Enabling the Army in an Era of Information Warfare

Lieutenant General Stephen G. Fogarty
Colonel (Ret.) Bryan N. Sparling

> We cannot be an Industrial Age Army in the Information Age. We must transform all linear industrial age processes to be more effective, protect our resources, and make better decisions.[1]
>
> *- General James C. McConville, 40th Chief of Staff of the U.S. Army*

Operations against ISIS, disrupting Russian attempts to interfere in the 2018 US midterm elections and, most recently, countering Iran's attempts to increase instability across the Middle East mark important efforts by the US military to find effective capabilities, doctrinal concepts, and appropriate roles in an era of information warfare. We must fight the battles our adversaries put before us. If our doctrines, systems, and processes do not match that reality, then it is time for new thinking. Through three decades of near-ceaseless global operations, "Information Operations," or IO has endured as the mainstay approach for how the Armed Services and the Joint Force conceptualize and apply informational power as an integral element of military operations. Despite evolving definitions, ever-changing formulations, and passionate assertions as to both its criticality and utility, IO remains doctrinal and relevant, though often misunderstood, a term of military art. Most often, IO has proved useful at tactical and operational levels of war. At more strategic and political levels, the efficacy of IO remains elusive, and US leaders, both civilian and military, have been less than adept at effectively realizing the potential of "informational power."

Lieutenant General Stephen G. Fogarty is the Commander, U.S. Army Cyber Command (ARCYBER). With more than 37 years of active service, LTG Fogarty was previously the first Commanding General of the U.S. Army Cyber Center of Excellence, and Commander, U.S. Army Intelligence and Security Command. His extensive Joint and Combined experience include assignments with U.S. Special Operations Command, U.S. Central Command, U.S. Cyber Command, three tours in Afghanistan, and Operation JUST CAUSE, Panama. LTG Fogarty holds Master's degrees in Administration from Central Michigan University and in Strategic Studies from the U.S. Army War College.

Given the US imperative of civilian control, and the military's supporting role in peacetime strategy and diplomacy, a perceived need for the military to play an expanded role, beyond tactical IO, in strategic, information-based influence remains limited and often contentious. The stunning social media-powered rise of ISIS in 2015, Russia's interference in the 2016 US Presidential election, Iran's increasing digital belligerence, and China's disinformation surrounding the COVID-19 pandemic are upending that perception and igniting a conversation across the defense establishment regarding appropriate roles for the uniformed armed services in this environment of unprecedented information warfare. Should the armed forces provide capabilities to protect not only US portions of cyberspace and the electric magnetic spectrum, but also the larger, and more challenging, Information Environment (IE)?[2] The Joint Chiefs of Staff have put forth the term "Operations in the IE (OIE)" to describe the Joint Force's growing informational mission; however, across the broader national security community, the term "information warfare (IW)"[3] is increasingly employed to connote an evolving suite of cyber, electromagnetic, and informational activities that the Army and other services are, or perhaps should be, developing, as part of a whole of government approach to counter adversary attempts to destabilize the US and its allies, and sustain a strategic competitive advantage in the IE.

The Army is currently evaluating whether OIE, IW, or some other concept should replace IO to describe an expanded Army mission in the IE. We are likewise considering whether Army Cyber Command (ARCYBER) should change its name to more accurately reflect the full spectrum of its mission portfolio. Regardless, ARCYBER is building upon a ten-year foundation of continual innovation, and accelerating its modernization efforts to enable information age Army operations across tactical, operational, and strategic echelons. As a functional Army Service Component Command (ASCC), ARCYBER

Colonel (Ret.) Bryan N. Sparling is a Highly Qualified Expert (HQE) serving as ARCYBER's Information Warfare Transformation Advisor. Sparling served over 27 years on active duty as a Signal Officer and Information Operations Officer. He was the Chief of IO and Special Activities, J39, U.S. European Command, 2011-2015, and the NATO Communication Director in Afghanistan, 2010-2011. He is a graduate of the U.S. Army School of Advanced Military Studies (SAMS), the National Defense University's Joint Advanced Warfighting School (JAWS), and holds a Masters in Telecommunications from the University of Colorado, Boulder.

supports Army and Joint Commanders by executing three major functions, detailed in Army Regulation (AR) 10-87[4]:

1. **Conduct operations** – Commander ARCYBER is dual-hatted as Commander Joint Force Headquarters – Cyber (Army) and plans, integrates and executes full-spectrum Cyber Operations (operate, defend, attack), Electronic Warfare (EW) and IO missions in support of US Cyber Command (USCC), designated Geographic Combatant Commands, and the Army.
2. **Provide forces** – ARCYBER supports USCC with Army Cyber Forces and supports Army operational commanders with tailored Cyber, IO, and EW forces. ARCYBER is the Title 10, "*Organize, Train, and Equip*" headquarters for specific force types identified by the Secretary of the Army.
3. **Accelerate the state of Army information convergence** – ARCYBER is the central focal point for identifying, synchronizing, and advocating operational Cyber, IO, EW, and other information capability needs supporting Army and Joint operational missions.

