School of Mathematical
and Physical Sciences

University of Reading

Department of Mathematics and Statistics

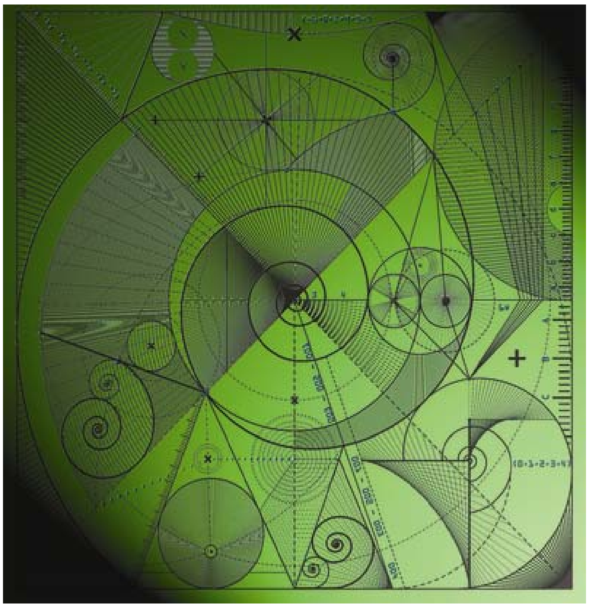
Preprint MPS-2011-09

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 difficult 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 affiliations appropriate to time-limited opportunities and *trophy* or Ò*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 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 affiliate group to Al-Qaeda, based in Pakistan (Lashkar-e-Taiba), with an agenda spreading from local (Kashmir) to global Jihad. 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, maintaining agility, with the key aim of the attack lasting out for seventy two hours so as to allow the world's press to assemble itself and thus maximize the impact (within the dissemination phase).

Such attacks have a trophy element and three distinct phases: the planning, sourcing, and preparation; the operation; and the spread of propaganda and threat. These correspond to the effectiveness of the actor, communication and dissemination networks respectively. Arguably the amplification achieved within the third phase is essential since the scale of enterprise means that the physical attacks must be highly limited in space and time. In the case of Mumbai the communications network was deployed to extend the time window specifically. We must counter all three phases.

Unfortunately it is not just the security services that take lessons from such attacks: 9/11, 7/7 and Mumbai are now textbook examples, and the leanings are there for all to exploit. The desire for increased agility and speed of response from military and civil security services within such asymmetric situations (by which we mean asymmetries of size and scale) is not the only corollary to be drawn here. We should examine the factors that make the different types of networks successful and put effort into defeating all three components. You may need three networks to defeat three networks.

The London riots required no planning: just a spark. In the aftermath of the death of Mark Duggan there was SMS-based discussions between immediate associates, friends and neighbours; and 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 rumours and discontent moved out and were picked up by the London gangland network. This is the true "actor network" in this example. Gang leaders have a need to exhibit their strength and importance by besting the police, and a desire to exploit such situations by looting and criminality. Such gangs 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 with the speed and scale of the events, so it was perhaps 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 (Twitter, Youtube, Facebook,...), was really for the social commentators and middle England to have its say. But the long tail of that interest, within the public memory, may have ramifications for public policy (emphasizing the difficulties posed by police redundancies and cut backs) and for the political futures of the Mayor and the Ministers, as their responses are judged through the harsh lens of hindsight.

2. COMPLEXITY IN SOCIAL SYSTEM

The triple of layered networks introduced above each have some intrinsic properties that in many circumstances are admired and desirable. Increasingly such emergent and phase-like properties are studied as a branch of complexity science applied within in the context of human and social behavior. This is a relatively new area of analytical scientific endeavor since most previous analysis of complex systems concentrates on interaction networks within the physical, chemical, biological or environmental sciences. Arguably this concentration has been driven by the push from academic interests, rather than the pull from the essential needs of the nation or national interests.

