
Copyright:

The definitive version of this chapter, published by Routledge, 2014, is available at: http://www.routledge.com/books/details/9780415663151/

Always use the definitive version when citing.

Further information on publisher website: http://www.routledge.com

Date deposited: 29th July 2014

Version of file: Author final

This work is licensed under a Creative Commons Attribution-NonCommercial 3.0 Unported License
Introduction

The early twenty-first century has been characterised by the emergence, refinement and entrenchment of a distinctive mode of warfare. Sometimes characterised as a ‘global civil war’ (Alexander, 2008; Tonnesson and Goldblat, 2002), this mode of warfare is framed as a militarised antagonism between the United States (US) and its allies on the one hand and a global array of perceived terrorists and their sponsors on the other (United States Department of Defense, 2006, pp. 20–24). While initially conceived in the language of inter-state conflict, this violence is better understood as a ‘global counterinsurgency’ (Roper, 2008). Instead of states at war (with one another) global counterinsurgency comprises a globalised state of war.\(^1\) Indeed, even though initial forays into this counterinsurgency were aimed at the governing authorities in Afghanistan and Iraq, the intent was to pre-empt the perceived threat of a so-called global terrorism waged by an array of non-state adversaries against the citizens and values – rather than states – of the US and its allies. In what follows I investigate this globalisation of counterinsurgency in order to delineate the central organising trope of this state of war.

The evolution of a global counterinsurgency

The origins of global counterinsurgency can be traced to post-Cold War interventions in Iraq, Bosnia, Somalia and Kosovo. Framed in 'humanitarian' terms, these interventions signalled the

---

\(^1\) It is worth noting that ‘state’ here captures at least 3 senses; juridical-territorial political entity; mode of existence; and condition. In addition, as a verb rather than noun, ‘state’ captures a performative dimension that will also be central to my discussion in this chapter.
perceived legitimacy of military intervention to realise the liberal foreign policy aims of the advanced industrial states that comprise NATO: in particular the protection of the individual through norms of Human Rights.\textsuperscript{2} Put differently, these interventions comprised a militarised response to perceived counter-liberal forces that threatened the propagation of global human rights norms in the post-Cold War era. Discursively these forces were positioned as linked insofar as each comprised a test for post-Cold War liberal order that, were the latter to fail, would open the door for other adversaries. In the absence of the bipolar stalemate, the liberal post-Cold War order created a sense of identity through a narrative of being besieged by multiple, linked counter-liberal forces with a singular purpose: to destroy nascent global norms focused on the promotion and protection of the individual (politically, economically, culturally).\textsuperscript{3} Faced with such a threat the post-Cold War liberal order, led by the US, developed a discourse, if not doctrine, of intervention that reached its apex with the publication of the International Commission on Intervention and State Sovereignty’s report \textit{The Responsibility to Protect} (2001).

Central to this discourse of intervention was the perception that global dynamics – particularly the transnational interconnections commonly referred to as 'globalisation' – were key to understanding the manner in which those insurgent forces were enabled, assembled and equipped (Kaldor, 2012). The discourse of a globalised illiberal threat was galvanised by the attacks on New York and Washington on September 11th 2001 and the ensuing 'Global War Against Terror'. In the aftermath of the destruction of the World Trade Center a narrative emerged drawing together the various attacks on the US and its allies in the preceding 10 years and positing the need for a more muscular and robust response (Posen, 2001). This narrative

\textsuperscript{2} Here I take ‘liberal’ to refer to multiple and complex phenomena. Uppermost in most accounts of liberalism in international politics are its idealistic vision of interconnection reducing the scope for global conflict (cf. Doyle 1986). Similarly, references to (neo)liberalism as a social-economic system tend to stress a distinctive form of economic organisation: specifically, the globalisation of a free market ideology (cf. Harvey 2005). However, from the perspective of political philosophy the heart of liberal values is a defence of the autonomous individual (cf. MacPherson, 1962).