Central to all these functions is the Army Network. As the foundational weapon system of a global, information age, land force, the Army Network is one of six specified Army modernization priorities.[5] Today, US forces are continually engaged in simultaneous competition and conflict around the world. Our adversaries recognize that our formations are highly dependent on data and connectivity, and thus our network presents a critical vulnerability. ARCYBER is the builder, operator, and defender of the Army sector of the Department of Defense (DoD) Information Network (DODIN-A). ARCYBER's ability to successfully defend the network, data, and interconnected weapons platforms from adversary attack is a critical prerequisite for all successful Army and Joint operations.

Within ARCYBER, and this article, "IW" refers to the converged employment of Cyber Operations (CO), EW, and IO forces, and the capabilities that support Army and Joint operations. Acknowledging the more extensive transformational requirements of the Army and the broader national security system, IW here refers to increasing the effectiveness of assigned ARCYBER forces through a mission-designed organization, experimentation, innovation, and systematic learning. By routinely deploying and employing converged IW formations, ARCYBER gains knowledge and experience through "sets and reps" as part of a larger Army campaign of learning.

THE ARCYBER TRANSFORMATION CAMPAIGN

To fulfill the full spectrum of AR 10-87 responsibilities, both specified and implied, and anticipating emerging requirements driven by accelerating technology advances, ARCYBER has committed to a multi-year modernization effort. The ARCYBER transformation is envisioned to last more than ten years and is focused on supporting the Army's evolving Multi-Domain Operations (MDO) concept. Through deliberate iteration, ARCYBER will play a critical role in the total Army's capacity and skill to operate within and achieve operational advantage through the IE. Army actions, contributing to Joint OIE effects, will involve continuously posturing, and skillfully communicating (or obscuring), the location, capability, and intent of Army forces to influence the decision calculus and behavior of principal adversaries. This work involves the integrated employment of conventional land forces together with information and cyberspace capabilities, synchronized through as-yet-undeveloped combined information arms techniques. ARCYBER must enable the operational Army to sense, understand, decide, act, and assess more rapidly than our adversaries and enable Army and Joint Commanders' ability to achieve decision advantage.

Internally, ARCYBER will work to build information capabilities into combined arms teams with converged cyber, influence, and electromagnetic capabilities that deploy to bring immediate, turn-key informational combat power to maneuver commanders. Externally, ARCYBER will work with TRADOC and the broader institutional Army to build IE literacy into commissioned and noncommissioned officer training and curricula, that we might collectively cultivate a new, 21st century Operational Art that leverages the ever-growing force of information and communication to amplify and empower the timeless, coercive power of violence. Simultaneous, parallel efforts—ARCYBER internal reorganization and transformation, external engagement and support to total Army information modernization efforts, and sustained experimentation and innovation in Army operations and execution of assigned Joint missions—will allow ARCYBER to provide a powerful center of gravity for improving land power effectiveness in modern military operations. Key to our success will be our ability to partner effectively with the U.S. Army Reserve and Army National Guard Cyber, and Information Forces.

The first phase of modernization, already well underway, aims to achieve irreversible momentum toward full-spectrum, integrated IW capability by the summer of 2021. From mid-2021 through 2028, Phase 2 will continue experimentation and innovation to meet operational

opportunities and challenges presented by emerging technologies. Sitting at a unique nexus of the operational and institutional sides of the Army, ARCYBER will connect academia, industry, and Army acquisitions directly to ongoing operations, and rapidly integrate cutting-edge solutions into the operational force. Beginning in 2028, Phase 3 will see the resourcing and fielding of IW capabilities and formations, tailored to enable IW in support of MDO. ARCYBER deployable capabilities will augment information capabilities by then increasingly organic to maneuver formations, that enable the Army to dominate competitive environments short of armed conflict, and set conditions for the Army to prevail, where deterrence fails.

