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.

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 affiliations appropriate to time-limited opportunities and *trophy* or *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 flow 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 independent networks operating on the side of those who would threaten our security at home and abroad.

The main exception to the tri-layered network framework, above, is the self-radicalized *lone wolf.* In such cases the dissemination network is often very carefully thought through to keep the impact rolling within the public/media sphere. The Norwegian gunman, Anders Brehing Breivik, is an example of this: 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 more typical of the class of threats we have in mind. For Mumbai the existing actor network was an affiliate group to Al-Qaeda (Lashkar-e-Taiba). The reconnaissance was carried out remotely employing Google Earth and other digital assets. The communications network was really the key though. There were six people in Pakistan monitoring the world's media throughout the duration of the attack, and providing real time feedback direct to the assailants by mobile phone.

The 2011 London riots required no planning: just a spark. In the aftermath of the death of Mark Duggan rumours circulated that he had been shot in a de Menezes style operation. Fuelled by the information vacuum, when the IPCC and the police failed to respond to the family-led demonstration, the discontent was picked up by the London gangland network. This was the "actor network" . Gang leaders need to exhibit their strength and importance by besting the police. They have established networks, using BBM secure messaging: the key communication network in this case. It is possible that even the gangs were surprised by how rapidly this cause was taken up by the youth opportunists (Blackberrys are the phone of choice with 37% of 10-16 year olds owning them). This network alerted youths, who were informed where and when to appear (almost on the off chance), inspired by summer nights, no school, good weather, and the prospect of free merchandise. The media images advertised that London police were seemingly unable to cope , so it was inevitable that *copy cat* events would spontaneously arise elsewhere in the United Kingdom. The *a posteriori* dissemination and response, via social networks in this example was for the social commentators and middle England to have its say.

2. ATTRIBUTES OF NETWORKS

What makes networks successful? Recent work on the growth and dynamics of evolving networks is suited to analyzing transient associations and interactions.

There are a number of properties that are desirable and successful: some of these properties occur naturally.

- Redundancy: no specific members or contacts are critical: a rough mesh rather than a treelike structure; evolvingmembers in the periphery to become weaved into the mainstream.
- Self-healing: in response to any insult or removal of parts of the network: local triangularisation, where friends of friends are introduced, is an effective way to ensure this.
- Resilience and substitution: if any part of the network is removed or failing there is another part that can take its place.
- Small-worldness: there may a high degree of clustering (like incomplete lattices) nut there are a few longer range connections that ensure that the average person to person distance between (called the diameter) is relatively small.
- Threshold effects (phase changes): to become effective the properties (diameter, clustering, comunicability, connectedness, viability) of a network do not change linearly with penetration (size or link density within a population); but there are discrete threshold levels, above which functionality is present.
- Absence of any central core: there is no “head” that if removed would result in a fragmentation (lack of connectivity) or a loss of global function.

When we consider the connectedness or other attributes of **evolving** networks one cannot analyze a few single snap shots: like seeing a photo of some dancers and asking what tune they are dancing to. Recent work on communicability [2, 4] indicates that the study of peer to peer dynamics can indicate who are the major influencers, or the sources of activity and information, and who are major listeners or sinks. Even those roles are not static, and members continuously evolve to display such functions.

3. SOCIAL ANALOGUES

It is not just within terrorism and insurgencies that dynamically evolving networks of actors; communications/operations, and dissemination are successful. For example, in almost any region of the UK there are groups of people who are goal or trophy driven; time/resource limited; risk taking and impulsive; decisive; competitive; unwavering in their self belief; highly self motivated; persistent and resilient; have a manic need to succeed; make huge personal sacrifices; see opportunities others cannot see; and never take time off. Moreover they operate in a loose array of informal networks, planning and operating together and separately. These are entrepreneurs [1]. An examination of the qualities of entrepreneurs and successful terrorists and insurgents reveals surprising similarities. It is possible that the best people to second guess (or red team) possible attacks may well be entrepreneurs, rather that security and defense experts.

Commercial competition for entrepreneurial start-up businesses is unlikely to come from large incumbent companies within sectors, exactly mirrors the asymmetries expected within future defense and security operations.

4. CYBER ENNABLED THREATS

Developing networks that can succeed against all three types of enemy networks requires an in-depth consideration of fundamental network attributes discussed here against a back drop of rapidly changing and emerging technology platforms. The uptake and resonance of digital technologies by the mass public (mobile communications, online, gps,...) not only enables those who would do society harm, but also provides a means of remaining hidden within the crowd.

It is often convenient and tempting to lump all “cyber” threats and activities together under one heading: but attacks on cyber infrastructure itself by cyber means, are very distinct from cyber enabled attacks, where cyber resources are used to de-risk, support, enable and extend physical attacks. The importance of both counter terrorism and cyber security was emphasized by their primacy in the recent Strategic Defence and Security Review [1]. So it is timely to ensure that the cyber security agenda should include a proper balance between cyber space attacks and the cyber enabled physical attacks.

5. ACKNOWLEDGMENTS

This work was supported by the RCUK Digital Economy programme via grant EP/G065802/1, *Horizon Hub.*

6. REFERENCES

[1] *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review.* HM Government, October 2010.

[2] E. Estrada and N. Hatano. Communicability in complex networks. *Physical Review E*, 77, 2008.

[3] P. Grindrod. Mathematical modelling for the digital society. *IMA Journal of Applied Mathematics*, 76(3):475–492, November 2011.

[4] P. Grindrod, M. Parsons, D. Higham, and E. Estrada. Communicability across evolving networks. *Physical Review E*, 83, 2011.

[5] P. Grindrod and D. Sloggett. From grievance to martyrdom: a mathematical perspective on the journey of radicalisation. *University of Reading, Dept of Maths and Stats, Technical Report Series 10 24*, June 2010.

[6] S. McCrystal. It takes a network: the new front line of modern warfare. *Foreign Policy*, March 2011.

[1] Qualities of entrepreneurs at www.whereonearthgroup.com/how-successful-entrepreneur.php