U.S. Army Heritage and Education Center

Historical Services Division

A Return to Information Warfare

Conrad C. Crane, PhD
Chief, Historical Services Division

Michael E. Lynch, PhD
Senior Historian

Jessica J. Sheets
Research Historian

Shane P. Reilly
Contract Research Analyst

U.S.ARMY

THE UNITED STATES ARMY WAR COLLEGE

U.S. Army Heritage and Education Center
Historical Services Division

Prepared By:

Conrad C. Crane, PhD
Chief, Historical Services Division

Michael E. Lynch, PhD
Senior Historian

Jessica J. Sheets
Research Historian

Shane P. Reilly
Contract Research Analyst

A Return to Information Warfare

Conrad Crane

The purpose of this paper is to come to grips with the expanded mission set for U.S. Army Cyber Command and to understand the evolution of Army concepts dealing with information warfare. In addition to this study, an appendix traces the evolution of relevant Army doctrinal terms for the most important and relevant components of information warfare.

The battle over information has been a part of warfare from its beginning. Advances in communication through the electromagnetic spectrum have further expanded the tools and possibilities in the field. Otto von Bismarck was able to incite the French into a very unfavorable declaration of war against Prussia just by manipulating the reported text of one telegram in 1870.[1] In 1905, the commander of the Russian fleet engaged in a lengthy battle to gather and deny signals intelligence as he steamed towards Vladivostok. He refused an opportunity to jam reports of the location of his ships being transmitted to the Japanese high command, instead dooming them to destruction at Tsushima.[2]

However, for American forces there has always been uncertainty about exactly what tasks comprise information warfare, who executes them, and how they should be organized and synchronized. The first field manual dealing holistically with Information Operations did not appear until 1996. At its core, information warfare is all about gathering, providing, and denying information in order to positively facilitate our decision-making while negatively influencing the enemy's. Historically, this has been accomplished mostly with various communication means, psychological operations, and

[1] Geoffrey Wawro, *The Franco-Prussian War* (New York: Cambridge University Press, 2003), 34-38.

[2] Mario De Arcangelis, *Electronic Warfare: From the Battle of Tsushima to the Falklands and Lebanese Conflicts* (New York: Sterling Publishing Company, 1985).

eventually electronic warfare and cyber operations. Achieving unification of those capabilities has always been a challenge, however, especially between the technical and informational elements. There have also been semantic difficulties with the baggage connected to terms. Since World War II, the United States has allowed the elements of information warfare to fragment and atrophy, while some of our potential enemies have not. The only exception to this trend was during the 1980s, when the focus on defeating the Soviets with AirLand Battle motivated a rejuvenated emphasis on countering certain information capabilities of that threat. A unifying but short-lived comprehensive definition of information operations incorporating all relevant functions reemerged by 2008, but later iterations became more vague about specific components.

In World War II, propaganda was still an acceptable term and a necessary mission. President Franklin Roosevelt realized very early that his nation had to not only be able to trumpet its lofty principles to the world, but also its power and capacity to wage war. For that purpose he eventually established the Office of War Information (OWI) to coordinate the American propaganda machine. But it had lots of competition. The Office of Strategic Services, precursor of the CIA, had psychological warfare functions connected to military operations overseas, and answered directly to the Joint Chiefs of Staff. Each theater commander had his own propaganda and psychological warfare programs. Supreme Headquarters Allied Expeditionary Forces in Europe had a very active psychological operations cell, and their Ops(B) section did a masterful job designing and executing Operation FORTITUDE, the deception plan surrounding the D-Day invasion. Gen. Douglas MacArthur was actively engaged in crafting messaging for his theater. OWI did provide some unity to America's information efforts, which might have been untidy but was very robust.[3]

Subordinate commanders also participated. In a very prescient consolidation that foreshadowed what our potential adversaries do today, but is anathema to civilian authorities in the United States, the 12th Army Group, the largest American field command in history, combined its publicity and psychological warfare elements into one detachment. Responsibilities included public relations, press censorship, and mobile radio broadcasting, in addition to normal publicity and psychological operations. This structure greatly facilitated synchronizing messaging in the Army Group's area of responsibility in Northwest Europe.[4] The Army Air Forces were very active in dropping leaflets and making radio transmissions to take advantage of the effects of strategic bombing. Maj. Gen. Curtis LeMay's 21st Bomber Command executed a very successful leaflet campaign to incite mass evacuations of Japanese cities that they were fire

