

UW in cyberspace

The Cyber UW Pilot Team Concept

BY LIEUTENANT COLONEL PAT DUGGAN

“Like artillery in Combined Arms Maneuver, regionally expert forces should never be in reserve – even in CONUS they need to continue to support the fight.”

– USASOC Commanding General, LTG Charles T. Cleveland, ARSOF 2022

Introduction

The employment of pilot teams in cyberspace would operationalize our CONUS base through militarizing social-media networks to shape the physical environment while simultaneously decreasing the strategic risk, exposure and attribution to U.S. forces in sensitive, hostile and denied environments.

The world has witnessed the militarization of social media over the last several years, from the serendipitous Arab Spring revolutions to the Israeli Defense Force’s social-media warfare.¹ Social-media networks possess great utility and extraordinary military potential, especially when harnessed for unconventional warfare. The advanced pilot team concept is a capability meant to harness social-media networks and execute specialized activities to shape the physical environment through digital means. Pilot teams in cyberspace would accomplish most of the traditional pilot team tasks by fusing advanced SOF tactics, techniques and procedures, clandestine methods, mission planning, UW assessments and other advanced skills in the 5th domain of warfare — Cyberspace.² The pilot team’s strategic benefit would be its ability to decrease the risk, exposure and attribution to

U.S. forces as well as any partnered resistance organizations. Pilot teams in cyberspace would also decrease the time required to execute initial-entry UW operations in sensitive, hostile and denied UW environments having pre-coordinated most activities prior to the team’s infiltration. Given appropriate authorities, these pilot teams would employ dual purpose technology, indigenous equipment and leverage networks of influence to digitally initiate then physically execute UW operations from beginning to end.

The Human Domain of Cyberspace

The essence of social media is about exchanging information and ideas in virtual communities resulting in unlimited possibilities.³ With more than 35 percent of the world’s population already having access to the Internet,⁴ the connectivity across the globe is staggering. There are roughly 1.2 billion Facebook users,⁵ 72 hours of video uploaded every single minute on YouTube,⁶ almost 400 million tweets on Twitter every day⁷ and more than 200 million Linked-in users.⁸ Social media’s allure and penetration of societies is vast, and its ubiquity will only continue to flourish. Additionally, Metcalfe’s Law will ensure global penetration whether

it’s a closed or open nation. “The law posits that with every nodal connection to the Internet it exponentially increases the networks value.”⁹ Therefore it’s truly only a matter of time before every nation is penetrated by the Internet’s compounding effects. The future opportunities for nations, non-state actors or individuals to exploit social-media networks to their advantage are also vast. With more than 2.5 billion current Internet users¹⁰ and another 5 billion current mobile broadband connections¹¹ opportunities are obvious. Those that seize the key terrain of social-media exploitation will have strategic military advantage.

The proliferation of smart phones continues to connect a growing global middle class. Economies of scale for increased smart-phone production will continue to drop the average price per unit from \$188 in 2011 to a projected \$152 in 2017.¹² Even North Korea is not immune from the cell phone’s reach, having doubled from 1 million to 2 million legal users on their 3G network in 2012 alone.¹³ Of course, this figure doesn’t account for the illicit phone users who control the robust black-market economy which keeps North Korea afloat. Social-media applications are the Trojan Horse of the modern age. Their allure, penetration

and availability provide pilot teams in cyberspace unique and innovative options that range from monitoring, influencing and engaging people to shaping and controlling resources. A trained operator's ability to affect the physical domain is only bounded by his imagination, or more accurately, his authorities to execute specific cyber UW activities.

Social media is a weapon

The Arab Spring demonstrated the sweeping effects of social media on the physical domain seemingly by accident. "Handheld technologies and social-media connectivity aggregated small acts of resistance that produced frenzied revolutionary momentum."¹⁴ In a few short weeks, Revolution 2.0 swept across the Middle East inspiring masses to take action.¹⁵ In Tunisia, crowds overthrew El Abidine Ben Ali. In Egypt's Freedom Square, protests, riots and mass unrest led to Hosni Mubarak's abdication. In Libya, social media was employed to coordinate disparate rebel forces to expel President Muammar Qaddafi. Words, pictures, texts, tweets, posts, videos, all much cheaper than bullets, motivated thousands of seeming strangers to take decisive action with regional and global impact. "Even if revolution was not the aim, it was the outcome. Social-media collaboration generated accidental revolutionaries."¹⁶

By contrast, the Israeli Defense Force's social-media warfare during Fall 2012 was a highly effective and calculated strategy. "The IDF cut out the media middle man and took their message straight to the masses."¹⁷ Ironically, it was the media outlets that propagated IDF blogs, messages, posts and tweets and unwittingly played into the IDF's intentions. The IDF's social-media strategy left less room for misinterpretation, media spin or uncontrolled sound bites by successfully integrating the three major categories of social media. They integrated collaborative platforms like blogs and YouTube, networking platforms like Facebook, and communicative platforms like Twitter. The IDF also boldly initiated its military offensive with a tweet. "The IDF has begun a widespread campaign on terror sites and operatives in the #Gaza Strip."¹⁸

