BRIEF

Black and White and the 256 Shades of Grey in Between - Reflections on the Question of Attribution for Psychological Operations.

By Thomas Elkjer Nissen, MA
Royal Danish Defence College
BRIEF

Black and White and the 256 Shades of Grey in Between - Reflections on the Question of Attribution for Psychological Operations.

By Thomas Elkjer Nissen, MA
Royal Danish Defence College

Thomas Elkjer Nissen, MA, has from 2001 worked at the Royal Danish Defence College (RDDC) as a Subject Matter Expert responsible for Strategic Communication (StratCom), Information Operations (Info Ops) and Psychological Operations (PsyOps). He conducts research, advises and teaches in the fields of Info Ops, PsyOps, Media Operations (Public Affairs) and the military’s role in Strategic Communications and Public/Defence Diplomacy.
The Royal Danish Defence College is the Danish armed forces’ powerhouse for education, training and research-generated consultancy. Our research is conducted within a broad range of military-related topics. Our research priorities, such as topics and resource allocation are determined by the Commandant of the Royal Danish Defence College, who is aided by a research council.

Research at the Royal Danish Defence College should enlighten and challenge the reader, whether they are in the armed forces or in the surrounding environment. This is only achievable if the employees have the freedom to administer their own research projects and draw their own conclusions. This is a principle, which is honoured at the Royal Danish Defence College.

We hope you enjoy reading the Royal Danish Defence College’s publications!

© Royal Danish Defence College

All rights reserved. Mechanical, photographic or other reproduction or photocopying from this book or parts thereof is only allowed according to agreements between The Danish Defence and CopyDan.

Any other use without written consent from the Royal Danish Defence College is illegal according to Danish law on intellectual property right. Excepted are short extracts for reviews in newspapers or the like.

Copenhagen March 2012
Royal Danish Defence College
Ryvangs Allé 1
DK-2100 Copenhagen
Denmark
Phone: +45 3915 1515
Fax: +45 3929 6172
Editor: LtCol Hans Henrik Møller (Head of Institute for Military Operations)
Layout by B-O. Kure
ISBN: 978-87-995140-0-7

Royal Danish Defence College Publishing House
Abstract
This paper discusses the question of attribution, or source acknowledgment, for psychological operations in the contemporary information environment. The paper furthermore discusses the challenges to the existing attribution policies, or paradigms, presented by the current operational environment predominantly characterised by counterinsurgency operations and the developments within information technology and especially social network media or “new media”.

Acknowledgments
The author would like to thank the staff of Royal Danish Defence College, several anonymous interviewees and contributors and especially LtCol Sean Ogorman (UK Development, Concept and Doctrine Centre), Col (rtd’) Larry Dietz (US Army) and not least Dr. William Mitchell (Royal Danish Defence College) for their comments to this paper.
Introduction

“No more secrets” was the main point in the 1992 Universal motion picture “Sneakers” with amongst others Robert Redford and Ben Kingsley. A movie about a “black box” that was able to decode all encrypted traffic and therefore leave no secrets safe. As Ben Kingsley’s character Cosmo says in the movie “there’s a war out there, old friend, a world war, and it’s not about who’s got the most bullets. It’s about who controls the information - about how we see and hear, how we work, what we think. It’s all about the information…” Now what does a nearly 20 year old movie have to do with Psychological Operations (PsyOps), and more specifically how does it relate to the question of attribution of PsyOps? Now, even more then 20 years ago, the information environment makes it very hard to confine a message or media product to a specific geographic area or to conceal the source of it. Events that only a few years ago could have remained state secrets indefinitely are being reported around the world in minutes. Not because of a “black box” but because of the characteristics of the modern information environment and especially “New Media”. One such “state secret” could be a government or military force’s desire to hide or even lie about the origin of a specific media product or message in order to achieve a specific effect in the information environment.

Traditionally PsyOps policies and doctrines have spoken about what have been labelled as “White”, “Grey” and “Black” PsyOps. These terms refer to the truthfulness of the source and not the content of a media product or message. Today these terms are no longer used to describe our own (NATO) operations, only opponents’ propaganda, but they are still valid as a framework for this discussion. It could even be discussed if they were not to be reintroduced? “White” is when there is a clear and correct attribution on a message or product, “Grey” is when there is no apparent attribution and “Black” is when the attribution is deliberately false. We will later go more into depth with these definitions.

