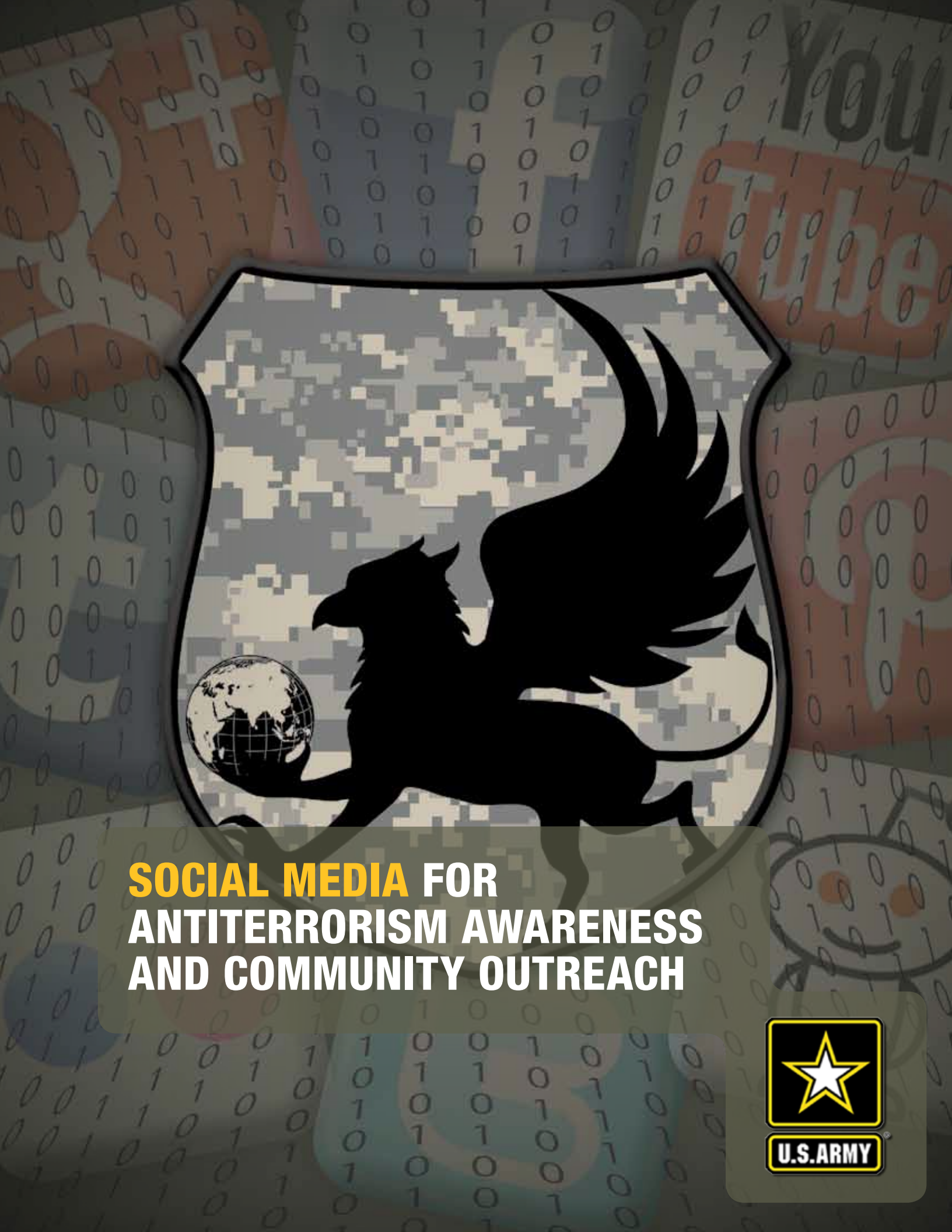


SOCIAL MEDIA FOR ANTITERRORISM AWARENESS AND COMMUNITY OUTREACH

U.S.ARMY

Photo by Master Sgt. Cohen Young, US Army / DVIDS

CONTENTS

Introduction 1

What are social media? 3

Establishing a social media presence to support antiterrorism awareness 5

Branding your social media presence 9

Managing a social media presence 13

How to leverage existing command, organization, and unit social media presence 17

Concerns about social media 19

Crisis communication 25

Resources 31

"Over the last year, Army organizations have used social media to not only communicate important Army messages, but they have used it to communicate during times of crisis. Hurricane Sandy was a perfect example of how effective social media use can help distribute information to those in need while also detailing how the Army supported relief efforts."

— BG Gary J. Volesky
Chief of Public Affairs

Photo by Staff Sgt. Felix Fimbres, US Army / DVIDS

INTRODUCTION

The Army's antiterrorism (AT) program protects personnel, information, property, and facilities in all locations and situations against terrorist activities. Leaders should instill Army-wide heightened awareness and vigilance to prevent and protect Army communities from acts of terrorism through a variety of mediums. Continued protection requires the eternal vigilance of every member of our Army Family and the successful integration of the Antiterrorism Principles: Assess, Detect, Warn, Defend, and Recover. This guide will focus primarily on how commanders, supervisors, and their antiterrorism officers (ATOs) execute the principles of Detect and Warn through the use of social media while maintaining operational security.

AT awareness and community outreach empower the entire Army (units, leaders, Soldiers, Department of the Army civilians, families, and contractors) to take prevention measures and encourage each individual to serve as a sensor—continuously aware of and reporting suspicious activity (iWATCH Army).

When a threat emanates or a crisis occurs, especially to an Army organization, it's big news. From installation shootings to natural disasters, the Army has encountered multiple crises over the years. When a crisis occurs, there is often little time to wait to respond. Crisis response must be swift. Effective communication with the media, Soldiers, and the public is crucial.

Leaders understand that AT awareness and communications must be a key element of command information programs. To ensure this, the best approach is to establish a close partnership between the AT staff and the public affairs staff. In today's society, social media moves information faster than ever. Therefore the effort of leaders at all levels of the Army must be to gain and sustain constant AT awareness. Leaders ensure that each member of the community has the requisite knowledge and skills for personal protection to help avoid terrorist attention. If Soldiers and the public are getting their information from a Twitter feed or their Facebook wall, then leaders and Army organizations need to be prepared to send the most updated and accurate AT information to those locations while being cognizant of potential breaches of operational security (OPSEC).

ANTITERRORISM PRINCIPLE

Detect. Detection identifies things that are out of the ordinary, suspicious activity, or distinct acts of aggression. It also supports the principles of Defend and Warn by providing appropriate information to law enforcement authorities, units, agencies, and command and control elements. Detection may identify an adversary's movement or suspicious activity via direct observation, intelligence, surveillance, and reconnaissance. Other examples of detection are perimeter patrols or security technology, unmanned aircraft systems, and reconnaissance and surveillance patrols.

