**SUPREME HEADQUARTERS ALLIED POWERS EUROPE**

**GRAND QUARTIER GÉNÉRAL DES PUISSANCES ALLIÉES EN EUROPE**

**B-7010 SHAPE, BELGIUM**

**Our Ref:** SH/SAG/PUA/EO/14-306961/1

**Date:** 16 September 2014

**Tel:** +32-(0)65-44-7111 (Operator)
**Tel:** +32-(0)65-44-4958
**NCN:** 254-4958
**Fax:** +32-(0)65-44-3545 (Registry)

## ACO DIRECTIVE (AD) 095-003

## ACO DIRECTIVE ON SOCIAL MEDIA

REFERENCES:
A. PO(2009)0141, NATO Strategic Communications Policy, dated 29 September 2009.
B. MC 0457/2(Final), NATO Military Policy on Public Affairs, dated 08 February 2011.
C. AD 095-002, ACO Strategic Communications, dated 21 May 2012.
D. AD 095-001, ACO Public Affairs, dated 04 June 2013.
E. 3400/SHSPSPAO/GJ/11-280987, Imagery Directive, dated 17 August 2011.
F. ACO and ACT Public Affairs Handbook, dated July 2010.

1. **Status.** This directive is a rewrite of Allied Command Operations (ACO) Directive 095-003, "Social Media", dated 03 December 2009.

2. **Purpose.** To provide guidelines for the military use of social media for military Public Affairs (PA) within ACO in support of peacetime and military operations (see Chapter 3).

3. **Applicability.** This directive is applicable to all ACO headquarters/units and should be used as a guide for the preparation of local directives.

4. **Publication Updates.** Updates are authorised when approved by the Director of Management (DOM), SHAPE.

5. **Proponent.** The proponent for this directive is the SHAPE Public Affairs (PUA) office.

FOR THE SUPREME ALLIED COMMANDER, EUROPE:

Eddy Staes
Brigadier General, BEL A
Director of Management

## TABLE OF CONTENTS

| | PAGE | PARA |
|---|---|---|
| **CHAPTER 1 – BACKGROUND** | | |
| Introduction | 3 | 1-1 |
| Key Challenges | 3 | 1-2 |
| Aim | 3 | 1-3 |
| Guidance to Subordinate HQs | 4 | 1-4 |
| Requirements | 4 | 1-5 |
| Key Military Public Affairs Communications Activities for Social Media Platforms | 4 | 1-6 |
| **CHAPTER 2 – ESTABLISHING AND MAINTAINING A SOCIAL MEDIA PRESENCE IN NON-OPERATIONAL ENVIRONMENTS** | | |
| Introduction | 6 | 2-1 |
| Develop a Social Media Strategy | 6 | 2-2 |
| Management of Social Media Sites | 6 | 2-3 |
| Release Authority | 7 | 2-4 |
| Engaging Audiences | 7 | 2-5 |
| Using Social Media as an Open Door | 7 | 2-6 |
| Enforcing Posting Policy and Monitoring Audience Feedback | 7 | 2-7 |
| Contact Information | 7 | 2-8 |
| Measures of Effectiveness | 8 | 2-9 |
| SHAPE Official / Corporate Sites | 8 | 2-10 |
| Personal Sites and Personal Interaction on Public Sites | 9 | 2-11 |
| **CHAPTER 3 – SOCIAL MEDIA DURING OPERATIONS** | | |
| Introduction | 10 | 3-1 |
| Coordination of Efforts | 10 | 3-2 |
| PSYOPS in Social Media | 10 | 3-3 |
| Official/Corporate Sites | 10 | 3-4 |
| Implementation | 10 | 3-5 |
| **CHAPTER 4 – SOCIAL MEDIA OPERATIONAL SECURITY** | | |
| Introduction | 12 | 4-1 |
| Security Considerations | 12 | 4-2 |
| **CHAPTER 5 – TECHNICAL CONSIDERATIONS** | | |
| Access | 13 | 5-1 |
| Account Names | 13 | 5-2 |
| **CHAPTER 6 – IMPLEMENTATION** | | |
| Introduction | 14 | 6-1 |
| Initial Steps | 14 | 6-2 |
| Measures of Effectiveness | 14 | 6-3 |