Why is this question of attribution debated in military and government circles in the first place? Firstly, if you as the sender of a message or product suspect that the target audience will mistrust or even disregard your message if it knows it comes from you, or if you believe that you can achieve a specific effect if the target audience believes that it comes from a source other than you, leaving out, concealing or even lying about the source might seem to an option. As seen in Afghanistan where NATO forces have no credibility with insurgent elements as the Taliban it has been argued that NATO should conduct “Black” PsyOps in order to be able to influence them. This could also be tied to potential PsyOps support to military deception operations where communication of true but misleading information can be a part. In military deception operations PsyOps could be used to produce messages and actions that can aid the creation of a perception affecting the enemy decision-making cycle, make the enemy draw wrong conclusions to induce him to react in a manner prejudicial to his interests in support of specific military objectives. However, the engagement of PsyOps capabilities to achieve deception objectives is very contentious.
PsyOps is generally dependent on credibility in order to be able to influence target audiences as desired, and if PsyOps is exposed in lying about the source of a message or product this credibility can very well be compromised. This would leave future PsyOps activities ineffective. On the other hand – what are the odds of getting exposed?

As alluded to earlier in the introduction – where perhaps in the past was easier to get away disseminating falsely attributed messages and products, the contemporary information environment has created both new possibilities and limitations on conducting PsyOps when it comes to attribution.

Two recent cases can help illustrate how it can be very hard to confine a message, or more specifically a broadcast, to a specific area or to hide the true identity of the source. In the early days of Operation Odyssey Dawn, the no-flight operations over Libya in 2011, a US Air Force EC-130 Commando Solo, broadcast PsyOps radio messages to the Libyan navy forces trying to persuade them not to go to sea to engage NATO maritime forces.1 The messages were broadcast with a limited range but within a few hours a Dutch radio enthusiast was able to break the news about the broadcasts on the internet.2 The other case is from the “Arab Spring”. There the news about a Syrian lesbian blogger in Damascus went around the world very quickly. Just as quickly “she” however turned out to be a “he”, more precisely, a middle-aged American man named Tom MacMaster, based in Scotland.3 In both cases the media coverage quickly focused on the process and the actions themselves and not about the actual content and what was the intention.

These two cases show clearly how the contemporary internet based information environment, limits the possibilities for attribution strategies for PsyOps. This is however a technical issue, other and more important issues are the normative questions of credibility, legitimacy and the democratic values upon which we, predominantly NATO countries, justify waging war today, when considered in the context of today’s information environment. These questions also have a bearing on the overarching framework for PsyOps – the strategic narrative. If NATO, a coalition or a nation in its strategic narrative use argumentation as transparency and democracy it is counter-productive to at the same time conduct “Black” PsyOps.

Why the title: Black and White and the 256 Shades of Grey in Between? It would be easy just to say that the risk of being exposed in lying about the attribution of a message or product in the contemporary information environment was too big, and you therefore should conduct only “White” PsyOps. Or to point out that there is precedents in modern war history from World War I to present day for using both “Grey” and “Black” as well as “White” PsyOps. There are probably many more cases

---

1 For more information on EC-130 Commando Solo see: http://www.af.mil/information/factsheets/factsheet.asp?id=182
2 http://www.wired.com/dangerroom/2011/03/secret-libya-psyops/
3 http://www.guardian.co.uk/world/2011/jun/13/syrian-lesbian-blogger-tom-macmaster
where we will never know whether the attribution of a message or media product in reality was what it claimed to be! Giving credence to the argument that it is possible to conduct these kinds of operations! At least for short term gains.

The contemporary operations and information environment, especially when looking at counterinsurgency operations, is though everything but black and white. There can be many reasons –including normative laden “good” reasons, for not wanting to be directly associated to a message or product. Like other value driven aspects of social life such as law and justice, this could also be considered a “Grey” area. As normative considerations are inherently subjective, it is just as well that there are different options for policy and doctrine on the question of attribution in the contemporary information environment. But do these reasons, at the end of the day, really outweigh the risk of compromising the both short and long term credibility of PsyOps capabilities? And more broadly, potentially compromise the legitimacy of the entire operation? Is it for example counter to the strategic narrative conducting these kinds of operations as discussed earlier?

