks to become effective cyber Marines. Culturally, however, geeks may be out of phase with what military traditionally sees as a warfighter. My personal empathy to the geekier few has inclined me to offer a different perspective to the Few and the Proud, who I believe, needs to look at creative ways to employ geeks within the ranks. And I do believe that there are geeks out there who not only want to serve, and there are Marine leaders out there who also want their talent, but may not yet have a process to show them the way in and up.

REPORT DOCUMENTATION PAGE

FORM APPROVED - - - OMB NO. 0704-0188

PUBLIC REPORTING BURDEN FOR THIS COLLECTION OF INFORMATION IS ESTIMATED TO AVERAGE 1 HOUR PER RESPONSE, INCLUDING THE TIME FOR REVIEWING INSTRUCTIONS, SEARCHING EXISTING DATA SOURCES, GATHERING AND MAINTAINING THE DATA NEEDED, AND COMPLETING AND REVIEWING THE COLLECTION OF INFORMATION. SEND COMMENTS REGARDING THIS BURDEN ESTIMATE OR ANY OTHER ASPECT OF THIS COLLECTION OF INFORMATION, INCLUDING SUGGESTIONS FOR REDUCING THIS BURDEN, TO WASHINGTON HEADQUARTERS SERVICES, DIRECTORATE FOR INFORMATION OPERATIONS AND REPORTS, 1215 JEFFERSON DAVIS HIGHWAY, SUITE 1204, ARLINGTON, VA 22202-4302, AND TO THE OFFICE OF MANAGEMENT AND BUDGET, PAPERWORK REDUCTION PROJECT (0704-0188) WASHINGTON, DC 20503

1. AGENCY USE ONLY (*LEAVE BLANK)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED *STUDENT RESEARCH PAPER*
4. TITLE AND SUBTITLE		5. FUNDING NUMBERS *N/A*
6. AUTHOR(S)		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) *USMC COMMAND AND STAFF COLLEGE* *2076 SOUTH STREET, MCCDC, QUANTICO, VA 22134-5068*		8. PERFORMING ORGANIZATION REPORT NUMBER *NONE*
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) *SAME AS #7.*		10. SPONSORING/MONITORING AGENCY REPORT NUMBER: *NONE*
11. SUPPLEMENTARY NOTES *NONE*		

12A. DISTRIBUTION/AVAILABILITY STATEMENT	12B. DISTRIBUTION CODE
NO RESTRICTIONS	*N/A*

ABSTRACT *(MAXIMUM 200 WORDS)*

14. SUBJECT TERMS (KEY WORDS ON WHICH TO PERFORM SEARCH)	15. NUMBER OF PAGES:
	16. PRICE CODE: N/A

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE:	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	*UNCLASSIFIED*	*UNCLASSIFIED*	

whoami (introduction)

I discovered, to my amazement that all through history there had been resistance ... and bitter, exaggerated, last-stitch resistance ... to every significant technological change that had taken place on earth. Usually the resistance came from those groups who stood to lose influence, status, money...as a result of the change. Although they never advanced this as their reason for resisting it. It was always the good of humanity that rested upon their hearts.

Isaac Asimov, lecture at Newark College of Engineering, Nov. 8, 1974

Generations apart from American youth and future cyber warfighters, senior Marine Corps decision makers battle a cultural gap between them and the future professionals destined to wage warfare in cyberspace. Almost five years ago, Gregory Conti, called for nerds and geeks to enter the cyber workforce, promoting their skills as counter-culture but 21st century warfare relevant.[1] But there are still no force generation models for identifying future cyberspace warfighter's career progression and retention inside a military occupational specialty (MOS) from entry to retirement.[2] Major General O'Donohue stated before the House Armed Services Committee that, "our most valuable resource is our people," "we believe the solutions to our shared problems in cyberspace revolve around our people, and not systems," "the number of feeder MOS [sic] available to lateral move into critical cyber related specialties has been increased in order to obtain a larger talent pool," and "we are leveraging academia and industry to understand how to better attract and retain talent."[3] This begs the question, is the Marine Corps employing the right people for the job?

The Marine Corps breeds a culture of warfighting and senior Marine Corps leaders know how to provide a force ready to fight. At the core of Marine Corps culture is the belief that "Every Marine is a rifleman." The Marine Corps also advocates that conflicts divide into respective domains: air, sea, land, and cyberspace.[4] MOSs reflect those divisions and include warfighting MOSs that serve a functional purpose like intelligence, communications, and logistics, connecting and sustaining the domains. Today,

however, the Marine Corps culture, rooted in marksmanship and physicality may fall short of attracting and nurturing individuals suited to tackle the metaphysical cyberspace.

Cyberspace emerged during the same years that Marine Corps leaders honed their understanding of the Cold War and emergent post-Cold War warfighting. Those years, and the years before them, generated a proficiency in and a preference for kinetic warfare. Doctrine writers eschewed fuzzy and highly technical concepts as information warfare (IW), and did not align them with the prototypical view of a warfighter.[5] But that IO environment, full of nuanced abstractions, technobabble, and a geeky subculture is a digital environment that underpins everything today. Children born in the 1980s and 1990s are native to the digital environment.[6]

Technology separates "digital immigrants" and "digital natives" by generations.[7] That separation obviates a framework to bridge understanding of cyberspace and warfighting. Senior Marine Corps leaders do not share the same predisposition for cyberspace of their new recruits.[8] Understanding cyberspace's interfaces and manipulations are more natural actions for natives than are for immigrants.[9] Interfaces and manipulations of cyberspace are the foundational components of cyberspace, and for some, especially younger generations, it is intuitive.

While leaders and rising leaders in the Marine Corps oversaw the end of the Cold War, Desert Storm, and Kosovo, some American youths emigrated from physical pastimes of playing outdoor sports to playing video games and exploring the internet.[10] What some may not realize is that many of the younger generation were also engaging in forms of warfare. Like the fictional character Ender Wiggin, of Orson Scott Card's *Ender's Game,* digital natives learned to coordinate information between players over long distances in near-real time.[11] They were also learning lessons from Captain James T. Kirk in Gene Roddenberry's *Star Trek II: Wrath of Khan* (1982) – that hacking a computer can give you a fighting edge.[12] There are many more examples of science fiction prognostications, suggestions, and challenges. In most cases, these did not form cautionary tales stemming from mere fanciful science fiction; rather

they formed the playbook of exploitable maneuver space. These references may seem unconventional, but science fiction has an important role in cyberspace and for the culture of digital natives.[13] Ultimately, recognizing the culture for what it is, harnessing its talent, and grooming the expertise of digital natives becomes an implied task for force generation models to support an effective cyber workforce. Embroiled in organizational downsizing, Marine Corps leaders also need to recognize that they are working with a "finite pool of talent."[14] Leaders will find the talent among tech nerds, engineers, or those inclined to electronic subtleties – geeks. Leaders will do well to employ them to win the future cyber war.

ps (current cyberspace processes and understandings)

> *In your high school geology class you probably were taught that all life on earth exists in a paper-thin shell called the biosphere, which is trapped between thousands of miles of dead rock underfoot, and cold dead radioactive empty space above. Companies that sell OSes exist in a sort of technosphere. Underneath is technology that has already become free. Above is technology that has yet to be developed, or that is too crazy and speculative to be productized just yet. Like the Earth's biosphere, the technosphere is very thin compared to what is above and what is below.*
>
> *-Neal Stephenson, In the Beginning…was the Command Line*

Born Digital, the book by John Palfrey and Urs Gasser, opens up the idea that there are fundamental differences between the generations, how they view and how they use technology related to cyberspace. *Born Digital* coins the terms "digital native" and "digital immigrant." It identifies the technological growth from the late-70s through the 2000s and how each evolution grew symbiotically with its primary users. Palfrey and Gasser describe how digital natives view information, cyberspace as creative space, and explain how the fundamental belief of freedom of information anchors the way they view the purpose of using cyberspace. These principles form the foundation of how one might view digital natives and their personalities as a culture that may be incongruent with Marine Corps culture.

