

SUPREME HEADQUARTERS ALLIED POWERS EUROPE

GRAND QUARTIER GENERAL DES PUISSANCES ALLIEES EN EUROPE

B-7010 SHAPE, BELGIUM

ACO DIRECTIVE (AD) 95-3

Our 207449
ref:

Tel: +32-(0)65-44-7111
(Operator)
Tel: +32-(0)65-44 + ext
NCN: 254 + ext

SOCIAL MEDIA

REFERENCES: A. PO(2009)0141, NATO Strategic Communications Policy, dated 29 Sep 09
B. ACO Directive 95-2, ACO Strategic Communications, dated 19 Nov 09.
C. MC 0457/1 NATO Military Policy on Public Affairs dated 18 Sep 07.
D. ACO Public Affairs Handbook 2008, dated May 08.

1. Status. This is a new Allied Command Operations (ACO) directive and is effective upon receipt.
2. Purpose. To provide guidance on the utilisation of social media for official business within ACO.
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. Supplementation. Supplementation is not authorised.
5. Publication Updates. Updates are authorised when approved by the Director of Staff (DOS), SHAPE.

6. **Proponent.** The proponent for the Directive is the Office of the Chief of Strategic Communications (CSC), SHAPE.

FOR THE SUPREME ALLIED COMMANDER, EUROPE

James Selbie, Brigadier General, CAN Army Director of Staff

2 Releasable for Internet Transmission NATO UNCLASSIFIED

Releasable for internet transmission NATO UNCLASSIFIED

TABLE OF CONTENTS	2-1
	2-2
	2-3
CHAPTER1-BACKGROUND	2-4
Introduction Key Challenges Aim Guidance to	
Subordinate HQs Requirements Ways and Means	2-5
	2-6
CHAPTER 2 -SOCIAL MEDIA TOOLS	2-7
Introduction Official Sites SHAPE Official Sites	2-8
Personal Sites & Personal Interaction on Public	
Sites Style Developing Engagement Posting	
Guidelines Comments	
	3-1
CHAPTER 3 -SECURITY AND TECHNICAL	3-2
CONSIDERATIONS	3-3
Introduction Security Considerations Technical	
Considerations	
	4-1
CHAPTER 4 -IMPLEMENTATION	4-2
Introduction Initial Steps Progress Reporting	4-3
	3
ANNEXES	
A. Social Media -ACO Comments Policy	
B. Guidance on Maintaining Security Online	
Page	

Paragraph

1-1 1-2 1-3 1-4 1-5 1-6

Releasable for Internet Transmission NATO UNCLASSIFIED

CHAPTER 1

BACKGROUND

1-1. Introduction

a. Reference A acknowledges that public electronic communications offer NATO additional means of communicating its message in order to meet its objectives. Reference B also highlights the important role to be played by new media¹ in the delivery of effective Strategic Communications outputs within ACO. One element of new media, social media², is a 21st century phenomenon which is yet to be exploited to any significant degree within ACO for a number of reasons including technical limitations associated with NATO information/ computer system architecture and concerns over INFOSEC/OPSEC. However, social media offers potential to amplify and extend the scope of messaging by ACO, through non-traditional means. Empowerment of the individual and decentralisation of message delivery lies at the heart of successful exploitation of social media.

b. This directive will focus on the use of social media as a means by which internal and external communications and messaging can be enhanced. In addition, they provide a powerful means by which commanders can outline their broad intent and promote the concept of Mission Command. Moreover, social media tools also have the potential to support development of new business processes which could provide enhanced organisational agility while reducing bureaucracy and manpower requirements.

1-2. Key Challenges. As with any Internet-based capability, there are challenges, vulnerabilities and risks that must be identified, understood and mitigated in respect of social media tools. We cannot promote the use of these social media tools for their own sake -they must provide value-added to ACO's operational and business outputs. However, nor can we ignore the prevalence and burgeoning growth of new media and social media. Through using social media tools, we can improve our awareness of what is happening and enhance our assessment of the reactions of a wide audience; and then engage as appropriate. The freedom to communicate using these tools must though be balanced with the need to protect OPSEC, the privacy of information, personal safety, and guard against cyber attack and hostile or inadvertent mis/dis-information. Commanders must therefore identify the desired effects to be achieved through the use of these tools, and then guide and actively manage their use accordingly. Similarly, while the use of social media offers potential to improve process efficiency in the medium to longer term, the 'cost' of diverting limited staff effort to social networking activities and local technical considerations (such as access to workstations and bandwidth limitations) must also be factored-in when developing local guidance and implementation plans.

