U.S. Special Operations Forces in Cyberspace

Colonel Patrick M. Duggan

with special contributions from
Elizabeth Oren

Cyberspace is a human space, as dynamic and uncertain as human nature. No longer simply a technical abstraction or manmade domain unto itself,[1] cyberspace is a growing facet of every-day life that increasingly cuts across all aspects of Special Operations. Cyber is a dynamic space, a global commons of human practice, which embodies the actions, behaviors, and decisions of man. Cyber is also an uncertain space; and although, its future impact to our national security is yet to be determined, it is clearly a space where United States Special Operations Forces (USSOF) have an increasing role in shaping the final outcome. Ultimately, cyber is a human enterprise which empowers and entangles countless global interactions,[2] and is rapidly becoming a preeminent space where human conflicts, and thus USSOF, must play a part.

Cyberspace

The enigma of cyberspace is in its contradictions. Cyber is both everywhere and nowhere at the same time, casting an invisible, yet powerful influence, which brings both comfort and stress to every-day life. On one hand, cyberspace helps foster human prosperity by flattening opportunities and improving quality of life. On the other hand, cyberspace inflames ethnic and religious tensions, sows dissent, and causes suffering. It is in these contradictions where cyberspace is most like human nature, and it is in these same spaces, both challenges and opportunities exist for USSOF.

Cloaking their roles and obscuring their actions, adversaries are increasingly exploiting the shadows of cyberspace to attack US national security interests. Ranging from lone cyber-terrorists, to state-sponsored cyber-units, adversaries use cyberspace's low barriers of entry, difficult attribution, and lack of clear borders for battle[3] to conceal their reckless ambitions. Fortunately, while adversaries may exploit cyber to strike from the shadows, it is in these same shadows USSOF must pursue, to help illuminate, uncover, and counter the growing array of technologically-savvy threats plaguing our nation.

Colonel Patrick Duggan is the Commander of Joint Base Myer-Henderson Hall in Washington D.C. He is a career Special Forces Officer, and participated in both invasions of Afghanistan and Iraq, and commanded Special Operations deployments across the Middle East and Asia. A Certified Information Systems Professional (CISSP), COL Duggan has authored numerous articles about Cyber-Special Operations in Joint Defense Quarterly, Special Warfare Magazine, Small Wars Journal, and The Cyber Defense Review, and is the recipient of the 2015 Chairman of the Joint Chiefs of Staff Strategic Research and National Security Award for his paper, *Strategic Development of Special Warfare in Cyberspace*. COL Duggan is a 2+/2+ Arabic speaker with varying proficiency in Tagalog, French, and Spanish.

National Cyber Roles

The Commander of the United States Cyber Command and Director of the National Security Agency, Admiral Mike Rogers, recently wrote that "No single entity has all the necessary insight, authorities, capabilities, or resources to protect and defend US and allied interests in cyberspace," [4] and I couldn't agree with him more. Cyberspace is not just an intelligence or communications thing; it is an 'everybody thing.' This includes the way in which we marshal the talent and intellect of our military, interagency, and private sector leaders, to build whole-of-nation strategies to protect the US.

The ubiquity of cyberspace means that no single US Agency, Department, or Service Component owns the market on good ideas, so it is imperative that we harness our country's diverse experience, amongst all institutions, to promote ever-adaptive strategies which secure our nation. We must also seek and examine new concepts, processes, and approaches to deal with these dynamic challenges, and each does our individual part, in a collective contribution to our national defense.

Special Operations Forces (SOF's) National Contribution

Part of SOF's contribution to confronting our nation's cyberspace problems, is asking ourselves how to best harness our own strategic strengths, and do it in a manner which best navigates cyber's dynamic and uncertain human nature. SOF's strategic value for the nation is in its unique small footprint, exercised through a global network of partners, providing persistent engagement and partner enablement, as well as, discreet and rapid response. These same strategic strengths provide new unconventional opportunities and asymmetric options that must be further developed and integrated into our national cyber-strategies.