ANNEXES:

A. Social Media - ACO Comments Policy.
B. Guidance on Maintaining Security Online.

## CHAPTER 1 – BACKGROUND

### 1-1. Introduction

a. Social media[1] gives NATO the ability to quickly and dynamically engage with widespread audiences in an economical and effective manner. It has become an important tool for NATO messaging, outreach, and communication with both internal and external selected audiences. ACO uses a wide variety of social media platforms, which support a range of media types including text, video, audio, and photography. ACO social media enables the entire ACO network, partners and allies across the globe to stay connected and spread NATO themes and messages. Social media is a cheap, effective and measurable form of communication. ACO uses social media to tell the ACO and NATO story, communicate messages and engage in a two-way discussion with social media users. In order to be successful, social media campaigns must be well planned and managed, adequately resourced, flexible, timely, as well as responsive and engaging and aligned with SACEUR's Strategic Communications (STRATCOM) guidance.

b. This directive will provide guidance for ACO units regarding the use of social media platforms for military Public Affairs (PA) purposes as a communications means to enhance NATO's engagement with key audiences and to increase understanding of the Alliance's objectives and activities in support of SACEUR's STRATCOM guidance. The directive distinguishes between peacetime, steady-state social media activities (see Chapter 2) and those conducted during operations (see Chapter 3).

1-2. **Key Challenges.** With increasing frequency, target audiences are utilizing social media as the primary platform from which to gather information, develop opinions, and become informed on events, issues and news from NATO and its strategic and subordinate commands. This rapidly expanding communications environment provides challenges, vulnerabilities and risks to ACO units that must be regularly assessed and managed. One key challenge is the need to keep informed regarding social media 'discussions' on NATO and global security matters in order to maintain situational awareness. Key vulnerabilities include security concerns and the ease by which information can be transmitted globally using social media tools. The dichotomy between the need for ACO to be aware of and engage in public debate versus security concerns, calls for a measured and managed approach to social media platforms within ACO. Such an approach must be permissive enough to enable effective communications campaigns to be conducted but managed to the extent that security concerns are minimized. The effectiveness of social media campaigns are generally in direct relation to the effort and manpower dedicated to their implementation. Communicators and commanders must therefore consider a number of factors when implementing social media strategies including the allocation of adequate resources, desired communications effects, access limitations, security precautions, and technical considerations.

1-3. **Aim.** This directive provides guidance for the military Public Affairs' use of social media during both peacetime (Chapter 2) and operations (Chapter 3) and to recommend best practices for use across ACO platforms.

[1] Web-based technologies used for social interaction and to transform and broadcast media monologues into interactive, social dialogues.

1-4. **Guidance to Subordinate HQs.** ACO subordinate headquarters are to adopt this directive and develop their own social media strategy to meet their particular set of circumstances and goals. Commanders are strongly encouraged to embrace and utilize the communication advantages of social media. Operational Security (OPSEC) and personal privacy concerns should be paramount when employing these tools.

1-5. **Requirements.** As with any communication method, the use of social media must be aligned with ACO's communication strategy, directives, themes, master messages, and STRATCOM guidance. The proper use of social media as an effective communications tool requires clear goals, clear messages and clearly identified audiences. Other key requirements are as follows:

a. **Access Requirements.** Access to social media platforms is often blocked by ACO computer security staff. If ACO units are to mount effective social media campaigns, access to these platforms must be enabled for commanders and communications staff. Access to social media platforms from select ACO smart phones should also be considered as a means to more effectively leverage this medium. Access to social media however, must be balanced with security regulations, privacy considerations, and the threat of cyber-attacks and disinformation campaigns. Communications professionals must identify the desired effects of social media, be aware of the liabilities and risks and actively monitor and manage these platforms accordingly.

b. **Training Requirements.** Ideally, ACO subordinate commands should have a social media cell made up of professional PA staff to run corporate web and social media platforms. Information Operations (Info Ops) and Psychological Operations (PSYOPS) personnel may also be involved in social media campaigns during operations. Training is required to ensure that ACO staff tasked with overseeing and managing social media campaigns and platforms have the required expertise and knowledge to execute their duties. In the first instance, the on-line training course provided by ACT should be utilised and further training should be sought out from NATO member nations or the private sector if required. As well, ACO should seek to harness the skills of existing members that have training and experience with social media by employing them in social media sections. The information above deals with individual training however, collective training skills will be practiced during the TRIDENT series of exercises carried out by ACT.