But before we go into the discussion of attribution policy and doctrine in the contemporary information environment, we will need to have a closer look at what PsyOps and attribution entail.

**Method**
The research for this brief is based on historical reference data, current policies and doctrines on PsyOps, and nine semi-structured interviews conducted in person, via telephone or e-mail with persons within government, military or the communication and PR industry in NATO countries working with or related to PsyOps or broader aspects of strategic communications at multiple levels.

**Psychological Operations**
Psychological Operations, or PsyOps, are military activities designed to influence selected target audiences, be it individual’s or group’s, perceptions, attitudes and behaviour in order to support political or military objectives and multiply the effects of other more traditional military activities. The main purpose is to gain and maintain support from already supportive audiences, convince and persuade the uncommitted and to undermine the credibility, understanding and will of, and support to, hostile audiences. This is done through communicating or conveying selected information and indicators relevant to target audiences in order to influence them. The effectiveness of this communication depends on the audience’s perception of the communicator’s credibility, and capability to carry out promises or actions.

There are various doctrinal definitions on PsyOps depending on which nation, or organisation’s policies and doctrines, one looks at. The bottom line is that the pur-
pose of PsyOps is to influence approved target audiences through communication in both words and deeds.

NATO defines PsyOps as: “Planned psychological activities using methods of communication and other means directed to approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives”.4

PsyOps are in other words, planned communications activities with the purpose of achieving effects in the battlespace. Moreover, PsyOps are intended to be integrated into operational planning at all levels – strategic, operational and tactical – and support across the full spectrum of operations.

Depending on the desired effect of PsyOps the target audiences, the methodology and the media used varies, but the basic considerations are the same as far as the communications planning goes.5

1. Mission support. PsyOps must be planned so that the desired effects on the target audience’s perceptions, attitudes and behaviour correspond to the supported commander or unit’s stated mission, objectives and end-state. Whether it is deliberate, framework, or targeting operations.

2. Intelligence support. In order to be effective, PsyOps must be based upon research, evaluation, and understanding of the target audiences conditions, vulnerabilities and motivations. An understanding that should be brought about through Target Audience Analysis (TAA). This is in order to be able to identify and select appropriate content in form of themes, lines of persuasion, symbols and messages and media to convey the content to the audiences.

3. Integration into planning. In order to be effective, PsyOps, along with other communication activities, must be integrated in the planning process early on and continuously coordinated with all other elements of the military staff in order to ensure that activities carried out supports the commander’s mission, objectives and end-state.

4. Timeliness. The context within which PsyOps communicates is critical. The content, symbols and messages, must be disseminated appropriately in time and space in order to achieve the desired effect.

5. Credibility. Credibility is, as mentioned earlier, a precondition for PsyOps ability to influence target audiences. Credibility in the eyes of the target audiences is though a question of perception – in other words “perceptions become reality”.

(4) NATO PsyOps policy. MC 402/1, April 2003, page 2.
(5) Based on NATO PSYOPS Doctrine, AJP 3.10.1., October 2007, page 1-5 to 1-6.
Even though the information communicated is factual and true the sender, or communicator, may not be perceived as a credible source of information in the eyes of the target audience. This is especially true where the sender is often perceived as an occupying force.

6. Truthfulness. In order to gain and preserve credibility PsyOps are based on factually true information. The use of false information is regarded as counter-productive to both the short and long term credibility and future ability for PsyOps to influence and be successful.

7. Source acknowledgement. Last but not least PsyOps are based on the principle of source acknowledgement, or attribution. This continues to be a point of debate for reasons given earlier in this paper!

What is attribution?
Attribution, or in some policy and doctrine, “source”, is the identification of the author or sender of specific message or product. The attribution can be in form of either a name of a person, unit and or organisation or in the form of a logo or symbol. In some cases it can also be in the form of a graphic or layout feature unique to the sender which the receiver immediately will associate or attribute to him. This form of attribution is often only applicable when it comes to actual media products, such as print and different forms of audio-visual products. When talking about face – to – face communication, the receiver will normally know, or associate, the person delivering the message as representing a specific sender. Although this is not the case when the person is appearing to be something they are not like an agent of another country.