¹ New media is a generic term for many different forms of electronic communications that are made possible through the use of computer-based technologies. ² Social media are designed for dissemination through social interaction using internet-and web-based technologies to transform broadcast media monologues (one-to-many) into social media dialogues (many-to-many).

1-3. Aim. The aim of this directive is to provide guidance to enable military and civilian staff within ACO to make use of social media, while protecting their own, subordinate headquarters, ACO and NATO interests, and to thereby contribute to the effective delivery of ACO's internal and external communications objectives.

1-4. **Guidance to Subordinate HQs.** ACO subordinate headquarters are to adopt this directive, but to develop their plans for the use of social media tools, as appropriate to their particular circumstances, within the guidelines provided. Commanders are strongly encouraged to embrace and exploit, to the maximum extent local conditions permit, the potential benefits of social media tools within their areas of responsibility. Notwithstanding an initial selection of tools to be used, flexibility will be required to determine the most appropriate tools for a given headquarters and a free exchange of experiences is actively encouraged in order to spread best practice. Moreover, Commanders are required to satisfy themselves that appropriate risk mitigation and risk management processes are in place. A key mitigation means is staff training and education, to include periodic social media refresher training, along with security awareness promotion for all staff. Notwithstanding, the underlying principle should be one of empowering staff to play an active role in the delivery of both internal and external communications objectives.

1-5. **Requirements.** Social media tools will complement traditional communications means in contributing to the delivery of ACO's internal and external communication requirements. Internal communication requirements will predominantly be met through the use of ACO's current intranet services and other traditional means. External communications requirements will be met through use of traditional means, and the full range of computer-based technologies, including social media, via the public internet.

a. **Internal Communication Requirements.** There are 4 primary internal communications objectives:

- (1) To convey the Commander's intent and philosophy to staff.
- (2) The timely passage of information from senior leadership to staff, and for dissemination of time-sensitive news.
- (3) To improve the level of awareness and understanding of staff of their role within the NATO 'corporation'.
- (4) To foster a sense of empowerment among the staff, and to promote internal innovation and interaction.

b. **External Communication Requirements.** There are 3 primary external communications objectives:

- (1) To broaden and deepen the understanding of ACO's role with external audiences.
- (2) To engage with external audiences, to explain our mission and generate additional support, and to temper opposing views.
- (3) To solicit ideas from external audiences that may help ACO develop its thinking on specific issues and to nurture 3rd party advocates.

1-6. Ways and Means. Meeting these diverse communication requirements demands a coherent multidimensional communication approach to maximise breadth of audiences and audience penetration. Social media tools have significant potential to support achievement of these objectives. Compared to traditional media, it is generally quicker, less-complex technically and cheaper to produce products for social media. In addition, social media tools provide a means for far swifter updating of information and near instantaneous responses, compared to traditional means. Contemporary audiences increasingly demand to be part of the discussion rather than the

passive recipients of information. Social media facilitates such engagement and enables us to reach both existing and additional, potentially significant, audience groups. Nevertheless, a valid and important place remains for traditional means such as verbal briefings and print copy.

CHAPTER 2

SOCIAL MEDIA TOOLS

2-1. Introduction. A large number of social media communication tools are readily and freely available. New products are being released continuously and there is a high software refresh rate. In addition to a wide range of Web log (blog) applications such as WordPress and Blogger, the most popular social networking and micro-blog tools include LinkedIn, Facebook and Twitter. Wikipedia is an example of a new media tool which has led to the development of an extensive information reference source through collaborative contributions. Each tool tends to develop its own market emphasis and associated share, and some are geographically concentrated. For example, LinkedIn tends to be used by business professionals, and claims 40 million users in over 200 countries. Facebook and Twitter also have a global presence³ focusing on social networking and have increasingly become a platform for marketing and public relations. Other tools, such as Skyrock (whose membership is concentrated in parts of Europe), may offer potential for reaching out and engaging with more specific audience groups.

2-2. Official Sites. In meeting the communications requirements outlined in Chapter 1, maximum use at all levels should be made of existing social media capability. When posting information in an official capacity, the following posting process is to be followed:

- a. Identify the specific audience for the information.
- b. Determine the appropriate social media tool to use.
- c. Perform content review of information prior to posting (see also Chapter 3).