[3] Charles Roeller, *The Art of Psychological Warfare* (Briarcliff Manor, NY: Stein and Day, 1974), 127-145; Scott C. Farquhur, "Deceive, Divert, and Delay: Operation FORTITUDE in support of D-Day," in *Weaving the Tangled Web: Military Deception in Large-Scale Combat Operations*, ed. Christopher M. Rein (Fort Leavenworth, KS: Army University Press, 2018), 137-154.

[4] Allied Forces, 12th Army Group, *History: Publicity and Psychological Warfare, 12th Army Group, January 1943-August 1945* (Washington, D.C.: Bureau of Public Relations, War Department, 1945).

bombing, eventually motivating over eight million civilians to flee to the countryside, causing significant disruptions of industry and widespread refugee problems.[5]

The Army Air Forces also were most energetic in the field of electronic warfare. Radio jamming had become widespread during World War I, but it was the advent of radar that really energized the field. During World War II it is estimated that American innovations to jam and confuse enemy detection systems saved 600 heavy bombers of U.S. Strategic Air Forces in Europe and 200 B-29 Superfortresses attacking Japan. Chaff and jamming also allowed aircraft to fly at lower altitudes where they could bomb more accurately.[6] Enemy electronic emissions also provided a wealth of intelligence, including direction finding. The cracking of German and Japanese codes contributed greatly to winning the war. Jamming, spoofing, and intercepting enemy radio transmissions were a common occurrence all along the battle fronts, often executed by special signals intelligence units, while measures to ensure and safeguard friendly communications were practiced by everyone.

Without any unifying American concept of information operations or warfare, the relevant Army functions and organizations went many different directions after World War II. For a while what we would term information operations were included in the linked concepts of propaganda and psychological warfare. However, as the former term was seen more as something the evil Communists did, it disappeared from the lexicon after the 1960s. Electronic warfare remained a major concern for air defense artillery and signal units and received significant coverage, as did psychological operations, in the AirLand Battle doctrinal manuals FM 100-5 aimed at defeating the Soviets in the 1980s. Of course military intelligence continued to focus heavily on electromagnetic emissions. Public Affairs officers appeared at all levels. Psychological operations (PSYOP) became more centralized and more neglected. PSYOP capabilities declined precipitously after every war, even after hard lessons from trying to rebuild PSYOP for Korea and Vietnam. Eventually Gen. Carl Stiner, second commander of the newly organized United States Special Operations Command (USSOCOM), convinced the Secretary of Defense to designate PSYOP and Civil Affairs as new capabilities under the control of USSOCOM in the early 1990s. This shift was also related to the separation of those Military Occupational Specialties from the Foreign Area Officer specialty which had provided their cultural foundation for so many years. The transfer actually went against the recommendations of a 1985 DoD Master Plan for PSYOP that feared their subordination under special operations would detract from the recognition of the applicability of psychological operations in all times of peace, crisis, and war, and would contribute to a lack of understanding about their uses and capabilities by military officers and senior civilians. In hindsight, these concerns appear to have been

[5] Conrad C. Crane, *American Airpower Strategy in World War II: Bombs, Cities, Civilians, and Oil* (Lawrence: University Press of Kansas, 2016), 176-177.

[6] Alfred Price, *The History of US Electronic Warfare* (Westford, MA: Murray Printing Company, 1984).

warranted, creating a vulnerability that can be exploited by potential adversaries with pervasive and integrated psychological operations that are also tightly linked to all their public affairs efforts.[7] The existence of "fake news" should be no surprise. It is nothing new, though the considerable expansion of means of communicating it is. But information warfare is not always fought with falsehoods. One of the primary tenets of General Petraeus's guidance for his forces in both Iraq and Afghanistan was to "Be first with the truth."[8]

