SMALL WARS JOURNAL

Viral Conflict: Proposing the Information Warfighting Function

*By **Terron Wharton***
Journal Article | *Mar 17 2017 - 1:12pm*

Viral Conflict: Proposing the Information Warfighting Function

Terron Wharton

Introduction

The Army's current operations structure is ill suited for its new maneuver concept, the Army Functional Concept for Movement and Maneuver 2020-2040 (AFC-MM). The specific shortfall lies with the warfighting functions. The current warfighting functions do not integrate all five domains, adequately leverage emerging capabilities in electronic, information, and cyber-warfare, and do not provide a framework to synchronize them with operations at the tactical, strategic, and operational levels. Establishing an information warfighting function provides three major benefits. First, it links information related capabilities (IRCs) to the five domains. Second, it provides a logical framework to incorporate IRCs into planning. Finally, it sets conditions to realize AFC-MM.

War is constantly evolving. Autonomous systems, robotics, electronic warfare, cyber warfare, the internet, social media, and individual access to global communications are changing the nature of conflicts at the tactical, operational, and strategic levels. In response, the Army developed the Army Functional Concept for Movement and Maneuver 2020-2040 (AFC-MM). The AFC-MM attempts to embrace these shifts and puts forth a concept aiming to maximize these emerging capabilities. It emphasizes that commanders should leverage capabilities between domains to create advantages.

ADP 3-0, Unified Land Operations, states that commanders must present the enemy with problem sets across multiple domains because they possess the simultaneity to overwhelm the enemy and strike across depth.**[1]** This allows commanders to achieve overmatch and defeat an adversary. If commanders and staff do not understand this concept it will put them at a disadvantage against those who do.

Unfortunately, the Army's current operations structure is ill suited for this new maneuver concept. Specifically, the problem lies with the warfighting functions. The current warfighting functions do not integrate all five domains, adequately leverage emerging capabilities in electronic, information, and cyber-warfare, and do not provide a framework to synchronize them with operations at the tactical, operational, and strategic levels. Establishing an information warfighting function provides three major benefits. First, it links information related capabilities (IRCs) to the five domains. Second, it provides a logical framework to incorporate IRCs into planning. Finally, it sets conditions to realize AFC-MM.

The Domain Disconnect

Published in February 2017, the AFC-MM's goal is to:

> "…describes how Army forces conduct combat operations against threats in the 2020-2040 timeframe. It proposes a concept and the required capabilities necessary to provide commanders with multiple options to seize and control terrain, defeat or destroy enemy forces, and protect populations, activities, and infrastructure to achieve military objectives. The AFC-MM offers a hypothesis to inform further concept development, war-gaming, experimentation, and capability development."**[2]**

The AFC-MM recognizes this fundamental shift in the operating environment and that our adversaries and near peers are adapting to it. In the introduction, LTG H.R. McMaster writes:

> "Today's adversaries have studied how the U.S. Joint Force prefers to operate and adapted to develop capabilities that contest our operations on land, at sea, in the air, in space and cyberspace, as well as the electromagnetic spectrum, information environment, and human perception. Defeating future enemies that possess advanced capabilities calls for land forces operating as integrated joint teams that conduct simultaneous and sequential operations across multiple domains."**[3]**

The AFC-MM spends a large amount of time speaking to and emphasizing the importance of cross-domain maneuver:

> "Cross-domain maneuver is the employment of mutually supporting lethal and nonlethal capabilities in multiple domains to generate overmatch, present multiple dilemmas to the enemy, and enable joint force freedom of movement and action. Integrating capabilities in all domains in such a way to achieve a synergistic effect increases relative combat power and enables Army maneuver forces to destroy or defeat enemy forces. Commanders employ cross-domain maneuver to concentrate effects in decisive spaces across the five domains to achieve physical, temporal, and psychological advantage over enemy forces."**[4]**

The AFC-MM emphasizes that future success requires commanders at all echelons to maximize cross-domain maneuver. In fact, cross-domain maneuver is mentioned over 65 times across the 60-page document. The repeated emphasis implies that current and future commanders and staffs must do more than understand the concept: they must master it.