As described in the introduction, the terms “White”, “Grey” and “Black” PsyOps have been used for many years. Although not used in current doctrine anymore to describe our own (NATO) PsyOps activities, but only our opponents’ propaganda in connection with propaganda analysis, the terms are still useful as an analytical framework for this discussion.

According to NATO policy on PsyOps, White attribution is when there is an acknowledged source. There is, in other words, talk about overt messaging that can be definitely attributed to a true source that is also willing to acknowledge having distributed the media product or message. Grey attribution is when a message or product comes from an unknown source, or where a source is concealed and not acknowledged by the originator. In some cases, even when confronted with the message or product by the media. Black attribution is when a message or product originates from a source other than the one that is claimed. There is, in this case talk about covert activities or deliberate deception where a false source is definitely implied.⁶

---

⁶ Based on NATO PSYOPS Doctrine, AJP 3.10.1., October 2007, Page D-1.
The tricky part comes when you are dealing with White and Black attribution – is it really the true sender attributed on the product or message? In both cases, there is an identifiable or at least visible attribution in some form or another. Another tricky part is when the source is there but not readily apparent. For example if a sender buries the attribution many layers down on a website. Is that then grey or white? However, as described above, attribution can come in many forms. Everything from a clear and unmistakeable logo or organisational name, over a variation of graphics, sound bites, symbols and unique use of colours, or simply the method of dissemination. For example leaflet drops when there is only one actor in a theatre of operations with the capability to do that.

The question of attribution is also closely linked to the question of credibility as discussed under the principles of PsyOps. For if you get exposed in lying, you lose credibility. It doesn’t matter if the actual content of the product or message is correct, if you are exposed in executing Black PsyOps and the audience perceives it as lying, it is you who are lying to them in their eyes. This perception will also reflect on the content of the product or message and not only the attribution. On the other hand one argument for doing it anyway is if you are targeting an audience with whom, an enemy element, you do not have any credibility anyway – what do you then have to lose? Do actions directed towards an enemy have bearing on other audiences’ perception of your general credibility? It is essentially a gain - loss calculation.

As credibility is a question of perception, consisting of the truthfulness of both the content and the source. Ultimately the credibility of the communicator, the PsyOps products or messages and source, are closely related.

The question of attribution and credibility is also linked to something more deep-rooted in the operational planning, namely the sender’s values represented in the strategic narrative deployed by him. This raises a normative question, as to whether or not democracies can allow themselves to lie about the origin of a messages or media product, even though the content is factually correct, and still keep normative credibility. Furthermore, if you can lie about the source of single messages in order to achieve specific effects in time and space despite of a risk of undermining one’s own strategic narrative, one will also be risking the democratic values and transparency of operations upon which the strategic narrative might be based. Even though lying about disseminating a message, or even lying in respect to the content of it, is not in violation of International Laws of Armed Conflict, it will potentially in the contemporary operation and information environment where legitimacy is imperative – when we fight wars of choice - undermine the strategic objectives.

The question of attribution of PsyOps products and messages are therefore more an issue of credibility and subsequent legitimacy, than one of legal issues in a modern operating and information environment dominated by the “battle of narratives” at every level. It is very much a part of a modern battlespace as the traditional physical battles.
Current policy and doctrine
The question of attribution is normally debated in PsyOps policy and doctrine and not in any other policies or doctrines related to the communication arena. It should be noted that they are very relevant when talking about Information operations (Info Ops) or to some extent even Public Affairs (PA) as well.

Both NATO PsyOps policy and doctrine talk about attribution. The policy states that “In order to preserve Alliance and PsyOps long-term credibility, PsyOps are based on true, factual and attributable information”.7 The policy is therefore quite explicit on the question. The doctrine elaborates a bit more on the question, but is also a bit ambiguous, when stating that in regards to acknowledgment of the source that “NATO PsyOps activities acknowledge the source, and all NATO PsyOps products and programmes should be ultimately attributable to NATO”.8 It has been argued that the last formulation can be seen as an opening for doing not only “White” but also “Grey” PsyOps, as long as NATO acknowledges the ownership of messages or products that initially have been disseminated as Grey. There is however no consensus in NATO regarding this interpretation of the doctrine.

Also the European Union (EU) has a doctrine for PsyOps. (The EU uses the term “concepts” instead of doctrine). As in NATOs policy, it also states that “PsyOps are based on true, factual and attributable information”.9

Most NATO countries have national policies and doctrines for PsyOps. Not all of them address the question of attribution directly, but many of those that do, are rather explicit on the question.