\textsuperscript{3} Perhaps the best known example of this narrative is Huntington’s notion of the ‘west versus the rest’ (2012, pp. 39–41). Hammond (2007) attributes the spectacular nature of intervention to a search for meaningful identity in the post-Cold War era.
portrayed the liberal order propagated by the US and its allies as threatened by a cooption of the very dynamics that had enabled the liberal order to prosper: namely the interconnections and technologies of globalization (Cronin, 2003). Global travel, communications, information technology and even the globalisation of norms and ideas (insofar as these were expressed in the ideas of a global Ummah) were the means by which an insurgency would reach the very heart of the global liberal order (Arquilla and Ronfeldt, 2001; cf. Roy, 2004).

While initially focusing on the perceived state sponsors of such an insurgency (the Taliban government of Afghanistan and the Hussein Regime in Iraq) this narrative very quickly expanded to comprise an interventionist call for a wider counterinsurgent effort to safeguard the perceived good of a global liberal order. Such a narrative quickly moved to justify the preemptive targeting of perceived insurgents who supposedly threatened the underpinnings of that order (Kegley and Raymond, 2003). Pre-emption was a short step from intervention, global targeting a logical endpoint of the military-technological forces assembled to enable interstate intervention. As such global counterinsurgency was born: an omnivalent strategy of pre-emptive targeting of that which is perceived to threaten liberal norms (of individuality, choice, freedom, markets) and the techno-logistical structures that underpins them.

The so-called war on terror has thus evolved from the initial targeting of particular international rogue states into a permanent, global dynamic of preemptive organised violence. Nothing perhaps exemplifies this better than recent killings carried out by US forces in Pakistan, Yemen and Somalia. The shooting of Osama bin Laden by a US Navy SEAL team in his compound in Northern Pakistan has resonances with drone strikes on Anwar al-Awlaki in Yemen and members of al-Shabaab in Somalia. Each of these attacks comprises an intervention across commonly accepted lines of international jurisdiction in order to target pre-emptively a threat deemed capable of bringing violence to the citizens of the US or its allies directly (as in the case of 9/11) or indirectly (as in the case of targeting of tourists in Bali). Each attack is intended to

---

4 This is the narrative of the ‘long war’ formalised in the 2006 Quadrennial Defense Review (United States Department of Defense, 2006)
disrupt the capabilities of a dispersed insurgent threat through the removal of key agents. Each is the product of a complex, transnational military-political assemblage comprising political-legal narratives, human and machine compiled intelligence, complex databases and guidance systems as well as weapons systems that allow for an agile deployment that evades or occludes the traditional boundaries that have circumscribed conflict zones. The end result is a counterinsurgency that is global in scope and transnational in character (cf. Gregory, 2011).

The network trope and global battlespace

Global counterinsurgency is an all encompassing discourse that posits its terrain of operation as a global battlespace. This concept of a global battlespace is predicated on an underlying discursive framing that posits commonalities between insurgents, their targets and the responses of counterinsurgency forces. In other words, the capacities and potentialities of object and actors within this global battlespace are derived from a perceived common set of characteristics. In particular, global battlespace is underpinned by a trope which envisages existence as a set of labile, flexible interconnections between multiple shifting nodal points: in short, a network. It is the flexibility of interconnections between individuals, cells and ideologues that defines the particular virulence that is said to attach to the contemporary insurgent threat. It is the dependence upon the interconnections of information, communication, transport and logistics infrastructures that define the contemporary vulnerability of the homeland. And it is the agility of densely interconnected forces that is said to comprise the strength of current counterinsurgent doctrine. In other words, underlying the concept of a global battlespace is the trope of the network: a web of interconnective links between a constellation of points.

Ubiquitous in the contemporary period the network has become an onto-epistemological prism through which the capacities and potentialities of the globalised era have been refracted. As Wigley (2001, pp. 83–4) notes: ‘We are constantly surrounded by talk of networks. Every third
message, article, and advertisement seems to be about one network or another... Nowhere escapes the net.’ Indeed, the network has been ubiquitous in accounts of the threats and vulnerabilities central to contemporary international security whether these are the spatially dispersed, horizontally affiliated ‘brand’ terrorism (Zelinsky and Shubik, 2009) associated with al-Qaeda, the nuclear proliferation associated with A Q Khan (Albright and Hinderstein, 2005), or the hackers leading both state and non-state strategies of ‘cyberwar’ (cf. Décary-Hétu and Dupont, 2012). In a seemingly endless chain of self-referral, threats to the network are made by networked threats that demand, in turn, the adoption of the capacities that make the network what it is by those that would defend it.