ADP 3-0 defines five domains of warfare: land, air, maritime, space, and cyberspace.**[5]** We already conduct multi-domain battle and cross domain maneuver to a large degree. A brigade combat team (BCT) using close air support (CAS) to destroy enemy defensive positions is using cross-domain fires from the air domain to enable actions in the land domain. Satellites in the space domain and terrestrial networks in cyberspace enable mission command systems used in land, air, and sea domains. The issue is not understanding "multi-domain battle" or "cross-domain maneuver". The challenge is integrating and synchronizing assets from multiple domains, especially cyberspace, at a single point in time and space to create overmatch in support of a maneuver plan (tactical), a campaign plan (operational), or strategic objectives.

The Army struggles with fully implementing multi-domain battle and cross-domain maneuver because our current doctrine does a poor job of framing the concepts for our planning methodology. The Army

organizes, plans, and fights around the warfighting functions. ADRP 3-0, Operations, describes the warfighting functions this way:

> "To execute operations, commanders conceptualize capabilities in terms of combat power. Combat power has eight elements: leadership, information, mission command, movement and maneuver, intelligence, fires, sustainment, and protection. The Army collectively describes the last six elements as the warfighting functions. Commanders apply combat power through the warfighting functions using leadership and information."**[6]**

It continues in more depth:

> "A warfighting function is a group of tasks and systems united by a common purpose that commanders use to accomplish missions and training objectives. The warfighting functions are the physical means that tactical commanders use to execute operations and accomplish missions assigned by superior tactical- and operational-level commanders. The purpose of warfighting functions is to provide an intellectual organization for common critical capabilities available to commanders and staffs at all echelons and levels of war."**[7]**

Simply put, the warfighting functions provide an organizational framework by grouping common, critical capabilities. Army doctrine defines six warfighting functions: Mission Command, Movement and Maneuver, Intelligence, Fires, Sustainment, and Protection. Each is clearly understood, with every branch and functional area of the Army aligned to one of the warfighting functions. In a greater sense, the warfighting functions link capabilities to domains, allowing a construct for employing them in one or more domains and synchronizing effects across multiple domains. Everything fits very neatly, except for the cyberspace domain and five of the branches and functional areas.

Knowledge is Power

Before we go any further, it is critical to define what "Information" and associated terms means. The Army defines information as an element of combat power. Specifically, it "…enables commanders at all levels to make informed decisions on how best to apply combat power."**[8]** FM 3-13, Information Operations, states information operations (IO) "… creates effects in and through the information environment. IO optimizes the information element of combat power and supports and enhances all other elements to gain an operational advantage over an enemy or adversary."**[9]**

Next, FM 3-13 defines the information environment as the "…aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information" and comprises three dimensions: physical, informational, and cognitive.**[10]** Finally, the Army employs IRCs, which are tools, techniques, or activities, to create effects in and through the information environment, thereby producing an advantage in the operational environment. While FM 3-13 does not give an exhaustive list of IRCs, it does mention four specifically: military information support operations (MISO), public affairs, electronic warfare, and cyberspace operations.**[11]**

The Army defines information as the thing that enhances all the other elements of combat power, to include the warfighting functions. However, despite that very narrow definition, FM 3-13 repeatedly mentions how IRCs are becoming increasingly powerful and influential. It speaks at length how information democratization, global communications, and social media are changing the way narratives

are shaped and disseminated.[12] It emphasizes that threats and competitors, both State and non-state, are investing heavily in IRCs because of the cyberspace domain's equalizing effect.[13] Finally, it provides a warning to commanders and their staffs:

> "Activities occurring in and through the information environment have a consequential effect on the operational environment and can impact military operations and outcomes. Therefore, commanders and their staffs must understand the information environment, in all its complexity, and the potential impacts it will have on current and planned military operations."[14]

A critical point FM 3-13 makes is explicitly linking the information environment to the cyberspace domain. Therefore, it is a logical extension to view IRCs as the primary method of leveraging the cyberspace domain to impact the operational environment and create effects in other domains as well. Unfortunately, our doctrine is not poised to fully integrate and leverage IRCs.

Per the current model, information and leadership enable the other six elements of combat power. The other six elements, the warfighting functions, organize the physical means commanders use to achieve objectives. However, during the operations process, the warfighting functions are what is used for planning and asset synchronization.[15] Our model forces commanders and staffs to consider the warfighting functions during planning, but not the elements of combat power. As such, information related capabilities are never part of the primary planning effort, becoming either an afterthought, underutilized, or poorly integrated, if they are used at all.