ANTITERRORISM PRINCIPLE

Warn. Warning includes the knowledge and communication of a broad range of dangers—from general to specific and imminent threats—due to the wide spectrum of potential adversary activities. Examples of warning tasks are training, education, and awareness of the terrorist threat; use of local area networks, electronics, and communication devices, such as social media, to disseminate threat warnings and indications; and imminent threat warning systems (command information networks).

Photo by Spc. Loren Cook, US Army / DVIDS

WHAT ARE SOCIAL MEDIA?

Social media rely on various forms of electronic communication (mobile and web-based technologies) through which users create online communities and highly interactive platforms to share information, ideas, personal messages, and other content (pictures and videos). On September 11, 2012, the Department of Defense published DoD Instruction Number 8550.01, "DoD Internet Services and Internet-Based Capabilities." The DoD Instruction outlines all elements associated with DoD social media use.

Why use social media?

Soldiers have always been the Army's best and most effective messengers, representing a small facet of an ever-growing technologically savvy society. Today, Army social media enable the Army Family around town, around the country, and around the world to stay connected and spread the Army's key themes and messages. Every time a member of the Army Family joins Army social media, it increases the timely and transparent dissemination of information. Social media are a cheap, effective, and measurable form of communication. The Army recognizes that social media give people the ability to communicate with larger audiences faster and in new ways. Even with their many benefits, social media should not be used for command and control, nor do they replace the traditional role of the organization chain of command. Social media simply serve an important tool for Army messaging and outreach. The Army uses a variety of social media platforms designed to support a range of media such as text, audio, pictures, and videos—all of which are generated and maintained by organizations and individuals within the Army Family. The Army understands the risks associated with social media and has developed training to help Soldiers and Family members use social media responsibly.

Photo by Spc. Elayseah Woodard-Hinton, US Army / DVIDS

ESTABLISHING A SOCIAL MEDIA PRESENCE TO SUPPORT ANTITERRORISM AWARENESS

Social media are a powerful communications tool. When used correctly, social media can help an Army organization reach an enormous audience invoking the AT principles of Detect and Warn. Social media can help organizations engage in the conversation on topics related to terrorism, suspicious activity, and reporting while promoting AT awareness. But not all Army organizations use social media effectively. Most social media failures can be attributed to organizations rushing into social media before determining what exactly the organization aims to achieve with social media platforms. Using social media effectively is a process, and it requires strategy, goals, manpower, and foresight. Here are some steps that will help your Army organization get started with the use of social media in support of AT awareness.

AT Awareness Products for Social Media

- iWATCH public-service announcements
- iWATCH brochures and posters
- Basic AT awareness information
- Crisis mitigation and response information
- Vignettes (over 40 vignettes available on ATEP)
- Advertisement for AT quarterly themes and messages

Step 1

Determine what you plan to achieve with your social media presence. Make sure you have a way forward and a set of goals. Developing a social media outreach plan requires a lot of thought, so make sure you know how you will weave AT themes and messages into your plan to use social media to communicate.

Step 2

Review all of the Army social media content already available. The *U.S. Army Social Media Handbook* is a great start, but there are more materials at your disposal. The Army maintains a SlideShare site (www.slideshare.net/usarmysocialmedia) where there are dozens of Social Media Roundups. These are brief, 10- to 15-slide presentations that discuss various social media topics. The AT Branch maintains the Army Knowledge Online Army Antiterrorism Enterprise Portal (ATEP) (https://www.us.army.mil/suite/page/605757), where a collection of AT strategy and communication products can be found to enhance unit messaging. This will help you understand the policies for social media use. If you want to get a better feel for how the other Services are using social media, you can check out www.defense.gov/socialmedia/.

Step 3

After you've done the basic research, work with your team to develop a social media strategy. The Army has a strategy for each social media platform. This helps your organization refine its focus. During this phase of the planning process, it's also helpful

to look at how other Army organizations are using social media. The Army OneSource website (www.myarmyonesource.com) is an example of how AT and Army Family messages are teamed to ensure that the entire Army community is informed of the terrorist threat. The U.S. Army on social media (www.army.mil/socialmedia) provides links to all of the Army's registered social media sites.

Step 4

Once you've done your research and you're confident in setting up a social media presence, be sure you set it up in accordance with the Army's Social Media standard operating procedures (see Resources).

Step 5

Once the page is complete, you need to register it with the Army. Registering organization social media sites through the social media directory is not just encouraged, it is required. According to Directive-Type Memorandum (DTM) 09-026, "Responsible and Effective Use of Internet-Based Capabilities," official online presences must "be registered on the external official presences list, maintained by the Assistant Secretary of Defense for Public Affairs … on www.defense.gov." Once your social media site is reviewed, approved, and registered on the Army's social media directory, your organization will be in compliance with DTM 09-026.

Registering your social media presence is quite simple. Once you've reviewed the standard operating procedure for standardizing official U.S. Army external official presences and your social media site meets all of the requirements, use the upper right side of the Army Social Media web page to submit your link. Once you submit your link, the Online and Social Media Division will review the submission to make sure it follows the standard operating procedure and has all the elements required of Army social media sites. Once Facebook sites are approved, they will be added to the directory and the URL will be sent to Facebook so that all paid ads will be removed from the page. When your designated social media manager leaves the position, be sure to email ocpa.osmd@us.army.mil to let the Online and Social Media Division team know of the change so it can adjust the social media contact list.

Step 6

Once you're up and running, the process isn't over. Make sure you post often and keep your social media presences active. A stagnant social media presence is an ineffective social media presence.

Directory

The U.S. Army on social media (www.army.mil/socialmedia) includes links to thousands of official Army social media sites on Facebook, Twitter, Flickr, and YouTube. The