2-3. SHAPE Official Sites. At SHAPE, SHAPE PAO will remain the sole entity managing SHAPE's official presence on social networking sites. Only SACEUR and designated representatives are authorised to publish to such a site on behalf of SHAPE; other personnel may do so only in a 'non-official' capacity, unless specific Command approval is first obtained. SHAPE PAO currently manages three social media capabilities: SACEUR's Blog, the SHAPE Facebook site and the SHAPE Twitter presence. Initial efforts within SHAPE will be targeted therefore at maximising SHAPE's internal and external engagement via these tools as complementary activity to traditional engagement means. The following sub-paragraphs (provided for information only) outline SHAPE's current position and plans to extend use of existing tools. Subordinate level headquarters are invited to adopt a similar approach.

- a. ACO 810g. Within the existing ACO Blog site at www.acositrep.com. SACEUR contributes with his periodic 'From the Bridge' posts. Additional posts from senior SHAPE leadership are encouraged in order to maintain an interesting and dynamic blog presence.
- b. SHAPE Facebook. The SHAPE Facebook site will continue to be managed by SHAPE PAO. It is accessed via links on the SHAPE website at www.nato.int/shape. This is an open group to which anyone with a Facebook account can contribute. However, as noted in paragraph 2-3, comments representing SHAPE official news will only be posted by authorized personnel. (Facebook claims to have 307 million registered users (August 2009).)
- c. SHAPE Twitter. The SHAPE Twitter site is managed by SHAPE PAO and is accessed via links on the SHAPE website at www.nato.inUshape. SHAPE's Twitter presence is focused on alerting 'followers' to content posted elsewhere (for example, SACEUR's blog). SHAPE PAO will continue to be the sole corporate face within SHAPE to 'tweet'.

2-4. Personal Sites & Personal Interaction on Public Sites. There is a growing trend toward a blurring of the division between personal and work related use of social media tools. While personnel are at liberty to maintain personal websites and blogs, access to such tools from NATO communications and information systems is governed by Reference 8, which requires individuals to gain prior approval from Commanders. Commanders are therefore to determine the relative merits of enabling or restricting such use, and to issue local direction accordingly. In addition, personnel who elect to post via their personal user account are to be reminded to exercise caution in offering personal opinion which could be interpreted or misconstrued as an official ACO/NATO position. Similarly, reasonable limitations on free speech (such as no political commentary while in uniform) extend equally to comments on social networking sites when identified by rank or photos in uniform. Personal posts should not contain product endorsements or inflammatory comments. Moreover, personnel are strongly encouraged to include a disclaimer in their posts when they are readily identifiable (via online profile or other means) as NATO staff members. For consistency across ACO, the following disclaimer message is recommended:

The views, thoughts, and opinions offered are personal and do not represent endorsed or official policy.

2-5. Style. Social media engagement is most successful when approached in a personalised, conversational, manner. There is little or no place for formal statements which are best-suited to formal corporate websites (such as www.nato.int), formal verbal or written statements (such as media releases) or publications (such as NATO's periodic Afghanistan Report). A conversational and relaxed style will attract others to offer opinions and to engage in discussion.

2-6. Developing Engagement. The life blood of successful social media networking is frequent, substantive and credible contributions. Commanders will need to consider how best to meet the demand for frequent contributions within their headquarters. However, a vibrant and dynamic engagement will be necessary sustain a meaningful social networking presence. In addition to senior leadership involvement, Commanders may consider identifying and encouraging specific staff members (from a broad spectrum of age/rank/experience) to participate in social media networking (either generally and/or on specific issues).

2-7. Posting Guidelines. All information that is posted to the Internet must be UNCLASSIFIED or non-classified and releasable to the public. Additionally, the following summary indicates the types of information that are not to be displayed on any public accessible website including personal blogs.

- a. Pre-decisional, proprietary, or commercially-sensitive information.
- b. Information that is not based either on personal experience or the scope of personal duties.
- c. Information -other than authorised news releases -about casualties prior to confirmation that next of kin have been notified.
- d. Information -other than authorised news releases -regarding events or incidents currently under investigation.
- e. Information that is under copyright (in particular photographs from the www) or trademark, without permission of the holder.
- f. Unit or other personnel lists/rosters, charts or directories, or names, addresses and telephone numbers of unit members.

g. Information about the future activities or movements of units or individuals which include details of time and/or location.

h. Any image, still or motion, of any military operation or activity unless that image has been cleared for release by the proper authority.