Information has long been an element of combat power. However, because information related capabilities have grown in scope, scale, and impact, they have ceased simply to exist as tools to optimize the warfighting functions. Their ability to directly impact the operational environment has made them just as important as capabilities within the other warfighting functions.

Currently, no warfighting function provides a logical link between the cyberspace domain, IRCs, and the operations process. While the Signal Corp and the Mission Command warfighting functions are often tied to the cyberspace domain, neither fully embraces or integrates other capacities for offense, protection, and information operations. The five branches and functional areas in the Army that have the potential to fully leverage the cyberspace domain and IRCs are electronic warfare (EW), cyber, information operations (IO), psychological operations (PSYOPS), and public affairs. Without a warfighting function, they possess no logical construct to organize and synchronize their capabilities in support of operations, preventing effective cross domain employment from cyberspace to other domains. Ultimately, it results in missed opportunities to achieve overmatch.

Young and (un)Tested(?)

In 2007, the Israelis conducted Operation Orchard, which aimed to destroy a suspected Syrian nuclear facility. A major obstacle for the Israeli air force was the Syrian integrated air defense network. For the mission to succeed, they had to mitigate or eliminate Syrian air defenses to allow the strike operation access to the target.

Using a combination of a cyber capabilities and electronic attack (EA), the Israelis suppressed the enemy air defense network, allowing the air force to successfully strike the target.[16] The Israeli military employed IRCs (cyber and EA) in the cyberspace domain to produce effects (suppression of enemy air defense) in the land domain, creating overmatch at a point in time and space. Operation Orchard demonstrated the effectiveness of cross domain maneuver by using the cyberspace domain to set

conditions in the land domain, allowing air domain fires to strike a land domain target.

From the tactical to the strategic level, IRCs are creating substantial impacts. Electronic warfare jamming systems prevent remote controlled IEDs from detonating.**[17]** In the Ukraine, Russia used EW capabilities to target Ukrainian formations for long range, massed fires, shaping the deep fight and setting conditions for combined arms maneuver.**[18]** Social media is used to coordinate protests, radicalize and recruit new personnel to extremist groups, and communicate plans for attacks.**[19]** Finally, at the strategic level, Russian information operations in Europe and the U.S. have manipulated public opinions, eroded confidence in government, and influenced elections.**[20]** Information related capabilities have grown and evolved into more than enablers. They are now distinct assets in their own right and possess the ability to significantly shape, and directly affect, the operational environment.

Our current IRCs suffer from two significant obstructions. First, EW and cyber are young branches within the Army, both poorly understood and rarely employed outside of niche scenarios. A chief factor in this problem is they do not cleanly align with one of the six warfighting functions. EW and cyber directly touch three of the current warfighting functions. Offensive cyber operations (OCO) and electronic attack (EA) are viewed as an effect, which falls under the fires warfighting function. Defensive cyber operations (DCO) and EW based counter IED fall under protection. Finally, both cyber and EW capabilities can serve as collection mediums under the intelligence warfighting function.

IO is also inadequately integrated and under leveraged. Information operations are often viewed by many as solely a counterinsurgency tool. Derisively, these capabilities are shoved into the “hearts and minds” toolkit, with little thought of how they can affect a complex, multi-domain operational environment

EW, cyber, and IO IRCs are often lumped together as “Effects” under the Fires warfighting function. The current method of grouping these branches under non-lethal fires and effects relegates them to second tier importance during the planning process. As stated before, our operations process focuses on the warfighting functions. Constantly time constrained, commanders and staffs at all echelons will focus on the primary aspects of each warfighting function during the planning process. This is especially true at lower echelons, where staffs are smaller, less robust, and may have officers managing war fighting functions outside their core competency. The current framework leaves IRCs and these five branches as an afterthought.

The second problem is where we place these capabilities. Currently, we view EW and cyber as assets to shape the deep fight and IO as a way the shape the environment at the operational and strategic levels. Per our doctrine, this places these IRCs at the Division level at the lowest. Typically, they reside at corps, combatant commands, and the national level, with significant restrictions on employment. Often, we treat these assets solely as strategic weapons on par with our nuclear arsenal. This is patently absurd.

EW, cyber, and IO IRCs belong at whatever level the effect is needed. A company commander who uses EA to jam an enemy platoon as part of his support by fire is not shaping the deep fight. The battalion employing cyber assets to disable enemy counter-fire radars prior to conducting a breach is not shaping the deep fight. Finally, the brigade commander waging an information campaign to delegitimize a local warlord and transition support to the local elected government is not shaping a deep fight.