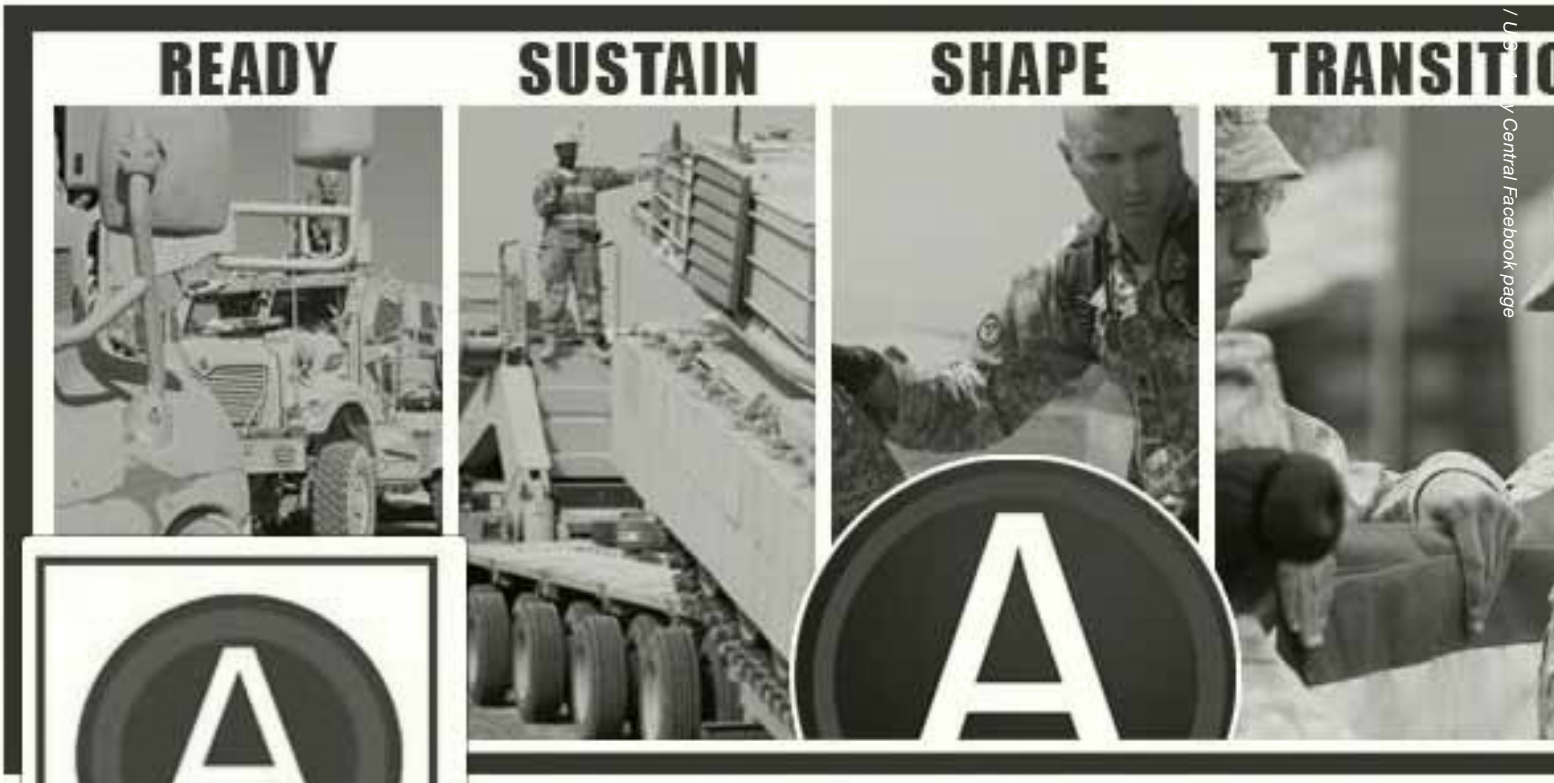
directory makes it easy for Army social media managers to submit social media sites. It also allows users to search for social media sites currently stored in the directory. Each entry has an icon for each social media site the users maintain. This makes it easier to search for all of the social media presences belonging to a specific Army organization.

Photo by Staff Sgt. Garrett Ralston, US Army / DVIDS

Third Army / U.S. Army Central Facebook page

facebook

Search for people, places and things



Third Army/U.S. Army Central

5,658 likes · 192 talking about this · 53 were here

Government Organization

This is the Official Third Army/ARCENT Facebook page. America's land force professionals, expert in the Middle East & Central Asia. HQ at Shaw AFB, SC with an Operational

About – Suggest an Edit

Photos

5,658

Likes

h Ca

Map

Posts by Page

Post | Photo / Video

Write something...

Third Army/U.S. Army Central
7 hours ago

*** EVENTS for 10MAY13***
DANCING at BUEHRING- Hip Hop Night at Oasis @ 1900

Third Army/U.S. Ar
about an hour ago

The US Embassy Doha, Q
America this past Monday
National Anthem was sung
stationed at Camp as-Sali
Ziadeh, was extremely im
the National Anthem was
you were a star!!!"

BRANDING YOUR SOCIAL MEDIA PRESENCE

What's in a brand?

A brand is not just a logo or an emblem. It's an organization's identity. So when using Army branding on social media sites, it's important to use the correct images. The Army's brand is one of strength. Everyone is familiar with the Army: the Apaches, the Humvees, the weaponry, and the pushups. But the brand brings everything together in a clear and recognizable visual presentation. This is equally true with the branding that has become AT communication. The griffin logo and the phrase "Always Ready, Always Alert—Because someone is depending on you" symbolize the ever vigilant attitude that the Army Family must take when defending against terrorism. When people see these brands, they know what they're going to get, and that's important when maintaining effective and informative social media presences.

Use approved artwork

A brand represents the organization through distinctive visual elements, which uphold the integrity of the brand when used consistently and correctly across all communications. There are a lot of copycats or imposter sites on social media platforms, so using the correct Army and AT branding sets your organization's platforms apart from the crowd and demonstrates a heightened level of professionalism. The Army.mil Create website, the Army Brand Portal, and the ATEP site are invaluable resources when your organization is looking for the correct way to use the Army and AT brand.

Use the right resources

The ATEP site provides to ATOs and social media managers the information and visual displays necessary to brand the information appropriately and link public-service announcements and posters associated with iWATCH Army. Each of these can be personalized to include the organization or installation's emergency and suspicious activity contact information. The ATO can also post quarterly themes or vignettes to remind your audience of the importance of remaining aware of their surroundings and reporting anything that seems out of the ordinary.

Select the right look

AT-related graphics can also be merged with your organization's insignia to provide more personalization. You can find unit insignia by visiting the Institute of Heraldry website at www.tioh.hqda.pentagon.mil or the U.S. Army Symbols and Insignia website at www.army.mil/symbols. This insignia should appear on all of your social media presences. Creating a brand is about creating a visual presentation people will

associate with your organization, so carefully consider the colors, backgrounds, and images you use. Many units use the Army combat uniform pattern as a background; others use a combination of colors. It's important to pick an insignia and a pattern that are unique to your organization and identifiable to a broader audience.

Unify the look on all platforms

Once you select your organization's style and logo, it's important to use them consistently on all of your organization's social media platforms. It's also important to keep the name of your organization consistent across all platforms as well. Your organization should work to make sure your Facebook Page, your Twitter handle, and your YouTube channel include the name of your unit rather than mascots or nicknames. For more information about standardizing official Army external presences, check out this standard operating procedure: http://slidesha.re/dkQ7u1.

Mix it up for special events

Every so often, it's encouraged to mix your branding up a bit. Special events such as national holidays, event remembrance such as 9/11, and AT awareness month present the opportunity to be creative, so don't be afraid to temporarily change the branding of your social media sites. The important thing is that you not deviate too much from your basic branding; you still want people to recognize your social media presences. It's also important to make sure that if you change your branding, you change it back once the event is over.