The Canadian PsyOps doctrine for example states in regards to acknowledgment of the source of a PsyOps product or message that “during PsyOps, CF (Canadian Forces) are only allowed to conduct White Propaganda, not Grey or Black”.10 With this the Canadian forces very clearly limits them self to only conducting “White” PsyOps.

UK doctrine includes the question of attribution in the definition of PsyOps itself when UK defines PsyOps as: “PsyOps are planned, culturally sensitive, truthful and attributable activities directed at approved target audiences within the Joint Area

(7) NATO Policy on Psychological Operations MC 402/1, SHAPE 2003, page 2. NATO UNCLASSIFIED.
(8) NATO Doctrine on Psychological Operations AJP 3.10.1. SHAPE 2007, page 1 – 6. NATO UNCLASSIFIED.
(9) EU military Staff Concept for Psychological Operations, 19 October 2004, page 3.
of Operations in order to achieve political and military objectives”.\(^\text{11}\) The doctrine furthermore directs in the principles of PsyOps when it comes to “attributability” that: “PsyOps products must be attributable to, and be acknowledged by, the sponsor. All products must clearly state their source”.\(^\text{12}\) Like the Canadian doctrine the UK one therefore also restricts PsyOps to only “White” activities.

Also German policy and doctrine on PsyOps, or “Operative Information” (OpInfo), states that there always must be a clear and truthful attribution to foster credibility and trust in the message, the messenger, and the product. Every PsyOps product and message therefore has to give clear evidence about its origin or source.\(^\text{13}\)

US joint doctrine on PsyOps (PSYOP)\(^\text{14}\) lists, unlike the English, Canadian and German policy and doctrines, three different attribution methods: United States attribution, concurring partner nation attribution and delayed attribution. Joint Doctrine on Psychological Operations furthermore states that “In addition to objectives and themes, national policies for PSYOP execution include the attribution posture the USG [United States Government] takes in acknowledging responsibility for PSYOP activities. US involvement can be open, partially (technical assistance only) or not acknowledged at all [non-attribution red.] as determined by the CCDR [Combatant Commander]. The attribution posture allows the commander to attribute actions to US, concurring partner nations, or, in the case of sensitive activities, acknowledged as soon as operationally feasible”.\(^\text{15}\) There are provided however, a series of conditions that have to be met before “delayed attribution” can be authorised.

One thing is, however, to have it stated policy and doctrine, another thing is its feasibility in the reality of current operations and an information environment driven by modern technologies.

The predominant view on attribution in NATO, and within most member nations, has for years been that all PsyOps messages and products should be attributable (“White”). Several NATO member countries have had the same view, although some have taken a more flexible view where it concerns national PsyOps. Now challenged by the contemporary operation and information environment, predominately characterised by counterinsurgency operations, and the developments within the social media sphere, these views are under pressure. The attribution of PsyOps is currently debated by many actors in both nations and organisations that are all struggling


\(^{13}\) Interview 3 (representative from the German Ministry of Defence, date 23/09/11).

\(^{14}\) US has changed the name of Psychological Operations (PSYOP) to “Military Information Support to Operations” or MISO in 2011.

with how to address the question in policy and doctrine. Some militaries on one hand even wish to be able to make more use of so called “non-attribution”, and on the other hand, it is pointed out by scholars and think tanks that PsyOps doctrine should be rewritten to ban misleading or false content or disseminating messages with false attribution.\(^\text{(16)}\)\(^\text{(17)}\) Both arguments are based on lessons identified under contemporary operations. The first argument tends to be based on more tactical experiences whereas the later tends to be based on a more strategic view.

**Challenges to attribution in the contemporary operations and information environment**

One of the challenges in attribution is when a message or product spreads beyond the initial dissemination point. One could argue that when for example a soldier disseminates a PsyOps handbill, without a name or a logo on it (“Grey”) on a market place in some theatre of operation the handbill is attributed to the soldier’s unit or force simply by time and space association. The same goes for a message delivered through face – to – face communication or dialog. However, when this handbill or oral message is then further distributed from the initial receiver to others by the initial target audience, the attribution does not necessarily follow. These two examples are classical issues, and the loss of attribution is generally accepted in respect to face – to – face communication. However the introduction of the use of so called “New Media” or social network media as dissemination methods for PsyOps products and messages, changes the character of this classical issue.

