Information Warfare
Farwell, James P.

Published by Marine Corps University Press

Farwell, James P.
Information Warfare: Forging Communication Strategies for Twenty-first Century Operational Environments.
What channels are available to reach your intended audiences? Some audiences depend on television (e.g., those viewing Al Jazeera or Al Arabiya). Others prefer word of mouth (e.g., Somalia). Still others have restricted access to the internet. Government censorship or filtering impacts how audiences receive information. This chapter provides an overview of social media—what it is, how it can and should be used, and when it can be an effective part of your communication strategy.

Thomas Elkjer Nissen of the Royal Danish Defence College in Copenhagen has articulated the emerging role of social media in engagements and conflicts and how it is being weaponized.¹ He demonstrates how, during the past 15 years, social network media has “become an integral part of the conflict environment” and progressed ever since Kosovo in 1999.² It includes counterinsurgency campaigns in Afghanistan and Iraq, conflicts between Israel and the Palestinians, and clashes in Lebanon, Afghanistan, Iraq, and Syria. Social media now plays an important role in the politics of nearly every nation, and its utility has been demonstrated by forces that represent democratic and authoritarian powers.³

As Rupert Smith pointed out, the internet has connected audiences globally, rendering every home with a television or computer a battlefield for control over the narrative.⁴ Journalist David Patrikarakos has offered excellent illustrations for how Palestinians and Israelis have employed Twitter to control the narrative, and in doing so, achieving international strategic effects.⁵ Retired Marine Corps colonel Thomas X. Hammes also wrote brilliantly about the impact of information warfare.⁶ In examining how social media has been weaponized, Nissen and others have defined many of its tactics and potential in influencing perceptions and opinions in the battlespace. As Nissen notes and David Kilcullen, former advisor to General David Petraeus, has pointed out, all of this occurs as the character of conflict has grown more urban, enabled by technology, and—by becoming more accessible to broad swaths of parties—empowering. That is rendering war more about local power, money, and control.⁷
The bottom line is that social media networks play an increasingly pivotal role in contemporary conflicts. Regardless of the specific social media platform, they are “all online technologies and practices that people use to share content, opinions, insights, experiences, perspectives, and media themselves.”

In the past few years, and notably since 2016, any analysis of the use of social media must account for the increasingly pervasive use of so-called fake news (i.e., propaganda) that has permeated much of the discourse about the use of social media. The intervention by Russia in the U.S. elections in 2016 has provided strong impetus and awareness of disinformation tactics. The increasing use of bots and fake accounts for social media posts complicates the challenge. The onset of artificial intelligence will further intensify the challenge.

A detailed discussion of social strategies and tactics lies beyond the scope of this book, but operators need to comprehend the utility of social media networks and technologies and how to capitalize on them, recognizing that they continue to rapidly evolve.

**Social Media: What Is It?**

*Social media* refers to internet-hosted digital tools used for sharing and collaboratively creating information by individuals and communities. It empowers individuals to participate in dialogue. A staggering 4.333 billion people in the world were active internet users as of July 2019, encompassing 56 percent of the global population. While technical definitions of social media vary, most agree that it is online media whose primary purpose is reader/viewer cocreation or reader/viewer interaction. This includes most blogs and all forums, microblogs (e.g., Twitter), discussion boards, websites, and sharing sites (e.g., YouTube, Pinterest, Instagram, Facebook). Any website that invites viewers to interact with the site and with other visitors falls into the broad definition of social media.

Social media offers many benefits for individuals and organizations, but there are drawbacks. The ability to reach global audiences is both a blessing and a curse; it also enables the uninformed (and others) to widely propagate narratives that bear little relation to the truth, distorting debate and spreading misinformation.

Traditional media, whether print or digital, such as daily newspapers or television, offers a more tightly controlled information environment. It is a one-way street; information flows in one direction only, with publishers and broadcasters serving as gatekeepers to decide what is disseminated. Social media is a multidirectional highway, but one that lacks proper lanes, speed limits, and dead ends.