Whether conducting virtual Foreign Internal Defense (FID) to build partner security and capacity, or executing cyber-enabled Direct Action (DA) to eliminate hostile threats, cyberspace amplifies "the elemental aspects of what makes a special operation, special." [5] Meaning, cyberspace amplifies a DA mission's lethality, precision, and discreet nature; while in FID's case, cyberspace amplifies connectivity, capability, and trust. [6] It is increasingly clear that every USSOF mission must be amplified by cyber so that we can evolve our strengths into new strategic instruments to protect and project our national interests.

SOF is Dynamic

With every passing day, our hyper-connected landscape seems to produce a new class of threats, more technologically evolved than the last, harnessing the explosion of technology, information proliferation, and network connectivity for ambiguous warfare. [7] This means that, "in the not too distant future, every Special Operations Forces practitioner will be required to understand the basics of cyberspace, computers, and coding; not because they're expected to be programmers, but because they'll need those skills to conduct special operations in an era vastly more interconnected than now." [8] USSOF must rapidly adapt and evolve, as they increasingly find themselves pitted against tech-savvy adversaries in dynamic situations, where they must employ some of the same cyber-technologies in unconventional ways. From high-tech to low-tech, and from human-centric to techno-centric, USSOF will employ cyber-technologies as a means to directly or indirectly strengthen our global network of partners, and amplify our unique capabilities exercised through a wide-array of options.

> Cyber is both everywhere and nowhere at the same time, casting an invisible, yet powerful influence.

USSOF will employ cyberspace as a means to better understand the passions, which drive human action and behavior, and will use cyberspace as a vehicle to identify conflicts earlier, seize opportunities to steer, and potentially, tamp down violence. [9] Synthesizing objective technical data with subjective human understanding, USSOF will develop a deeper nuanced understanding of global and regional situations. USSOF will also generate new thinking and unconventional approaches to recruit people to noble causes, and use cyberspace as a means to engender the positive aspects of human behavior, such as decentralized and participatory action. Using their access, placement, and most importantly their influence, USSOF will help build holistic networks, which support national cyber-strategies, and assist in weighing psychological and technical acts against the competing needs for secrecy and credible action.

Just like cyberspace, USSOF operations are not a monolithic enterprise dependent upon one tightly woven centralized system. Instead, USSOF operations resemble cyber-

space itself, resiliently designed to leverage global networks riding across open architectures. Meaning, USSOF can assemble, swarm, disaggregate, or even replace one another, without disrupting the rest of the system. As with cyberspace, USSOF networks are a heterogeneous mix of Joint, Coalition, and other partners whose operations can be scaled up or down to attack and defend human and information networks. Similar to cyberspace, USSOF operations are not dependent on just a handful of brittle nodes, but operate across vibrant, expansive, and living global networks. Most importantly, just like cyberspace, the true power of USSOF operations are the humans behind them.

SOF Thrives in Uncertainty

In a recent speech, Director of National Intelligence (DNI), James Clapper, stated that cyber threats to US national security are increasing in frequency, scale, sophistication, and severity, and that since 2013, have "bumped terrorism out of the top spot on our list of national threats." [10] Adding that the trend will continue, the DNI underscored the importance of having "the best minds of our nation working this range of cyber problems." [11] Making matters particularly acute for USSOF, is that global terrorism and weapons of mass destruction (WMD) and proliferation perennially top the list of national security threats. This dangerous mix of cyberspace threats, terrorism, and WMD is a volatile brew, and poses serious dangers to the nation, in which USSOF must not fail.

With every passing day, our hyper-connected landscape seems to produce a new class of threats, each more technologically evolved than the previous.