1-6. **Key Military Public Affairs Communications Activities for Social Media Platforms**

a. **Internal Communication.** Social media tools are an effective means to keep internal audiences informed and motivated. ACO has identified 5 primary internal communications activities for consideration when drafting internal strategies:

(1) Communicate the Commander's intent.

(2) Disseminate information to internal audiences in a timely and effective manner.

(3) Communicate ACO key themes and messages to internal audiences.

(4) Build esprit de corps.

(5) Dispel rumours, control the flow of information and prevent mis/disinformation.

b. **External Communication.** Social media tools can efficiently communicate to vast and diverse audiences and promote two-way communication and engagement. Objectives: ACO has identified 5 primary external communications activities for consideration when drafting external strategies:

(1) Inform international audiences on the role and mission of ACO.

(2) Communicate ACO key themes and messages.

(3) Promote the operations and accomplishments of ACO units and personnel.

(4) Increase the level of engagement with key audiences.

(5) Dispel rumours, control the flow of information and prevent mis/disinformation.

## CHAPTER 2 – ESTABLISHING AND MAINTAINING A SOCIAL MEDIA PRESENCE IN NON-OPERATIONAL ENVIRONMENTS

2-1. **Introduction.** Social Media related platforms connect and communicate with a wider audience than any other media in history. Facebook alone has almost 1.3 billion users[2]. Over 90 percent of global marketing is conducted through social media. In developed countries, over 50 percent of people receive breaking news from social media and 46 percent of people use social media as their weekly news source. With numerous platforms available, social media provides an ever-expanding tool chest of methods to reach intended audiences. Any refusal to utilize or the misuse of social media can seriously hinder an organization's ability to effectively communicate with both internal and external audiences.

2-2. **Develop a Social Media Strategy.** SHAPE and ACO subordinate commands should create social media strategies that are synchronised with overall STRATCOM and PA objectives. Social media should be used as a tool to position key themes and messages into the social space. As social media is a two-way conversation, ACO units should create content that informs audiences, engages with them and facilitates feedback. Language should be open, engaging, and interesting. Social media cells should be provided with key themes and messages, along with some guidance and direction, and then given the latitude to engage with audiences in creative, consistent and meaningful ways. Posts to social media platforms must be dynamic and social media staff must have the authority and flexibility to respond and react within established parameters.

2-3. **Management of Social Media Sites.** In non-operational environments/peacetime, ACO PA staff will manage corporate web and social media platforms on behalf of the Commander. Other entities may certainly have input to content placed on these platforms, but the overall management rests with PA staff. The situation is different during operations and these considerations are covered in Chapter 3 of this document. On the rare occasion where there are disagreements regarding web or social media content and/or strategy, the Commander shall always hold the final authority. A management plan should be established for each platform that clearly designates the following:

a. Site Administrators: Who will have access and permissions for the platform? Ensure there are multiple administrators to avoid single points of failure.

b. Objectives: What ACO Communications objectives will be reinforced by communicating on this site?

c. Selected audiences: Who are you trying to reach using this platform?

d. Type and frequency of content to be posted: What is important and interesting to your audience? How will you engage them in conversations?

e. Comment/Engagement Policy: Who is responsible to monitor comments and feedback? Will comments be moderated or automatically posted? What is the policy regarding inappropriate comments?

[2] Registered users in March 2014.

f. Transition Plan: When key personnel are posted, how will responsibilities and permissions for the platform be transferred?