Although Nov. 11, 2012 was the first time a tweet served as the opening salvo for a major military offensive, it probably won't be the last. The IDF incorporated teams of social-media warfare operators into its force "Armed with Facebook profiles, Twitter accounts and

Lavazza espresso, warriors fearlessly and tirelessly scoured the cyber battlefield searching for enemy (blog) outposts. Outfitted with high-tech ammunition like HD video cameras, fire wire 800s and white phosphorescent keyboards, they attacked one-sided videos, slanted essays and enemy propaganda with propaganda of their own."¹⁹



SOCIAL SUCCESS A post on the Israeli Defense Force's Facebook page.

Today, the IDF's Facebook page <https://www.facebook.com/idfonline> remains a masterpiece of integrated platforms and communities; all of them disseminating information, coordinating efforts, raising money and facilitating activities.²⁰ The IDF demonstrates its mastery of seizing social media as key terrain in support of national military objectives.

Defining pilot teams in cyberspace

Pilot teams operating in cyberspace are doctrinally and conceptually no different from its older physical version. They would employ the same UW principles to execute most of the traditional pilot-team activities, but would instead leverage digital tools and cyber methods to do so. Additionally, pilot teams in cyberspace would provide fresh ideas and new approaches to some of the same military problems vexing us for years.

As paraphrased by the John F. Kennedy Special Warfare and School's Unconventional Warfare Training Circular (TC 18-01) pilot teams are comprised of USSF members, augmented by interagency and joint experts, designed to infiltrate designated areas for sensitive preparation of the environment activities as well as conduct UW assessments.²¹ The pilot team's missions are to conduct detailed area assessments and develop their understanding of the human and physical domain, as well as assess the viability of future UW efforts amongst the population. Ultimately, traditional pilot teams evaluate indigenous information capabilities to determine the level of support necessary to fully mature those capabilities for maximum military effectiveness.²² From a doctrinal perspective, "what" a traditional pilot team is and "what" it does is no different than its virtual variant. It is only the "how" that's the difference, with advanced pilot teams being digitally empowered to harvest, process and sift, through the Internet's rich and readily available social-media networks. Operators harness specialized software and hardware, clandestine methods, dual-purpose technology and networks of advantage as well as leverage widely available shareware applications and commercial software. The beauty of the advanced pilot team capability is its scalability. Although force investment to outfit the teams could require a host of expensive technical capabilities using a wide range of technologies, the capability could also be fielded on a shoe-string budget. And in today's era of fiscally constrained military portfolios, pilot teams in cyberspace would offer disproportionate value for any level of investment.

Just like the IDF's social-media teams, pilot teams in cyberspace would likely be comprised of a younger demographic ranging in age from 25-35. These adults came to age in a pre-wired world and are "digital natives" versus the "digital immigrants" that account for almost all of today's senior military leaders.²³ Author Marc Prensky coined those phrases in 2001 to reflect his theories of difference between digital natives and digital immigrants. He asserted natives and immigrants differ with respect to their behavior and thought process, as well as, the disadvantage suffered by immigrants because of their inability to incorporate technology into their everyday life. Although in this author's opinion, age and social-media literacy may not be as mutually exclusive as once thought, pilot teams operating in cyber-

space would undoubtedly be anchored by the rare breed of talented younger operator who possesses both the technological creativity and the strategic-level maturity required for sensitive missions. A collateral benefit of advanced pilot teams would be flatter organizational communications between talented operators and their senior military leaders. This fruitful exchange would serve to both professionally develop the next crop of senior leaders as well as vertically integrate operational decisions back at the CONUS base.

Operationalize the CONUS base

Pilot teams in cyberspace would operationalize the CONUS base by offering innovative options and viable capabilities for UW campaigns in sensitive, austere and denied environments. *ARSOF 2022* states, “Our formations must be organized, postured, and networked in a manner that enables them to anticipate and prevent or rapidly respond to regional contingencies or threats to the stability of our allies.”²⁴ Tailor-built pilot teams in cyberspace would navigate social media’s grey and dark networks with a focus on long-term national military problems from the comforts and safety of their home base. Another example of this concept is the Common Operational Research Environment Labs at the Naval Postgraduate School. CORE has performed groundbreaking research in the areas of social network analysis on grey and dark networks “enabling operators to collect, manage and fuse data in order to create a more complete picture of the common operational environment.”²⁵ The significance of black and grey social networks are key because it’s the cyberspace that best decreases the risk, exposure and attribution to U.S. forces as well as any partnered resistance organization.