In light of this ubiquity one would expect the ‘potential “powers” of [networks]’ to be well defined. On the contrary, Hayward Alker (2011, p. 355) notes that ‘their conceptual presuppositions and potential pathologies are ... not clear’. The conceptual assumptions – and the pathologies these entail – of the network trope are key to understanding the assemblage of global counterinsurgency. I will contend that the network comprises an organising onto-epistemological trope that structures our understanding of political violence in a distinctive manner. This trope carries certain assumptions as well as certain entailments that, once unpacked, reveal troubling questions about the deployment of organised violence.

**The geometry of networks: beyond planes and contiguity**

As a trope, the network is constitutive of a particular political imaginary: it refers to, or performs, a perceived ontological entity, its dynamics, capabilities and potentialities. When viewed through the onto-epistemological prism of the network ‘the world’ is understood to be composed and structured in particular ways. Networks are accordingly seen to acquire specific capabilities and potentialities (and, by extension, pathologies). Such an understanding of the network trope inverts the positivist assumption that networks and networking are ontologically
real independently of our understanding of the world.\textsuperscript{5} On the contrary, it is the conceptual trope of the network that structures what we take to be ontologically real. Such an inversion suggests that, rather than asking what properties networks ‘possess’, we might instead ask what the politico-military consequences of constituting the world as networked are: how does it performatively constitute distinctive state(s) of war.

At the core of the network trope is a geometric image: a representation of the manner in which the network assembles entities into a distinctively spatialised ensemble. This geometric image is predicated on the twin figures of the node and the interconnection understood as linking line, or bond. The entities assembled in the network are viewed as nodes, poles from and to which information, goods, power and waste ebb and flow. Abstracted from the assembled network, nodes form a flexible constellation of points: a cloud of entities without predetermined volume or spatial-cartographic coordinates. Just as a constellation of stars is a set of unrelated points linked only by the relationships ascribed by human imagination and perception, it is the linkages, the relations or bonds that give a particular network its dimensions and significance. Nodes only gain meaning insofar as they are connected to other nodes. Their capacities and significance in the network are a consequence of these interlinkages. Indeed, the node is a simply point of articulation, of relay or destination. It is the ways in which they are bound together, of how circuits of flow are established that gives a particular network its distinctive characteristics.

Viewed geometrically, the network is a reticulated space, a set of interconnecting lines drawn – unevenly – between points. The interconnecting lines of the network are substantially different to the grids of the cartographic imagination. While the latter organises space by imposing an

\textsuperscript{5} This is the central error of Chad Whelan’s distinction between networks as metaphors and networks as method or unit of analysis (Whelan, 2012, p. 3). Whelan fails to note that insofar as all are tropes of thought, the latter are just as much a metaphor as the former. Indeed, Whelan misuses the concept of metaphor. It would be more accurate to say that while some writers use the metaphor of the network as an analogy, others deploy the metaphor to effect particular modes of investigation. In both cases the network is a trope of thought: a prism through which the world is refracted, not a simple tool or unmediated apprehension of the ontological nature of the world.
abstract measure on it, the former is a temporary, emergent form established by the contingent linking of otherwise disparate points. The interconnections in the network are not regular and shift as nodes are added or removed. Indeed, this is reflected in the evolution of the representational regime of network thinking (Wigley, 2001, pp. 108–110). Initial network thinking represented interconnection in a regular, orthogonal grid fashion – drawing, by analogy – on the modern urban plan epitomised by downtown Manhattan. However, later network thinking gravitated to representations of interconnection as a more fluid, irregular pattern akin to a spider’s web. It is precisely the irregularity of interconnection and thus the irregularity of the geometry of networks that is significant. No two networks are the same and in any given network the interconnections between nodes are not isomorphic. In this manner interconnections make each node, and each configuration of nodes specific, singular. The geometry of the network is thus that of a shifting constellation of nodes bound by irregular connections. This geometry, I would contend, has certain, linked entailments that are key to understanding the politico-military pathologies of network thinking.