ARCYBER's transformation will be significantly less successful without thoughtful integration of Army Reserve and Army National Guard Cyber, and Information Warfare capabilities and forces.

ARCYBER PROGRAMS AND INITIATIVES

Phase 1—by Mid-2021, Achieve Irreversible Momentum. Multiple programs and new formations are already expanding ARCYBER's reach and effectiveness; these include:

- ARCYBER Headquarters move from Fort Belvoir, VA, to Fort Gordon, GA. In preparation for more than five years, 2020 will see this relocation of the ARCYBER Commander and headquarters staff to a state-of-the-art-facility co-located with the National Security Agency, and thereby optimizing seamless access to critical infrastructure enabling ARCYBER's core defense, offense, and network operations missions. For the first time, the Army's operational and institutional Cyber forces will enjoy unprecedented synergies by operating from a single, information power projection platform.
- Cyber Protection Brigade (CPB)—Activated at Fort Gordon in 2014, the CPB trains and deploys specialized Cyber Protection Teams (CPTs) to defend key cyberspace terrain. CPTs augment supported unit network defense ability to provide advanced assessments and defense against sophisticated and persistent cyber threats on Army and partner networks, systems, and data within the Army portion of the DODIN. CPB also provides the Army with unique, centralized analysis of threat data, trends, forensics, analytic support, and capability requirements. The CPB's two battalions provide 20 CPTs in support of Army and Joint operational forces. Of increasing importance, the Army Reserve and Army National Guard are fielding an additional 21 CPTs. These Compo 2 and 3 forces meet the same training standards as their active duty counterparts and are already contributing to operations.
- 915th Cyber Warfare Battalion (CWB)—Activated at Fort Gordon in 2019, the 915th CWB trains and deploys Expeditionary Cyber Teams (ECTs) to augment corps and below formations. ECTs provide offensive Cyber, IO, and EW capability not now fielded to tactical units. At full operating capability, each of 12 ECTs will have organic cyber development capability, network support, and capability to operate independently or as integrated into a supported unit headquarters.

- 1st IO Command (1st IOC)—The Army's only active duty IO brigade, operational since 1994, has initiated a Force Design Update (FDU) that reorganizes the Brigade to increase the number of IO Field Support Teams (FSTs) available, expanding reach-back and social media capability, and adding capacity to support both conventional and Special Operations Forces. By late 2020, 1st IOC will also be directly assigned to ARCYBER and continue to provide expert IW planning support to include Operations Security (OPSEC), Military Deception (MILDEC), and IO's core synchronization and integration functions.
- Offensive Cyber Operations (OCO) Signal Battalion—ARCYBER has the approval to stand up a long-needed OCO Signal Battalion at Fort Gordon in late 2021, which will provide critical, dedicated support to Army cyber forces and Joint operational missions. The OCO Battalion will be a multi-compo organization, reflecting the critical mission previously performed by Army National Guard Cyber forces as "Task Force Echo."

Phase 2—2021-2027, Experiment and Innovate. Upon consolidating and achieving full operating capability at Fort Gordon, ARCYBER transformation will focus on employing and discovering newly possible operational capabilities enabled by the multiple new capabilities established in Phase 1. As Army commanders gain increased "sets and reps" integrating information capabilities into sustained operations, ARCYBER, in conjunction with TRADOC and Army Futures Command (AFC), will serve as the Army's key knowledge collector for emerging 21st century warfighting art in the IE. Critical initiatives during this phase will include:

- Information Warfare Operations Center (IWOC)—ARCYBER's Cyber Operations and Intelligence Center (ACOIC) will continue its transformation to become a full- spectrum IWOC. Featuring multidisciplinary, regionally focused cross-functional teams, the IWOC will give the ARCYBER Commander unprecedented, real-time ability to *sense* and *understand* the global IE, with 24/7 connectivity to all Army Service Component Commands (ASCCs) operational priorities, thereby leveraging the power of centralized visibility for all Army network traffic. This unique vantage point will allow ARCYBER to sense, understand, decide, and respond to emerging global IE conditions, providing options to Army senior leadership and regional Army and Joint Commanders with unmatched speed, enabling strategic decision advantage.
- Military Intelligence Brigade—Critical to IWOC success and decision advantage will be the establishment of a specialized Military Intelligence (MI) Brigade organic to ARCYBER and focused on the IE, including Cyberspace and the Electromagnetic Spectrum. This not-yet resourced Brigade will partner with the Intelligence Community, AFC, industry, and academia to continually develop, test, and employ cutting-edge technologies (AI, augmented reality, and human-machine interfaces) to analyze the massive data sets by combining traditional all-source intelligence with commercial threat data and open-source information.
- Network Command (NETCOM) Modernization—To achieve full operating capability, the ARCYBER IWOC will need to transfer many of its current functions to other organizations.