Operations DESERT SHIELD and DESERT STORM launched widespread speculation about a new Revolution in Military Affairs and the advent of warfare in the Information Age. All the elements of contemporary information warfare were present. A team of U.S. intelligence operatives slipped several virus-laden computer chips into a French-made computer printer that was smuggled into Baghdad. The printer was eventually delivered to a command bunker of the Iraqi air defense network, where the viruses helped degrade command and control of the whole system, which was also targeted by anti-radiation missiles and intensive electronic warfare.[9] The 4th Psychological Operations Group (Airborne) handled propaganda broadcasts and leaflet campaigns for CENTCOM. There were some problems with the USSOCOM-centralized psychological operations, however, as elements of the group supplied to the United States European Command were limited in scope and efficiency by Turkish intransigence. There were also problems coordinating messaging for the home front. Both civilian and military leaders were particularly displeased with Peter Arnett's CNN broadcasts from Iraq, and coalition planners went so far as to indict him as a conduit for Iraqi disinformation. Images of the "Highway of Death" displayed in newspapers and on television screens played a key role in President George H. W. Bush's decision to end combat after only 100 hours.[10]

The technological euphoria that afflicted many military analysts after the Persian Gulf War also affected the Army. The 1993 FM 100-5 *Operations* replaced AirLand Battle with a new doctrine that assumed "near perfect, near real-time intelligence systems, sufficient lethality with precision strike systems, and massing of lethal effects,"

[7] Alfred H. Paddock, "No More Tactical Information Detachments: US Military Psychological Operations in Transition," in *Psychological Operations: Principles and Case Studies*, ed. Frank L. Goldstein (Maxwell Air Force Base, AL: Air University Press, 1996), 25-50; USSOCOM History and Research Office, *United States Special Operations Command History* (MacDill Air Force Base, FL: HQ USSOCOM, 1998), 7; AirLand Battle FM 100-5 *Operations* were published in 1982 and 1986.

[8] Headquarters, Multi-National Force – Iraq, "Multi-National Force-Iraq Commander's Counterinsurgency Guidance," 15 July 2008; Headquarters, International Security Assistance Force/ United States Forces-Afghanistan, " COMISAF's Counterinsurgency Guidance," 1 August 2010.

[9] U.S. News & World Report, *Triumph Without Victory: The Unreported History of the Gulf War* (New York: Times Books, 1992), 224-225.

[10] Richard D. Johnson, *Seeds of Victory: Psychological Warfare and Propaganda* (Atglen, PA: Schiffer Military/Aviation History, 1997).

along with “the use of overwhelming force as a way of achieving victory with minimum cost to friendly forces.”[11] While the flaws in the new 100-5 would not be apparent until a decade later, the perception of a new age of warfare also motivated the adoption of FM 100-6 *Information Operations* in 1996. This was the Army’s first attempt to come to grips holistically with the concepts and execution of information warfare in doctrine, and as first editions of field manuals often are, remains the most comprehensive service treatment of the subject.

Unlike the current FM 3-13, the 1996 manual attempted to grapple directly with the execution of information warfare, which it defined as “actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems and computer-based networks while defending one’s own information, information-based processes, information systems and computer-based networks.” There were three interrelated operational components: Command and Control Warfare (C2W), Civil Affairs, and Public Affairs. The most complex was C2W, which attacked and defended with electronic warfare, destruction, psychological operations, operational security (OPSEC), and deception components, all undergirded with relevant intelligence and robust information systems. Civil Affairs was primarily concerned with relationships between military forces, civil authorities, and people in the area of operations, including Non-Governmental Organizations and Private Volunteer Organizations. Public Affairs was focused on working with the media. Cyber capabilities were part of all of them, and there was a whole chapter describing various information systems and capabilities. But the manual recognized that Public Affairs was an important component of information warfare, and therefore linked with other elements like psychological operations. Our adversaries have been much more willing to directly link Public Affairs and PSYOPS than we have been.

I wish I had been aware of FM 100-6 in 2011. Aware of the work I had done with FM 3-24 *Counterinsurgency* for my West Point classmate Gen. David Petraeus, another classmate, Gen. Keith Alexander, head of the National Security Agency, asked me to help with an effort to develop a similar operational manual for USCYBERCOM, which he also led. The effort eventually failed, primarily because everyone looked at the project and subject as all brand new, with no prior precedents to build upon. FM 100-6 actually would have been a good model to use to provide some ideas for a structure and approach that could never be established.