The nodal interconnection on which network geometry is predicated surpasses classical conceptions of territory. The latter are predicated on a distinctive geometrical image: a single uniform, continuous, planar surface that can be sub-divided into discrete, bounded domains. It is these bounded domains that constitute governable territories. The continuous nature of the planar surface out of which territories are carved is central to the geometry of territory. Both the whole plane itself and the bounded units into which it is divided must be continuous since to admit that there are either gaps, warps or glitches is to begin to question the integrity of territorial unit. We see this in the case of so-called ‘ungoverned’ areas such as North Western Pakistan or Somalia, each denied the proper status of territory as a consequence of being regarded as comprising gaps in the normally uniform territorial surface on which global politics is played out.

---

6 An early expression of the network as grid can be seen in Le Corbusier’s plans for urban traffic flow (cf. Le Corbusier, 1967)
7 The hegemony of irregularity in representations of contemporary information networks is illustrated in detail by Manuel Lima (2011)
Central to the image of a uniform, continuous plane is the idea of contiguity. Any point within a territory is in principle connectable to another by moving through a succession of contiguous points that lie between them. Indeed, until the advent of air travel this was the principle manner in which territory was known – as a journey through a series of contiguous points. The importance of contiguity cannot be understated in relation to network thinking. Classical schemas of territory are informed by a sense of propinquity, of ‘next-to’ or ‘nearby-ness’. Each place has a sense of being located on a surface and thus of having neighbouring places. Similarly each territorial parcel or bounded unit is constituted by a sense of being a delimited part of a larger surface and thus surrounded by other such parts of that surface. Indeed, it is this sense of propinquity that is at the heart of classical schemas of international politics such as that espoused by Morgenthau (1985) or Waltz (1979): a schema in which states compete with each other as a consequence of the existential fact of their propinquity in a world of limited resources.

Network thinking surpasses this classical territorial schema however, by displacing the importance of contiguity. Indeed, proximity in the network is a function of the interconnection of nodes rather than transit across a planar surface (Castells, 2000, p. 410). Nodal interconnections have no regard for the contiguous places that might have previously been conceived of as being ‘between’ nodes. The network is comprised of a series of interconnected points without any substantial surface between them. As such, this surpasses the classical conception of territoriality. This a-territoriality can be seen in the social network analysis of Valdis Krebs. Krebs’ rendering of the relationship between the 9/11 hijackers as a network (2002, fig. 4) has no regard to geo-spatial emplacement, no trace of the borders that might have been crossed or constitutive of their identity. The 9/11 hijackers are shown as nodes drawn into an a-territorial network by the relationships formed around the event of the 9/11 hijackings. As such this network is a contingent, temporary, a-territorial entity.
The model for this deterritorialised cloud of interconnected nodes is the interconnections of information technology. The image of the cloud is ubiquitous in representations of information technology networks. Indeed, as Scanlon and Wiener (1999) note the cloud is ‘the icon of choice’ for representing the interconnections of the global networks that comprise the internet. Hal Burch and Bill Cheswick’s Internet connectivity graph provides a visual representation of this cloud (Dodge and Kitchin, 2001, p. 43). This image of the cloud has been co-opted for networked warfighting doctrine: for example, the Ministry of Defence acknowledges that the swarms of drones it envisages delivering future warfighting capacity explicitly mirror such visualisations of the internet (2011, pp. 7–6). As William J Mitchell (1996, p. 23) noted as long ago as 1995 ‘[y]ou get from place to place in cyberspace by following logical links rather than physical paths’. Hence, Mitchell argued, information technology makes us connected, not contiguous (1996, pp. 21–24).

Nowhere have this trope of connection been clearer than in discussions about the nature of global urbanisation.