Other experts look at different approaches to define that same gap. *Cyber Warfare and Cyber Terrorism*, by Lech J. Janczewski and Andrew M. Colarik, breaks down a historical perspective of cyber terrorism and attacks, drawing out the trends linking each successive attack. Tracing evolutionary steps in cyberspace shows that nefarious actors were able to generate hemorrhagic losses of information. Explorations by security experts leads to an understanding of human psycho-social interactions and motivations in cyberspace, which, in turn, leads to developing more effective security strategies. These psychosocial interactions and motivations are key components of an effective cyber user, an imperative for a cyber-warfighter.

The Ingenuity Gap emphasizes that technology offers new opportunities for social interaction and cooperative development. Cyberspace, Thomas Homer-Dixon argues in this book, is a fertile breeding ground for the introduction of new ideas. It is a venue for exchange and interplay. The book connects the idea that cyberspace connotes a social interaction all unto its own and an integral part of daily living for Digital Natives of today. Author Franklin D. Kramer et al add to this view in, *Cyberpower and National Security,* which addresses the social interaction derived from the convenience cyberspace provides.

Of course, social interaction is usually a far cry from acts of war, yet cyber has had to force many to rethink this relationship. *Cyber Warfare* is a comprehensive look at the nature of conflict in cyberspace. Paul Rosenzweig outlines several models for conceptualizing cyberspace, the actors within it, and the components that make up the environment. *Cyber War: The Next Threat to National Security and What do Do About It,* is the preeminent book on cyber strategy and international considerations for the employment of warfare in cyberspace. Richard Clarke, advisor to presidents Reagan through George W. Bush, explains rational decision making by states, non-state actors, and individuals conducting actions within cyberspace. Even in this context, what constitutes a war in cyberspace remains unclear, as does how generations understand what conflict in cyberspace does and should mean.

As might be expected, bringing generations into a discussion of cyber lends itself to a myriad of other sources. For example, *The Enlightened Soldier,* by Charles Edward White, Scharnhorst's presentation of his experiences as a student and an instructor in the German military academy, shows how education reformed the German officer cadre into a professionalized organization brimming with creative and critical thinking problem solvers. Overcoming a generation gap cemented many German reforms. Another approach is in *Organizational Culture and Leadership,* the premier model for understanding cultures within organizations. Edgar Schein provides references and detail on how to change cultures or adopt them notwithstanding gaps in group dynamics for any number of reasons.

This more theoretical work is valuable and key to this study, but by far the most essential element that defines and lends understanding to the generation most shaping cyber realities today comes from

science fiction. This genre is not simply vindicated that when its prophesies come true, as is the case in so many instances related to cyberspace i.e. blogs, email, interactive games, and others. Digital natives have embraced this fiction as fact, as it now is, validating this obsession with technology as a element improving life and having a clear and positive impact on that generation. Some key works include, *Outliers: The Story of Success*, a book that highlights what makes individuals proficient and exceptional in a profession, and while not science fiction, gets this line of analysis started.

Neuromancer is a science fiction novel by William Gibson that tells a story about a downtrodden hacker who executes a heist using a combination of social networking, cybernetic devices, and a keen understanding of virtual reality. *Snow crash*, written by Neal Stephenson, is a science fiction novel that offers ideas of how cyberspace can parallel real space. The ability to exercise one's skills within the real world is a direct reflection in cyberspace, and the things created there within are equally as powerful in both worlds. Many more science fiction books like *Schimatrix* by Bruce Sterling, and *Do Androids Dream of Electric Sheep* by Philip K. Dick, typify science fiction literature that speaks to both a physical component and an intellectual outgrowth of such hardware/software, a combination that has shaped, predicted, and challenged what makes up cyberspace today.

While these books collectively appear somewhat disparate and perhaps incompatible, especially science fiction, they coalesce the idea that Digital Natives, their upbringing, their ability to imagine future technologies, and their understanding of technology and its nuanced evolutions, enjoy an edge over others who have not grown in the same fashion. What they accept as fiction, has in fact come to pass and may well do so again. That is the main challenge undergirding cyberspace.

who (the cyber culture)

I've come up with a set of rules that describe our reactions to technologies:

Anything that is in the world when you're born is normal and ordinary and is just a natural part of the way the world works.

Anything that's invented between when you're fifteen and thirty-five is new and exciting and revolutionary and you can probably get a career in it.

Anything invented after you're thirty-five is against the natural order of things.

-Douglas Adams, The Salmon of Doubt

The late Douglas Adams describes the human condition and their admiration and aversion for technology throughout a person's lifespan. More importantly, he highlights the rift that can and often occurs in a lifetime – in the case of this analysis between senior Marine Corps leaders and their warfighters. Many things can exacerbate that problem, especially the growth and expansion of technology. Though somewhat cliché, Moore's law, or the observation that, computing power doubles approximately every two years, lends to sustaining or exacerbating that gap.

Moore's law urges industry and military alike to keep pace with changing technology. Both the users and the developers are in a symbiotic and cooperative relationship for growth.[15] Consequently, understanding what makes the current generation of digital natives so accustomed to the technology that makes up cyberspace is critical to developing the bridge between decision makers and future cyber warriors. Understanding how they trust the technology and pushing its limits will enable leaders to trust the decisions and recommendations of the cyber warriors that they lead.

Sociologists, psychologists, and demographers define generations as a group of people, or birth cohorts, born within a period.[16] Events that influenced them, not exacting dates, form a social datum, and cognitive bias for that period.[17] Common generational references are Baby Boomers, Generation X (Gen

X), and Millennials (sometimes referred to as Gen Y).[18] Each has marked historical events that have bonded them together. Baby Boomers are the products of the end of World War II and saw the beginning of Space Race, and witnessed a television arrive in every home, roughly 1946-1960s. Gen X saw the end of the Vietnam War, the rise of the film industry to new heights best depicted in science fiction terms with *Star Wars*, *Tron* and the introduction of VHS and cassette tapes, roughly 1965-1979. Millennials saw the fall of the Berlin Wall, Operation Desert Storm, and the advent of the internet, compact discs, satellite television, and .mp3s, roughly 1979-2000s. Despite the labels, cyberspace's entrance into mainstream society affects the late Gen X and Millennials in a profound way. Simply stated, they are the future leaders of Marine Corps cyber warfare.

The culture of this group is an amalgamation of those events that bounded them together but also the world they interacted with and how. Using music as a function of culture, Millennials, often referred to as the MTV generation, experienced music differently than their seniors. Millennials experienced a transition in music medium and availability, the music video making popular inroads even as critics decried the visual debasement of the medium, a loss of artistic authenticity even in the process of creating something new.[19] Music doomsayers of senior generations expected that MTV would decouple the music industry from its artistic bases. Instead, MTV embraced the rise of technology incorporating emergent technology and mediums, from cassette tapes to VHS to compact discs (CD).[20] A decade later, Millennials saw the rise of the .mp3, slowing CD thefts, and giving rise to music sharing. In the wake of Napster music sharing, many digital natives were involved in illicit music trade. Music sharing demonstrates how Millennials viewed artistic things, and understood techniques and interfaces, like peer-to-peer sharing. The product was democratized to a point of undermining the previous economic normal of capitalism best defining quality; what sold well denoted artistic virtue. Since the relationship was suspect from the start, Millennials had ushered in a new means of measuring success and how that success should be shared.

Technological advances capture how the digital natives view their interconnected world, its proclivities, and achieving their objectives. Their view of the world is both technological and human.[21] While they grew up, some immersed themselves in a genre and a theme that merged the human and cyber worlds together. "Cyberpunk," captures this ability. It comes from ideas introduced by many science fiction authors including Isaac Asimov. He and many other science fiction writers prognosticate and imagine futures that include robotics, artificial intelligence, cybernetic devices, and supercomputing. Novels, films, and games take root in the society in new ways that begin to weave the arcane cyber world and the physical human world. The visualization of their interconnectivity becomes the user interfaces (UI).

UIs have many faces. Some earlier and crude versions by today's standards were bulletin board systems (BBSs) that gave a textual ASCII representation of information. BBS coding created character-by-character pictures and text via a command line. UIs represented the information beneath it, much like a stage, with certain mechanisms hidden from view and only available to backstage workers. Users, in some cases, challenged themselves to bypass security to discover hidden or inaccessible things. By trial and error, motivated by curiosity or ego, digital natives grew with their UIs.[22] Some more technically inclined, grew even more.