Photo by US Army / www.army.mil

Photo by Staff Sgt. Shawnon Lott, US Army / DVIDS

MANAGING A SOCIAL MEDIA PRESENCE

Today, the Army understands that social media have increased the speed and transparency of information. More Army organizations are using social media for strategic online engagement. Social media are used in garrison environments, operational environments, and Family Readiness Groups. Developing a successful social media presence does not happen overnight. It is a detailed process that requires extensive planning and execution. It all starts with stating the organization's missions, messages, and themes.

Developing a strategy

Once an organization establishes a direction, it can begin to develop a detailed social media communication strategy that provides input into all the social media platforms supported by the organization. Organizations should turn to the ATEP site, which provides resources to aid in developing an AT awareness strategy that enhances the AT principles of Detect or Warn into a cohesive public information and gathering tool for the command. The purpose of using social media is to place your unit's messages in the social media space and provide key contact information for the community to reach law enforcement officials. But to keep people coming back to the pages, units should develop a strategy that mixes messages with items the audience finds interesting. Language should be conversational, fun, and engaging. Also, keep in mind that official use of social media platforms must comply with Army public affairs policy. Content must be in the public domain or approved for release by the commanding officer. Commands are ultimately responsible for content posted on their platforms.

Contact information

It is vitally important to provide up-to-date organization, emergency, and suspicious activity reporting contact information on your social media platforms. Facebook pages and YouTube channels are required to provide an AKO email address and a mailing address for the organization. However, since some platforms such as Twitter allow less space for this information, it is sufficient to provide just an email address.

Terms-of-use statement

Each social media presence must have a terms-of-use statement that informs visitors of what is authorized when interacting on the platform. This terms-of-use statement should include a general disclaimer, privacy and security disclaimers, a copyright and trademark disclaimer, a moderated presence disclaimer, and a Freedom of Information Act notice. For an example, review the terms-of-use statement on the Army's official Facebook page (goo.gl/ySaQx).

Enforce posting policy and monitor comments

It is good to have a posting policy, but just because a posting policy is in place does not mean everyone will follow it. Make sure to review wall posts frequently and remove posts that violate the posting policy. Be mindful of breaches of the organization's cyber-security and hijacking of social media pages. Keep in mind that social media don't take a break for the weekend. In some instances, weekend activity on Facebook can be busier than during the week, so watch the organization's wall every day, even on days off, holidays, and weekends.

Engage the audience

Social media are more than just a platform to push command messages; they are a social community. Platforms such as Facebook and Twitter help people bridge geographical gaps to connect, talk, and interact. Using social media can be valuable to a communication strategy, but it needs to be more than a sounding board for organization messages. Social media should be used to facilitate the conversation, engage the population, and keep people interested in the discussion to bring America closer to its Army.

Listen to the audience

By reading the comments on a Facebook wall or blog post, social media managers can get a feel for what the online community wants to hear. It is also useful to talk to your audience directly. Ask for feedback and suggestions, and then act on their responses. A social media presence accomplishes very little if the audience is not interested in what is being said.

Mix it up

Balance "fun" with "information." It is important to post command AT messages and organizational information, but try to keep the page entertaining enough for people to want to follow it. Don't be afraid to have fun by posting interesting links or asking trivia questions. Try posting a photo of the day or asking a weekly question. Social media are social, so it is important not to fall into the trap of talking at your audience.

Answer questions

Once a social media presence grows to a certain size, the population will likely use it as a resource and forum to ask questions. It is important to spend time responding to questions to establish a valued relationship with users. The one-on-one conversations will show the community that their voice is being heard.

Measurement

Ten years ago, the success and reach of a news story could be measured by the size of a newspaper's circulation or the number of clicks on a website. Today, measurement is about more than just numbers. It is about trends and human feedback. Social media sites such as Facebook, Twitter, Flickr, and YouTube provide their own free analytics tools that allow administrators to track views, impressions, and comments. By using numbers in conjunction with comments and reader feedback, it is easier than ever to determine how organizational messages are received and how the audience is responding to the content.

Photo by Staff Sgt. Shawnon Lott, US Army / DVIDS

HOW TO LEVERAGE EXISTING COMMAND, ORGANIZATION, AND UNIT SOCIAL MEDIA PRESENCE

Throughout most of the Army, the ATO position is likely not a full-time duty. Because of this, ATOs may not have the time or staff capacity to establish their own unique social media presence. However the ATO can take advantage of existing organization social media presence, especially a site that already has community and media following, to enhance AT awareness (Warn) and provide contact information for suspicious activity reporting (Detect) in the command.

The idea of having multiple Facebook pages or Twitter accounts may sound appealing as a means to increase the likelihood that members of the community or media will discover your organization. However the adoption of multiple social media sites and accounts may tax the personnel resources that are already engaged in organization-specific functions and unit readiness. Social media require continuous observation to ensure that the content and the discussions taking place on the site are appropriate. Managing multiple sites may become too burdensome for the individual responsible for site upkeep. Also, too many pages or sites may water down the organization or command's messages. The community will have trouble understanding which of the pages is the "official" page and in a crisis may not go to the correct organizational page for critical information.

Alternatively, ATOs should work with their command to secure a corner or space on the official organizational page to express command messages related to AT awareness with critical contact and reporting information that is visible all the time. Social media managers should direct AT-specific questions or conversations that arise on social media sites to the ATO for feedback in order to link expertise to the topics being discussed. Delivering AT messages on the official command page can also help support and show the command's support of the AT program and the importance of the information to the community.

CONCERNS ABOUT SOCIAL MEDIA

Safe social networking

Social media have become a big part of our Army lives. They help organizations share information and keep Soldiers, Family members, and Army civilians connected to loved ones. We depend on social media, but they can be extremely dangerous if you are not careful. Do you know what information you can post about your job? Did you know that people can use social media to steal your identity? Did you know you can be at risk, even if you don't use social media? OPSEC, breaches in cyber-security, and personal privacy concerns should be paramount when using social media.

OPSEC in daily interactions

Since social media use is so commonplace in our day-to-day interactions, it is easy to become complacent.

- A U.S. Government official on sensitive travel to Iraq created a security risk for himself and others by Tweeting his location and activities every few hours.
- New computer viruses and Trojans that successfully target information on social networking sites are on the rise.
- Social networking sites have become a haven for identity thieves and con artists trying to use your information against you.

To maintain OPSEC and your organization's cyber-security posture, it is important to remain vigilant at all times. Sharing seemingly trivial information online can be dangerous to loved ones and fellow Soldiers—and may even get them killed. According to the Al Qaeda Handbook, terrorists search online for data about "Government personnel and all matters related to them (residence, work place, times of leaving and returning, children and places visited)."[1] Never accept a friend request from someone you don't know, even if the person knows a friend of yours. Don't share information that you don't want to become public. Someone might target you for working in the DoD, so be cautious when listing your job, military organization, education, and contact information. Providing too much information in your profile can leave you exposed to people who want to steal your identity or sensitive operational information. If you detect a cyber-security breach or takeover of your social media site, report it immediately. Understanding what you can and cannot post on social media platforms goes a long way in protecting yourself online, but more can be done by adjusting your privacy settings.