Nearly every capability can be echeloned. ICBMs and nuclear weapons are strategic fires used for strategic objectives. However, we don’t keep all fires assets at the national level. Corps and Divisions do not have ICBMs, but they do have missiles and rockets. An infantry battalion does not have HIMARS, but it still has its own mortars. Each echelon has a fires capability that corresponds with its overall place in our military structure, needed lethality, and relevant authority.

If you told a room full of battalion and brigade commanders that all mortars and cannon artillery now fell under division's direct control and they had to route fire support through the division, two things would happen. First, it would drastically slow and minimize the employment of those assets at the battalion and brigade level. Second, over time, commanders and staffs would no longer have the expertise to synchronize those assets at the battalion and brigade level. Unfortunately, that exact scenario is what has happened with our IRCs, resulting in a force with no experience in planning, synchronizing, or employing IRCs, the very assets that are critical to fully realizing cross-domain maneuver and AFC-MM.

The Information Warfighting Function

I propose the Army establishes the information warfighting function. The Information warfighting function would comprise EW, cyber, IO, public affairs, and PSYOPS and their associated IRCs as a cohesive "group of tasks and systems united by a common purpose that commanders use to accomplish missions and training objectives."**[21]** Establishing the Information warfighting function accomplishes three things.

First, it fully links IRCs to all five domains. As I stated before, each of the warfighting functions provide a logical link between their capabilities and how they can affect one or more of the five domains, except for the cyberspace domain. Tied to a warfighting function, IRCs can be deliberately integrated into the planning process. This forces staffs to plan, consider, and employ IRCs to shape the greater operational environment and affect the other four domains.

Second, it provides a logical framework to incorporate IRCs into planning. Specifically, it aids in synchronizing them with the maneuver plan. For the information warfighting function, there is no practical difference between coordinating an electronic attack to support a combined arms breach and executing military information support operations as part of a corps campaign plan. The information warfighting function, via the operations process, provides a framework for integrating IRCs into planning and the imperative to do so.

Finally, it sets conditions to realize the AFC-MM. By linking the cyberspace domain and IRCs to other domains, we can fully synchronize operations across all five domains. This opens and emphasizes a whole new set of tools and options for commanders to achieve overmatch via cross domain maneuver.

A very simple challenge to the information warfighting function is that many of its capabilities are already covered by other warfighting functions. As I mentioned before, EW, cyber, and IO already interact heavily with the fires, protection, and intelligence warfighting functions. While true, it is not abnormal, nor is it disqualifying. Intelligence routinely supports fires and movement and maneuver. Fires shapes operational environments in preparation for maneuver. Protection preserves capabilities across the other warfighting functions.

More than any other, the mission command warfighting function serves as the grand enabler. The mission command warfighting functions serves to "… balance the art of command and the science of control in order to integrate the other warfighting functions."**[22]** Mission command exists to generate situational awareness, facilitate situational understanding, and allow commanders to make decisions. In essence, it is a supporting capability to the other warfighting functions.

Proposing a new warfighting function is meaningless without a plan. While the information warfighting function's logical construct is value added in itself, it must be fully realized if we want to successfully implement the AFC-MM. The Army should take the following steps in implementing the information warfighting function.

First, the Army must establish an Information Center of Excellence (ICoE) as the proponent for developing, assessing, and integrating the five subcomponents and their IRCs into a cohesive concept and doctrine. ICoE, in partnership with the Combined Arms Center, integrates information warfighting function doctrine into Army doctrine writ large. Finally, ICoE should possess oversight of all subcomponent training and doctrine.

Include IRC overviews and training on planning and employment at all Captain's Career Courses, Command and General Staff College, and Army War College. Next, include a robust selection of IRCs in all planning exercises at those institutions. If we want general officers who have mastered these concepts and capabilities, we must start by training and exposing them as captains.

Next, leverage proposed troop and funding increases to grow the EW, cyber, and IO career fields. EW and cyber accessions must be increased, with IO becoming an initial branching option instead of functional area. We cannot look to voluntary transfers to fill the requirements of growing these branches. Direct commissions and appointments from the civilian sector, while appealing, should be handled with care. This option makes sense for National Guard and Army Reserve units where their civilian experience would bring maximum utility while allowing them to stay current in emerging technologies and threats. However, to create true experts in the active component these officers must be grown from the ground up, developing experience of integrating the information warfighting function and IRCs over years of service.