Looking at the U.S. Army Cyber Command mission today, which “integrates and conducts full-spectrum cyberspace operations, electronic warfare, and information operations, ensuring freedom of action for friendly forces in and through the cyber domain and the information environment, while denying the same to our adversaries,” it appears to be heading back towards the all-encompassing vision of information warfare from FM 100-6, that appeared in its clearest expression for a short time in FM 3-0 and

[11] Deputy Chief of Staff for Doctrine, *Reader’s Guide: FM 100-5, 1986-1993 Comparison* (Fort Monroe, VA: HQ TRADOC, 1993), 1.

JP 3-13 in 2008. At that time, however, there was no single organization with overall responsibility for that line of effort. U.S. Army Cyber Command now seems ready to fill that role. Perhaps it should be called the U.S. Army Information or Information Warfare Command, though it should also be noted that the definitions of cyber operations and electronic warfare are now very similar, both discussing attack, protection, and system support. There are many obvious challenges. The Army's Electronic Warfare (EW) capabilities, omnipresent in my Air Defense Artillery career in the 1970s and 1980s, have atrophied. It is revealing that in order to conduct EW against enemy improvised explosive devices (IEDs) in Iraq, the Army had to bring in electronic warfare personnel from the Navy. Psychological Operations and Civil Affairs are the domain of USSOCOM now, and have also declined in overall capability and awareness. Attitudes and policies about cyber capabilities tend to discourage or discount their many links to other aspects of information warfare. I would argue that the name of the command contributes to that. And the whole idea of American information warfare suffers from a lack of a controlling national policy and structure. In addition, we live in an era where potential adversaries will try to keep their challenges in the realm of competition below any combat threshold, but they still engage in constant information warfare that has domestic impacts in the United States every day. This is a mission the Army must exercise diligently and robustly all the time, constantly adjusting its targeting strategies to deal with the level and type of threat offered by competitors or adversaries.

However, this appears to be a time of opportunity for U.S. Army Cyber Command to reestablish Army dominance in information warfare. In my opinion, that will require a change in name, new doctrine, and regaining control of relevant organizations. Joint and national reform is also probably necessary. But considering the displayed competence and unity of effort of potential adversaries in information warfare, an aggressive and innovative response is required.

Appendix A: The Evolution of Definitions Concerning Information Warfare

Propaganda:

Propaganda Branch, War Department General Staff, G-2, “A Syllabus of Psychological Warfare,” 1946 - Propaganda may be loosely described as “organized non-violent persuasion.” More technically, it may be defined for Army purposes as follows: Military propaganda consists of the planned use of any form of communication designed to affect the minds and emotions of a given enemy, neutral, of friendly foreign group for a specific strategic or tactical purpose.

FM 33-5, Psychological Operations, 1962 - What do we mean by propaganda? In its broadest sense, it is the technique of influencing human action by the manipulation of representations. These representations may be in spoken, written, pictorial, or musical form. For the purpose of this manual we define it as any information, ideas, doctrines, or special appeals disseminated to influence the opinions, emotions, attitudes, or behavior of any specific group, to benefit the sponsor, either directly or indirectly.

FM 33-1, Psychological Operations, 1968 - Propaganda is any form of communication designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly.

JP 3-53, Doctrine for Joint Psychological Operations, and also in JP 1-02, 2003 - Any form of communication in support of national objectives designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor either directly or indirectly.

Definition is no longer in JP 1-02.

Psychological Warfare/Operations

“A Syllabus of Psychological Warfare,” 1946 – Psychological Warfare has been defined as warfare psychologically waged: that is, military operations carried out with close and studied reference to the politics, opinion, and morale of the enemy. It is not in this sense that the term has been used in American practice during World War II. Psychological warfare has been, more narrowly, defined as comprising the use of propaganda against an enemy, together with such other operational measures of a military nature as the effective use of propaganda may require.

FM 33-5, 1962 – Psychological operations in its broadest sense means the use of propaganda and other political, economic, military, and ideological actions to influence human actions and behavior favorable to the originating agency for a specific purpose in peace or war. Within this broad concept are included the simplest advertising appeal and publicity techniques, including public relations.