2-4. **Release Authority.** Like any news release, public statement, or any other type of official product, social media posts on ACO corporate platforms are all official and 'on-the-record'. Therefore, all posts shall be subject to an official release process, much like any other form of official release. Care needs to be taken to ensure social media posts are relevant, factually correct and in-line with the Commander's intent and established communications objectives, themes and strategies. ACO PA staff will manage release authority on behalf of commanders for ACO corporate sites operating in non-operational environments/peacetime. The situation is different during operations and these considerations are covered in Chapter 3 of this document. When establishing release procedures, the speed and unique nature of social media platforms must be considered. Social media does not have standard 'business hours'. It operates 24 hours a day, seven days a week. This necessitates streamlined approval processes that facilitate the rapid approval and dissemination of appropriate content to audiences, while it is still relevant and topical. In order to function properly, certain authorities will need to be delegated, alternate approving authorities will need to be designated and guidelines and procedures will need to be clearly understood by involved staff.

2-5. **Engaging Audiences.** Social media should not be used solely as an outlet to release command messages and information or repeatedly 'share' information from other military organizations. Social media is best viewed as a virtual community. Organizations must engage audiences in two-way conversations that encourage audiences to respond, interact, share and stay interested in ACO/NATO activities. Social media content should consist of an equal balance of command information together with entertainment and 'fun'. Audiences will ignore a social media platform that does not provide the right mix of engagement, entertainment and information.

2-6. **Using Social Media as an Open Door.** Social media is an extension of communications and PA activities. It is an informal community designed to facilitate conversations between people and audiences across the globe. Units within ACO are therefore strongly encouraged to foster engagement with audiences by encouraging dialogue, developing innovative ways to facilitate interaction, answering questions, responding to comments and soliciting feedback and ideas. Building a rapport with an audience who is involved and engaged can have significant benefits, especially during a crisis. Social media is an excellent forum to dispel rumours, provide needed context and prevent mis/disinformation.

2-7. **Enforcing Posting Policy and Monitoring Audience Feedback.** Each official social media platform within ACO must have a link to a 'terms of use statement' (see Annex A). This will ensure that users understand the rules regarding what is allowable and appropriate for posting on each site. The statement will also outline the grounds on which a user may be blocked or removed from using or posting on a social media platform. Administrators must also consistently monitor social media platforms to ensure guest content is appropriate, evaluate and respond to any feedback and analyse what topics are most engaging for users. This will allow administrators and communicators to refine and adapt the evolving social media strategy.

2-8. **Contact Information.** Social media is an ongoing conversation and users must have the means to contact the organization and receive feedback. All ACO platforms must contain up-to-date contact information that includes an official e-mail address and phone number of the PA office or social media administrator as a minimum. ACO platforms should also contain convenient links to other important sites within ACO as well as the main NATO webpage.

2-9. **Measures of Effectiveness.** As with all communications activities, ACO units must set objectives for all social media campaigns and establish the means to evaluate progress and refine efforts to better engage audiences. Best practices should be followed to ensure evaluation programs are realistic and meaningful. For example, the number of 'likes' or 'followers' does not provide a comprehensive picture of a platform's social media influence. ACO units should also consider levels of participation, engagement, user feedback and the shares/reach of social media content to establish a more complete picture of audience engagement and interaction. There are numerous free analytical tools available online that can provide effective ways of monitoring and evaluating a unit's social media presence.

2-10. **SHAPE Official/Corporate Sites.** At SHAPE, SHAPE Public Affairs Office (PAO) will remain the sole entity managing SHAPE's official/corporate presence on social networking sites. Only SACEUR and designated representatives are authorised to publish to these platforms on behalf of SHAPE; other personnel may do so only in a 'non-official' capacity, unless specific approval is first obtained. SHAPE PAO will coordinate with any division or staff entity wishing to communicate via SHAPE on-line platforms. SHAPE PAO currently manages nine social media capabilities; the SHAPE/ACO Facebook and Twitter accounts, SACEUR's Blog, SACEUR's Facebook and Twitter accounts, ACO Command Senior Enlisted Leader's (CSEL) Blog, a NATO NCO Facebook account and a SHAPE Flickr and YouTube account. All of these platforms are aligned and support ACO's overall STRATCOM and PA objectives. The following sub-paragraphs outline SHAPE's current platforms and subordinate commands are invited to adopt a similar approach using the platforms that meet their specific communication goals and are manageable given existing resources.