Coded to suit specific purposes, UIs correspond to the development of the technology behind them. Digital natives understand each of these developments.[23] Understanding each step, version, or modification gives digital natives a decisive edge over individuals who do not possess that familiarity. Since the Intel 8086 16-bit microprocessor, released in 1978, personal computers (PCs) supplanted terminals, that very limited UI imprisoned in a lab due to their attachments to a mainframe. PCs gave digital natives unfettered access to learning without being constrained by time or money. Malcolm Gladwell describes, in his book *Outliers,* that to become proficient, Bill Gates, too, needed a substantial amount of access to a terminal.[24]

As the PC came into homes, digital natives continued to press the boundaries of the technology. While one could purchase more software for his or her PC, the demand for connections to additional information sources ushered in the use of modems (modulator-demodulators). With increasing demand for higher baud rates, the limitation of finding cheap, high-noise, and ubiquitous copper twisted pair eventually gave way to LANs (local access networks) or alternatives like Direct Subscriber Lines (DSL). As the connections improved, so did the UIs. BBSs gave way to the internet and UIs now morphed into hypertext markup language (HTML) or graphical UIs (GUIs pronounced *gooey*), including many online games today. Those graphical representations pressed digital natives to understand their inner workings to both facilitate their needs and use them to their maximum potential, but not just any digital native; the nerdier ones.

Looking closer at GUIs designed for games, reveals a trend toward realism and instantaneous feedback. Games, ranging from first-person shooters (FPSs) and massive multiplayer online role-playing game (MMORPG or MMOs for short) become part of digital native thinking, interaction, and social communities like a soccer team. Some of the first FPS PC games were *Wolfenstein 3D*, released in 1992, shortly before the iconic *Doom*.[25] Those games featured a customizability that allowed the digital natives to alter the game slightly, to cheat, or to change the gameplay. Others popular games followed that allowed game hosting like *Quake* and *Half Life: Counterstrike* that continued this trend. [26]

Digital natives have grown with the expectation that GUIs can be modified, tailored, or cheated to support function of their choosing. With each game sequel, three-dimensional environments demanded more of the PC and its peripherals, allowing users to imagine a more complex environment, but the inner workings, principally, retained the same framework that allowed modifications, or "mods." One notable mod for *Quake II* named "Rocket Arena," written by David Wright, was so intensely popular that the sequel, *Quake III*, resembled the popular user-made mod, named *Quake III: Arena*. Digital natives were driving industry and industry formed a direct feedback loop with the consumers. In effect, digital natives

were unwitting or willing partners in mainstream technology. Digital natives had become a part of code development and showed that individual effort could outpace industry.

The film industry grew during those developments too and had an impact on digital natives as well. Movies inspired digital natives to seek out technology, and motivated them to create and interact using PCs. Movies like *Tron* (1982) predated the coming three-dimensional world and the alterations of code defining so much of that new UI. The story explored concepts of coding, intellectual property, gaming ego, mathematics and physics, and hardware-software-wetware interaction.[27] *Tron*, and others like *Wargames* (1983), became touchstones for the digital natives and cyber aficionados, geeks.

By 1985, these geeks thrust themselves into the cyberpunk literature and surrounded themselves in the latest technological developments. The culture embraced concepts of malleable GUIs and the hardware-software-wetware interaction. Cultural touchstones, like *Neuromancer* by William Gibson and *Snow Crash* by Neal Stephenson, offer examples of differing GUI techniques.[28] These touchstones and others form key components of their lexicon. The term "cyberspace" itself originated from *Neuromancer*. Geek language and common references form their cultural artifacts that are largely intellectual conceits, and therefore very powerful.[29] Vastly different from popular culture, forming the darker recesses of a complicated and highly-technical culture that could fix elevators, open electric cipher locks, and bypass coin operated public telephones, geeks could accomplish these feats later to become the driving forces of modernity. Military disrespect for geeks, stems from that time, reflecting society's view of them, which, when they were useful, was moderately palpable.

Geek culture socialized more via cyberspace. Movies like, *The Net* (1995), featuring Sandra Bullock, exemplify the geek tendency to shy away from personal interaction and prefer cyber interaction. From the perspective of war gaming and coding, multi-user dungeons (MUDs), available on BBSs originally, to MMOs today, geeks have learned to socialize through cyberspace during their pastimes, which formed key components of their identity.[30] Several MMOs emerged *Ultima Online* (1997),

Everquest (1999), and *World of Warcraft* (2004). Geeks involve themselves in collaborative ways to further their interests in games or other coding or gaming endeavors. Movies like *Hackers* (1995), *The Matrix* (1999), and *Black Hat* (2015) underscore a geek culture that thrives on online interaction and collaboration rather than face-to-face discourse. As geek culture revels more of iteself in cyberpunk literature and movies, their cultural artifacts do not necessarily include rituals and ceremonies, but intellectual motifs rooted in technological gains based on computer development. Not until the internet made this obsession global did the Marine Corps have to confront public aspirations that failed to align with the Marine Corps' typical view of a warfighter.

Is (identifying future cyber warriors)

Each generation imagines itself to be more intelligent than the one that went before it, and wiser than the one that comes after it.

-George Orwell Review of A Coat of Many Colours: Occasional Essays by Herbert Read, Poetry Quarterly (Winter 1945)

From usenet groups, to blogs, Twitter, Facebook, Pintrest, Reddit, Instagram, Orkut, Second Life, MySpace, LinkedIn, and many others, including online games, each social group forms a portion of a human identity, in the digital world.[31] They are projections of a human personality into cyberspace. Each venue provides the ability to create or perform actions or functions. In most cases the ability to conduct commonplace functions, like banking, requires an online identity. Other online functions focus more on one's ability to create and share, or stay in tune with a social network. Online identities are the expected. Even MySpace, whose accounts have fallen off over the years, had 300 million accounts in 2007.[32] These geek identities, however, do not typically align with that of the Marine Corps.

Geeks project themselves into cyberspace akin to cyberpunk heroes like *Johnny Mnemonic* or *Neo,* two films that defied norms accepted by too much of a non-thinking public. Even the user names or handles they use become the first representation of their identity – what they can do, and what they have done. For example, America Online and CompuServe were two of the first consumer available internet services that allowed for the creation of online identities. Those identities allowed the user to choose a user name. That user name did not have to be the actual name of the user but could resemble a "handle" or "callsign." Those identities became reflections of the user's personality, traits, or anonymizing representations of their actual self. Those identities were also replicable or reinventable. Identities in cyberspace are both true and false at the same time, which is a boon to geeks and a precious resource because they have the ability to deny, degrade, disrupt, and destroy information gathered passively and actively.

Marine Corps identity steeps itself in tradition. From the Marine Corps Hymn to the eagle, globe, and anchor insignia the Marine Corps surrounds itself with artifacts of its organizational culture. Schein describes organizational culture through observable events and underlying forces, including embedded skills and habits of thinking and linguistic paradigms.[33] In referring to high quality people as the foundation of Marine Corps readiness, Expeditionary Force 21 (EF21), the current mandate of the USMC's role going forward states, "Marines are forged in hard training, made wise through years of combat, and imbued with an expeditionary mindset."[34] That statement and the EF21 attributes, including the corresponding pictures, are foundational parts of the Marine Corps' vision. That message is also non-specific to cyber warfare. Besides planning for and expanding capabilities of as a necessary bow to an unavoidable reality, even if not understood since the portions devoted to cyber warfare direction and professionalization are pallid at best.