The first signs of this tendency was seen already back in 1999 under the Kosovo Air Campaign (Operation Allied Force) over Serbian and Montenegro, where the use of e-mails began to be a widespread way of communicating information about what was happening on the ground during the air campaign. The BBC reported back then: “There is a problem with the personal accounts of the war – how do we know they are true? It is easy to spot the propaganda Web-sites [sic] of the actors such as NATO or the Serbia Ministry of Information, but e-mails are supposedly individual points of view rather than concerted campaigns attributable to the actors. Yet they could be written en masse by government press officers or by hoaxes in California”.\(^\text{(18)}\)

Today New Media, be that Twitter, Facebook, YouTube, blogs, chat rooms, simple e-mails as shown above or other social network media provides PsyOps with possibilities to address target audiences in a new way, both directly and indirectly through mainstream media. Just look at the use of Twitter in Libya by many different actors, or Al-Jazeera’s reliance on tweets in their news reporting. As with the

\(^{\text{(16)}}\) Christopher Paul, Psychological Operations by Another Name are Sweeter, RAND, in Small Wars Journal, July 29, 2010.

\(^{\text{(17)}}\) Interview 4, representative from US Army MISO community, date 02/11/11.

e-mails under Operation Allied Force, no one really knows who tweeted under the conflict in Libya!

Often, these social network sites and profiles can be interlinked or hyperlinked to each other and/or to a main website in different ways. That does not, in itself, represent a challenge regarding attribution as you easily can put a logo or something else on to indicate the source. Where it becomes challenging is when the content, or especially parts of it, starts to go viral - crossing over to other parts of social networks, or when the platforms used by PsyOps give the audience the possibility to adopt or “User Generated Content” (UCG) onto the sites. One of the ideas with using social networks can be exactly that in order for the target audience itself to begin to discuss the themes and topics that supports the PsyOps effort. It now becomes hard to distinguish who the author of a message or product is. New Media therefore also gives plentiful opportunities to conduct “Grey” or even “Black” messaging. One such opportunity is the use of so called “sock puppet” programs. Sock puppet is where a single person or organisation controls a large number of social network profiles in order to create the perception that many people have the same attitude towards a specific topic or theme. US Central Command (CentCom) was accused of trying to set up such a program, in the spring of 2010. Though technology and special software give some possibilities for tracking and revealing who, or at least from where, these activities are conducted, it can be very hard to detect and identify the real source behind it. Cases like the “Syrian Blogger” show that it is possible to some extent to reveal the source. The question now is if a “host server” can be considered as a source acknowledgment? You do not put a clear source on the website, but you do not on the other hand conceal or hide which server your web site is hosted on. In this way, it is possible to identify who is behind a website. It is technically possible so they question in every circumstance to consider would be do your target audience have the knowhow and software to do it?

Another issue in the contemporary operations environment is the question of attribution in counterinsurgency operations (COIN). In COIN one of the principles are that it should not be the international elements of a counterinsurgency force that is attributed to a specific message or product but the local security forces in order to empower them over the long term. It does so by putting a local face on the message or product so the local government or security force can gain credibility and legitimacy. One of the problems in COIN will be the credibility of the external force supporting a local government and its security forces with local target audiences. A second problem is whether or not the local security forces can carry on the security tasks themselves - including the communication to those around them, after external assistance forces leave. A key point is that in order for the target audi-

(20) Thomas Elkjer Nissen, Tactical Information Operations in Contemporary COIN Campaigns, Royal Danish Defence College, Copenhagen, 2011.
ence to respond to the message or product in the desired manner it must perceive
the sender as credible. An issue that gain greater significance in for an example
Afghanistan in view of US president Obama’s intent to accelerate the withdrawal of
conventional forces and increase the use of Special Forces.