Although these are serious challenges, it is in adversity where USSOF best excel. USSOF is specially trained for ambiguous conflict, and thrive in complex challenges, which do not always lend themselves to obvious approaches. [12] With no clear decisive points or geometries in battle to guide them, USSOF must blaze new trails in an ever expanding wilderness of dangerous and complex problems. Our national defense requires unconventional approaches to counter unconventional problems, so USSOF will not only employ new cyber-technologies, but more importantly, innovate new concepts and tactics to do it. USSOF will fuse emerging capabilities into time-tested practice to create new solutions and provide new strategic opportunities for the nation.

As an example, envisioning options for future command and control relationships, such as the creation of a Special Operations Command-Cyberspace (SOC-CYBER), as a means to provide national strategic capabilities and specialized expertise no other DoD service can provide. [13] A SOC-CYBER could enrich perspectives during the development

of national cyber-strategies, and infuse unconventional insights and asymmetric options during the process.[14] USSOF could also relay observations from the field, derived from their global footprint, to add nuance and context to some of the human-complexities of psychological, cultural, and societal dynamics; then, discreetly tie back into ongoing operations.[15] Ultimately, investing USSOF in cyber-organizations mixes some of the best and brightest US talent and expertise, and the diversity of its spirit is in the best interest of our nation.

Keys to a Human Space

USSOF operations provide keys to unlocking deeper understanding of human interactions in cyberspace, and a means to contextualize the sociocultural, political, and historical factors which all too frequently fuel strife.[16] Cyberspace provides USSOF new opportunities to leverage culture to build relationships, and deter our adversaries with a wide array of lethal and non-lethal options. Cultural intelligence equates to influential power,[17] and its instrumentality is driven by humans in cyberspace.

Successfully navigating our hyper-connected world means better understanding its cultural landscape, and requires blending emerging cyber-technology with unconventional approaches. Using cultural intelligence as an emerging tool, USSOF can better target, influence, degrade and destroy our nation's shadowy adversaries.[18] Whether they operate virtually via social media, or through digital communications, an adversary's human networks remain physical, and are susceptible to cross-cultural and transnational targeting. Despite attempts to conceal their actions, USSOF can find points of leverage in the cultural details to influence strategic outcomes with cyber capabilities.[19]

The US must continue to work together to confront vast cyber challenges by increasing our collective institutional efforts.

Providing persistent partner engagement is increasingly dynamic, as the convergence of cyberspace and the physical world cause both partners and adversaries to assume different roles depending on the circumstance. It is increasingly important to correctly interpret events, information, and disinformation, so that USSOF can more accurately influence outcomes in any environment, in any situation, no matter the actor.[20] This will require USSOF's unique access and placement, and most of all, their influence, to better understand the increasingly complex cultural cross-sections of human and digital interaction.

Although it is clearly an uncertain world, USSOF will use their cultural expertise in building cyber-partnerships to better assess partner realities, strengths, and vulnerabilities,[21] and ensure USSOF provide culturally attuned security assistance. Additionally, USSOF will evaluate the social and economic factors shaping partner circumstance,

to ensure they provide culturally compatible means and solutions for partners to solve their own problems, once USSOF depart. USSOF will also use cyberspace to understand better their partners' cultural values, and examine where and how our nation's values square against the enduring viability of potential relations,[22] and better calibrate US support accordingly.

Cyberspace is rapidly changing the world's cultural landscape and will increasingly challenge and redefine traditional concepts of society and national identity.[23] The proliferation of cyber-technology pressures cultures to change, and requires USSOF to keenly monitor cultural trends, as cultural dynamics steadily shape world events and competing perspectives. Cultural intelligence is a part of USSOF's approach to understand better evolving cultural dynamics, and cyber is the indispensable space to harnessing new strategic opportunities for the nation.

Conclusion

The contradictory nature of cyberspace will continue to shape our lives, as it does our national security. Just like the human's cyberspace emulates, cyber is dynamic and uncertain, and presents both serious challenges and unrealized opportunities for USSOF and our nation. The US must continue to work together to confront our vast cyber challenges by increasing our collective institutional efforts, as well as, challenging our respective organizations on ways to improve what we individually bring to the table. Although cyberspace's future impact on national security is yet to be determined, it is increasingly clear that USSOF will have an expanding role in shaping the outcome. Ultimately, cyberspace is a human space; and, it is exactly where USSOF needs to be.