a. **ACO/SHAPE Facebook and Twitter.** As the main ACO/SHAPE official/corporate social media presence, these pages are used to engage social media communities in conversations related to our activities and operations while communicating key themes and messages to internal and external audiences. Subordinate commands are strongly encouraged to create and maintain an official social media presence for their own command. Organizations are encouraged to 'like', 'share' and repurpose posts from SHAPE social media platforms. In turn, the SHAPE PAO will regularly use and highlight information found on the platforms of subordinate commands. These ACO/SHAPE official/corporate social media platforms are managed on behalf of SACEUR by SHAPE PA.

b. **SACEUR/Commander's Blog.** A blog from the Commander's perspective is an excellent platform to inform audiences regarding the Commander's focus, priorities and to highlight other information of note. It is also an appropriate venue to solicit feedback and to engage with interested communities. Subordinate commands are encouraged to create their own leadership blog and/or share SACEUR's blogs.

c. **SACEUR/Commander's Social Media.** SACEUR maintains individual Twitter and Facebook accounts and engages audiences on day to day activities and priorities. Commanders in subordinate commands are similarly encouraged to create an official social media presence. Much like a blog, a social media presence allows for a continual and open conversation with audiences including feedback from users. ACO organizations are encouraged to ‘like’, ’share’ and repurpose posts from the SACEUR's social media pages for use on their own official pages. The SACEUR's social media pages are managed by the SACEUR and ACO PA staff.

d. **ACO Command Senior Enlisted Leader (CSEL) Blog.** Much like the SACEUR/ Commander’s blog, a blog from the ACO CSEL bring enlisted issues, concerns and information to the attention of the audience. It is appropriate for the CSEL blog to create new content or to reinforce the Commander’s position from an enlisted perspective.

e. **NATO NCO Social Media.** The NATO NCO Facebook page is a specific effort by the SHAPE PA Office and the ACO CSEL to highlight the accomplishments of the enlisted service members of NATO and promote ongoing development of the NCO Corps within NATO and ACO. Organizations are encouraged to ‘like’, ’share’ and repurpose posts from the NATO NCO page for their own official pages. The NATO NCO social media pages are managed by the ACO CSEL and the SHAPE PA Office.

f. **ACO/SHAPE Flickr Site and YouTube channel.** Images and video are powerful assets that can underscore key communications, themes and messages as well as capture the imagination of audiences. Operational imagery is particularly sought after by audiences. SHAPE uses imagery across all social media platforms, but maintaining a catalogue of outstanding images on Flickr and video on YouTube enables both internal and external audiences to find quality imagery on NATO operations quickly and easily. During exercise and operations, photo and video repositories such as these will likely attract more visitors than all other platforms combined. These platforms should always be considered an important part of a social media strategy. ACO/SHAPE Flickr and YouTube platforms are managed by SHAPE PA.

2-11. **Personal Sites and Personal Interaction on Public Sites.** The distribution of content related to NATO activities by internal members presents challenges and risks pertaining to OPSEC, but also present NATO members with excellent opportunities to distribute useful and compelling information about NATO activities to a wide array of audiences. The key to exploiting benefits while minimising the risks of social media activity by ACO members lies in effective governance and education of personnel. MC 0475/2, NATO Military Policy on Public Affairs, states that NATO personnel are “advised to consult with their chain of command before publishing NATO-related information and imagery to the internet. The chain of command has expert advisors, such as public affairs and intelligence staffs, who will ensure that such published information is not ultimately prejudicial to NATO operations and personnel.” Commanders and PA staffs should regularly remind ACO personnel of the need to clear content related to NATO operations and activities prior to publishing on private social media accounts. Further, ACO personnel are reminded to exercise caution in offering personal opinion which could be interpreted or misconstrued as an official ACO/NATO position. Opinions on political or policy matters related to NATO should not be expressed publicly by military members. Other personal views should be clearly indicated as personal using a disclaimer such as: “the views, thoughts and opinions offered are personal and do not represent endorsed or official policy.”