Additionally, personnel should be strongly advised against posting personal information that might compromise the security of the poster and/or his/her family.

2.8. Comments. Participation in social media networking sites (for internal or external communications objectives) is to actively encourage comment, discussion and potentially argument. Candid, substantive debate is a fundamental characteristic of a successful social media site; opinions that differ from those of NATO and its subordinate headquarters contribute positively to the debate. Exclusion of counter-views will swiftly limit popularity and credibility, disruptive or malicious contributions are readily identified and contributors generally selfregulate content after a very short period. However, when available, the ability to screen out comments before they are posted shall be used. The ACO Comments policy is at Annex A.

CHAPTER 3

SECURITY AND TECHNICAL CONSIDERATIONS

3-1. Introduction. The use of social media explicitly involves the posting of information to publically-accessed websites. They consequently lead to an increased potential for INFOSEC/OPSEC infringements resulting from unintentional release of sensitive or classified information to a public forum. Social media tools do not, of themselves, introduce any new INFOSEC threats. However, from an OPSEC perspective, social media tools extend the scope (in terms of means and time) by which threats may occur. For example, social media tools have been used to socially engineer individuals and, in cases of identity theft, authorised use in the workplace may extend individual vulnerability if social media tools are already being used outside the workplace. However, misuse of social media, including its potentially diversionary effects, is not a technology or security problem, but primarily a management issue addressed through education and managerial supervision. Blanket bans on the use of social media tools would deny ACO the opportunity these tools represent for better internal and external communications, collaboration and public outreach. Whereas the release of information into the public domain has previously been tightly controlled (with release authority usually vested in the CPAO of the relevant headquarters), exploitation of social media will require a measured and carefully managed deregulation of authority to release information and greater empowerment of the individual. Equipping the individual with the means, training, and relevant guidance to release information is therefore vital. Deregulation will also place additional technical demands on the information architecture which has limited bandwidth, and with limited availability of, and staff access to, unclassified workstations. In addition, expanded use of social media will expose the information infrastructure to increased risk of compromise.

3-2. Security Considerations

- a. Operational security 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, or may provide information that puts personnel in specialist roles or their families at risk. Further guidance for individuals on maintaining security online is provided at Annex B.
- b. All information that is posted to the Internet must therefore be UNCLASSIFIED or non-classified and releasable to the public. Knowingly or unknowingly releasing classified information into the public domain may violate specific regulations and could lead to legal and/or disciplinary action being taken. Therefore, if there is any doubt about the OPSEC implications of content, authors/originators must first consult with their line manager and seek specialist advice as appropriate.
- c. In order to mitigate the risks of OPSEC violations, individuals authorised to use social media on an official basis are to be specifically briefed on the potential risks associated with their use, by the J2 Security Awareness Cell (or similar headquarters body). They should also be issued with an aide memoire to reinforce the briefing. In addition, access to social media tools should be configured to allow the display of a workstation screen splash page to further reinforce the "DOs and DON'Ts" of social media networking.

3-3. Technical Considerations

- a. Local bandwidth availability and access to NATO Unclassified workstations will influence the degree to which social media can be employed in each headquarters. Moreover, the current information systems do not prioritise between applications and bandwidth to/from the internet is shared equally amongst all applications and users. It will therefore be necessary to assess locally

the potential impact of extended use of social media on business outputs and to regulate their use accordingly. Simple operating restrictions may help mitigate the impact, such as avoiding use of video streaming which is extremely bandwidth heavy. While ACO aspires to enable universal staff access to social media, selective lifting of restrictions by workstation will also help limit the impact, as well as potentially constraining the scope for OPSEC breaches. However, the technical and administrative management burden of such an approach needs to be factored-in to local judgements.

b. As social media tools require access to the public internet, their use will inevitably increase the risk of malware, spam, phishing and hacking (and impersonation) being introduced into ACO information systems. Although defence in depth exists (including Intrusion Detection Systems, Firewalls and anti-virus software), previous incidents have confirmed that NATO is a target for cyber espionage and that our systems may be compromised prior to alerts from defence systems. However, the ability of network perimeter defences to adequately protect the internal systems will be constrained when using social media networking sites as most of the associated security risk is at the application level; user awareness and user end point services (anti-virus) are the key security protection mechanisms.