Special Contributor

Elizabeth Oren

Elizabeth Oren specializes in cultural analysis, and supports both conventional and SOF communities with qualitative analytics. Over the last 10 years, Ms. Oren has conducted specialized research on refugee and immigration trends, machine translation, and cultural networks. Ms. Oren has worked in France, Turkey and Germany, and is a graduate of Texas A&M University and the University of Texas at Arlington holding degrees in international studies and foreign languages.

NOTES

1. Patrick Duggan, "Harnessing Cyber-technology's Human Potential," *Special Warfare 28,* no.4 (October-December 2015), 12. http://www.soc.mil/swcs/SWmag/archive/SW2804/October%202015%20Special%20Warfare.pdf (accessed February 25,2016).
2. Patrick Duggan, "Why Special Operations Forces in US Cyber-Warfare?" *Cyber Defense Review,* January 8, 2016, 1. http://www.cyberdefensereview.org/2016/01/08/why-special-operations-forces-in-us-cyber-warfare/(accessed February 22, 2016).
3. Ibid., 3.
4. Michael S. Rogers, "A Challenge for the Military Cyber Workforce," *Military Cyber Affairs:* Vol. 1: Iss. 1, Article 2. (2015), 1. http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1012&context=mca (accessed March 2, 2016).
5. Patrick Duggan, "Man, Computer, and Special Warfare," *Smallwarsjournal.com,* January 4, 2016, 4. http://smallwarsjournal.com/jrnl/art/man-computer-and-special-warfare (accessed February 22, 2016).
6. Ibid., 4.
7. "Man, Computer, and Special Warfare," 1.
8. Patrick Duggan, "SOF's Cyber FRINGE," *Smallwarsjournal.com,* February 10, 2016, 1. http://smallwarsjournal.com/jrnl/art/sof%E2%80%99s-cyber-fringe (accessed February 22, 2016).
9. "Why SOF in US Cyberwarfare?" 8.
10. Aaron Boyd, "DNI Clapper: Cyber Bigger Threat than Terrorism," *FederalTimes.com,* February 4, 2016, 1. http://www.federaltimes.com/story/government/cybersecurity/2016/02/04/cyber-bigger-threat-terrorism/79816482/ (accessed March 2, 2016).
11. Brian Murphy, "Director of National Intelligence Visits USNA for Cyber Lecture," *The Trident,* February 18, 2016, 1. http://usnatrident.blogspot.com/2016/02/director-of-national-intelligence.html (accessed March 2, 2016).
12. "Why Special Operations Forces in US Cyber-Warfare?" 7.
13. Ibid., 8.
14. Ibid., 8.
15. Ibid., 8.
16. Patrick Duggan, "Strategic Development of Special Warfare in Cyperspace," *Joint Forces Quarterly 79,* (4th Quarter 2015): 49. http://ndupress.ndu.edu/Media/News/NewsArticleView/tabid/7849/Article/621123/jfq-79-strategic-development-of-special-warfare-in-cyberspace.aspx (accessed February 22, 2016).
17. Elizabeth Oren, "Culture in a Murky World: Molding the Field of Cultural for International Security," *University of Texas at Arlington, Iss.1* (unpublished) 4.
18. Elizabeth Oren, *"Report on Islamic State's Asymmetric Information Campaign,"* (Oberammergau, Germany: NATO, January 4, 2015) 4.
19. "Culture in A Murky World", 5.
20. Elizabeth Oren, "A Dilemma of Principles", *Special Operations Journal,* Spring 2016, 8. Vol. 2, No. 1.
21. "Culture in a Murky World", 6.
22. Ibid., 6.
23. Ibid., 6.