The people components of the actor network should be willing (radicalized) and able (prepared to commit). Individuals become so though their own journeys of radicalization. Two extreme paths are obvious: those who first become radicalized (in a response political and cultural causes or in response to perceived and actual attacks) and then subsequently need to get involved and activated; and those who are active and looking for involvement who subsequently become radicalized. Recently this has been conceptualized as a journey like that of player moving through a snakes and ladders board [5]. The catastrophic convergence of external events result in the sudden appearance of (accelerating) ladders across the board: the counter terrorist strategy should prevent people from reaching the higher squares on the board, rather than simply defending and monitoring those most radicalized players.

Beyond security and defence there are many fields where public policy is out of step with (or outrun by) the dynamics of human and societal behavior, attitudes, norms and sensitivities. Equally, many large customer-facing businesses (new media, advertising, retail, telecommunications, finance and consumer goods) need to be able to anticipate and respond to such small and large scale behavioral changes within their addressable populations. So the recent and continuing work of the intrinsic properties of social and communication networks have a very wide set of potential applications indeed.

3. 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. In principle this is highly applicable to all three networks identified above: indeed any assumption of a static network (friendship, peer to peer or many to many communication, or social interactions) will never capture some of the properties that make such networks effective. So an analysis of the dynamics and evolution of networks, how they form and how they change, will be the key to understanding successful networks and countering them.

There are a number of properties that are desirable and successful: some of these properties occur naturally. They 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 specific 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.
- Self-healing: in response to any insult or removal of parts of the network, new contacts can occur dues to local interactions that will ensure that global properties and functionality are retained: sociologists recognize that that 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; so whole subsets of the network and slot into replace others.
- Small-worldness: although within any local part of the network there may a high degree of clustering (like incomplete lattices) there are always a few longer range connections that ensure that the average person to person distance between any pair or members (usually called the diameter) is relatively small. This is a natural in most social networks (any of us is only "six hand shakes" away from the president of the US).
- 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, just as we see within the epidemiology of diseases, there are discrete threshold levels, above which functionality is present: networks are either effective or ineffective and there is no graduated scale.
- 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. Similarly though networks may possess apparent"wisdom", or behave as if there is a collective will, there is in fact no specific place where such properties reside, and thus they cannot removed by any partial interruption.

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. And one cannot take any average: like listening to that average noise that a speaker makes. Neither of these approaches produce results that are specific nor recognizable. Instead evolving networks require new ways of characterizing the roles of them members. 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.

4. SOCIAL ANALOGUES

It is not just within terrorism and insurgencies that dynamically evolving networks of actors; communications/operations, and dissemination are successful. There are some intriguing social analogues from which we can learn much, and form which we may drw some skills and know-how. 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 who have succeeded through their careers within a very different milieu and mind set. Indeed their management and organizational training may well have selected for the very traits that would make them fail as entrepreneurs.

Commercial competition for entrepreneurial start-up businesses is unlikely to come from large incumbent companies within sectors, as their scale and their own organizational decision making network makes them risk averse, lacking in agility, and prone to apply process and justification drag. Large incumbents within any sector must also manage complex strategic, regulatory, reputational and perception (transparency) issues that hinder their local empowerment, responsiveness and innovation. They are thus vulnerable to agile, innovative and radical market entrants. This exactly mirrors the asymmetries expected within future defense and security operations.

5. CYBER ENNABLED THREATS

Building, or rather developing, networks that can succeed against all three types of enemy networks requires an indepth consideration of fundamental network attributes discussed here against a back drop of rapidly changing and emerging technology platforms. The uptake and resonance of certain 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. The *digital society* carries threats – not just to individuals, but to society itself [3]. It also poses opportunities, if we can exploit the data that becomes available with new analytics capable of isolating the many needles within these super digital haystacks.

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 former is about security within a technological context, and protecting ourselves within cyber space, and

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

there are now many centres of excellence in that field. The latter is about exploiting available digital assets (communications, data access, mass participation) so as to enable or increase the effectiveness of the tri-layered networks that underpin successful 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.

It is this last field that should be the focus of future: where are the centers of excellence in such fields that can bridge the human, societal and technological divides? Effort should be invested in understanding how entrepreneurial adversaries, exploiting modern technologies at low cost, can build and flex their effective and evolving networks so as to undermine society, brick by brick, mind by mind, future by future, rather than that seeking to win out in traditional conflicts with physical force.

6. ACKNOWLEDGMENTS

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

7. 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.