CHAPTER 4

IMPLEMENTATION

4-1. Introduction. The successful exploitation of social media in support of ACO's internal and external communications requirements, and the potential they offer to support changes to business processes, will be dependant 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 practice'. 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.

4-2. Initial Steps. In recognition of the security and technical considerations previously outlined, and of ACO's very limited experience with social media, Commanders are encouraged to consider a measured approach. They should consider where the benefits of social media might allow most leverage. In addition, they should consider an initial degree of empowerment commensurate with local technical limitations.

a. By beginning to use social media networking tools in a relatively modest fashion, OPSEC/INFOSEC concerns can be managed, while allowing for a degree of experimentation. In addition, training can be focused on a limited audience and subsequently adapted on the basis of experience and as conditions demand.

b. The number of social media tools available for use should also be restricted initially, until experience has been developed and judgements can be made on their utility. To provide a common ACO-wide approach, Commanders are encouraged to limit access to the following single tools which provide a social networking tool (Facebook); a bookmarking tool (Delicious); a micro-blog tool (Twitter); a stills photo tool (Flickr); and a video tool (Vimeo). Other tools may provide greater utility for discrete user groups but approval for their use shall be considered on a case-by-case basis, having first conducted an INFOSEC assessment of the tool under consideration.

4-3. Progress Reporting. In order to formally gauge progress on the use of social media across ACO, Commanders are to provide a brief 6 monthly update to SACEUR by 30 April 10 and 31 October 10. The report should highlight positive and negative aspects of the use of social media and their future plans.

SOCIAL MEDIA -ACO COMMENTS POLICY

1. It is ACO policy to allow comments by external users on its corporate web presences where this supports wider communications objectives, for example by enabling better engagement with audiences.
2. Where an answer can be given quickly and simply, we will respond directly to online questions and queries. More difficult or detailed questions should be referred to existing official channels of accountability. Press queries should be directed to the appropriate ACO Public Affairs office.
3. External users are to be asked to follow the same guidelines as apply to ACO staff when they use social media. Namely, users must not knowingly transmit:
 - a. Offensive, indecent or obscene material or abuse images and literature.
 - b. Material which can reasonably be considered as harassment or, or insulting to, other people or organisations.
 - c. Material in violation of copyright or used in breach of a licence agreement.
 - d. Spam (electronic junk mail) or chain mail.
 - e. Material that could be, by its presence on an ACO website, reasonably expected to embarrass or compromise ACO (although comments that disagree with ACO **are** allowed).
 - f. Commercial activities which are not connected to ACO business.
 - g. Material designed to mislead people about who originated or authorised it (for example, through misuse of signatures).
 - h. Attempts to compromise ACO CIS, prevent legitimate access to them, damage them or seek to cause degradation of performance or denial of service.
 - i. Attempts to gain unauthorised access to ACO CIS or content for which there is no permission (hacking).
 - j. Attempts to access, amend, damage, delete or disseminate another user's files, emails, communications or data without the appropriate authority.

A-1

Releasable for Internet Transmission NATO UNCLASSIFIED

Releasable for internet transmission NATO UNCLASSIFIED

k. Material in violation of the right of privacy as understood under applicable international treaties, agreements, Host Nation laws and NATO regulations

3. Comments which are judged as in violation of these guidelines will be withheld, edited or removed. ACO reserves the right to ignore, limit or suspend comments or responses to comments, locally or universally and without prior notice if it is judged that these are becoming a waste of official funds or time.

A-2

Releasable for Internet Transmission NATO UNCLASSIFIED

Releasable for internet transmission NATO UNCLASSIFIED

GUIDANCE ON MAINTAINING SECURITY ONLINE

1. The following paragraphs outline the main categories of information that could be at risk when using social media, the hostile groups that might seek this information 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 you or your family. It is also possible to give away information about yourself unintentionally through linkages made with other people. It is important therefore to safeguard details of your personal information. Items of information which could be used to take advantage of you and your family include:
 - a. Full Name, Date and Place of Birth.
 - b. Full Home Address, Telephone Numbers.
 - c. Passport details, National ID 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.
1. Details About Your Work. Hostile intelligence services and terrorist organisation may seek details about your work or your unit/establishment. Information such as establishment/unit locations, telephone numbers, rank, staff number, position 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 screen, paper documents and other potentially sensitive materials or equipment are not visible.
2. 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

B-1

Releasable for Internet Transmission NATO UNCLASSIFIED

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 Commander or Line Manager, 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.