EF21 refers to cyberspace operations as a capability subset or capability within "Fires" but does not devote any of the 10 specific considerations of fires to cyberspace operations.[35] The C2 section refers briefly to cyberspace operations under the "Cyber Electromagnetic Warfare Coordination Cell" (CEWCC) but only within under the context of increased capability for reliable communications.[36] While occupying its own section, between C2 and Force Protection, "Cyberspace and the Electromagnetic Spectrum" may suggest that it is on par with other warfighting functions, amidst the overall "Focus Areas" which also include "Naval Integration" and "Seabasing". Most importantly, it offers no useful direction toward the professionalization of cyber warfare. The portion is but half a page, it is obfuscating, and it offers platitudes of "exploiting the porous nature of the domain," and "making use of…game-changing technologies…to stage operations…at the time and place of their choosing."[37] "Time and place of our choosing" is verbiage echoed from MCDP 1-3, *Tactics.*[38]

Every other warfighting section includes identity references for professionalization.[39] Maneuver refers to maneuver platforms, vehicles, teams, ranges, speeds, and training. Fires refers to systems, platforms, specialties, and new weapons. C2, force protection, logistics, and intelligence have references

too. Cyber warfare, though given a title as a domain and a section with the other warfighting functions, still lacks platforms, systems, training, or organizational structure. Providing geeks the opportunity to professionalize, through identities that the Marine Corps ascribes to, gives meaning and impact, which is essential for generating a strong cyber workforce. Malcolm Gladwell notes that giving meaning to work makes work preferable and significant when he writes, "It is not how much money we make that ultimately makes us happy…it's whether our work fulfills us…because there is complexity, autonomy, and a relationship between effort and reward in doing creative work, and that's worth more to most of us than money."[40]

Cyber warfare professionalization is difficult because its accomplishments have less visible effects than those of the real world. Recruiting videos for the Marine Corps often feature physical prowess, or sharply dressed Marines. The Marine Corps birthday messages, performed annually, honors Marines who have fought and died throughout its history, with emotive images of amphibious landings and combat on the battlefield. Executing offensive cyberspace operations (OCO) or defense cyberspace operations (DCO) do not yield the same kind of footage, if any at all, yet the results can be equally devastating and accomplished.

For example, the distributed denial of service (DDOS) attack on Hansapank, an Estonian bank, in 2007, or the DDOS on Georgian media during the Russian invasion of South Ossetia in 2008, both were massive and significant cyber operations.[41] Suspending judgment and connotation of those events, the geeks who executed the DDOS in each case receive no public credit, despite the magnitude and strategic implications of those actions. While attribution remains a difficult task for the international community and explains part of this neglect, geeks clearly have the ability to become influential warfighters.[42] Yet, the contribution of geeks may still not align with a uniformed image of a Marine.

Geeks among the civilian population who could be, cyber warfighters perceive a gap between them and the culture of the Marine Corps. Studies suggest that geeks more likely believe this statement:

"increased militarization of civilians in their tolerance of military matters but clear separation from matters military."[43] That suggestion offers a means to bridge the rift between the two cultures. Geeks may be best suited to work with the Marine Corps if they perceive that the Marine Corps promotes and encourages "thought diversity."[44]

Their goals for the defense of the nation align with senior generations, but geeks express that in thinking that is counterculture to current military culture. They, too, want to fight and win the nations wars. They support foreign policy goals like counter-proliferation and counter-terrorism.[45] Differently, however, they see opportunities like Black Hat and DEFCON conferences as enhancing workshops that promote cyber professionalism by providing a feedback loop to gain greater understanding of cyber warfare, especially on tactics, techniques, and procedures (TTPs) of adversaries – adversaries who commit acts against governmental systems and private systems alike. Geeks may embody other unconventional suggestions like including techy periodicals to supplement their self-education of examining leading theories, threats, and technologies.[46] In this cyber culture lies a budding warrior albeit one honing him or herself for the defense of the virtual world, now no longer a remote reality but indeed a domain needing this protection.

grep (seeing the cyber environment)

You know what you're trouble is? You're the kind who always reads the handbook. Anything people build, any kind of technology, it's going to have some specific purpose. It's for doing something that somebody already understands. But if it's new technology, it'll open areas nobody's ever thought of before. You read the manual, man, and you won't play around with it, not the same way. And you get all funny when somebody else uses it to do something you never thought of.

-William Gibson, Burning Chrome

While the Marine Corps accepts cyberspace as a domain, understanding the environment, the actors within, and the means by which one can affect both lacks clear definition. JP 3-12 *Cyberspace Operations* outlines, in broad terms, how cyberspace operations underpin each one of the six joint warfighting functions. It also identifies it as an "interdependent domain."[47] JP 3-12 also sorts geeks into a three-layer model.[48] That model correctly identifies, the geek, but oversimplifies the concept. It does not proffer any additional information on adversaries or potential adversaries in cyberspace, their proficiencies, or their motivations. Paul Rosenzweig breaks down that structure into more complicated but precise five-layer model showing how each person becomes a part of the internet.[49] These layers, constructed from the bottom up, are geographic, physical, logic, cyber, and persona. This abstraction is rather a grouping of each piece of what makes up the chain of actions that occur to create the time and space for a person to create an existence or projection into the internet. To understand a geek in cyberspace, and his or her modus operandi, one must thoroughly understand the supporting structure that made that actor possible in order to capitalize on talent or dissuade its effects.

The layers themselves are simple enough to understand, especially from a perspective of targeting. JP 3-12 discusses targeting, in terms those layers.[50] Using the five-layer model, one must understand the locations of the cyber equipment as the first layer. The second layer is its physical make up, which does not assume a time-space or distance relationship as a prerequisite. The third layer is the

logic, represented by the binary transmission, encoded, possibly encrypted, and traveling or stored geographically and physically. The fourth layer is the cyber persona or manifestation of the data projected by a person, where false projections, mirror images, unintentional representations, and pseudo-accurate renditions exist. The final layer is the person themselves, the human dimension. As MCDP 1 states, "no degree of technological development or scientific calculation will diminish the human dimension in war."[51]

MCDP 1 also characterizes physical, moral, and mental forces as imperatives to understanding war and adversaries.[52] In similar fashion, geeks can also be broken into three categories with varying degrees of professionalism and commitment to malicious acts.[53] The first group is often like that of digital natives who have expanded their grasp of coding and modification of computer utility. They are general computer hobbyists and amateurs who seek a personal challenge. The second group surpasses amateurs in their proficiency and problem solving, and money or revenge motivates them. The third and most dangerous are that of state and non-state actors who have not only the professionalism, but are also in the regular service of an employer to conduct espionage, sabotage, or censorship. The best cyber warfighters, for the Marine Corps, would fall into the third category of professionals, though their adversaries would fall into all three.

Without addressing legal ramifications or US code responsibilities, but addressing actions from all three types of geeks in order to understand their motivations, Paul Rosenzweig uses a pyramid to describe the varying degree of malicious acts occurring in cyberspace.[54] At the bottom of the pyramid are common instances of criminal acts, including cyber frauds, theft, and fraud. Higher on the pyramid is cyber espionage. Above that is cyber insurgency and at the top of the pyramid is cyber war. The pyramid reflects not only the frequency of the acts occurring, fewer at the top, but also the potential of those higher actions to cause harm to many. The pyramid demonstrates that each tier carries with it a valuation of the act committed, and of course, a criminal penalty if caught. Understanding the thinking of geeks reveals the ethos to which they ascribe themselves.

Onel de Guzman, in 2000, at 23 years old created one of the most destructive and simple malicious codes called the "Love Bug." The ILOVEYOU virus did an estimated $10 billion USD in damages.[55] The act itself resided primarily in the logic layer by taking advantage of Microsoft Windows' use of Visual Basic scripting, a language Microsoft created to allow developers to write programs for Windows. The geographic and physical were affected too, though not in a way that could do damage to their layer. Guzman was also of hobbyist to amateur level proficiency, motivated by revenge with more than just average cyber skills. Investigators speculated that his actions were for retribution against his college who rejected his undergraduate thesis, which was a proposal for people to receive free internet.[56] His desire for free internet underscores both the desire for personal gain and revenge, and espouses a key component of digital natives' most sacrosanct beliefs: internet should be free for all.

From the earliest beginnings of the internet, its advocates have argued for an "open internet."[57] The belief that information should be free, regardless of viewpoint, is a fundamental pillar of information. Vint Cerf, considered the father of the internet, envisioned an internet of complete transparency.[58] The Department of Defense (DoD), with its classifications of information, comes in great contrast to forming a potential rift between those who believe in information for all, and those who believe that some information needs to be protected.

