

12-1-2009

## Cyber Influence

William Hutchinson  
*Edith Cowan University*

Follow this and additional works at: <https://ro.ecu.edu.au/isw>



Part of the [Digital Communications and Networking Commons](#)

---

DOI: [10.4225/75/57a7eecf9f47f](https://doi.org/10.4225/75/57a7eecf9f47f)

10th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia,  
1st-3rd December, 2009

This Conference Proceeding is posted at Research Online.

<https://ro.ecu.edu.au/isw/1>

# Cyber Influence

William Hutchinson  
secau - Security Research Centre,  
School of Computer and Security Science  
Edith Cowan University

## Abstract

*This paper explores influence in the cyber-world and the ability and effectiveness of influence campaigns in this medium. It examines the possibilities of influence in the online world as examines the potential of mobile technologies in this area. The contentious link between influence and behavioural change is investigated. Counter-influence in the context of radicalisation is also looked at. Whilst it is inevitable that the digital medium is and will be used for influence campaigns and will be influential regardless if there are concerted 'campaigns' or not, its effects in terms of behavioural change are still open to question.*

## Keywords:

Influence, persuasion, attitudes, behaviour, behavioural change, radical groups, cyber-influence, counter-influence, mobile technology, social networking sites.

## INTRODUCTION

Terrorists and radical groups have harnessed the Internet for a multitude of reasons ranging from publicity and propaganda to data mining, command and control, and organizational networking (Weimann, 2006). Bergin et al (2009) emphasise the role of cyberspace in the process of radicalisation by avenues such as *Youtube* and attractive web sites (these authors do not discount networks of direct personal communication either). In this paper, the effectiveness of this influence on actually changing attitudes and, perhaps more importantly, behaviour will be examined. Increasingly in the online world, the targets of influence and propaganda are becoming active participants in the process – the targets of influence are not passive and actually become actors in the process (Kramer and Wentz, 2008). This two-way process of indoctrination has brought a new dimension to the development of influence campaigns

Basically, there are three domains for influencing communication: the emotive/value laden ('hot' messages), rational/cognitive argument ('cool' messages) and social/conforming communication (Larson et al, 2009). The cyber-world has the tools to convey of these factors both at blanket and individual targets. As the reach of digital communications via the Internet has become almost universal when such elements as satellite telephones are considered, the importance and dominance of this medium in influence operations will dominate.

## THE POSSIBILITIES OF ONLINE INFLUENCE

The development of the Internet and associated software has meant that the model of communication has shifted somewhat from a centralised 'push' mode where messages sent are 'consumed' by target populations to one where messages are sent into networks where they are changed by the consumers of those messages. The development of products such as social networking sites, texting, and 'communal' gaming sites has meant that communicating has an immediacy that makes long term tactical planning for influence campaigns become, by necessity, more tactical in nature. Radical groups with their innate flexibility in relation to government entities have had the advantage in exploiting a situation, and as an important elements of influence is get your interpretation of events in the population first. Of course, there is still a need for the credibility of the source and message to be accepted. The official televised execution of Saddam Hussein is a case in point – the silent edited images were in stark contrast to those taken by a mobile telephone posted on the Internet soon afterwards. The disparity between the official almost dignified, official presentation and the chaotic, abusive unofficial version destroyed the credibility of official sources.

The whole point of influence is to exert some form of power. Larson, et al (2009) posits that there are six bases of social power: informational, coercive, reward, legitimacy, expert and referent power. If one aspect of cyber-influence is considered - social networking - sites such as *MySpace* and *Facebook* illustrate the ability to exert various levels of influential social power. The information provided to individuals has been personalised, timely and from (probably) a trusted source. Because of this it has legitimacy as the people in the network would have similar worldviews. This avenue of influence is very effective and even an element of coercion can be found as the gregarious nature of humans means that social exclusion is a form of coercion. Thus, a form of 'Groupthink' (Janis, 1982) can develop and the influence of the group's perception of events will become very strong. This has meant that official government or corporate sites are challenged by the 'wisdom' of the group's network whose legitimacy is considered to be higher. Even official news sites are being challenged by online sites such as *twitter* where the normal verification of information has been replaced by 'network wisdom' which ironically means that influence can be exerted by the 'first in' perception of an event plus the virally spreading nature of this first story. It is put through a network of individuals that can ironically, contradict this wisdom unlike a medium such the conventional mass media where the information flow is one-way.