Geotagging safety

Geotagging is the process of adding geographical identification to photographs, videos, websites, and Short Message Service messages. It is the equivalent of adding

a 10-digit grid coordinate to everything posted on the Internet. Some smartphones and digital cameras automatically embed geotags into pictures, and many people unknowingly upload photos to the Internet that contain location information.

A variety of applications are capitalizing on users' desire to broadcast their geographic location. The increased popularity of location-based social networking is changing the way we view security and privacy on an individual level and creating OPSEC concerns on an Army level. One Soldier exposing his or her location can affect the entire mission or can place the Soldier and the Soldier's family at risk. These services have the potential of telegraphing an operational location of vital importance, where Soldiers live, the contents of their home, places their children may play, and the hours they leave and return home from work, bringing a homegrown extremist or criminal right to their doorstep.

Online impersonation

Fraudulent online activities involve a wide variety of sophisticated schemes designed to take advantage of and defraud unsuspecting individuals. The Internet Crime Complaint Center—a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center that receives, tracks, and analyzes cyber-crime activities—has continually warned that online fraudsters are impersonating U.S. Government officials online in order to defraud potential victims. To this end, cyber criminals also impersonate Service members, including senior officers. Scammers use both actual and fictitious information about Service members in a variety of Internet ploys designed to extort information or money from victims. General officers and high-ranking Army officials are not immune to these online schemes, as perpetrators use their identities and photographs to lure and defraud victims.

General officers and high-ranking Army officials appear to be more susceptible to online impersonation than other Service members because of the prevalence of personal and professional information posted online. Biographies of them and of dignitaries posted on military websites are of particular concern because they typically include exhaustive career information and official photographs. A simple Internet search for "general" and "military" returns hundreds of profiles and photos from official and nonofficial websites. Criminals looking to impersonate Service members with credibility can find an abundance of personal information about many general officers and high-ranking Army officials online—information that can be manipulated to commit fraud.

Although such personal information can easily be manipulated into a conduit for criminal activity, the mere act of online impersonation does not constitute a crime. Thus, law enforcement authority to investigate such instances is limited.

Despite the fact that the general officers and high-ranking Army officials are seldom victims of scams themselves, they should remain vigilant against these types of online activities. They should attempt to safeguard and reduce their online footprint. Additionally, to help preclude their identities from being used in such scams,

recommend that they designate someone on their staff to routinely search the Internet for these false accounts and notify the applicable site to remove the account from circulation (listing at www.search.org/programs/hightech/isp). When individuals on a general officer's staff identify a false account (Facebook, Twitter, or Skype), they should also notify the Army's Online and Social Media Division at ocpa.osmd@us.army.mil. The Division maintains contacts with the government representatives at Facebook, Twitter, and Skype and can work with these organizations to eliminate false accounts much faster than the reporting mechanisms available to the rest of the public. Often, the sites will request an email or written correspondence from the official. Should further assistance be necessary to close the account, the staff personnel should contact their Staff Judge Advocate or local Criminal Investigation Command office.

ALARACT—Army Operations Security

In 2011, the U.S. Army Audit Agency determined that not all social media managers had received appropriate OPSEC training before posting content to external social media presences. "ALARACT [All Army Activities]—Army Operations Security (OPSEC) Training for External Official Presence Sites (EOP) Operators (Enclosure 4)" states that all commanders will ensure that those personnel who publish information on external online presences receive mandatory OPSEC training. Social media managers are required to take two OPSEC courses. The Information Assurance Training Center offers the computer-based Social Media and Operations Security Training Course (ia.signal.army.mil/sms.asp). It is a self-paced class that takes approximately 60 minutes to complete. Social media managers must also take the Defense Information Systems Agency Social Networking Class (iase.disa.mil/eta/sns_v1/sn/launchPage.htm). The class is available 24 hours a day, seven days a week, and takes approximately 50 minutes to complete. The Online and Social Media Division is working with G 3/5/7 to create a more intensive online training for Army social media managers. This training is still in the planning stages but is expected to be available sometime late 2013. In the meantime, continue using the training outlined in the ALARACT to meet all social media training requirements.

Social media in the operational environment

While mission success and Soldier safety are most often the primary concerns in operational environments, communicating to the public is also key. Social media can help organizations and ATOs in operational environments tell the Army's story, dispel rumors, inform the local community (Warn), and enlist their participation in locating and thwarting potential terrorist attacks (Detect).

Social media, wireless Internet, and cellular phones are increasingly the predominant methods of transmitting compelling narratives. The Arab Spring, the London riots, the Occupy movements, and the Boston Marathon manhunt are examples of the

emergence of a visually oriented, ideologically impulsive Internet culture with the means to rapidly and collectively plan and act.[2]

The speed of the Internet makes timely communication from the battlefield more important than ever. To counter misinformation, Combined Joint Task Force-82 in Afghanistan posted a video to its YouTube channel. It showed an air weapons team engaging and killing insurgents who were attacking a small patrol base in Paktia Province. While the Taliban claimed that Americans had randomly killed innocent civilians, this video allowed Combined Joint Task Force-82 to accurately portray the actual event to the news media and the world. This example illustrates the importance of social media in operational environments, but social media use should not always be reactive. It should be part of the initial communication plan.

Commanders and planners must consider the social media space when conducting battle planning and mission analysis. Commanders must develop and maintain a strong knowledge of the social media space to stay ahead of the increasingly quick flow of information. News happens fast in operational environments. If it is advertised and publicized correctly, people will turn to an organization's social media sites for information, so make sure the information gets out to the public quickly. Don't rely on the news media to tell the organization's story. News media outlets will publish what they want, but with social media, the organization controls the message.

Terrorist recruitment and insider threat

Organizational attempts to provide a site to enhance AT awareness may also serve as a location to fuel terrorist recruitment. Social media managers should remain aware of the content and discussion taking place on an organization's social media site. Suspicious discussions between visitors or the appearance of sympathetic speech about international or domestic terrorist causes should be reported to the chain of command. Domestically the changing face of U.S. homegrown extremism is disturbing as a growing number of unlikely militants in small-town America become radicalized using the Internet and then plot attacks at home and abroad. The ease with which people can be influenced by extremists through online social media sites makes it hard to identify possible militants within the United States and the Army.

Security elements within the Israeli Ministry of Defense have recognized terrorist use of social networking as a means to meet Israeli Soldiers to abduct them, kill them, or recruit them as spies.