**Networks and the Urbanisation of (In)Security**

Networks have refigured our understanding of urban life and space in the contemporary era. On an inter- and intra-urban scale, connection has been given increasing priority as the infrastructures of connection become ever denser as urbanisation progresses. As observers of recent urbanisation have noted, ‘institutions, buildings and urban districts … become intensively woven together across international space through the mediating power of local-global infrastructure networks’ (Graham, 2002, p. 74; see also Sassen, 2001, pp. 171–196). Indeed, Taylor (2004, pp. 7–30) refers to this urban networking as the ‘second nature’ of cities. Inter-city networking is reflective of (though not isomorphic with) the intensification of intra-urban infrastructural development. Global urbanisation is marked by the development of dense infrastructural networks that gather large swathes of geographically dispersed urban fabric into singular networks. Of course, neither inter- nor intra-urban networking is even. Indeed, the urbanism associated with contemporary global urbanisation is, as Graham and Marvin (2001) note, ‘splintered’. Infrastructure is itself splintered insofar as it is bundled up into discrete,
private ventures. As this splintering proceeds, so infrastructures fragment cities and communities according to the differential access they are afforded. Indeed, as Graham (2002, p. 74) notes, ‘global relational connections can...be combined with very powerful local disconnections ... local-global infrastructure networks ... can ... cease to be articulated in any meaningful way with their local hinterlands’. Indeed, there are dark, empty interstices between all the bright pathways that might be drawn between the various interconnected nodes of the city (Moss, 2008, pp. 438–9). Treated as non-space, these infrastructural cold-spots are the dark matter of the urban network: its constitutive other, forgotten about in the disavowal of contiguity in favour of connectivity.

The networking of the city has given rise to a sense of the urban environment as complex and vulnerable. The city is conceived as a ‘plastic’ (Warf, 1998, p. 255) space in which the ‘recombinant architectures’ (Mitchell, 1996, pp. 46–105) that are constituted by interconnected networks create complex topologies that surpass the simple planar, territorial schemas that have dominated military thinking since Clausewitz (Department of the Army, 2006, pp. 2–2–2–5). As such it is a space that offers advantages to insurgent forces by problematising the projection of force as it has been traditionally conceived by military planners (that is, in terms of mass travelling across a plane). Moreover, the infrastructural density on which this complexity is predicated is a vulnerability of contemporary urban life. Dependent as it is on various infrastructural pathways, urbanity is vulnerable to disruption and, ultimately, ‘switching off’ (Graham, 2005) whether by advanced industrial armies or insurgent forces commandeering commercial airliners (Hevesi, 2001, p. 6). The network trope is thus at the heart of the urbanisation of security: the nexus of dynamics that both securitise the urban and inflect military-security planning/practice with distinctively urban problematics (such as mastering so-called ‘complex’ urban space).

The elimination of contiguity, and hence the surpassing of territorial schemas, characteristic of the network thinking at the heart of the urbanisation of security raise important issues around military targeting. Specifically, the norms and rules that have previously governed targeting
have rested on notions of contiguity. For example, the norm/rule of proportionality – that any destruction should have an effect proportional to the value of eliminating the target – is predicated on considerations of contiguity. Indeed, proportionality pertains to the amount (or value) of contiguous material destroyed. Only by considering whether the destruction of the target outweighs the possible impact on contiguous material, personnel and civilians can proportionality have any meaning. Proportionality is thus determined not by the target itself but by all that is contiguous to it. However, ‘nodal targeting’ (Mattis, 2008, p. 23) is blind to contiguity, seeking to destroy only the connected entities perceived to form a network. The concept of proportionality thus becomes fatally compromised. Unable to conceptualise the nature of the damage that a strike might cause on contiguous actors, targeting becomes blind to the casualties so-called surgical strikes might cause.

Indeed, nodal targeting could be said to increase, not decrease, the destruction visited on contiguous civilians and civilian structures. In commenting on the increase in the use of GPS directed weapons in Operation Enduring Freedom in Afghanistan, Conetta (2002) notes that:

Most current GPS directed weapons, such as the Joint Direct Attack Munition (JDAM), are simply less accurate than laser-guided bombs. Indeed, GPS-directed weapons are not routinely called "precision" weapons at all, but "accurate" or "near precision" ones. Under test conditions, JDAMs have been able to reliably achieve a Circular Error Probable (CEP) of approximately 10-13 meters -- meaning that fifty percent of the JDAMs dropped will hit within 32-42 feet of their programmed coordinates. By comparison, laser-guided bombs routinely achieve CEPs of 3-8 meters. Even a difference as small as an 8-meter versus a 10-meter CEP equates to being able to put 50 percent of expended weapons within a 2100 square foot circle versus being able to put them in a circle of 3300 square feet. Should an intended target sit among a cluster of buildings, the difference between these two circular areas is significant. And, of course, in either case 50 percent of the weapons fall outside the circles.
Nodal targeting at the start of the Iraq war demonstrates this principle well, with strikes aimed at key nodes in the leadership network killing or injuring contiguous civilians (Human Rights Watch, 2003, pp. 27–40). However, since the leadership network is conceived in abstraction, contiguous civilians are excluded from the targeting calculus. As such, the urbanisation of security, suffused as it is with network thinking, is characterised by a deterritorialised conception of targeting that leads to extant norms of conflict being compromised.