NETCOM, the long-standing strategic Army Signal command that secures, configures, operates, extends, maintains, and sustains the Army portion of the DODIN, is modernizing to take on the Defensive Cyber Operations (DCO) functions now performed by ARCYBER's ACOIC.

- Joint Force Headquarters Cyber-Army (JFHQ-C (A))—As ARCYER develops and converges IW capabilities, JFHQ-C(A) (once co-located with ARCYBER Headquarters at Fort Gordon) will immediately benefit and provide enhanced capabilities to USCC missions in support of U.S. Africa Command, U.S. Central Command, U.S. Northern Command, and other missions, as tasked.
- 780th Military Intelligence Brigade (Cyber) – The 780th is the Army's offensive cyberspace operations contribution to USCYBERCOM, providing 21 teams in support of National and Combatant Command requirements. In addition, it also maintains the Army's portion of the cyberspace operations infrastructure and owns the Army's Capability Developers, skilled coders whose skills enable both offensive and defensive cyberspace operations. These National Mission Teams and Combat Mission Teams are effects focused; they destroy, degrade, disrupt, deny, and manipulate targets in and through cyberspace. As IW matures, the missions assigned to these teams may shift towards shaping the information environment, particularly as cyberspace operations and operations in all other domains converge to enable MDO.
- Operational Experimentation—A key focus during Phase 2 will be ARCYBER support to emerging warfighting formations. As the entire Army experiments to develop capabilities that enable MDO, new, innovative formations will emerge. Already in 2020, ARCYBER is providing support to three such mission-specific formations:
  - Multi-Domain Task Force (MDTF)—The MDTF, developed by the Fires Center of Excellence (FCoE), provides an unprecedented long-range fires capability to theater-level commanders. ARCYBER is assisting in training and readiness support to the first MDTF's organic Intelligence, Information, Cyber, Electronic-Warfare, and Space Battalion (I2CEWS BN) that integrates a spectrum of information capabilities to enable long-range targeting.
  - Theater Information Command (TIC)—This Army Futures Command (AFC) concept is for a 2-star, forward-positioned command, providing theater commanders with enduring influence capabilities throughout competition, armed conflict, and consolidation operations. Similar concepts for IW Brigades are emerging from TRADOC for regional collection, analysis, and informational effects-generation formations, focusing full-time on the IE for ASCC and Joint commanders. ARCYBER will robustly support experimenting with these formations during the Joint Warfighting Assessments and DEFENDER exercises.

– Information Warfare Task Force-Afghanistan (IWTF-A)—The Army Special Operations community led the IWTF-A development during combat operations. The IWTF-A was formed in theater, with augmentation from 1st IO Command, around a revolutionary operational approach, designed and focused on achieving cognitive effects through the synchronized employment of maneuver forces and information activities. Leveraging hostile fire zone authorities, the IWTF employs Military Information Support Operations (MISO), social media collection, data analytics capabilities, and cutting-edge digital advertising technology to deliver highly effective influence messaging.

- Army Tactical Force Modernization—ARCYBER is proactively engaged in ongoing modernization efforts to embed appropriate, affordable IW capabilities in ASCC and below formations. Throughout Phase 2, current Cyber-Electromagnetic Activities (CEMA) cells will expand to include increased IO, PSYOP, and Public Affairs personnel, and upgraded capability packages to improve tactical commanders' information capabilities. ARCYBER will build mission-tailored, combined information arms teams to augment maneuver commanders with state-of-the-art, full-spectrum IW capability.
- Reserve Component Optimization—The overwhelming majority of information capabilities aligned to support conventional forces are found in the reserve component. These include Cyber, IO, Civil Affairs, PSYOP, and Public Affairs formations. Throughout Phase 2, ARCYBER will work to optimize the force structure, composition, and mobilization of Compo 2 and 3 forces to ensure conventional force commanders have the right capabilities to train and influence adversaries during competition.

