School of Mathematical
and Physical Sciences

Department of Mathematics and Statistics

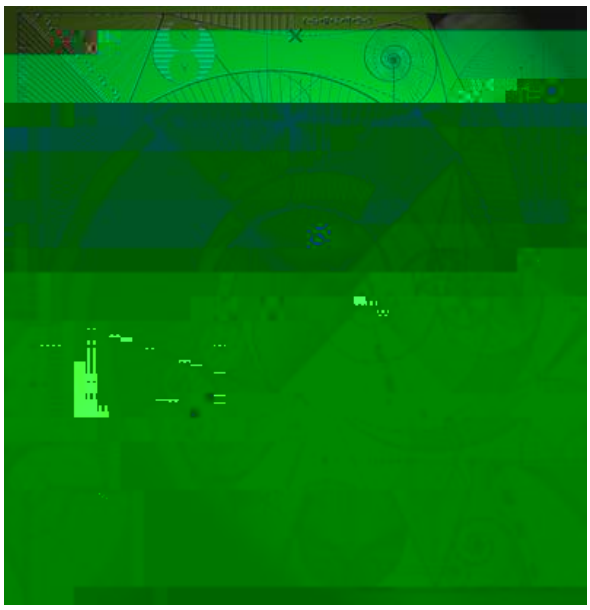
Preprint MPS-2011-09

18 August 2011

Successful Networks in Security and Defence

by

Peter Grindrod and David Sloggett



Successful Networks in Security and Defence

Peter Grindrod
Centre for Mathematics of Human Behaviour
School of Mathematical and Physical Sciences
University of Reading
Reading RG6 6AX UK
p.grindrod@reading.ac.uk

David Sloggett
Centre for Mathematics of Human Behaviour
School of Mathematical and Physical Sciences
University of Reading
Reading RG6 6AX UK

ABSTRACT

This paper discusses the importance of social and communications networks in enabling threats to defence and security. We consider a framework where distinct social and communications networks underpin the preparation, operation and dissemination tasks, with examples drawn from recent events. We argue that all three functions of such networks should be countered. We discuss the attributes of networks which make them di cult to challenge and thus successful, and we consider the extent to which their deployment is supported by the digital society. Finally we suggest that a better understanding of such evolving networks, and the qualities of those most likely to succeed through them, would provide important underpinning for national defence and security strategy and operations.

Keywords

Counter Terrorism, Social Networks, Complexity Theory, Social Analogues, Digital Society, Cyber Threats, Defence and Security

1. THE NATURE OF THREATS

\It takes a network to defeat a network" is the mantra expressed by the most senior US command, facing the insurgency challenges in Afghanistan and Iraq [6]. Equally this might be said of the threats posed by Al-Qaeda and others to the homeland, and even by the recent summer riots and looting within UK cities. But what type of networks must be defeated, and what type of networks and thinking will be required?

Consider the following framework. Modern adversaries may be most likely to be

- organized through an actor network of transient a liations appropriate to time-limited opportunities and *trophy* or O*inspired* goals; procurement, intelligence, reconnaissance and planning; empowering to individuals and encouraging both innovation and replication through competition;
- employing an operational digital communication network (selected form a variety of public and private platforms) that enables and empowers action whilst maximizing agility (self adaptation and reducing the time to act) through the ow of information, ideas and innovations; and
- reliant upon a third party dissemination network within the public and media space (social media, broadcast media and so forth) so as to maximize the impact of their actions.

There are thus at least three networks operating on the side of those who would threaten the security of our operations abroad and the public back at home. None of these networks is reliant upon the others; each is a necessary for the whole enterprise. Critically none of these is in the form of the command and control (hierarchical) networks that we have so embedded within the security forces, the military, and even the government level decision-making.

The main exception to the tri-layered network framework, above, is the self-radicalized *lone wolf*. In such cases the communication network is entirely absent and the actor network limited to procurement, intelligence and some background exploration of intentions. However the dissemination network is often very carefully thought through, prepared, and managed with images, propaganda and threats that will keep the impact rolling within the public/media sphere. The Norwegian gunman, Anders Brehing Breivik, is an example of this: he may have taken some part in online discussions with members of the EDL and other anti-Islamic groups and he needed to procure fertilizer (he could have been picked up though both of these activities); the communication networks appears absent though (there being no known associates involved); yet he went to some lengths by preparing materials for post action dissemination (the online manifesto and posed photographs). That he surrendered so willingly is clear evidence of the importance to him of the third \dissemination" phase.

The Mumbai attack in November 2008 and the London riots of August 2011 are perhaps more typical of the class of threats we have in mind. For Mumbai the existing actor network was an a liate group to Al-Qaeda, based in Pakistan (Lashkar-e-Taiba), with an agenda spreading from

local (Kashmir) to global Jihad. The reconnaissance was

also occur in network models, and may be tested to destruction. The observable and potentially desirable attributes of dynamic networks are interrelated and codependent, and include the following.

- Redundancy: networks that naturally develop redundancies so that no speci c members or contacts are critical: a rough mesh rather than a treelike structure; with no head and a way of evolving those members in the periphery to become weaved into the mainstream.
-

there are now many centres of excellence in that eld. The