**Flexibility, ambivalence, recombinance**

The surpassing of territorial figures through the disavowal of contiguity is, however, only one element of network thinking. Indeed, network thinking’s tendency to foreground geometrical-spatial representations occludes further important assumptions about the nature of the elements that are said to comprise networks. In particular, network thinking makes certain assumptions about the nature of the nodes that comprise the targets of network-oriented forms of warfighting. Seen through the lens of network thinking, nodes are defined by the relations and links for which they comprise a locus. As relations and links change, so does nature of the node/loci at which they converge. The network is thus conceived as a flexible structure capable of multiple, heterogeneous reiterations. As a consequence, nodes are conceived as being capable of articulating multiple, heterogeneous relations/links both simultaneously and over time. Nodes are understood to be both multivalent - agnostic about the nature or number of connections that link them – and receptive to multiple interconnections. The flexibility of a network is thus matched by the promiscuity of its constituent nodes: a multivalent engagement in many different relations both at any given time and over time. These twin characteristics make recombinance – the capacity for multiple, varied reiterations – a key characteristic of networks.

The promiscuity and flexibility of the network is a powerful discursive tool for network thinking. The multivalent relational capacity of promiscuous network nodes underscores a discourse about the severity of threat posed by networks. Indeed, networks are said to be distinctive and
particularly threatening precisely as a consequence of the flexibility of their structures and promiscuity of nodes. This discursive positioning of networks as dangerous because of their flexibility can be seen in counter-terror discourses. Starting with Arquilla and Ronfeld’s (2001) invocation of the hydra, considerations of the threat posed by networks specifically drew attention to the manner in which flexibility and the tendency towards recombinance made network actors particularly dangerous. For Arquilla and Ronfeld (2001, pp. 12–14) this danger stems from three capacities. Firstly, individual elements of a network have an indeterminate nature as a consequence of their potential for recombinance. Since an element may play multiple different roles in multiple different iterations of a network it is hard to say with certainty what its precise function is. This is, of course, in direct contrast to the way in which hierarchical, military organisations have traditionally specified their parts very tightly and prevented unorthodox recombinations (or multiple possible uses for particular elements). In other words, the classical hierarchical organisation reiterates itself in a singular, not multiple form. Second, the potential for recombinance means nodes can be replaced. Discursively the network is presented as a series of substitutable elements, dangerous precisely because of the manner in which any individual element can be replaced to allow the organisation to continue functioning. The danger of this recombinance lies in being purportedly unable to deal a fatal blow to an organisation that would prevent it continuing. Instead counter-terror discourse portrays its engagement with networks as one that requires sustained attempts at disruption. Finally, flexibility allows for omnidirectional attack or, as Arquilla and Ronfeld (2001, p. 12) refer it, ‘swarming’. Networks are represented as having the capacity to form and re-form in ways that allow them to deliver force(s) from multiple directions – in contrast to the traditional military tactic of massing force at a particular location.

The deployment of these purported tropes in counter-terror discourse after the 2001 attacks on New York and Washington was common. Al Qaeda was represented as a ‘shadowy network’ and much effort was devoted – especially in the field of social network analysis – to mapping
the linkages that defined the organisation’s nodes. Moreover, al Qaeda was portrayed as a resourceful and indefatigable opponent, with reservoirs of recruits to draw upon should any particular node be removed. Attention also focused on the recombinant potential that gave al Qaeda supposedly superior organisational learning, allowing it to reiterate itself in novel forms in response to counter-terror initiatives. Refracted through the onto-epistemological prism of network thinking, al Qaeda was represented as dangerous precisely because of the recombinant properties of its purported network form.