Scholars Jennifer Aaker and Andy Smith label the successful use of social media the “Dragonfly Effect.” Their model is based on the mechanical functions of a dragonfly’s four wings. Each wing serves a different purpose, but they all must move in harmony. An effective social media communications campaign should emulate this.

- Focus on a single, measurable goal.
- Grab attention—cut through the noise that clutters other social media chatter.
- Hook the audience with a personal connection or higher emotion to engage an audience more fully.
- Take action that moves audiences from being listeners to team members. If you have a call-in number, make sure you have someone there to answer the phone who can do something with the call.
The theory applies to military operations or strategy. All four components (wings) are vital to effective communication.

**Difference from Traditional Media**

Social media differs from traditional media in its interactive component and user-generated content. Social media comes in different forms, including blogs, microblogs, wikis, forums, podcasts, social networking sites, and virtual worlds.

- Blogs are websites that allow users a venue for publishing their points of view, allowing readers to comment, and carrying on conversations using the commenting feature. This medium has become popular in target countries where media environments are tightly monitored and controlled.
- Microblogs are websites similar to blogs, but with user-generated content limited to 140 characters. This medium allows users to quickly and efficiently disseminate information to large networks in short segments. Twitter is an example.
- Wikis are informal information sites that allow users to create and edit content on webpages. Wikipedia is the classic example.
- Forums are online discussion sites that often include reposting of traditional media content. Many forums are password protected or require registration to participate and/or view discussions.
- Podcasts are online digital audio or video media files.
- Social networking sites such as MySpace and Facebook allow users to list interests and link to friends, sometimes annotating these links by designating trust levels or qualitative ratings for selected friends.
- Virtual worlds are computer-based simulated environments that allow users to socialize via online personalities (avatars).

Social media generally reaches fewer people than well-circulated newspapers or magazines, but social media platforms are extremely dynamic. New topics constantly emerge and are readily overtaken by even newer topics. Different types of social media will rise and fall in popularity, making it challenging to maintain visibility of some sites and issues.¹⁵

**A Historic Geographic Shift**

The global online population is shifting dramatically and growing fast. Today about one-third of the world’s population is online.¹⁶ New users tend to be young and from the developing world. Nearly one-half the online population is under age 25. Users in the developing world increased from 44 percent to 62 percent from 2006 to 2011.¹⁷

The most striking shift has come from burgeoning populations in the southern and eastern parts of the globe. In 2011, Atlantic and European populations accounted for only 35 percent of online users. The Asia-Pacific region boasted 45 percent of users even though only 24 percent of those populations had access to the internet.¹⁸

Most of the new users will use mobile devices as 3G services spread throughout the Asia-Pacific region.¹⁹ Many developed nations there already boast a 90-percent penetration rate. Globally, there are 3.3 billion smartphone users in the world today, and 5.13 billion people have mobile devices
in 2019. There are nearly 9 billion mobile connections among a world population of 7.7 billion.\textsuperscript{20} 

**Going Viral**
Communication specialists deftly use social media outlets to propagate a narrative. You need to watch for the pitfalls of doing so. Those who obtain information through social media do not always distinguish between a trained communications expert and a novice blogger. When a story becomes popular online, it can spread like an uncontrolled virus and reach audiences beyond the world of social media. That is called *going viral*.

Narratives that go viral elude an obvious pattern. They vary in content and format. Some are video clips, texts, games, images, webpages, emails, or audio recording. Some are hilarious anecdotes of animal behavior, political mishaps, songs, or even online ads.

**Using Social Media to Influence Target Audiences**
When does it make sense to use social media? It depends on the target audience. Those with limited access to the internet or heavily state-controlled internet usage may still find it is a key source for

---

**KEY SOCIAL MEDIA TYPES**

Social media is evolving, with new tools, services, and consumers:

- Blogs (WordPress, Blogger)
- Conversation applications (Facebook Messenger)
- Crowdsourcing (Tweetbrain, YahooAnswers)
- Discussion forums
- Gamification
- Geolocation
- Image content sharing services (Pinterest, Instagram)
- Microblogs (Twitter)
- Mobile calling (callwave)
- Multimedia
- News aggregators (digg)
- Photograph sharing (Flickr, Picasa)
- Podcasts
- Search (Google, Ask, Bing)
- Social bookmarking
- Social knowledge
- Social networking (Facebook, MySpace, LinkedIn)
- Video sharing networks (YouTube)
- Virtual worlds (Second Life, Kaneva)
- Wikis (Wikipedia)
command and control, collecting or receiving information or intelligence, surveillance, or reconnaissance. Rebels fighting Bashar al-Assad’s government found themselves in that position.