Although both physical and virtual pilot teams are inherently joint and interagency, the cyber domain version would have its advantages. They would possess more regional, technical and language experts because of its flexibility to work from any location outfitted with high-speed Internet access. Pilot teams in cyberspace would also be easier to man and simpler to logistically support from their CONUS locations. The advanced pilot team concept exemplifies *ARSOF 2022* by “providing regional expertise to the TSOCs from CONUS-based regionally expert forces. By physically and virtually synchronizing the capacity of regional experts from across the U.S. Government, academia and

industry, ARSOF will leverage the nation’s CONUS-based regional expertise for continuous support to global special-operations mission requirements.”²⁶

Pilot teams operating in cyberspace would harness social-media networks to identify leaders, assess motivations, categorize sub-networks and even stitch together UW complexes from the virtual environment. Just like modern day threat networks, advanced pilot teams can “cloak themselves in the human activity of the modern, increasingly interdependent and virtually connected world.”²⁷ They would open doors to social network communities while simultaneously decreasing exposure and attribution. By removing time limitations imposed by physical constraints, virtual pilot teams instead offer a long-term understanding through blending into the backdrop of social media. CONUS-based advanced pilot teams could also support real military plans by militarizing social-media networks to prepare conditions in a designated physical environment. They could remotely identify UW planning vulnerabilities and shortfalls, as well as, identify, map and expose networks of influence to exploit. Once the advanced pilot team achieved acceptable physical conditions and authority for initial entry UW operations, pre-established regional mechanisms would conduct pre-designated activities to decrease the risk to the force. Ultimately, the same SF ODA who once digitally initiated their planning in the Cyber Domain would now execute their plan in a denied and hostile physical one.

Conclusion

Pilot teams in cyberspace would operationalize our CONUS base by militarizing social-media networks to provide unique options and capabilities for future UW campaigns in sensitive, hostile and denied environments. They are a viable modern day enabling UW concept that strategically offers ways to shape the physical environment while decreasing the risk, exposure and attribution to U.S. forces. **SW**

Lt. Col. Pat Duggan is the Commander, 3rd Battalion, 1st Special Forces Group (A) and was previously assigned to 5th Special Forces Group (A). He participated in the invasion of Afghanistan and invasion of Iraq and has deployed multiple times across the Middle East and Asia, including Operation Enduring Freedom-Philippines and Joint Chiefs of Staff Exercise Key Resolve/Foal Eagle.

Notes

1. <http://blog.heritage.org/2012/11/27/social-media-in-warfare-the-new-battleground/>
2. http://www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive?utm_source=World+Affairs+News+letter&utm_campaign=63c3895834-WAJ_Gjeltlen_1_8_2013&utm_medium=email
3. http://en.wikipedia.org/wiki/Social_media
4. <http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/>
5. <http://www.statisticbrain.com/social-networking-statistics/>
6. <http://www.youtube.com/yt/press/statistics.html>
7. http://articles.washingtonpost.com/2013-03-21/business/37889387_1_tweets-jack-dorsey-twitter
8. <http://blog.linkedin.com/2013/01/09/linkedin-200-million/>
9. http://en.wikipedia.org/wiki/Metcalfe's_law
10. <http://www.internetworldstats.com/stats.htm>
11. <http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/>
12. <http://www.eweek.com/mobile/smartphone-prices-to-continue-falling-informa/>
13. <http://www.northkoreatech.org/2013/04/26/koryolink-nears-2-million-subscribers/>
14. <http://www.soc.mil/swcs/SWmag/archive/SW2502/SW2502SocialMediaAndUW.html>
15. Wael Ghonim. *Revolution 2.0: The Power of the People is Greater than the People in the Power*, (Houghton Mifflin Harcourt, 2012).
16. <http://www.soc.mil/swcs/SWmag/archive/SW2502/SW2502SocialMediaAndUW.html>
17. <http://www.forbes.com/sites/alexkanrowitz/2012/11/18/israel-and-hamas-social-media-battle-goes-from-groundbreaking-to-bizarre/>
18. <http://www.washingtonsblog.com/2012/11/israel-winning-the-war-in-social-media.html>
19. <http://www.pbs.org/mediashift/2009/02/how-social-media-war-was-waged-in-gaza-israel-conflict044>
20. <http://www.washingtonsblog.com/2012/11/israel-winning-the-war-in-social-media.html>
21. Department of the Army Training Circular No. 18-01, *Special Forces Unconventional Warfare*, (Washington D.C.; US Government Printing Office, 28 January 2011; distribution restriction)
22. Ibid.
23. Prensky, Marc. “Digital Natives, Digital Immigrants Part 2: Do They Really Think Differently?” *On the Horizon* 9.6 (2001): 1-6. Print.
24. *ARSOF 2022*
25. CORE Quarterly Newsletter April 2013. Naval Post Graduate School
26. *ARSOF 2022*
27. http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/adp3_05.pdf