## MOBILE INFLUENCE

The development and expansion of mobile technologies have had a profound affect on the communication of information. This has enabled the ability to influence individuals directly and groups indirectly (via a virally spread story from targeted individuals to their peer network). The nature of mobile device usage is that it can be assumed that a target can be reached 24 hours a day. The features of this technology mean that users can be targeted at an individual user basis, or be chosen by their geographic position, in fact, when coupled with databases and search engines any criteria stored in those databases can be used if they can be linked to user numbers. At a service level this can mean that all mobile devices in a geographic area can be alerted to some impending peril such as a bush fire, or at a more devious level, a group with an age range can be targeted to sell a product or an idea wherever they are

Mobile devices have become ubiquitous in the last decade and are ideal for influence campaigns. Fogg and Eckles (2007) explain the attractiveness of mobile digital devices and offer three metaphors to explain their attraction:

- The *heart* metaphor : we love them
- The *wristwatch* metaphor : they are always with us
- The *magic wand* metaphor: they have so much capability.

Whilst these metaphors are hardly scientific, they do encapsulate ideas of why these technologies are so attractive as a medium for influence. If there is an emotional attachment to these personal devices then credibility if the message is more likely to be high as their users personally identify with them; as the ability to contact someone is almost constant they are an ideal medium to get the message through, and, as they have so much capability, messages can be sent in various formats from a simple text message to a sophisticated real time video. The personalised nature of personal mobile devices makes them seductive and ideal for influence operations.

## INFLUENCE VERSUS BEHAVIOUR

Whilst there is a potential to use digital networks as medium to exert influence and thus change attitudes, it must be noted that the relationship between attitude and behaviour is a problematic one (Erwin, 2001; O'Keefe, 2002). Cragin & Gerwehr (2005) note that, in the context of the radicalisation of terrorist groups, there are a number of stages needed to radicalise anyone, there are:

- **Compliance:** requires a short term effort is needed and uses tactics such as coercion and enticement,
- **Conformity:** requires a medium term effort and uses tactics such as social and environmental manipulation, and
- **Conversion:** requires a long term effort and uses indoctrination.

The goal of most influence campaigns is to get to the 'conversion' stage and this requires long term efforts such as this found in conventional education systems or really consistent and long term advertising campaigns. However, Larson et al. (2009) posit that strong attitudes and beliefs (that is, those more accessible from memory) are more resistant to persuasion and are more likely to predict behaviour. So paradoxically, if influence is successful it will be

more difficult to alter that attitude and behaviour patterns by future influence efforts. As influence on Internet based media is relatively new compared to those found in education and religious institutions. The long term efficacy of this medium has yet to be established. Geltzer and Forest (2009) further complicate the issue when they state that influence is almost impossible to measure either qualitatively or quantitatively as it is transient and its effect on behaviour is tenuous. Thus by their reckoning, Internet and other digitally based campaigns might be able to marginally effect behaviour and attitudes but only in the short term.

To further complicate the issue Cragin & Gerwehr (2005) state that there are six stages from 'influential' messages to action, they are:

- **Exposure:** message should reach audience
- **Attention:** message should overcome background noise
- **Comprehension:** intended audience understands message
- **Acceptance:** appropriate *schemas* must be used that makes comprehension easy
- **Retention:** message should be durable (this time is determined by objectives)
- **Translation:** a cognitive change leads to behavioural change (circumstance has an important part to play here).

Thus, in their model behaviour can be changed if the above stages are fulfilled. Such creations as social networking sites could meet the criteria for Exposure, Attention and Comprehension (and perhaps Acceptance by default as the *schemas* needed might be there because of the self selection of the group) but Retention and Translation would require a strong link between the message and the psyche of the recipient.