Operational exposure to actions in the area of operation, in conjunction with challenged personal situations or crises that shake belief systems, can test an individual's loyalty to the unit, fellow Service members, and the nation and make the person vulnerable to extremist influence. As the U.S. and its allies shut down terrorist websites, terrorists are beginning to take to Facebook and Twitter as a means to get their message out to supporters and potential recruits.

FORT HOOD SHOOTING

5 November 2009

In the course of the shooting at Fort Hood, a single gunman killed 13 people and injured more than 30. It is the worst shooting ever to take place on an American military base.

The Fort Hood rampage highlighted the emerging role of social media, particularly Twitter, in producing instantaneous accounts of breaking news events. Before the shootings, conversation on social media platforms about Fort Hood was negligible, but on the day of the shootings, mentions of Fort Hood skyrocketed on social media. A number of Twitter users and bloggers claiming to be stationed on the base quickly posted eyewitness accounts, which some mainstream outlets then incorporated into their own online coverage.

Tearah Moore, who identified herself as a Fort Hood soldier just returned from Iraq, posted a number of tweets that were picked up throughout the Web. "Ft Hood is on lockdown. Some guys just shot 19-25 people. As least 11 died so far. I'm at the hospital right now. Please pray for all of em," Moore wrote.[1]

However, in the rush to report on events at Fort Hood, some misinformation spread quickly, most notably that there was more than one shooter in the attacks and that one was killed during the incident. By the time it was corrected, many in both the mainstream press and social media had reported it.[2]

"We will never be accustomed to losing one of our own. But we can more easily accept it when it happens on foreign soil against a known enemy. Fort Hood has lost 545 from its formations in Iraq and Afghanistan. But never did we expect to pay such a high price at home, a place where soldiers feel secure."[3]

— LTG Robert Cone
Commander, III Corps, Fort Hood, TX

[1] Information found at www.journalism.org/print/18295
[2] Ibid.
[3] Quote taken from the LTG Robert Cone Fort Hood Memorial Speech

Photo by Sgt. Joshua Risner, US Army / DVIDS

CRISIS COMMUNICATION

Much of the stress associated with a crisis can be mitigated with a strong crisis communication plan. Through the AT principle Warn, each organization should have a crisis communication plan in place, but it's important to include social media in this plan. An organization needs to be prepared to post pertinent information on social media sites. It should also listen to the conversation online, respond to rumors, and provide updates when they become available.

Crisis management

Using social media to communicate with stakeholders during an increased threat (such as an increase of force protection condition levels) or during a crisis has proven to be effective due to its speed, reach, and direct access. In recent crises, such as Hurricane Sandy and the Boston Marathon bombing, social media have helped distribute command information to key audiences and media, while providing a means for dialogue among the affected and interested parties.

Build a community early

The time to start using social media isn't in the middle of a crisis. To build credibility, you need to establish a presence in social media platforms before a crisis even occurs. Establishing a site that emphasizes AT awareness (Warn) and suspicious activity reporting through iWATCH Army (Detect) sets the foundation for a site the community knows it can go to for important information. A large social media following doesn't happen overnight, so relax and execute your social media strategy. The better you are at providing good information and engaging your audience, the faster your following will grow.

Promote organizational social media presences

It is important to tell the social media community that you're out there. Organizations should advertise their social media presences through internal organization communications, outgoing press releases, email signatures, websites, and conversations with reporters. The more you spread the word about a social media presence, the faster the community that follows it will grow. Make sure your organization and the public know that your social media presence is a good resource for information.

Post content to social media platforms often

A static social media presence is ineffective, because visitors will lose interest quickly and stop coming to view the page. Social media platforms are designed to support various forms of content. Take advantage of this by posting stories, AT vignettes,

public-service announcements, videos, and photos related to your organization's AT mission.

Post cleared information as it comes in

Social media move information quicker than ever, so when a crisis hits, don't wait for a formal press release. When you have solid, approved, cleared information, post it. This includes changes in force protection condition level, gate closures, and information about negative news items, as well. You can always post updated information as it becomes available. Not posting updates quickly during a crisis, or not keeping the community informed, may damage the organization's credibility.

Monitor content and conversations

Avoid just posting information on a social media presence. Monitor content posted by users to get a better understanding of what information they want and need. Use search engines and other monitoring tools to track discussions of various topics.

When a crisis strikes, those first few hours are the most critical. Not only is it vitally important to control the situation on site, but it's important to inform the public and disseminate the most up-to-date information. Organizations must get in front of the story. Give the basic facts early and provide more information as it becomes available. News media members do not have open access to installations, so provide information in a timely manner.

Once accurate stories are published by the news media, it helps to link to the coverage on Facebook. This helps distribute information to a broader audience.

Informing the media

It's the job of the news media to report the news. They will report on an event whether or not you reach out to them. To make sure the correct information gets out to the public, organizations need to communicate with the news media during crises.

Social media are an excellent way to put out information to a broad audience. Rather than waiting to put out a press release, or reaching out to each individual reporter, social media tools help spread information quickly and effectively. Social media resources can be used to tell Soldiers where to go, whom to call, and locations to avoid and give them basic information that will help keep the Soldiers safe during a crisis or unplanned event.

One of the most important aspects of a social media crisis communication plan is monitoring the conversations occurring across social media platforms. Organizations need to be prepared to correct misinformation and rumors.

- Social media, by design, are conversational. People use social media to discuss events and interact with one another.

- Monitor the conversations that occur after information is posted about a crisis or unplanned event. Be sure to correct misinformation and respond to rumors.
- By watching the conversation, organizations can also determine what information the public is looking for.

Trust doesn't happen overnight

It is important to have a regularly updated channel of communication open between the organization and the key audiences before a crisis hits. Use social media platforms to communicate regularly.

Build trust

Building a solid social media following prior to a crisis is key. Become the go-to resource for timely and accurate information. Distribute community news such as school closures, road closures, and event information. When a crisis occurs, organizations should expect the public to look for information on social media platforms, so establish credibility on these sites beforehand. To build trust and credibility on a social media platform, it's important to post often, but there are a few other measures an organization can take to make sure social media platforms are accessed in a time of crisis. Ways to establish trust:

- **Make sure you designate the social media site as "official."** Some users are still apprehensive about social media, so a paragraph indicating that the site is official puts many at ease.
- **Post links to social media sites on official websites.** This allows users to confirm the legitimacy of a social media presence.
- **Promote social media sites on press releases and during interviews.** Get the word out about social media sites. This will help drive people to social media presences for information during crises.
- **Post information as it comes in:** There's no need to wait for a formal press release. When you have verified information that an audience wants to know, post it.
- **Answer questions:** Answer questions as often as possible. Avoid just posting information on a social media presence. Be prepared to receive questions. Respond as quickly as possible through the most appropriate means of communication.
- **Share information:** Share critical information with a network of trusted social media sites, such as other Army command sites and official nongovernmental sites. Create a hashtag that all organizations can use when updating on Twitter.
- **Encourage people on the scene to send in information:** Have individuals on the scene provide updates on their personal accounts or feed you information

to post on the official command social sites. This is where a designated hashtag is very useful.