With the anonymity that cyberspace brings one, if one wanted to read "The Anarchist's Cookbook," read reviews on the best local abortion clinics, or watch some esoteric pornography, one could and should have that option, according to the principles that cyberspace was founded upon. Thus, in its purist form, the internet has grassroots in democracy as part of its design.[59] That ethos supports the belief that music is art and art is free, thus music should be free. No different that visiting the pyramids of Giza, Great Wall of China, or Machu Picchu, digital natives see the world as a creative construct to be experienced and then, in Facebook or Instagram fashion, liked or disliked. That ethos is to remain true to two things: the purest form of freedom of speech or expression, and promotion of the betterment and improvement of the former. Both are value judgments though still have polarizing effects.

Hackers defined the original ethos despite any misunderstandings in connotation of the term "hacker." At one point, "cracker" had indicated nefarious or unlawful action by hackers, though over time journalists have obviated the term.[60] Today, few are familiar with the term "grey hat," a portmanteau of a "white hat" and "black hat" – white hats being hackers who perform cyber security analysis for organization. Grey hats are those who have dabbled on both sides for proficiency, employment, personal gain, personal betterment, abandonment, or respect for legality of their actions. The difference between the two is a difference of perspective, which poses a difficult task for the Marine Corps and other cyber organizations within the DoD.

It is important to understand that hacking originally received its definition in the 1950s when an MIT model railroad club received a donation of telephone equipment. They needed to control the railroad through a combination of hardware and software engineering. Reverse engineering the systems and redesigning switches, offered new ways to manipulate the track, thus "hacking."[61] Rooted in computer and electronic engineering, the culture that emerged was one that attempted to solve a problem. Within the solution, hackers found two characteristics: its efficacy and its efficiency. The two measures became the unwritten stigma that hackers prided themselves on.[62] In essence, two hackers could write code to achieve a goal, but the more concise code was better, as with mouse traps and good writing. Opportunity existed for any new coder to attempt to oust the reigning code. This ethos gave a hacker esteem and status. One must code to appreciate fully the elegance and splendor that concise and effective code brings. The skills of the culture originate in computer science and engineering, electrical engineering, and systems engineering. These backgrounds and penchants for gear from Radio Shack and the best programming solution predispose one to become a geek hobbyist and amateur, the pool from which professional geeks matriculate.

kill (how do we bridge the gap)

Any sufficiently advanced technology is indistinguishable from magic.

-Arthur C. Clarke, Profiles of the Future

In the 1920s and 30s the Marine Corps adapted techniques for amphibious warfare that became critical for the success of the Pacific Campaign in WWII. MCDP 1-3 recognizes this astute fact and implores its readers to challenge doctrine and promote the evolution of warfare.[63] Yet cyber warfare and the Marine Corps share few common cultural commonalties. Culture change mechanisms, based on Edgar Schein's research, suggest that the Marine Corps is in the "Founding and Early Growth" stages of professionalization of cyber warfare.[64]

MCDP 1 states that, "As military professionals charged with the defense of the Nation, Marine leaders must be true experts in the conduct of war."[65] MCDP 1 also calls for a three-tiered approach to training a leader: an apprenticeship where they learn their trade at a tactical level, a master where they apply broader operational level understanding, and a senior level where they integrate the MAGTF into joint and multinational warfighting capabilities.[66] MCDP 1 further states that, "we should recognize that all Marines of a given grade and occupational specialty are not interchangeable," highlighting that specialties are necessary and specific.[67] Thus as each general was once a lieutenant, MCDP 1 suggests that generals are the summation of tactical, operational, and strategic expertise. Yet, Generals in charge of cyber defense are working without the benefit of a career of cyber experience. Worse, they are personifying the generation and cultural gap.

There are no force generation models that support the development of an officer or enlisted Marine to become a cyber-defense general. Many individuals share a belief that cyber warfare could and should be an adaptation of our current cyber force generation. According to former Marine Forces Cyber Command (MARFORCYBER) Chief of Staff Colonel Steve Zotti, "We may look at some MOS

designations, at what the structure should look like but there's [sic] really no new skill sets we weren't already doing."[68] While Lieutenant General George Flynn called cyberspace a "domain" and the "newest and possibly most complicated we must now dominate," there have been no major movements to identify, select, recruit, and channel an MOS for cyber warfare. These remarks come in stark contrast to MCDP 1-3 *Tactics*' suggestion that, "No amount of technology can reduce the human dimension… [It] must be based on human characteristics rather than on equipment or procedures."[69]

Instead, what Colonel Zotti and perhaps other senior leaders appear to suggest is that warfighting in the cyber domain takes no specialized experience to have developed from, or to lead. Gregory Conti and David Raymond suggest the opposite, that "leading cyber warriors takes a different type of leader, one who is comfortable in the inherently technical cyber domain, appreciates technical expertise, and understands the personality types, creativity, culture, motivations, and intellectual capability of cyber warriors."[70] If the Marine Corps expects a junior officer to develop and execute a training plan for their MOS, they should also be able to inspect, monitor, and coach Marines, in the proficiency of that MOS.[71] According to MCRP 3-0A *Unit Training Management (UTM) Guide,* "All leaders are considered trainers and coaches."[72] Career progression should reflect this.

Marine Corps culture needs to spur enough momentum to address personnel, training, and organizational solutions to maximize the intellectual capital of the rising generation[s], and vectoring the cyber defense force along coherent national lines of effort. Identifying individuals who already have a bachelor's of science in science, technology, mathematics, and engineering (STEM), a line of study identifying those preferring computer engineering and electrical engineering, the step can provide a base from which to develop a long-term cyber workforce strategy.[73] Identifying talent in those who would succeed in an MOS is something the Air Force implemented with success in undergraduate pilot training (UPT) because the "foundation provides the prerequisite grounding in the immutable fundamentals of cyber operations and prepares cyber officers for the challenges of an uncertain future."[74] This is a core component of education, different from training.

Training, as Kamal Jabbour notes, "provides Airmen with proficiency to operate current tools, whereas education builds a foundation that prepares officers to deal with uncertain future challenges."[75] The Air Force makes the distinction between training and education, and the Marine Corps' approach is similar but mixes terms of training and education, which may undermine the intensive study required to prepare a cyber warfighter adequately. In the UTM, it identifies that skills are the "cumulative effect of training," indicating that performance is based on preparation of a series of steps or drills.[76] From Marine Corps Order (MCO) 1553.1B, education is specifically defined and separated from training, as the "process of moral and mental development; the drawing out of students to initiate the learning process and bring their own interpretations to bear-the product of which is a creative mind."[77] General Al Gray, widely considered the father of modern Marine Corps training and education, when he signed that order in 1991, was encouraging the growth of intellect to satisfice the uncertain future battlefields that were emerging and professionalize. The Marine Corps does promote freethinking, creativity, self-study, and problem solving. Where it again confuses understanding of professional performance is in "traits."

MCO 1553.1B does note that "Essential Skills Training" is that which "promotes the practice of those personal and professional traits that distinguish them as Marines."[78] These traits bind Marines of all MOSs together as *Marines*. MCO 1553.1B does not encompass academic or undergraduate degrees that may make an effective cyber warfighter. There are efforts to develop a hybrid solution. Major General O'Donohue testified that MARFORCYBER is investing in a web-based training hosted by Carnegie-Mellon University Software Engineering Institute, a leading computer science and engineering school, to train and develop Marines and enhance MOS proficiency.[79]

Like Scharnhorst, Major General O'Donohue has begun to promote the professionalization of a new arm within the Marine Corps. From the 1840s, Scharnhorst, while at Wilhelmstein, learned that the "process of development could not be mastered by simply learning existing techniques," and "the methods of organizing and equipping, educating and training a military force were intimately related to the entire cultural pattern of society."[80] Adapting and adopting societal and cultural changes for cyber

warfare is imperative to effective warfighting. Even in Scharnhorst's time, mathematics, physics, chemistry, engineering, economics, geography, and languages, were appropriate and necessary for developing well-trained leaders.[81] With such highly-technical subjects, that academia deems to require at least a four-year degree to become proficient, and something industry considers "entry-level," web-based training for part-time students while executing duties at MARFORCYBER, may be the first bridge across the gap to forming a strong cyber workforce.

exit (conclusion)

I used to think that cyberspace was fifty years away. What I thought was fifty years away was only ten years away. And what I thought was ten years away… it was already here. I just wasn't aware of it yet.