Phase 3—2028 and Beyond – Multi-Domain Capable—By 2028, multiple capabilities and formations identified in 2020 and earlier will come online across the force, greatly enhancing Army commanders' ability to operate in the IE as part of MDO. The ability to conceptualize, design, and execute activities that effectively influence adversary perceptions and actions will be a critical aspect of an MDO-capable Army, particularly in increasingly important, never-relenting competition environments. MDO concepts will continue to evolve over the next decade. Already, TRADOC Pam 525-3-1 amply illustrates that information and influence are critical to the three "Competition Actions"[6] that Army forces conduct during MDO:

1. **Enable the Defeat of Information and Unconventional Warfare** — The Army defeats adversary Information Warfare[7] by Operations in the Information Environment (OIE).
2. **Conduct Intelligence & Counter-Adversary Reconnaissance** — This task is fundamentally information and analysis-based, and requires mastery of adversary military capabilities, collecting and analyzing the Operational Environment, including civil networks, and conducting deception.

3. **Demonstrate Credible Deterrent** — Deterrence requires communication. Adversaries obviously will not be deterred by capabilities we have that they do not know about. The Army must establish command and control mechanisms, ensure interoperability, and protect forward presence forces (including cyber and information protection) that achieve deterrence.

As part of the Joint Force, the Army must master these essential Competition Actions through what MDO calls "*active engagement*"[8] to become MDO-capable. In each critical task, ARCYBER will play an essential supporting role as the Army better develops its ability to conduct active engagement through the converged employment of maneuver and information capabilities focused on achieving desired cognitive effects and behaviors in our adversaries.

JOINT OPERATIONAL CONCEPTS

The Joint Force continues to adapt to changes in the OE through the publication of Joint Concepts such as the Joint Concept for Operations in the Information Environment (JCOIE), the Joint Concept for Integrated Campaigning (JCIC), and the Joint Concept for Human Aspects of Military Operations (JC-HAMO).[9] These powerful concepts each grapple with varying dynamics of information and how they impact the design and execution of military operations and the use of military force in the emerging Operational Environment. These Joint Concepts are driving better Army concepts, capabilities, and requirements that, in turn, enable Army forces to support Joint Operations in the IE (OIE). For example, in early 2020, the Army Cyber Center of Excellence (CCOE) completed an OIE Force Modernization Assessment (FMA), which generated 33 DOTMLPF-P[10] recommendations to mitigate identified gaps in the Army's IE capabilities. In 2021, the CCOE will produce an AFC-directed Information Functional Concept, which will articulate a long overdue theoretical foundation for viewing information as a military concept and driving doctrinal improvements to posture the Army to win in future competition and conflict.

CONCLUSION

When we look back as an MDO capable force, 2020 will stand out as a pivotal year for Army Cyberspace, EW, and IO forces. After decades of dabbling in tactical IO, the Army undertook a sweeping series of robust modernization efforts to dramatically transform ARCYBER to better enable commanders across the Army with the ability to sense, understand, decide, act and assess faster than our competitors and adversaries, gaining critical decision advantage in an era of information warfare.

NOTES

1. General James C. McConville, 40th Chief of Staff of the U.S. Army, https://www.army.mil/article/225605/40th_chief_of_staff_of_the_army_initial_message_to_the_army_team.
2. Joint Pub 3-13, 2014, U.S. Joint Doctrine defines the Information Environment as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."
3. Information Warfare is not a doctrinally defined term. Further, the acronym "IW" within DOD commonly connotes Irregular Warfare. In this article, "IW" refers only to the concept of information warfare, as described in the text.
4. Army Regulation (AR) 10-87, Army Commands, Army Service Component Commands, and Direct Reporting Units, 2188 Washington, DC: Government Printing Office, 2017, para 14-2, 17, details 10 specified tasks that are here grouped for clarity as three major functions.
5. The Army Modernization Strategy, https://www.army.mil/standto/archive_2019-10-17/.
6. TRADOC Pamphlet 525-3-1, The U.S. Army in Multi-Domain Operations, Fort Eustis, VA: US Army Training and Doctrine Command, 2018, https://adminpubs.tradoc.army.mil/pamphlets.html, 27.
7. The MDO concept internally defines IW as an enemy activity, see p. GL-6: "Employing information capabilities in a deliberate disinformation campaign supported by actions of the intelligence organizations designed to confuse the enemy and achieve strategic objectives at minimal cost."
8. TRADOC Pamphlet 525-3-1, para 3-5b, 27.
9. Joint Concepts, https://www.jcs.mil/Doctrine/Joint-Concepts/Joint-Concepts/.
10. Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy, http://acqnotes.com/acqnote/acquisitions/dotmlpf-analysis.