- **Analyze results:** Evaluate metrics and track user feedback. It's important to evaluate how a social media presence performs during a crisis so adjustments can be made for the future.

Antiterrorism Communication Plan cover

BOSTON MARATHON BOMBING

15 April 2013

Two bombs exploded, 13 seconds apart, at 2:49 p.m. on Boylston Street near the finish line of the Boston Marathon—killing three people and injuring 183 others.

In the aftermath the FBI and local authorities sought the public's assistance in helping identify those involved. On 18 April, the FBI released photographs and videos of two suspects.

Before officials identified the suspects, citizen journalists on Reddit.com were working hard to figure out the names based on blurry photos released by the FBI. Users created a subreddit, or a dedicated home, devoted to the manhunt called r/findbostonbombers.[1]

Through photos found on social networks and the nearly constant chatter of police communications on scanner frequencies, two incorrect names surfaced. That information quickly made its way to media organizations, including the widely popular Buzzfeed, and prompted tweets like this one from @CBSNews, which has been retweeted several thousand times:

"UPDATE: Boston Police are asking social media users not to post information they hear on police frequencies/scanner channels."[2]

Facebook and Twitter were widely used by the Boston Police Department, the Massachusetts State Police, and the FBI throughout the four-day manhunt to create two-way dialogue with the public.

[1] Scott Kleinberg, Boston Marathon bombing suspects: The social media manhunt and the arrest, Chicago Tribune, April 19, 2013

[2] Ibid.

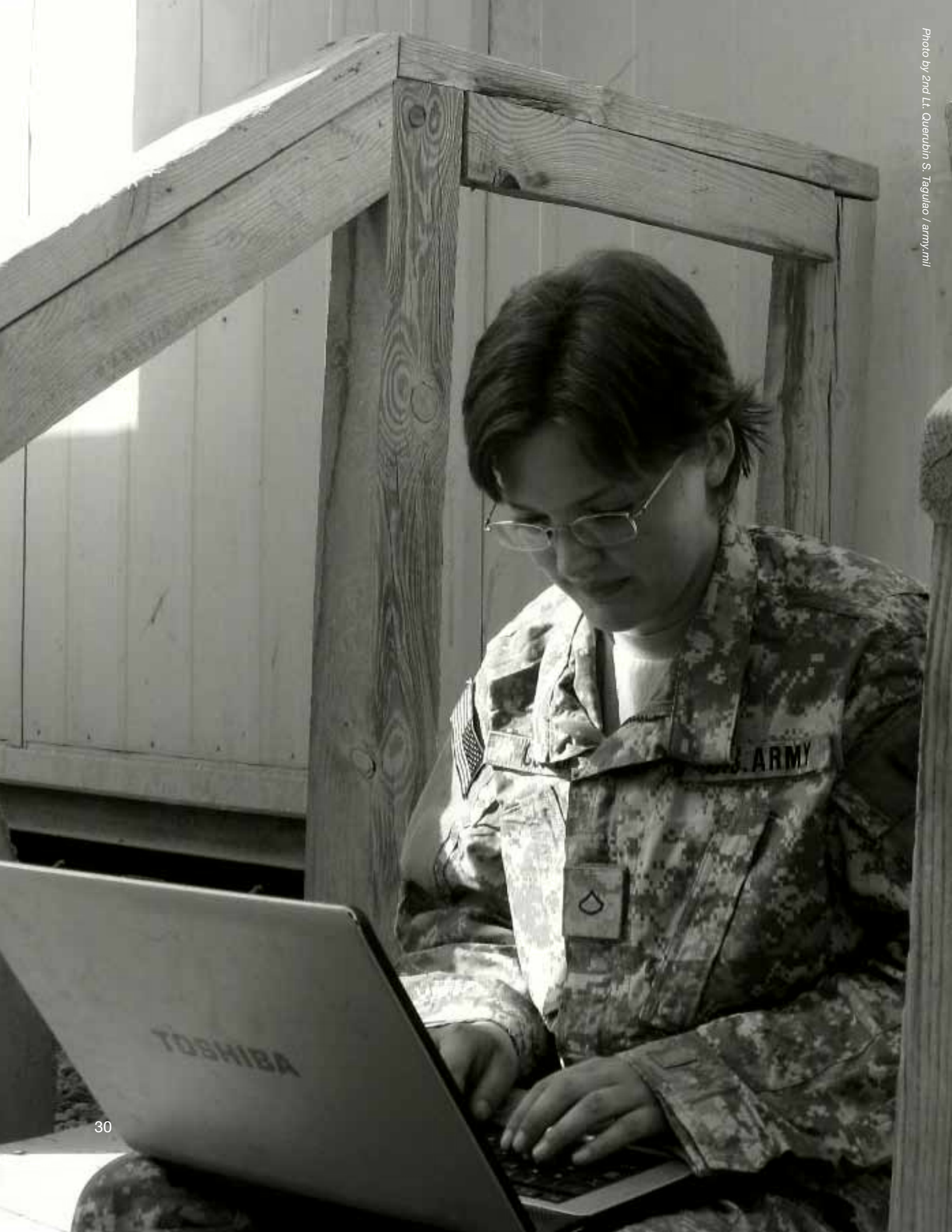


Photo by 2nd Lt. Querubin S. Tagulao / army.mil

RESOURCES

Social media site description[3]

"Facebook is an online social networking service, whose name stems from the colloquial name for the book given to students at the start of the academic year by some university administrations in the United States to help students get to know each other.… Users can create profiles with photos, lists of personal interests, contact information, and other personal information. Users can communicate with friends and other users through private or public messages and a chat feature. They can also create and join interest groups and 'like pages' … some of which are maintained by organizations as a means of advertising.… Critics … state that Facebook has turned into a national obsession in the United States … Quantcast estimates Facebook [had] 138.9 million monthly unique U.S. visitors in May 2011. According to *Social Media Today*, in April 2010 an estimated 41.6% (129.5 million) of the U.S. population had a Facebook account."

"Twitter is an online social networking service and microblogging service that enables its users to send and read text-based messages of up to 140 characters, known as 'tweets' … Twitter has become of the ten most visited sites on the Internet." "The service rapidly gained worldwide popularity, with over 500 million registered users as of 2012, generating over 340 million tweets daily and handling over 1.6 billion search queries per day.… Tweets are publicly visible by default, but senders can restrict message delivery to just their followers. Users can tweet via the Twitter website, compatible external applications (such as for smartphones), or by Short Message Service (SMS) available in certain countries.… Users may subscribe to other users' tweets—this is known as *following*, and subscribers are known as *followers* or *tweeps*. The users can also check the people who are un-subscribing them on Twitter, better known as unfollowing via various services. In addition, users have the capability to block those who have followed them."