## COUNTER-INFLUENCE

There is an acceptance that certain sites espousing violent and radical actions have influenced some in the community (Bergin et al., 2009). The two basic counter-measures to these sites that the state can use are: close the offending sites down, which is often not effective as the sites can pop up somewhere else and also, does not counter the messages sent by them, or set up counter sites as well as monitoring the offending sites for intelligence. If counter sites are set up, it is essential to understand the social norms of a group to influence and this includes the political, tribal, and religious background of the target group as well as the underlying power and economic influences on that group (Larson, 2009). Influence campaigns need to have specific desired effects on a target audience using a combination of information channels. They should consider the characteristics of the audience, timeliness, and if the messages are produced professionally to a standard and format that appeals to the specified audience – if possible, an avenue for feedback should be included (Larson et al, 2009). The Internet is especially suited to this as many varied sites targeted at various audiences can be set up relatively cheaply.

The tactical messages sent out on these sites should do such things empower the powerless and use ridicule against the offending group (Waller, 2007), although ridicule should be used carefully to ensure that it is not also taken by the audience as ridiculing them as well. Few messages have immediate effect and repetition is often necessary (Kramer and Wentz, 2008). Both the timing and the messenger have an effect on the impact of the message. The medium of delivery must be tailored to suit the target. The audience should be segmented, and the means and format of the information conduit should be suited for each case. Non-verbal messages are often equally if not more, important than the verbal, and symbolism can have a profound influence.

## CONCLUSION

Cyber-space like many other media has profound potential for influence. At the level of getting a message to a large and, if required, targeted audience, it has the ability to produce speedy results. However, the link between the sending of the message and producing influence is problematic and the further link between that and changing behaviours is even more so. It is accepted that the digital world offers cheap and effective ways to produce both high quality and fast simple messages to a large and/or targeted audiences. As such, it is inevitable that this medium will be used for influence campaigns. The challenging issue is whether these campaigns actually do influence and to what level they do so – it is even more problematic if this influence then converts to behavioural change or compliance. It is fairly certain that the cyber-world is used to reinforce existing belief systems and behaviours but the effect of change, especially in a fundamental way is less certain.

## REFERENCES

- Bergin, A., Osman, S.B., Ungerer, C. & Yasin, N.A.M. (2009) *Countering internet radicalisation in Southeast Asia*, Canberra, Australian Strategic Policy Institute, 22, March, 2009, RSIS–ASPI joint report.
- Cragin, K. & Gerwehr, S. (2005) *Dissuading Terror: Strategic Influence and the Struggle Against Terrorism*, Santa Monica, RAND.
- Erwin, P. (2001) *Attitudes and persuasion*, Hove, Psychology Press.
- Geltzer, J.A. & Forest, J.J.F. (2009) Conclusion: Assessing the Conceptual Battlespace, in J.J.F. Forest (editor), *Influence Warfare*, Westport, Praeger Security International.
- Janis, I.L. (1982) *Groupthink – second edition*, Boston, Houghton Mifflin Company.
- Kramer, F.D. & Wentz, L. (2008) Cyber Influence and International Security, *Defense Horizons*, 61, (January), Washington, Center for Technology and National Security Policy, National Defense University.
- Larson, E.V., Darilek, R.E., Gibron, D., Nichiporuk, B., Richardson, A., Schwartz, L.H. & Thornston, C.Q. (2009) *Foundations of Effective Influence Operations*, Santa Monica, RAND.
- O.Keefe, D.J. (2002) *Persuasion: Theory and research*, Thousand Oaks, Sage Publications.
- Waller, J. M., (2007) *Fighting the War of Ideas like a Real War*, Institute of World Politics Press, Washington.
- Weimann, G. (2006) *Terror on the Internet: The new arena, the new challenges*, Washington, United States Institute of Peace Press.

## COPYRIGHT

W. Hutchinson ©2009. The author assigns the Security Research Centre (SECAU) & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. The authors also grant a non-exclusive license to SECAU & ECU to publish this document in full in the Conference Proceedings. Any other usage is prohibited without the express permission of the authors.