## CHAPTER 3 – SOCIAL MEDIA ACTIVITY DURING OPERATIONS

3-1. **Introduction.** The general practices and principles governing the use of social media during operations do not vary significantly whether they are being conducted during peacetime in a corporate construct or during operations overseas. This chapter provides clarification regarding the areas of responsibility and authority regarding social media activity during operations.

3-2. **Coordination of Efforts.** Additional entities other than PA will be involved in the content creation, posting and approval processes during operations. In order to maximise the desired effects and ensure a consistency and harmony, social media activities must be coordinated. Within each HQ, the commanders will ensure this coordination through existing information environment coordination boards (where all information disciplines are represented) such as, Information Operations Coordination Board, Strategic Communications Working Group and the Information Environment Working Group. Any conflicting issue on the usage of social media which cannot be agreed in these coordination boards will be solved and decided by commanders.

3-3. **PSYOPS in Social Media.** Unity of effort is essential to achieve consistency of word and action in all operations. National and NATO PSYOPS in a theatre must be closely coordinated to present consistent messages aligned with the NATO STRATCOM guidance to audiences, approved by North Atlantic Council in support of alliance goals and objectives. PSYOPS are generally planned under the authority of the J5/Plans section and executed under the authority of the J3/Operations section. Because of its potential complexity and inherent risks, PSYOPS are planned, conducted and represented on staffs by a special staff element, especially trained in the planning and execution of PSYOPS. PSYOPS activities are incorporated within the normal planning and targeting cycles of a unit and are reflected in the products developed within these cycles. PSYOPS activities in social media will be coordinated through the Info Ops staff function within the existing working groups and boards in the relevant headquarters.

3-4. **Official/Corporate Sites.** Communications platforms that purport to officially represent a NATO command, unit, or mission are to be primarily administered by PA staffs on behalf of the commander and coordinated among all the information disciplines. Other entities may be involved in populating and monitoring these sites, but the overall coordination and responsibility will rest with PA. To that end, any conflicting issue will be handled as per para 3.2. This includes official web sites as well as official social media sites for commands, units and operations. It also encompasses platforms focused on both international audiences as well as local audiences (regardless of the language used) in the theatre of operations. Official public communication, whether via the media or via other tools such as social media, must be consistent, controlled, and carefully coordinated to ensure Alliance credibility is maintained. Official communications have the highest level of risk, which is why a higher degree of management and centralisation is required.

3-5. **Implementation.** The best-practices for the implementation of social media campaigns do not differ widely between those that are operational and those that are corporate. Therefore, the guidance found in all other chapters of this document is generally applicable to an operational setting as well. There will be obvious variances including language and cultural differences and these will differ greatly depending on the operational context.

Therefore, it will be imperative that staffs managing on-line communications campaigns have direct access to local interpreters/translators as well as cultural and communications experts in order to effectively tailor and conduct their campaigns.

## CHAPTER 4 – SOCIAL MEDIA OPERATIONAL SECURITY

4-1. **Introduction.** The use of social media, like any other form of communication, poses risks regarding OPSEC and complacency can lead to OPSEC violations. NATO adversaries are known to scan blogs, forums, chat-rooms and other social media to collect information that may be harmful to ACO operations or personnel. Understanding what may or may not be released via social media will do much to protect an organizations' online identity and protect OPSEC. Education of ACO personnel and proper management of social media tools are keys to maintaining effective and secure social media campaigns. Outright bans on the use of social media are not the solution, as this would deny ACO from exploiting the numerous advantages these platforms bring in the realm of communications.

4-2. **Security Considerations**

a. OPSEC is paramount. It is incumbent upon all personnel to consider the potential of creating risk to themselves, their families, their peers and the mission by publishing information to the Internet. Information and/or imagery may individually, or in conjunction with other information, provide insights into current ACO operations, equipment, capabilities, tactics and intentions. Further guidance for individuals on maintaining security online is provided at Annex B.

b. All information that is posted to social media sites must be approved for public release. Knowingly, or unknowingly releasing classified information into the public domain violates specific regulations and could lead to legal and/or disciplinary actions. If there is any doubt regarding the OPSEC implications of posting certain information, social media administrators should consult with PA or security staff.

c. The following OPSEC guidelines should be practiced by all units and headquarters in ACO involved with social media campaigns:

(1) Designate an official social media administrator or administrative team.