Where internet connectivity is more widespread, social media can be vital to reaching key decision makers. Social media can add depth, reach, and perspective to a campaign that use of traditional media sources cannot equal.

Social media invites shorter texts. Language is often less formal and often grammatically deficient. That is not necessarily bad. In *Twitterville*, Shel Israel comments that “Twitter lets us behave online more closely to how we do in the tangible world.” David Patrikarakos has offered keen insights into how Twitter is reshaping conflict, empowering individuals, and breaking down traditional barriers that existed when institutions acted as gateways to information. The impact, for example, that a single Palestinian tweeter, Farah Baker, had on shaping public perceptions was so strong that it sent the imaginative Israelis scrambling to match her messaging with their own ingenuity. In Ukraine, the power of Facebook has proven indispensable to marshalling support for anti-Russian forces.

The internet can be weaponized to communicate a message through action. In 2015, Russia launched BlackEnergy, a malware program. It struck the power grids of the Ivano-Frankivsk region of western Ukraine, knocking out electrical grids during a cold period. Former FBI agent and social media expert Clint Watts accurately points out that such attacks sought to damage infrastructure and undermine Eastern European countries through humiliation and confusion. The actions communicated a message about power and the price of opposition, and it inflicted harm.

Understand how target audiences consume social media information and engage by using social media tools. Persuasive messaging must blend into the social media environment. Tone, language (e.g., colloquial speak), acceptable misspellings for shortening phrases (e.g., Twitter users’ preference), and the frequent inclusion of website links embedded in social media text are important.

Watts has offered compelling insights into the use of weaponized social media that operators may have to contend with. Effective social media armies, he contends, consist of three types of accounts:

- **Hecklers**: these identify and drive wedge issues into target audiences, talking up online allies and arming them with propaganda that confirms audience member beliefs. They also target social media adversaries to arouse hostility against them. Hecklers, he says, do not hack computers. They hack minds. They seek to change audience perceptions on issues or personalities. They try to batter adversaries off social media.

- **Honeypots**: these aim to lure unsuspecting targets into engagement that may cause them to divulge location or personal information that forms valuable intelligence. This is the type of tactic that an enemy can be expected to use against soldiers. You might receive a Facebook message from an account that appears to belong to a gorgeous woman or handsome man. The profile image will seem real, but it may be an avatar—an artificially generated image. The account’s goal is to gain insights and intelligence.

- **Hackers**: sometimes highly networked with honeypot accounts, these attackers may deliver malware to elicit valuable personal information. The danger that hacking or honeypots pose for field oper-
ators is that if they can penetrate firewalls or overcome passwords and steal personal information, they may find a fact they can use to blackmail you.24

Such tactics require commanders and operators to learn and apply basic lessons of cybersecurity defenses, starting with password security and staying on the alert to guard against spear phishing—getting tricked by attackers when receiving apparently legitimate emails into giving away passwords or other personal or sensitive information.25

Bots present an increasing threat. German researchers concluded that bots are “capable of massively distributing propaganda in social and online media” and can be “partly responsible for election results.”26

Bots enable operators to flood voter perceptions with false or misleading assertions. They can overwhelm the capacity of humans to respond. Aided by a coming era of artificial intelligence (AI), the dangers posed by bots will escalate. Foreign service officer Matt Chessen has articulated the dangers of a dystopian social media environment that this poses in his report The Madcom Future, which this book’s author recommends to every reader.27 Chessen points out that soon enough, the image of a close friend you may see on your cell phone, tablet, or computer may be an avatar yet know more about you than any friend—or even you—know.