Recombinant Resilience

Recombinance resonates with another trope central to contemporary security discourse: resilience. Variously understood as the capacity to return from, or master and thrive on, disruption, resilience has become a common organising trope for security practitioners as well as a central term in security scholarship (Lundborg and Vaughan-Williams, 2011, p. 368). Originating in ecological science, resilience arose out of dissatisfaction with the idea that natural ecosystems were fundamentally in a state of equilibrium (Cote and Nightingale, 2011, p. 476). While such conceptions viewed responses to disruption in terms of return to an assumed equilibrium state, new ecological thinking conceptualised ecosystems in terms of multiple equilibria (Cote and Nightingale, 2011, p. 476). Such systems do not respond to disruptive events by retuning to a single notional state of equilibrium. Rather, disruption leads a system to establish new points of equilibria. As such, ‘ecological resilience is not understood as the amount of time that systems take to return to an initial stable state, but the capacity of systems to absorb disturbance while retaining the same populations or state variables’ (Cote and Nightingale, 2011, p. 476). Resilience is not, however, limited to natural systems. Indeed, even within ecological studies there is a realisation that the systems under consideration are better

---

8 A good example of the ‘shadowy network’ trope can be seen in Colin Powell’s remarks on Hwala Finance (Department of Justice, 2001); Social network analysis is best represented by the work of Valdis Krebs (2002).

9 A good example would be the use of the trope of the hydra in counter-terror discourse (Crane, 2002; Grint, 2004; Kalic, nd; Wechsler, 2001) to imply the reconfiguration of Al Qaeda after each instance of intervention by the US.
described as ‘social-ecological systems’ in order to recognise the mutual imbrication of human and natural elements (Cote and Nightingale, 2011, p. 475).

While originally intended as a way to recognise the impact of human factors in ecological systems, the incorporation of the social has led to thinking about the resilience of social actors: specifically individuals and communities. Such ‘social resilience’ has been ‘defined as the ability of communities to withstand external shocks to their social infrastructure’ (Adger, 2000, p. 361). Coaffee notes that ‘metaphors of resilience have been used to describe how cities and nations attempt to “bounce-back” from disaster’ (Coaffee, 2006, p. 396). Similarly, Lundborg and Vaughn-Williams note that resilience implies the capacity to ‘recoil from shocks’ (Lundborg and Vaughan-Williams, 2011, p. 376). Referred to by Coaffee and Murakami-Wood (2006, p. 509) as ‘bouncebackability’ this conception echoes original, ecological conceptions. Such accounts imply that social resilience comprises the ability to return to equilibrium after disturbance. However, such a conception of resilience could be argued to fail to properly capture the complexity of social systems. Society could be said to be a complex system of systems with multiple equilibria. As Walker and Cooper (2011, p. 157) demonstrate there is a tradition of thinking about complex systems that views resilience not as recoil from disturbance back to a ‘normal’ (Lundborg and Vaughan-Williams, 2011, p. 373) state of affairs. Rather, writers as diverse as Hayek and Luhmann argue that a ‘complex social system ... thrives upon disruptions to its own state of equilibrium’ thus suggesting that it is important to recognise ‘disequilibrium itself as a principle of organization’ (Walker and Cooper, 2011, p. 157 & 154 respectively). Walker and Cooper thus trace a shift in security thinking from conceptualising security as a conservative logic intended to protect and restore the status-quo, to considering security to comprise adaptive capacities for living and thriving in far-from-equilibrium systems. Such an account can be found ‘in the creative destruction of a ... Hayekian financial order’ that celebrates the opportunities opened up by destabilisation of existing orders and challenges the status-quo approaches of, for example, attempts to manage environmental resources.
It is precisely through this conception of complex systems operating far from equilibrium that network thinking is inextricably linked with conceptions of resilience. Indeed, the network is thought to be inherently resilient precisely due to the manner in which its recombinant potential allows for an adaptive embrace of disequilibrium. The motif of recombinance implies that it is (capacity for) networking per se, not the particular configuration of nodes at any particular time, that is important for understanding the potency of al Qaeda style organisations. The virulence of this type of violence is said to lie in the manner in which there is a built-in substitutability of nodes. While the configuration of actors in any given local instantiation of al Qaeda inspired cell may well be somewhat fixed (as such local cells have small numbers and thus finite permutations), as a global organisation al Qaeda is portrayed as a shifting set of associations and affiliations in which any one group can be replaced with another. This, it is proposed, is the strength of the so-called ‘brand’ model of al Qaeda organisation (Zelinsky and Shubik, 2009, p. 330). At the heart of the brand model is the conception of local al Qaeda ‘cells’ operating nearly autonomously from formal leadership of the organisation. Indeed, what matters for the brand-oriented organisation is branding, not hierarchical structure. Indeed, symbolic rather than real capital holds such brand-oriented organisations together; association with a leadership is less a formal, hierarchical organisational tie, more an affiliation with an idea that has global resonance. As such, the brand-oriented organisation is able to recombine in a number of configurations. Local cells can be incorporated into a network of affiliated entities as long as they are able to articulate their association with the global brand. Brand-oriented organisations can thus add new elements and recombine almost infinitely.