"Google+ (pronounced and sometimes written as Google Plus, sometimes abbreviated as G+ or GPlus) is a multilingual social networking and identity service owned and operated by Google Inc. It is the second largest social networking site in the world, having passed Twitter in January 2013. As of December 2012, it [had] a total of 500 million registered users of whom 235 million [were] active in a given month. Unlike other conventional social networks which are generally accessed through a single website," Google+ (as described by Google) is "a 'social layer' consisting of not just a single site, but rather an overarching 'layer' which covers many of its online properties."

Tumblr "is a microblogging platform and social networking website, owned and operated by Tumblr, Inc. The service allows users to post multimedia and other

content to a short-form blog. Users can follow other users' blogs, as well as make their blogs private. Much of the website's features are accessed from the 'dashboard' interface, where the option[s] to post content and posts of followed blogs appear. As of April 13, 2013, Tumblr [had] over 102 million blogs."

"Pinterest is a pinboard-style photo-sharing website that allows users to create and manage theme-based image collections such as events, interests, and hobbies.… Pinterest users can upload, save, sort and manage images, known as pins, and other media content (e.g. videos) through collections known as pinboards. Pinterest acts as a personalized media platform, whereby users' content and the content of others can be browsed on the main page. Users can then save individual pins to one of their own boards using the 'Pin It' button, with Pinboards typically organized by a central topic or theme. Content can also be found outside of Pinterest and similarly uploaded to a board via the [']Pin It' button which can be downloaded to the bookmark bar on a web browser, or be implemented by a webmaster directly on the website.… Pinterest also allows businesses to create pages aimed at promoting their businesses online. Such pages can serve as a 'virtual storefront.'"

Flickr is an image-hosting and video-hosting "website, web services suite, and online community that was created by Ludicorp in 2004 and acquired by Yahoo! in 2005. In addition to being a popular website for users to share and embed personal photographs, the service is widely used by bloggers to host images that they embed in blogs and social media. Yahoo reported in June 2011 that Flickr had a total of 51 million registered members and 80 million unique visitors. In August 2011 the site reported that it was hosting more than 6 billion images and this number continues to grow steadily according to reporting sources. Photos and videos can be accessed from Flickr without" registering an account, but an account is required for uploading "content onto the website."

"YouTube is a video-sharing website … on which users can upload, view, and share videos. The company is based in San Bruno, California, and uses Adobe Flash Video and HTML5 technology to display a wide variety of user-generated video content, including movie clips, TV clips, and music videos, as well as amateur content such as video blogging, short original videos, and educational videos.

"Most of the content on YouTube has been uploaded by individuals, although media corporations, including CBS, the BBC, Vevo, Hulu, and other organizations offer some of their material via the site, as part of the YouTube partnership program. Unregistered users can watch videos, while registered users can upload an unlimited number of videos."

Reddit is a social news and entertainment website where registered users submit content in the form of either a link or

a text ("self") post. Other users then vote the submission "up" or "down", which is used to rank the post and determine its position on the site's pages and front page. The entries are organized into areas of interest called "reddits". Historically, the front page was the main reddit, and other areas were "subreddits".

Publications

U.S. Army Criminal Investigation Command Report, "Online Impersonation of General Officers (GOs) and High-Ranking Army Officials," January 2013.

Special Warfare, April to June 2012, Volume 25, Issue 2, "Social Media—A New Form of UW."

Army Social Media Handbook Version 3-1 (January 13)

Army Social Media Policy

Army Social Media Standard Operating Procedure

Branding Your Social Media Presences

Cyber Threat Resource Guide

DoD Instruction 855001

Facebook Boot Camp

Facebook Military Guide

Facebook Pages Insights Guide

Facebook Quick References Sheet

OPD Twitter (April 2011)

OPSEC and Social Networking

Phishing Brochure

Social Media Roundup Greatest Hits

Social Media and the Hatch Act

Twitter Quick Reference Sheet

U.S. Army Branding Guide

Social Media Roundup (SMR) Slides

SMR Week 1

SMR Week 2 Social Media Policy

SMR Week 3 Facebook for Army Organizations

SMR Week 4 Geotagging Safety

SMR Week 5 Telling a Story with Social Media

SMR Week 6 Online Engagement

SMR Week 7 Social Media for Family Readiness Groups

SMR Week 8 Measuring Social Media Success

SMR Week 9 Social Media in the Operational Environment

SMR Week 10 Army Social Media Handbook (January 2011)

SMR Week 11 Social Media in Crisis Communication

SMR Week 12 Personal Conduct on Social Media Platforms

SMR Week 13 Maximizing the Effectiveness of a Twitter Account

SMR Week 14 Changes to Facebook Layout

SMR Week 15 9 Critical Steps—Protecting Yourself

SMR Week 16 Social Media with Limited Manpower

SMR Week 17 Social Media Policy Update

SMR Week 19 7 Blogging Tips

SMR Week 22 Social Media Branding

SMR Week 23 OPSEC and Safe Social Networking

SMR Week 24 Protests, Fake Accounts, and Imposters

SMR Week 25 Online Town Hall Meetings

SMR Week 27 Social Media Planning

SMR Week 28 Marketing Your Social Media Program

SMR Week 29 Listening with Twitter

SMR Week 30 Effective Tweeting

SMR Week 31 Google+ The Basics

SMR Week 32 Case Study—Driving the News

SMR Week 33 Social Media Directory

SMR Week 34 7 Tips for Better Social Media

SMR Week 38 Introduction to Tumblr

SMR Week 39 5 Tips for Better Social Media Communication

SMR Week 40 Social Media and UCMJ [Uniform Code of Military Justice]

SMR Week 41 Introduction to Pinterest

SMR Week 42 Dangers of Location-Based Social Networks

SMR Week 43 New Facebook Pages

SMR Week 44 Tagging Effectively

SMR Week 45 Google Privacy Policy

SMR Week 51 10 Tips All Social Media Managers Should Know

SMR Week 52 Scheduling Social Media Posts

SMR Week 53 Bloggers Roundtable

SMR Week 54 Bad Social Media

SMR Week 55 30 Minute Social Media

(Endnotes)

[1] OPSEC and Safe Social Networking Brief, https://ia.signal.army.mil/SocialmediaandOPSECbrief1.pdf.

[2] *Special Warfare*, April to June 2012, Volume 25, Issue 2, "Social Media—A New Form of UW," p. 26.

[3] "Social Media." Wikipedia: The Free Encyclopedia. Wikipedia Foundation, Inc. Web. 21 Apr 2013.

U.S. ARMY

ARMY STRONG®

Always Ready, Always Alert

Because someone is depending on you