The potential for use offensively and defensively in tactics and operations is enormous. It is vital for operators to learn how to use them tactically. Your cell phone or tablet is a mobile office, if used correctly. Just ensure that proper steps for encryption are taken to preserve security at rest, in transit, and at destination and that use of mobile devices or computers comports with the security guidelines that govern your operations. Never presume the adversary is less sophisticated than your side. ISIS demonstrated a high order, and state proxies or states aligned against us are supple, flexible, agile, and imaginative.

**Social Media as an Intelligence Tool**

Social media intelligence (SOCMINT) and open source intelligence (OSINT) are invaluable in developing situational awareness and strategy. For example, tracking social unrest in social media channels provides key data points:

- What are the topics being discussed?
- Who are the key messengers?
- Where are they spreading these messages?
- Are there discernible networks?
- How are they doing it?
- What is the reaction to these messages and messengers?
- Are there countermessages emerging?

Intelligence analysts and military operators can use social media analysis in a variety of ways to aid them in fulfilling their missions.

- Early detection and assessment of emerging issues
- Identification and tracking of key communications by influential individuals, organizations, and their networks
- Analysis of recurring communications and messages and how they shape attitudes and behaviors to push perceivers to act

Social media enables you to monitor unofficial online dialogue. It helps detect emerging narratives and key voices that have resonance, which can enable an intelligence analyst to track discourse on issues and key messages in open source media and
to apply emerging technology to assess the resonance of each. It helps develop countermessaging and countermessengers. It enables you to help analyze an entire media campaign related to a military operation: editorials, authors, media type, etc.

Measuring how audiences are exposed to certain messaging—favorable or unfavorable to your military strategy and desired outcome—aids in determining support or opposition to on-the-ground tactical military efforts.

**Direction of Social Media**

Technology is advancing what is possible in social media. Various platforms illustrate how the social media landscape is rapidly changing and affecting the capacity of parties to articulate story, narrative, theme, and message, as well as to recruit and mobilize.²⁸

- Twitter has acquired unprecedented influence. Diverse parties including ISIL, Israel, Palestine, Russia, and famously, President Donald J. Trump, have employed it extensively and demonstrated its impact.
- Facebook is closing in on the 2 billion-user mark each month. ISIS used it, YouTube, and Twitter extensively to intimidate enemies and to recruit, mobilize, and drive its narratives.²⁹ Yet, the example of Facebook shows how rapidly situations evolve. In late November 2017, Facebook reported that it was successfully removing 99 percent of content related to militant groups tied to the Islamic State and al-Qaeda, blunting their ability to exploit the platform.³⁰ Some have argued that Facebook appeals to older generations, but political campaigns as well as violent extremist groups such as ISIS have made strong efforts to capitalize on it.
- YouTube is used by 1.3 billion people. About 300 hours of YouTube content are uploaded to the site every minute. Nearly 5 billion videos are watched on it every day. About 80 percent of those age 18–49 watch it, and 60 percent prefer online video platforms to live television.³¹
- Instagram enables you to post photographs with a caption. It is especially popular with younger audiences.
- Chirp is an enhanced shared media, offering a free, open-source tool for programming amateur radio.
- Flayvr is a photo and video sharing program. It is a gallery app that organizes photographs and videos into moments.
- Conversations is a tool to integrate social media and interoffice communications into business operations.

**Emerging Technologies and Their Impact on Operations**

The internet and social media rank among key drivers that influence people around the world. They fuel emotions, shape perception, and provide understanding into what motivates and shapes behavior. Technology is enabling us to understand the emotional affinity between language and target audiences, and how language can be used to motivate audiences to act. This technology moves us beyond measuring sentiment—whether a party holds a favorable or unfavorable view toward statements, ideas, or people—into understanding emotional triggers that can be integrated into strategy, operations, and tactics.