(2) Ensure all social media content is approved for release by the proper authority.

(3) Monitor official social media presence and ensure users are not posting inappropriate or sensitive information on the official pages.

(4) Conduct regular social media OPSEC training with the administrative members.

(5) Be vigilant. Once information is posted to social media, your control on dissemination has been taken out.

## CHAPTER 5 – TECHNICAL CONSIDERATIONS

5-1. **Access.** Local bandwidth availability and access to NATO UNCLASSIFIED workstations will influence the degree to which social media can be employed in each headquarters. A priority should be placed in providing all communications practitioners with access to unclassified systems that can monitor and engage in social media activity. When bandwidth issues are constricted to the point where social media access is not feasible, headquarters should consider contracting civilian internet connections for staff tasked with responsibilities related to social media.

5-2. **Account Names.** Lessons learned indicate that it is a good practice to reserve several account names that are close in syntax to official account names. This prevents 'hacktivists' from creating false accounts that attempt to portray themselves as official sites. Only one official account should be used and the remainder can simply point to the official account.

## CHAPTER 6 – IMPLEMENTATION

6-1. **Introduction.** The successful exploitation of social media in support of ACO's internal and external communications requirements will be dependent on a number of factors. These include, availability/access to appropriate social media tools, familiarity with and confidence in their use, and staff discipline to remain 'in their lane' of expertise/responsibility when posting information into the public domain. The value-added for staff participants will vary from post to post and individual to individual. There should be no compulsion to use social media and national restrictions on the use of social media shall be respected. Commanders should seek to encourage authorised staff to determine themselves how they might best exploit the capability, to experiment and innovate and to share their experiences widely (both internally and throughout ACO) to promote the spread of 'best practices'. By empowering and enabling staff and by harnessing staff creativity and enthusiasm, ACO can gain considerably from the extended use of social media in support of its operational and business outputs. However, the risks associated with expanded use of social media and deeper empowerment of the individual as a communicator requires command acknowledgement and active management.

6-2. **Initial Steps.** The first step in implementing social media within a unit or headquarters should be to develop a social media strategy that clearly articulates objectives, authorities, resources, tools/methods to be employed and measures of effectiveness. This strategy must be aligned with STRATCOM objectives, the PA communication plans, Commander's intent, and the overall themes and messages from ACO and NATO. Social media administrators should create a plan that best fits their goals and communicates to the information needs of their particular audiences.

For developing and implementing this plan, social media administrators should:

a. Review social media guidance from NATO, ACO and the subordinate commands. This guidance provides the basic information needed to fully implement a social media strategy. Social media experts working within PA may request the assistance of other personnel that have social media experience to assist with certain tasks.

b. Using the social media platforms that best meet the organization's goals and needs to create a social media presence. It is best to start with a small number of platforms and execute an effective campaign, rather than to try to have a presence on too many platforms.

c. Register all social media sites with the ACO PA Office Social Media Section.

d. Maintain all social media sites with up-to-date and relevant information by using feedback from the audience and adapting to the Commander's intent and the organizational goals.

6-3. **Measures of Effectiveness.** Social media strategies should be regularly reviewed to ensure organizational objectives and audience needs are being met. There are a wide range of metrics that can be analysed and software programmes that can measure various impacts. Do not just focus on total numbers of followers, but rather seek to measure the level of engagement and interaction occurring with audiences. Track increases in followers and interaction and try to ascertain what factors were behind any increase or decrease in performance.  Finally, attempt to tailor your strategy and methodology to incorporate lessons learned and avoid previous mistakes.  Personnel employed in social media positions should receive formal training in measuring the effectiveness of online campaigns if practicable.  Such training is available via numerous civilian workshops.