In some cases there can also be target audiences that need to be addressed that
perceive neither the international counterinsurgency force nor the local government
or security forces as credible sources of information, and therefore will automatical-
ly reject the message or product. It can also be out of fear of reprisals from the
insurgents that a local population will not be seen with PsyOps or other information
products from the counterinsurgency force or the local security forces. These cases
present a specific challenge in regards to attribution of PsyOps in COIN. One of the
ways to mitigate this challenge is to use what is called “proxy-communicators”, or in
other words, individuals or organisations that act on some else’s behalf and hold
a higher degree of credibility with the intended target audience. Also described by
one of the interviewees as “right message – right messenger”.21

In counterinsurgency operations also the so called technical support to host nation
government and security forces has been debated in respect to attribution. One thing
is simply providing technical support in form of printing or broadcast capability for
messages and products developed by the host nation itself. Another thing is when
the international counterinsurgency force, or single troop contribution nations, it
self produces the message or product and disseminates it in the name of the local
government, security forces, or third party, without their knowledge or consent.

To avoid these challenges and the demands for attribution some have suggested
that military forces simply should designate the activities as something other than
PsyOps for example Information Operations (info Ops) and thereby avoid the attri-
bution policies, or having contracted communication companies, do it for them.22
To this there is only one thing to say – it should be the activity, not the name of it
that decides what policies applies. You cannot say that you do Info Ops in order
to avoid PsyOps attribution policies. It is still you that communicates – contracted
communication company or not - neither the target audiences nor the media will
likely accept this artificial distinction.

**Conclusion**

The question of attribution of PsyOps messages and products is currently widely
debated. The question is linked to both issues of narratives and credibility, legiti-
macy, with their ethical – political considerations on the one side, to issues and
challenges created by the developments in the contemporary operation and infor-
mation environment on the other.

---

21 Interview 1, representative from the Communications Industry, date 21/06/11.
22 Interview 4, representative from US Army MISO community, date 02/11/11.
On the one hand, the demands for credibility, constant legitimisation of actions – to include information activities based on the strategic narrative in the contemporary operation and information environment are high. False attribution can be counter-productive to the strategic narrative and may ultimately damage the political/normative legitimacy for the whole campaign.

On the other hand, with the increasing use of new media for PsyOps purposes and the operational picture in counterinsurgency operations, and in operations for the foreseeable future, the need for flexibility is arguably there. The possibilities for being exposed are higher in an information environment saturated with media and technology that can reveal such activities.

NATO's current statement on attribution, as it is found in the NATO Doctrine on PsyOps seems to work in the contemporary information environment. It allows for flexibility – the possibility for using “Grey” attribution under certain circumstances – but on the other hand it also forces NATO to acknowledge the ownership of a message or product if, for example, asked by journalists. Conceptually this would preclude the possibility that the message is overshadowed by the “process story” of NATO conducting shady operations, or in other words overshadowed by the need for “meta communication” - communication about the communication. It does, however, not take into account the potential operational requirement for having a third party attribution – that being something other than NATO “White” or “Grey” attribution.

“Black” attribution does, however, not seem like a variable option in the contemporary information environment. The advantages if successful are first of all short lived and the possible damage to credibility, undermining of the strategic narrative and future operations is high.

But this still leaves the question of how to deal with situations where a sender of a message or product for ‘good’ reason, cannot be attributed to it.

It can therefore, especially in counterinsurgency operations, be the most appropriate attribution strategy to use a “proxy-communicator” – or in other words “right message – right messenger”. That will say having a host nation government, security forces or a third party attribution on the message or products, as well as being in charge of the dissemination. If this strategy is chosen, it is recommended that the host nation agency, organisation or third party involved is included in the approval process and therefore can acknowledge the ownership of the product or message if asked and if it so pleases.

With the developments in the modern information environment and the challenges with maintaining attribution in the New Media, along with the characteristics of the contemporary and projected operation environment, future policy on attribution should perhaps rather be focused on acknowledgement of the activities then on attribution on individual products and messages. Meaning that the sender should
public acknowledge that he is conducting influence (PsyOps) activities using a specific types of platforms, such as Facebook or YouTube for example, in a specific context in time and space, rather than having a clear attribution on every media product and message.

As suggestion for future attribution policy could therefore be: “In order to preserve XX and PsyOps credibility, PsyOps activities are based on factually true information, and are generally attributed to XX or a concurring partner nation or organisation”.

However, a lot of considerations have to be made both in nations and in different organisations in respect to all the different aspects of the question of attribution for PsyOps as discussed throughout this paper before new policies and doctrines can be implemented.

--- # ---