-Bruce Sterling

While current military force generation models lack progression for cyber warriors, they more importantly fail to address the culture of cyberspace, which, like military aviation, has its own unique attractions and stigma associated with it. Schein suggests that culture is "an abstraction, yet the forces that are created in social and organizational situations deriving from culture are powerful."[82] Each culture surrounds itself with three levels of culture: artifacts, espoused beliefs and values, and basic underlying assumptions.[83] For geeks, those ideas and culture come from a myriad of science fiction literature, journals, and even Hollywood cyber cult classics.[84]

Perhaps MARFORCYBER is already implementing many of these changes, unseen by the public. Clarke suggests that such is the case, but also that while we understand the demand for more cyber security our mitigation of cyber threats is still lacking.[85] Regardless, USMC strategies to force readiness need to account for the rapid growth of technology and promote a development of benefiting the service.

Cyberspace is a canvas. It is expanding, and painted over constantly. Digital natives know this and are eager to make their mark on it, if given the opportunity, geeks especially. As digital immigrants, senior officers and strategists see things through an entirely different lens, one that fundamentally separates the cyber world from that of the real. Digital natives, are yet to or still are learning the basics of warfighting and as future cyber warfighters, both parties need to work together with their leaders to dissolve the gap that separates them. But the USMC, to be ready for the cyber conflicts of the future, probably need geeks more than the geeks need the USMC.

While there will always be generational gaps between seniors and subordinates, the key recognition is that cyberspace underpins every aspect of the real world. A failure to understand the governing principles, both spoken and unspoken, hardwired and coded, of cyberspace breeds a profound distrust in its uses and mistrust in those who are proficient at using them. Digital natives find the changes of human relationships due to cyberspace second nature.[86] For geeks, it is doubly so, and today, digital natives and immigrants alike are unwitting participants in cyberspace. Digital immigrants struggle to understand this connection, let alone start acting to capitalize on that reality.

Laced with policy and strategy, the Marine Corps leadership's bid for success in the cyber domain lays within the professionalization of cyber warfare. Scharnhorst called it, *Bildungsprinzip*, or the "rigorous process to identify, select, train, and educate the best minds."[87] It requires a heavy background of STEM and a personal professional education program that includes a heavy emphasis on non-traditional DoD affairs that merge academia and industry. Potential hires are too often counter-culture to the Marine Corps and may not embody the traits of a typical recruit, capable of running a physical fitness test to the satisfaction of his or her recruiter.

Pilots already benefit a model for screening individuals with testing and examination. UPT for the Air Force includes rigorous screening, and Naval Aviation is no different. Prospective naval aviators take an Aviation Selection Test Battery (ASTB) that assesses their math skills, reading comprehension, mechanical comprehension, aviation and nautical information, Naval Aviation traits, performance based measures, and biographical inventory.[88] Like prospective pilots, prospective cyber warriors should have a requirement for an undergraduate degree in computer, electrical, or systems engineering, and complete a selection test battery. With bonuses, like those already offered to enlisted Marines, these adaptations could form a stronger cyber workforce to promote recruitment and retention.[89] Conti also compares Google's effort to do the same, using the "Google Aptitude Test," but for this there must be a screened and channeled MOS.[90]

Science fiction set lofty goals for society – many of which have come true. Digital natives and geeks especially know this. First seen in and Stanley Kubrick's film and adaptation of Arthur C. Clarke's *2001: A Space Odyssey* (1968), video calls are now a thing of science fact, made possible by technologies like Skype that ride on the backbone of a robust network of high-bandwidth fiber optic cables, microwave towers, and satellite links. With each iteration of technological advancement, users and especially geeks, embroiled themselves in the version changes and upgrades. Knowing these steps gives them a decisive advantage to knowing and understanding the seams and exploitable gaps in technology. The ability to execute effective DCO and OCO stems from this knowledge. One cannot gain knowledge that requires more than four years of undergraduate study in on-the-job training in a three to four-year duty station. Predisposition to electrical and computer problem solving may be an inherent trait of only certain individuals, like geeks. The adaptation and adoption has begun and needs to continue, with the development of a fully professionalized cyber workforce. One can conjure a clichéd image of a naval aviator and a geek. Marine Corps leaders now need to conjure an image of what that geek looks like in uniform.

Conti is correct in believing that the Marine Corps and others need to address the way that they "leverage the talent."[91] Geeks are the kind of potential Marines who can fix your garage door opener with the same skill as they can figure out why the battery on your mobile phone drains too quickly. They are adept at the mesh between electronic devices and the coding that dances within them and the airwaves they ride on. They see no difference in electronic warfare, information warfare, and cyberspace – they are all connected, they are all part of resonant waves, oscillated to form squares, saws, or sines, through the air and cables. Geeks understand that oscillations are vibrations, no different from a voice, and that languages are encoding, cipher are encryption, and reverse engineering is the key to engineering a solution. Alan Turing knew that, and he certainly did not fit into mainstream culture, but he is one of the greatest geek success stories to date for the military. Perhaps if the Marine Corps could find a place for more Alan Turing's, it would suddenly possess more solutions than not to problems it has yet to identify.

Even without Turing, the Marine Corps leaders need analyze the spectrum of talent and raise their threshold for talent to be able to see the freaks that matter (geeks), from the noise.

Notes

[1] Gregory Conti and Jen Easterly, "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture." (*Small Wars Journal,* 2010), 5.

[2] Marine Corps Order 1200.17E Military Occupational Specialties Manual Aug 08 2013

[3] Daniel J. O'Donohue, Major General. "Operationalizing Cyberspace for the Services." *House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities.* Washington, D.C.: First Session, 114th Congress. March 4, 2015).

[4] Headquarters U.S. Marine Corps, *Expedtionary Force 21.* (Washington, D.C.: United States Marine Corps, March 4, 2014), 35.

[5] Department of Defense. *Joint Publication 3-13: Information Operations.* (Washington, D.C.: Department of Defense, 2012)

[6] John Palfrey and Urs Gasser, *Born Digital: Understanding the First Generation of Digital Natives.* (New York: Basic Books, 2008), 1-4.

[7] John Palfrey and Urs Gasser, *Born Digital: Understanding the First Generation of Digital Natives.* (New York: Basic Books, 2008), 14.

[8] J. R. Wilson, "MARFORCYBER: Marines Fight in a New Domain." (*Marine Corps Outlook,* 2012) 50-53.

[9] John Palfrey and Urs Gasser, *Born Digital: Understanding the First Generation of Digital Natives.* (New York: Basic Books, 2008), 12-15.

[10] John Palfrey and Urs Gasser, *Born Digital: Understanding the First Generation of Digital Natives.* (New York: Basic Books, 2008), 111-130

[11] Orson Scott Card, *Ender's Game.* (New York: Tom Doherty Associates, LLC., 1977).

[12] *Star Trek II: Wrath of Khan*, Film, directed by Nicholas Meyer, (1982; Hollywood, CA; Paramount Pictures; 1982).

[13] Gregory Conti, James Caroland, Thomas Cook, and Howard Taylor. 2011. "Self-Development for Cyber Warriors." (*Small Wars Journal*, 2011), 7.

[14] SWJ

[15] John Palfrey and Urs Gasser, *Born Digital: Understanding the First Generation of Digital Natives.* (New York: Basic Books, 2008), 5-13.

[16] Morten G. Ender, David E. Rohall, and Michael D. Matthews, *The Millennial Generation and National Defense: Attitudes of Future Military and Civilian Leaders.* (New York: Palgrave Macmillan, 2014), 3.

[17] Morten G. Ender, David E. Rohall, and Michael D. Matthews, *The Millennial Generation and National Defense: Attitudes of Future Military and Civilian Leaders.* (New York: Palgrave Macmillan, 2014), 4.