Additionally, designate all three as donor branches for the branch detail program. The maneuver experience gained will aid these officers when they plan, synchronize, and employ these capabilities in support of a maneuver plan. Expanding accessions, leveraging direct commissions in the National Guard and Army Reserves, and branch detail programs will allow the Army to develop breadth and depth in these competencies. However, it will still take time and the longer we delay, the longer we lack the competency.

We must establish a primary staff position for information, staffed by an information warfighting function officer and manned by Soldiers and NCOs in information warfighting function MOSs. This provides a proponent for integrated information planning. Make these staff positions in maneuver battalions and BCTs key development jobs and weight them accordingly for boards. Finally, make the positions at Division and higher centralized selection list (CSL) billets.

Next, push IRCs down to battalion level now, with goal of pushing limited capabilities to the company level. AFC-MM challenges commanders to create overmatch by synchronizing assets across all domains in support of a maneuver plan. However, current commanders and staffs below division have zero experience doing this. Even worse, most staffs don't even know what IRCs we possess, let alone how to effectively employ them.

Most importantly, we must allow Soldiers, commanders, and staffs to try out these capabilities, develop TTPs, and get comfortable using them. Maneuver commanders need to be as comfortable with IRCs as they are with artillery. At some point, you must put the tools in a Soldiers' hands and let them play around. While it will take time to grow this competency, we must start somewhere.

Above all, we must conduct experiments in cross-domain maneuver to integrate the information warfighting function into planning, synchronize the capabilities with maneuver, and develop future concepts of employment. TRADOC already provides multiple venues for this. The Army Expeditionary Warrior Experiment is positioned to enable development of information warfighting function related capabilities and TTPS at the small unit level.

At the other end of the spectrum, The U.S. Army Joint Modernization Command's (JMC) Joint Warfighting Assessment (JWA) provides a venue to test concepts and capabilities at the BCT level and higher while integrating joint and multinational partners, SOF, and an Army BCT across a live, virtual, and constructive environment. In addition to the JWA, the Army should conclude Network Integration Evaluations (NIE) and transition them to Multi-Domain Battle Assessments (MDBA).

The MDBA serves four purposes. First, it allows a comprehensive and integrated assessment of multi-domain battle and cross-domain maneuver capabilities and concepts in a rigorous and realistic operating environment. Second, it allows the Army to experiment and further develop the AFC-MM towards ultimate realization. Third, it allows us to develop concepts and capabilities for operating in contested, and denied, cyberspace domain environments. Fourth, it allows assessments and evaluations of Network 2020 related systems in both a contested and denied cyberspace domain.

JMC provides the personnel, facilities, local training area, and institutional expertise to conduct large scale exercises that integrate thousands of personnel across multiple different concepts and capabilities. JMC has run these large-scale exercises and tests bi-annually since 2011, and has the experience to integrate a live BCT, multinational and joint partners, and experimental concepts and capabilities across a live, virtual, and constructive environment from company to corps level. By leveraging existing opportunities, we can rapidly begin experiments and assessments while keeping opportunity cost low.

Embracing Change

As time progresses, IRCs will only grow in potency and importance. If, as an Army, we want to maintain overmatch we must embrace, integrate, and develop these concepts and capabilities now. The Army is implicitly moving this way to a degree. Not only does AFC-MM emphasizes cross-domain maneuver, but Army Directive 2017-18 established the Information Dominance competitive category for majors to colonels comprising EW, cyber, and IO officers.

No successful operation begins without setting conditions first. While the AFC-MM has set an excellent foundation to change the way we fight, we have failed to set the conditions for success. Establishing the information warfighting function is the first step in setting those conditions, realizing the AFC-MM, and ensuring our dominance during this next evolution of warfare.

The views and opinions expressed in this article are those of the author, and do not represent the policies or the positions of the United States Army, the United States Department of Defense, or any agency of the United States government.

End Notes

[1]. U.S. Army, *Unified Land Operations*, ADP 3-0, (Washington, D.C.: Headquarters, Department of the Army, 2016), 7.

[2]. U.S. Army, *The U.S. Army Functional Concept For Movement And Maneuver 2020-2040*, TP 523-3-6 (Washington, D.C.: Headquarters, Department of the Army, 2017), 7.

[3]. Ibid, iii.

[4]. Ibid, 8.