These drivers affect every country and culture. They affect messages articulated by influencers.
Emerging technologies are enabling us to help measure how influencers affect outcomes. The information derived can support

- Operational plans
- Current and emergent operations
- Strategic planning operational teams
- A better understanding of intelligence and enemy objectives
- Strategic appreciation of ground realities
- Commanders’ strategic planning process
- Understanding to help identify and counter adversarial story, narrative, themes, and message
- Measuring the impact of influencers and operations on target audiences

**Emerging Capabilities**

New automated technologies have had a dramatic effect on the collection of information and intelligence. Technology enables real-time search-based capabilities on most social media outlets; adversary communications in print, broadcast, and online; image/object data extraction; social network mapping; sentiment detection; automatic translation; and internet infrastructure monitoring.

- Social media collection includes custom drawing and indexing of sources on both the light web and dark web.
- Information can be collected on internet providers, domains, uniform resource identifiers (URI), and autonomous system numbers (ASNs) for organizations and individuals, as well as on passive domain name systems (DNS).
- Advanced machine learning algorithms and natural language processing technology can help measure emotions and motivations. It can ingest any text content: emails, instant messages, social media, online news, print newspapers, and television and radio broadcasts. It can analyze audience response within minutes.
- Technology can be used to measure the effectiveness of messaging on target audiences; rank the persuasive influence of individual groups on specific subjects; and identify extremists not in contact with known radicals, foreign terrorist organizations, or criminal organizations.
- Technology enables advance warning of social unrest disruptions.

The ideal technology would enable measuring the persuasive impact on audiences in any medium. Changes in an individual’s emotional response to events, messages, or people can be important security indicators. Gathering metrics that enable analysts to establish an individual’s emotional baselines and to receive alerts when those emotions depart significantly from the norm is important. Such technology uses emotional metrics that correlate strongly with the likelihood of violent action. Certain emotional affinity scores correlate strongly, for example, with the recruitment into violent extremist organizations.

The approach employs four vectors. Rooted in the science of Plutchik’s Wheel of Emotions, two are emotional: *grief to ecstasy* and *loathing to admiration*. Two are motivational, observes George Bebe, a leading former social media analytics expert with the CIA: *apathy to attention* and *calm to panic*. The intersection of emotional and motivational responses generates inclination toward behavior and changes in that behavior.
Changing Communication Response Times
The speed at which information is put out and the need to respond affects the pace at which military commanders must respond in real-time. That has changed the way communication strategy must be thought through and executed.

Social media amplifies the widespread intentional use of disinformation. Misdirection is not new. What is new is the proliferation of disinformation unwittingly by online users who trust their social media networks and aid in the widespread dissemination of false information.

Afghanistan-based Taliban elements have used social media outlets to spread disinformation. Through Facebook and Twitter, Taliban members have used social media for recruitment and to spread false or misleading information. In 2012, NATO forces voiced concern about keeping pace with the Taliban’s use of social media, which outpaces that of NATO and U.S. forces in the information warfare campaign.  

Countering anticipated disinformation campaigns in social media must form part of your communication strategy:
1. Be prepared to disseminate countermessages through preidentified online supporters.
2. Assess the damage. How far has the disinformation spread, for example, beyond online media into traditional channels?
3. Assess the strength of your message against the disinformation through the use of monitoring tools. Whose narrative is dominant: yours or the enemy’s?
4. Recognize lessons from any disinformation campaign to plan ahead in future campaigns.

Tactically Using Social Media
Social media is a game changer. Using it well may spell the difference between victory and defeat for an operation. Small Wars Journal author Jeff Gilmore raise key points regarding the power and value of social media as it impacts several feared dictators:
1. Dictators live in fear of the power that is represented by social media:
   - China and Iran banned certain social media sites (e.g., Facebook) due to loss of information control.
   - If social media scares these established forces, why does the U.S. military not more fully invest in embracing the power of social media tools?  
2. Nonprofit organizations and cause-driven entities flood the system with core messages and track the receptivity to their online themes, adjusting as necessary.
   - Militaries can draw a lesson from their work. Anticipating counterstrategy messaging is one part of the solution. A second is having the capacity to nimbly respond in a social media environment with core messaging, using effective messengers without bottleneck delays in the approving authority channels. Close coordination with public affairs can help ensure this is achieved.

Examples of Military Application of Social Media Outlets
Social media users have used such channels as a personal outlet for commenting or venting, not fully appreciating the potential impact their comments or postings could have.