[18] Morten G. Ender, David E. Rohall, and Michael D. Matthews, *The Millennial Generation and National Defense: Attitudes of Future Military and Civilian Leaders.* (New York: Palgrave Macmillan, 2014), 4.

[19] Morten G. Ender, David E. Rohall, and Michael D. Matthews, *The Millennial Generation and National Defense: Attitudes of Future Military and Civilian Leaders.* (New York: Palgrave Macmillan, 2014), 52.

[20] Morten G. Ender, David E. Rohall, and Michael D. Matthews, *The Millennial Generation and National Defense: Attitudes of Future Military and Civilian Leaders.* (New York: Palgrave Macmillan, 2014), 56.

[21] John Palfrey and Urs Gasser, *Born Digital: Understanding the First Generation of Digital Natives.* (New York: Basic Books, 2008), 5-6.

[22] John Palfrey and Urs Gasser, *Born Digital: Understanding the First Generation of Digital Natives.* (New York: Basic Books, 2008), 111-130.

[23] John Palfrey and Urs Gasser, *Born Digital: Understanding the First Generation of Digital Natives.* (New York: Basic Books, 2008), 185-208.

[24] Malcolm Gladwell, *Outliers: The Story of Success.* (New York: Little, Brown and Company, 2008), 51-58.

[25] Edward F. Halpin, Philippa Trevorrow, David Webb, and Steve Wright, *Cyberwar, Netwar and the Revolution in Military Affairs.* (Palgrave Macmillan, 2006), 14.

[26] Edward F. Halpin, Philippa Trevorrow, David Webb, and Steve Wright, *Cyberwar, Netwar and the Revolution in Military Affairs.* (Palgrave Macmillan, 2006), 20.

[27] Gregory Conti, James Caroland, Thomas Cook, and Howard Taylor. 2011. "Self-Development for Cyber Warriors." (*Small Wars Journal*, 2011), 20-21.

[28] Gregory Conti, James Caroland, Thomas Cook, and Howard Taylor. 2011. "Self-Development for Cyber Warriors." (*Small Wars Journal*, 2011), 8-9.

[29] Edgar H. Schein, *Organizational Culture and Leadership.* (San Francisco: Jossey-Bass, 2010), 23-25.

[30] John Palfrey and Urs Gasser, *Born digital: understanding the first generation of digital natives.* (New York: Basic Books, 2008), 26-29, 35.

[31] John Palfrey and Urs Gasser, *Born Digital: Understanding the First Generation of Digital Natives.* (New York: Basic Books, 2008), 19-23.

[32] Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz,*Cyberpower and National Security.* (Dulles: National Defense University Press and Potomac Books Inc., 2009), 168.

[33] Edgar H. Schein, *Organizational Culture and Leadership.* (San Francisco: Jossey-Bass, 2010), 15.

[34] Headquarters U.S. Marine Corps, *Expedtionary Force 21.* (Washington, D.C.: United States Marine Corps, March 4, 2014), 44.

[35] Headquarters U.S. Marine Corps, *Expedtionary Force 21.* (Washington, D.C.: United States Marine Corps, March 4, 2014), 33.

[36] Headquarters U.S. Marine Corps, *Expedtionary Force 21.* (Washington, D.C.: United States Marine Corps, March 4, 2014), 34-35.

[37] Headquarters U.S. Marine Corps, *Expedtionary Force 21.* (Washington, D.C.: United States Marine Corps, March 4, 2014), 35.

[38] Headquarters Marine Corps, *MCDP 1-3, Tactics.* (Washington, D.C.: United States Marine Corps, July 30, 1997), 119.

[39] Headquarters U.S. Marine Corps, *Expedtionary Force 21.* (Washington, D.C.: United States Marine Corps, March 4, 2014), 29-45.

[40] Malcolm Gladwell, *Outliers: The Story of Success.* (New York: Little, Brown and Company, 2008), 149-150.

[41] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It.* (New York: Harper-Collins Publishers, 2010), 13-18.

[42] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It.* (New York: Harper-Collins Publishers, 2010), 213-215.

[43] Morten G. Ender, David E. Rohall, and Michael D. Matthews, *The Millennial Generation and National Defense: Attitudes of Future Military and Civilian Leaders.* (New York: Palgrave Macmillan, 2014), 56.

[44] Morten G. Ender, David E. Rohall, and Michael D. Matthews, *The Millennial Generation and National Defense: Attitudes of Future Military and Civilian Leaders.* (New York: Palgrave Macmillan, 2014), 56.

[45] Morten G. Ender, David E. Rohall, and Michael D. Matthews, *The Millennial Generation and National Defense: Attitudes of Future Military and Civilian Leaders.* (New York: Palgrave Macmillan, 2014), 54.

[46] Gregory Conti, James Caroland, Thomas Cook, and Howard Taylor. 2011. "Self-Development for Cyber Warriors." (*Small Wars Journal*, 2011), 9-19.

[47] Department of Defense, *Joint Publication 3-12: Cyberspace Operations.* (Washington, D.C.: Department of Defense, Februrary 5, 2013), viii, I-2.

[48] Department of Defense, *Joint Publication 3-12: Cyberspace Operations.* (Washington, D.C.: Department of Defense, Februrary 5, 2013), I-2-4.

[49] Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and the World.* (Santa Barbara: Praeger, 2013), 19-20.

[50] Department of Defense, *Joint Publication 3-12: Cyberspace Operations.* (Washington, D.C.: Department of Defense, Februrary 5, 2013), IV-3.

[51] Headquarters Marine Corps, *MCDP 1, Warfighting.* (Washington, D.C.: United States Marine Corps, June 20, 1997), 14.

[52] Headquarters Marine Corps, *MCDP 1, Warfighting.* (Washington, D.C.: United States Marine Corps, June 20, 1997), 15.

[53] Edward F. Halpin, Philippa Trevorrow, David Webb, and Steve Wright, *Cyberwar, Netwar and the Revolution in Military Affairs.* (Palgrave Macmillan, 2006), 42.

[54] Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and the World.* (Santa Barbara: Praeger, 2013), 15-16.

[55] Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, *Cyberpower and National Security.* (Dulles: National Defense University Press and Potomac Books Inc, 2009), 167.

[56] Mark Landler, *A Filipino Linke to "Love Bug" Talks about His License to Hack.* (Manila, October 21, 2000)

[57] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It.* (New York: Harper-Collins Publishers, 2010), 275.

[58] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It.* (New York: Harper-Collins Publishers, 2010), 275.

[59] Thomas Homer-Dixon, *The Ingenuity Gap*. (New York: Alfred A. Knopf, 2000), 360.

[60] Jon Erickson, *Hacking: The Art of Exploitation.* (San Francisco: No Starch Press, 2003), 3.

[61] Jon Erickson, *Hacking: The Art of Exploitation.* (San Francisco: No Starch Press, 2003), 2.

[62] Jon Erickson, *Hacking: The Art of Exploitation.* (San Francisco: No Starch Press, 2003), 2.

[63]Headquarters Marine Corps, *MCDP 1-3, Tactics.* Washington, D.C.: United States Marine Corps, July 30, 1997), 82.

[64] Edgar H. Schein, *Organizational Culture and Leadership.* (San Francisco: Jossey-Bass, 2010), 273-274.

[65] Headquarters Marine Corps, *MCDP 1, Warfighting.* (Washington, D.C.: United States Marine Corps, June 20, 1997), 56.

[66] Headquarters Marine Corps, *MCDP 1, Warfighting.* (Washington, D.C.: United States Marine Corps, June 20, 1997), 62.

[67] Headquarters Marine Corps, *MCDP 1, Warfighting.* (Washington, D.C.: United States Marine Corps, June 20, 1997), 64.

[68] J. R. Wilson, "MARFORCYBER: Marines Fight in a New Domain." (*Marine Corps Outlook,* 2012) 50-53.

[69] Headquarters Marine Corps, *MCDP 1, Warfighting.* (Washington, D.C.: United States Marine Corps, June 20, 1997), 78.

[70] Gregory Conti and David Raymond, "Leadership of Cyber Warriors: Enduring Principles and New Directions." *Small Wars Journal,* 2011), 1.