[5]. *Unified Land Operations,* 1.

[6]. U.S. Army, *Operations*, ARDP 3-0, (Washington, D.C.: Headquarters, Department of the Army, 2016), 4-3.

[7]. Ibid, 5-2.

[8]. Ibid.

[9]. U.S. Army, *Information Operations*, FM 3-130, (Washington, D.C.: Headquarters, Department of the Army, 2016), 1-1.

[10]. Ibid, 1-2.

[11]. Ibid, 1-3.

[12]. "Across the globe, information is increasingly available in near-real time. The ability to access this information, from anywhere, at any time, broadens and accelerates human interaction, across multiple levels (person to person, person to organization, person to government, government to government) … From a military standpoint, information enables decision making, leadership, and combat power; it is also critical to seizing, gaining and retaining the initiative, and consolidating gains in the operational environment." Ibid, 1-1.

[13]. "States and non-states are rapidly expanding their investment in cyberspace and space capabilities and forces. They recognize the leveling effect these domains, especially cyberspace, offer in terms of achieving parity or overmatch at minimum relative cost. A significant portion of the threat's information asymmetry comes from its growing capacity in space and cyberspace." Ibid, 1-2.

[14]. Ibid.

[15]. "In execution, the staff—primarily through the current operations integration cell—integrates forces and warfighting functions to accomplish the mission." U.S. Army, *The Operations Process*, ADRP 5-0, (Washington, D.C.: Headquarters, Department of the Army, 2012), 4-3.

[16]. David A. Fulghum and Douglas Barrie, "Israel used electronic attack in air strike against Syrian mystery target," ABC News, October 7, 2007, accessed March 9, 2017, http://abcnews.go.com/Technology/story?id=3702807&page=1.

[17]. "AN/VLQ-12 CREW Duke Electronic Warfare System," SRC, Inc., accessed March 9, 2017, http://www.srcinc.com/what-we-do/ew/crew-duke.html.

[18]. "Russian electronic warfare can detect all electromagnetic emissions, including those from radios, Blue Force Tracker, Wi-Fi and cellphones, which can then be pinpointed with unmanned aerial systems and targeted with massed artillery." Phillip Karber and Joshua Thibeault, "Russia's New Generation Warfare," The Potomac Foundation, May 13, 2016, accessed March 9, 2017, http://www.thepotomacfoundation.org/russias-new-generation-warfare-2/

[19]. "Testimony of Michael Steinbach, Executive Assistant Director, National Security Branch,

Federal Bureau of Investigation." Senate Committee on Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations, ISIL Online: Countering Terrorist Radicalization and Recruitment on the Internet and Social Media, 114th Cong., 2d sess., 2016, https://www.hsgac.senate.gov/subcommittees/investigations/hearings/isis-online-countering-terrorist-radicalization-and-recruitment-on-the-internet_social-media

[20]. Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections*, ICA 2017-01D, (Washington, D.C.: ODNI), ii.

[21]. *Operations*, 5-2.

[22]. Ibid, 5-3.

About the Author

Terron Wharton

Major Terron Wharton is an Armor officer, political theorist, and published author. He holds undergraduate and graduate degrees in international relations. Previous publications include the original political theory, "Through the Looking Glass: The Reflectionism Theory of International Relations", which appeared in the *InterAgnecy Journal*; the book "High Risk Soldier: Trauma and Triumph in the Global War on Terror", a work dealing with overcoming the effects of PTSD; and "The Overlooked Mentors" in *Armor Magazine*, which discusses the NCO role in officer development and mentorship. He has deployed to Iraq and Afghanistan as part of Operation Iraqi Freedom and Operation Enduring Freedom where he took part in combat operations, counterinsurgency, and security force assistance. He is currently assigned to the United States Army Joint Modernization Command at Ft Bliss, TX.

Available online at : http://smallwarsjournal.com/jrnl/art/viral-conflict-proposing-the-information-warfighting-function

Links:
{1} http://smallwarsjournal.com/author/terron-wharton
{2} http://abcnews.go.com/Technology/story?id=3702807&page=1
{3} http://www.srcinc.com/what-we-do/ew/crew-duke.html
{4} http://www.thepotomacfoundation.org/russias-new-generation-warfare-2/
{5} https://www.hsgac.senate.gov/subcommittees/investigations/hearings/isis-online-countering-terrorist-radicalization-and-recruitment-on-the-internet_social-media