In Abbottabad, Pakistan, in early May 2010, a computer programmer began tweeting about the noisy helicopter above his quiet town. This tweeter, Sohaib Athar, was unknowingly tweet-
ing live accounts of the takedown of Osama bin Laden. His simple tweets describing a helicopter above Abbottabad at 0200 quickly generated more than 14,000 followers.\textsuperscript{39} The tweets captured an innocent blogger’s curiosity about the purpose and ownership of the helicopters.

Militaries have used social media to help manage wartime public perception. The Israel Defense Forces (IDF) launched a media campaign following its November 2012 military operation in Gaza: Pillar of Defense. It included a constant stream of updated postings on Facebook, Twitter, and YouTube during Israeli airstrikes. Israel used these outlets to promote its cause and generate support. One Twitter account, @IDFSpokesperson, urged followers to retweet its core message if they supported the Israeli airstrikes. The IDF used a similar tactic with Facebook, requesting viewers to share a flier-style image with other friends to signify support for Israeli actions.\textsuperscript{40}

Hamas responded with its own Twitter messaging. User @AlqassamBrigade declared, “Our blessed hands will reach your leaders and soldiers wherever they are.”\textsuperscript{41} This message was less about influencing social media consumers than making a threat against Israeli military action.

In Ukraine, David Patrikarakos described how anti-Russian Ukrainian civilians used Facebook to recruit volunteers and supply its forces against pro-Russian forces and Russian troops.\textsuperscript{42} The success of Egyptian protestors in igniting the Arab Spring by using Facebook to organize and demonstrate was political, but the flexibility and agility of the tool offers a lesson for operators.\textsuperscript{43}

Weaponized social media is already playing a pivotal role in engagements. Its potential is growing and evolving. Operators and commanders need to understand how adversaries use it and how to capitalize on its potential to advance their own strategies, operations, and tactics.

Endnotes
1. Thomas Elkjer Nissen, #TheWeaponizationOfSocialMedia: @Characteristics_of_Contemporary_Conflicts (Copenhagen, Denmark: Royal Danish Defence College, 2015).
5. Patrikarakos, War in 140 Characters, chapters 1 and 2.
8. Nissen, #TheWeaponizationOfSocialMedia, 35.
15. Finin et al., “The Information Ecology of Social Media and Online Communities.”
A variety of terms related to the web are often bandied about, including dark net and light, dark, or deep web. The term dark net refers to networks not indexed by search engines and only available to specific people or groups, requiring authorization or specific software and configurations. The term light web refers to a special place on the internet that appears to preserve its golden age and often carries a nostalgic appeal. The term dark web refers to websites that use the public internet but require specific software for access and are not indexed by search engines to ensure anonymity for those who may be sharing illegal data. The term deep web refers to about 90 percent of the internet that is just below the surface of the world wide web and is not searchable but can be accessed by entering a direct web address.

34. George Beebe, interview with author, June 2017. Information theory and the science of using the Wheel of Emotions is rooted in the psycho-evolutionary theory of emotion pioneered by Dr. Robert Plutchik. His research centered on the study of emotions, violence, and psychotherapy process.

35. This approach was used by Element Data (formerly BehaviorMatrix), an innovative company that the author has advised. At this writing, Element Data has sold its technology to another entity whose plans are unknown. Its technology could identify key communicators and the emotional and motivational impact messages have on microsegmented audiences. A distinguished retired British colonel, Dr. Steven Tatham advocates a somewhat different approach. He favors the use of “multisource, scientifically verified, diagnostic methodology undertaken in-country and in the local language to identify specific motivations for behavior.” See Steven Tatham, Using Target Audience Analysis to Aid Strategic Level Decisionmaking (Carlisle, PA: U.S. Army War College Strategic Studies Institute, 2015), 8.


39. While Americans tend to be asleep at that time of night, Pakistanis stay up late. The town was very active at the time of the attack. Pakistani Chief of Army Staff Ashfaq Parvez Kayani, for example, was working at his desk as the attack unfolded.


42. Patrikarakos, War in 140 Characters, chapter 4.