FM 33-1, 1968 – Psychological operations: The planned use of propaganda and other measures to influence the opinions, emotions, attitudes, and behavior of hostile, neutral, or friendly groups in such a way as to support the achievement of national objectives.

FM 100-5, Operations, 1982 – Propaganda and other PSYOP techniques for changing the attitudes and behavior of target groups provide the commander with his primary means of communication with opposing military forces and civilian groups. When effectively integrated with other operations, PSYOP add to the relative combat power of the force. They manipulate the psychological dimension of the battlefield –

> To reduce the combat effectiveness of enemy forces.
>
> To promote support for friendly forces by foreign populations or groups.
>
> To reduce the effectiveness of enemy PSYOP directed toward friendly forces and supporting civilian groups.

FM 100-6, Information Operations, 1996 – Psychological operations are defined as operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately, the behavior of foreign governments, organizations, groups, and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.

JP 3-53 and JP 1-02, 2003 – Psychological Operations: Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign government, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.

Definition is no longer in JP 1-02.

Electronic Warfare

FM 24-1, Tactical Communications Doctrine, 1968 – Today's arts of war must include action to degrade or destroy the enemy's effective use of communications-electronics systems. At the same time, we must take all possible action to insure our own effective use of communications-electronics equipment and systems. Electronic warfare consists of the fields of electronic countermeasures and electronic counter-countermeasures. Total understanding of the field of electronic warfare also requires an understanding of the fields of communications intelligence and communications security.

FM 24-1, Combat Communications, 1976 – EW is actions taken to prevent or reduce the enemy's effective use of the electromagnetic environment, and actions taken to insure our own effective use of radiated electromagnetic energy. (Added Electronic Warfare Support Measures to ECM and ECCM as components of EW.)

FM 100-5, 1982 – Armies based on the Soviet model will attempt to control the electromagnetic spectrum through the use of radio electronic combat. They will analyze an opponent's communication system by signals intelligence to find the terminals, links, and relays vital to command and control. Then, following their commander's priorities, they will attempt to destroy or disrupt those communications. Soviet forces will try to jam selected air defense radars, but they will target most radars for destruction by artillery.

FM 100-5, 1993 – Electronic warfare uses the electromagnetic spectrum to locate enemy units and facilities, to intercept enemy communications, and to disrupt enemy C2 and target acquisition systems at critical moments. Commanders employ joint EW systems as they employ fires. They use the effects of these systems to slow, misdirect, or confound enemy operations and synchronize them accordingly. EW operations occur concurrently at all levels. (With demise of Soviet threat, focus has shifted from defense to offense.)

FM 3-38, 2014 – Electronic warfare is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or attack the enemy. EW consists of three functions: electronic attack, electronic protection, and electronic warfare support.

FM 3-12, 2017 – Electronic warfare refers to military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. EW capabilities enable Army forces to create conditions and effects in the EMS to support the commander's intent and concept of operations. EW includes EA, EP, and ES and includes activities such as electromagnetic jamming, electromagnetic hardening, and signal detection, respectively.

JP 1-02, 2019 - Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. (Still includes EA, EP, and ES as components.)

Information Operations/Warfare

FM 100-6, 1996 – Information warfare: Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks.

FM 3-0, Operations, 2008, and JP 3-13 – Information operations: The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decisionmaking while protecting our own.

FM 3-13, Information Operations, 2016 and JP 1-02, 2019 – Information operations: The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.

Cyberspace Operations

FM 3-38, Cyber Electromagnetic Activities, 2014 – Cyberspace operations are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Cyberspace operations consist of three functions: offensive cyberspace operations, defensive cyberspace operations, and Department of Defense information network operations.

FM 3-12, Cyberspace and Electronic Warfare Operations, 2017 – Cyberspace operations are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. The interrelated cyberspace missions are DODIN operations, DCO, and OCO. A cyberspace capability is a device, computer program or technique, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace.

JP 1-02, 2019 - Cyberspace operations: The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. (There are other definitions for cyberspace attack, capability, defense, exploitation, security and superiority.)

U.S. Army Heritage and Education Center
U.S. Army War College
950 Soldiers Drive
Carlisle, PA 17013

http://ahec.armywarcollege.edu