## SOCIAL MEDIA – ACO COMMENTS POLICY

1. It is ACO policy to allow comments by external users on its social media sites.

2. Where an answer can be given quickly and simply, respond directly to online questions and queries. More difficult or detailed questions should be referred to existing official channels. Media queries should be directed to the appropriate ACO PA office.

3. All ACO social media platforms should include a clearly posted comment policy that indicates to users the rules surrounding online interaction with ACO. This maintains ACO credibility when deleting comments that do not adhere to the policy. An example of a comment policy is as follows:

a. No graphic, obscene, explicit, abusive, hateful, racist or defamatory comments will be tolerated. These will be removed as soon as identified and offenders may be banned.

b. No solicitations or advertisements. This includes promotion or endorsement of any financial, commercial or non-governmental agency. Similarly, we do not allow attempts to defame or defraud any financial, commercial or non-governmental agencies.

c. Details about ongoing investigations, or legal, or administrative proceedings that could prejudice the processes or could interfere with an individual's rights will be deleted from this page.

d. Apparent spamming or trolling will be removed and may cause the author(s) to be blocked from the page without notice.

e. No copyrighted or trademarked images or graphics may be posted. Imagery posted should be owned by the user.

f. No comments, photos or videos that suggest or encourage inappropriate or illegal activity.

g. No documents of any kind should be posted on this page.

h. You participate at your own risk, taking personal responsibility for your comments, your username and any information provided.

i. All information posted to social media sites will be no higher than unclassified.

j. The appearance of external links or the use of third-party applications on this site does not constitute official endorsement on behalf of NATO or SHAPE.

## GUIDANCE ON MAINTAINING SECURITY ONLINE

1. The following paragraphs outline the main categories of information that could be at risk when using social media and the potential consequences if this information is compromised.

2. **Personal Information.** Personal information is always at a premium in the criminal and espionage world. Personal information may also enable hostile intelligence agencies or terrorists to target military personnel or their families. Items of information which could be used to take advantage of you and your family include:

a. Date and Place of Birth.

b. Full Home Address, Telephone Numbers.

c. Passport details, National lD Card Details.

3. **Account Details.** Criminal groups may try to gain access to online, telephone or other accounts using your account details. It is important that such information is not given to third parties. Information such as that listed below could be used for criminal activity or blackmail:

a. Account Numbers, Logins, or User IDs.

b. Passwords, Pin Numbers.

c. Memorable Phrases, Security Questions.

4. **Details About Your Work.** Hostile intelligence services and terrorist organizations may seek details about your work or your unit/establishment. Information such as establishment/unit locations, telephone numbers, ranks, unit strength, position details or role, could enable your establishment/unit to be targeted. Moreover, images can give away important information, so check to make sure that ID cards/official passes, keys, computer screens, paper documents and other potentially sensitive materials or equipment are not visible.

5. **Operational Information.** When directly involved in operations or supporting them, information protection becomes even more important and attempts to gather information by hostile agencies or groups may become more determined. The hostile exploitation of information may be used by an adversary to counter our operations putting lives and assets at greater risk. It may also damage our credibility with allies and potentially lead to withdrawal of their support. Do not release online information about:

a. Operational Programmes, Deployment Details, Mission-Specific Information.

b. Capability Shortfalls, Casualty Details, Morale.

6. **Protecting Information.** In addition to withholding the types of information described above, there are a number of simple steps to protect you, friends and colleagues online:

a. Understand and apply your security settings; do not give out unnecessary information when registering; do not share logins or passwords and change passwords regularly.

b. Make sure photographs do not give away information you want to protect.

c. Only post items that would be acceptable to your family, friends or colleagues.

d. Choose online friends carefully and be circumspect in the information you share; be respectful about disclosing information about friends and colleagues; respect their privacy and maintain their security.

7. **Information Released in Error.** Security is everyone's responsibility. If you see information on the public internet that you believe may have been released without appropriate authorisation, report the matter immediately to your chain of command so that mitigation action can be taken. If information is sensitive, personal or operational in nature, report the matter immediately via the chain of command to the local Security Officer.