Chapter 13
The Islamist Cyberpropaganda Threat and Its Counter-Terrorism Policy Implications

Nigel Jones  
King’s College, UK

Paul Baines  
Cranfield University, UK

Russell Craig  
Cranfield University, UK

Ian Tunnicliffe  
Accordance Associates, UK

Nicholas O’Shaughnessy  
Queen Mary University of London, UK

ABSTRACT
This chapter examines Islamist cyberpropaganda case studies live in 2014, namely Al Qaeda, Islamic State, Boko Haram and Al Shabaab. The authors define cyberpropaganda as the exploitation of the generative characteristics of online interaction for the production and reproduction of propaganda. The cross-case analysis identifies key messages and themes, how cyberpropaganda is generated and spread, and how it is made attractive to those who may act on it. In the discussion that follows implications for the policy-maker are identified and addressed. These include whether to tackle symptoms or causes of the problems and whether to treat the problems as essentially global or local. The final issue is how the counter-propagandist can make themselves heard.

INTRODUCTION
A layered model of cyberspace is usually represented in defence publications as including the physical space, the physical network of connected equipment, the data and information flowing on the logical network, the electronic personas of people, and the people acting in social groups in the ‘real’ world and online (United States Army, 2010). This chapter examines an issue that spans all the ‘layers’ of cyberspace, straddling the organisational boundaries that law enforcement, defence and intelligence organisations (and universities) set themselves in terms of managing expertise, budgets and responsibilities. The study of terrorist and insurgent use of the internet must necessarily work through these layers simply by asking

DOI: 10.4018/978-1-4666-8456-0.ch013
questions such as, who is using which platform to communicate with whom for what effect? This endea-
vour represents a key challenge for the intelligence community seeking to exploit online interaction to
understand the command and control arrangements of a group, their motivations and intentions, gather
evidence for prosecution and data for operations support. This context is not without controversy, as
highlighted by the arguments between government and private companies arising over statements made
by Richard Hannigan, the head of the UK’s GCHQ intelligence agency, in November 2014. Hannigan
has stated that “... increasingly [internet firms’] services not only host the material of violent extremism
or child exploitation, but are the routes for the facilitation of crime and terrorism” (BBC, 2014). This
serves to highlight the importance attached to online activities by government agencies.

Conway (2007) argues that terrorist use of the Internet has five key purposes: 1) information provi-
sion, 2) recruitment, 3) financing, 4) networking and 5) information gathering. Conway (2007) was right
to identify the properties of the internet which differentiate it from traditional media such as volume,
speed, two-way communication and global scope. Much of the intended persuasive power implicit in
online terrorist activities is driven by propaganda, defined here in its contemporary understanding as
“information, especially of a biased or misleading nature, used to promote a political cause or point
of view” (Oxford Dictionaries, n.d.). The idea that the internet acts as an echo chamber is considered
further in a 2013 RAND study on radicalisation and digital media (Von Behr et al., 2013). It examines
individual radicalisation through 15 case studies and argues that these case studies confirm the notion
that that the internet “…allows individuals to seek material that they are interested in, and to reject that
which does not support their worldview. The Internet can give the illusion of strength of consensus…”
(Von Behr et al., 2013:27). The study also discusses the far reach and speedy distribution of extremist
material through online active participation (Von Behr et al., 2013:26).

This chapter seeks to examine through a short review and comparison of current Islamist cases stud-
ies, what we term cyberpropaganda. We define this as the exploitation of the generative characteristics
of online interaction for the production and reproduction of propaganda. We do not wish to generalise
further on Conway’s (2007) work or specifically look at radicalisation as undertaken in the RAND study,
but we acknowledge the characteristics of online communications that they outline. Instead this chapter
explores the generative characteristics of social communications in cyberpropaganda cases live in 2014.
It examines group emergence, specific communication platforms, audiences, messages, themes and pos-
sible effects. This is undertaken in the context of understanding the issues and policy implications for
trying to counter, when necessary, violent extremist cyberpropaganda.

The four cases chosen in this chapter for examination of this important topic include the cyberpro-
paganda activities of Al Qaeda, Islamic State, Boko Haram and Al Shabaab. It is of course tempting in
choosing these case studies to assume that they are connected as simply local expressions of the same
Islamist campaign. A surface reading can focus on shared characteristics such as violent extremist views
in an Islamist context and similar social media platforms. Killcullen (2009) has argued that the internet
and global communications have served to give the impression of a connected global insurgency emerg-
ing from what could be interpreted as essentially local disputes. This raises a question about whether
in countering cyberpropaganda similar approaches should be taken to similar dispositions or thematic
postures as may be apparent across cases, or whether a highly local or targeted and specific form of
counter-measure is required that takes account of critical and, perhaps, not so apparent differences. Each
case is examined in turn, before a comparative discussion is presented. The chapter will conclude with
recommendations for counter-terrorism (CT) policy.