[71] MCWP – Systems Approach to Training

[72] *MCRP 3-0A, Unit Training Management Guide.* (Washington, D.C.: United States Marine Corps, November 25, 1996), 1-2.

[73] Kamal Jabbour,"Cyber Vision and Cyber Force Development." (*Strategic Studies Quarterly*, 2010), 69.

[74] Kamal Jabbour,"Cyber Vision and Cyber Force Development." (*Strategic Studies Quarterly*, 2010), 71.

[75] Kamal Jabbour,"Cyber Vision and Cyber Force Development." (*Strategic Studies Quarterly*, 2010), 70.

[76] *MCRP 3-0A, Unit Training Management Guide.* (Washington, D.C.: United States Marine Corps, November 25, 1996), 4-1.

[77] *Marine Corps Orders 1553.1B, The Marine Corps Training and Education System.* (Washington, D.C.: United States Marine Corps, May 24, 1991).

[78] *Marine Corps Orders 1553.1B, The Marine Corps Training and Education System.* (Washington, D.C.: United States Marine Corps, May 24, 1991).

[79] Daniel J. O'Donohue, Major General. "Operationalizing Cyberspace for the Services." *House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities.* Washington, D.C.: First Session, 114th Congress. March 4, 2015).

[80] Charles Edward White, *The Enlightened Soldier: Scharnhorst and the Militärische Gesellschaft in Berlin, 1801-1805*. (Westport: Praeger Publishers, 1989), 5-6.

[81] Charles Edward White, *The Enlightened Soldier: Scharnhorst and the Militärische Gesellschaft in Berlin, 1801-1805*. (Westport: Praeger Publishers, 1989), 6.

[82] Edgar H. Schein, *Organizational Culture and Leadership.* (San Francisco: Jossey-Bass, 2010), 7.

[83] Edgar H. Schein, *Organizational Culture and Leadership.* (San Francisco: Jossey-Bass, 2010), 24.

[84] Gregory Conti, James Caroland, Thomas Cook, and Howard Taylor. 2011. "Self-Development for Cyber Warriors." (*Small Wars Journal*, 2011), 1.

[85] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It.* (New York: Harper-Collins Publishers, 2010), 44-47.

[86] John Palfrey and Urs Gasser, *Born Digital: Understanding the First Generation of Digital Natives.* (New York: Basic Books, 2008), 4.

[87] Charles Edward White, *The Enlightened Soldier: Scharnhorst and the Militärische Gesellschaft in Berlin, 1801-1805*. (Westport: Praeger Publishers, 1989), 176.

[88] Headquarters Marine Corps, *Marine Corps Order 1532.1, U.S. Navy and Marine Corps Aviation Selection Test Battery*. (Washington, D.C.: United States Marine Corps, March 13, 2008).

[89] Daniel J. O'Donohue, Major General. "Operationalizing Cyberspace for the Services." *House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities.* Washington, D.C.: First Session, 114th Congress. March 4, 2015).

[90] Gregory Conti and Jen Easterly, "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture." (*Small Wars Journal*, 2010), 3.

[91] Gregory Conti and Jen Easterly, "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture." (*Small Wars Journal*, 2010).

Works Cited

Card, Orson Scott. 1977. *Ender's Game.* New York: Tom Doherty Associates, LLC.

Clarke, Richard A., and Robert K. Knake. 2010. *Cyber War: The Next Threat to National Security and What to do About It.* New York: Harper-Collins Publishers.

Conti, Gregory, and David Raymond. 2011. "Leadership of Cyber Warriors: Enduring Principles and New Directions." *Small Wars Journal* 1-10.

Conti, Gregory, and Jen Easterly. 2010. "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture." *Small Wars Journal* 1-11.

Conti, Gregory, James Caroland, Thomas Cook, and Howard Taylor. 2011. "Self-Development for Cyber Warriors." *Small Wars Journal* 1-34.

Crosston, Matthew. 2012. "Virtual Patriots and a New American Cyber Strategy: Changing the Zero-Sum Game." *Strategic Studies Quarterly* 100-118.

Department of Defense. 2013. *Joint Publication 3-12: Cyberspace Operations.* Washington, D.C.: Department of Defense.

Department of Defense. 2012. *Joint Publication 3-13: Information Operations.* Washington, D.C.: Department of Defense.

Ender, Morten G., David E. Rohall, and Michael D. Matthews. 2014. *The Millennial Generation and National Defense: Attitudes of Future Military and Civilian Leaders.* New York: Palgrave Macmillan.

Erickson, Jon. 2003. *Hacking: The Art of Exploitation.* San Francisco: No Starch Press.

Gibson, William. 1984. *Neuromancer.* New York: Penguin Putnam.

Gladwell, Malcolm. 2008. *Outliers: The Story of Success.* New York: Little, Brown and Company.

Halpin, Edward F., Philippa Trevorrow, David Webb, and Steve Wright. 2006. *Cyberwar, Netwar and the Revolution in Military Affairs.* Palgrave Macmillan.

Headquarters U.S. Marine Corps. March 4, 2014. *Expedtionary Force 21.* Washington, D.C.: United States Marine Corps.

Headquarters U.S. Marine Corps. August 08, 2013. *Marine Corps Order 1200.17E, Military Occupational Specialties Manual.* Washington, D.C.: United States Marine Corps.

Headquarters U.S. Marine Corps. March 13, 2008. *Marine Corps Order 1532.1, U.S. Navy and Marine Corps Aviation Selection Test Battery.* Washington, D.C.: United States Marine Corps.

Headquarters U.S. Marine Corps. May 24, 1991. *Marine Corps Order 1553.1B, The Marine Corps Training and Education System.* Washington, D.C.: United States Marine Corps.

Headquarters U.S. Marine Corps. June 20, 1997. *MCDP 1, Warfighting.* Washington, D.C.: United States Marine Corps.

Headquarters U.S. Marine Corps. July 30, 1997. *MCDP 1-3, Tactics.* Washington, D.C.: United States Marine Corps.

Headquarters U.S. Marine Corps. November 25, 1996. *MCRP 3-0A, Unit Training Management Guide.* Washington, D.C.: United States Marine Corps.

Headquarters U.S. Marine Corps. November 25, 1996. *MCRP 3-0B, How to Conduct Training.* Washington, D.C.: United States Marine Corps.

Homer-Dixon, Thomas. 2000. *The Ingenuity Gap.* New York: Alfred A. Knopf.

Jabbour, Kamal. 2010. "Cyber Vision and Cyber Force Development." *Strategic Studies Quarterly* 63-73.

Janczewski, Lech J., and Andrew M. Colarik. 2008. *Cyber Warfare and Cyber Terrorism.* Hershey: Information Science Reference.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. 2009. *Cyberpower and National Security.* Dulles: National Defense University Press and Potomac Books Inc.

Landler, Mark. 2000. *A Filipino Linke to "Love Bug" Talks about His License to Hack.* Manila, October 21.

Lubin, Andrew. 2013. "Marine Forces Cyber: Protecting the Corps." *Marine Corps Gazettle* 22-24.

O'Donohue, Daniel J., Major General. March 4, 2015. "Operationalizing Cyberspace for the Services." *House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities.* Washington, D.C.: First Session, 114th Congress. 7.

Palfrey, John, and Urs Gasser. 2008. *Born Digital: Understanding the First Generation of Digital Natives.* New York: Basic Books.

Rosenzweig, Paul. 2013. *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and the World.* Santa Barbara: Praeger.

Schein, Edgar H. 2010. *Organizational Culture and Leadership.* San Francisco: Jossey-Bass.

*Star Trek II: Wrath of Khan.*Film. Directed by Nicholas Meyer. 1982; Hollywood, CA; Paramount Pictures; 1982.

Stephenson, Neal. 1992. *Snow Crash.* New York: Random House.

White, Charles Edward. 1989. *The Enlightened Soldier: Scharnhorst and the Militärische Gesellschaft in Berlin, 1801-1805.* Westport: Praeger Publishers.

Wilson, J. R. 2012. "MARFORCYBER: Marines Fight in a New Domain." *Marine Corps Outlook* 50-53.