However, this is only half the story. Recombinance is significant insofar as it confers particular potency on so-called networked terror. Recombinance may – according to counter-terror discourses – facilitate growth, flexibility or adaptability of the network and thus make networked terror virulent. It also underpins a second aspect attributed to networked terror: its resilience. Cells in the brand-oriented organisation are largely substitutable: it is their association with the brand (which can be self-ascribed) that is important, not their specific character or planned activities. And thus the wider brand-oriented organisation is resilient to
disruption. This discursive linking of substitutability and resilience can be seen in the frequent deployment of the trope of the hydra in counter-terror discourse. The hydra responds to the disruption of losing a head by growing several more (Grint, 2004, pp. 86–88). Similarly al Qaeda is said to thrive on disruption, capitalising on the perceived interventionism of western military strikes on its members and thus ensuring that the crisis which gave rise to its initial global appeal is perpetuated and the flow of new brand-oriented cells maintained. Network terror is thus portrayed as infinitely extendable and resilient to – by thriving on – disturbances. Its virulence and potency is thus a consequence of the attributes network thinking perceives to characterise its linked, nodal organisational form.

**Expansion and omnipresence**

This purported resilience of networked terror provokes a dual, pathological response from network thought. Firstly, networking thinking attempts to mimic the perceived strengths of the enemy it has identified (substitutability, recombinance). Networks were initially acknowledged as a key facet of the future battlespace in the late-Cold War doctrine of network centric warfare (Cebrowski and Garstka, 1998). In the past twenty years a number of other trends have radicalised these early network-centric conceptions. In this period the armed forces of advanced industrial states – the US in particular – have been transformed and informationalised. Restructured forces have leveraged informational technologies to generate gains in agility and lethality. At the same time, in the period since 2003 those forces have faced enemies perceived to have gained significant asymmetric advantage from their networked capabilities. These trends converged in General Stanley McChrystal’s maxim that ‘it takes a network to fight a network’ (McChrystal, 2011). As Commander of first Joint Special Operations Command and later US and NATO forces in Afghanistan, McChrystal perceived the networked resilience of the enemy to demand a networked response (Ackerman, 2011). As such, the wars in Iraq and Afghanistan were refracted through network thinking.

---

10 Note that the idea that ‘it takes networks to fight networks’ was introduced by Arquilla and Ronfedlt (2001, p. 15) 10 years before McChrystal used it.
The networking of the war on terror is closely imbricated with a second response to the perceived resilience of networked terrorism: the temptation to interdiction and an associated extension of battlespace this implies. The disavowal of contiguity and avowal of recombinance at the heart of network thinking has had a substantial impact on global counterinsurgency, most notably in the emergence of a distinctive global strategy of targeted airstrikes by unmanned aerial vehicles (UAVs). The use of UAVs has expanded significantly from a supporting role in the wars in Afghanistan and Iraq to become a campaign in itself ranging from the Horn of Africa to Pakistan via Yemen. The deployment of UAVs epitomises the temptation of interdiction. This temptation rests on a perception that in order to counter resilient, networked terror, force must be agile and capable of being routed wherever the enemy is. When hybridised with the disavowal of contiguity that underpins network thinking, this gives rise to a notion that UAVs should roam globally without regard for territorial determinations of space. Deterritorialised recombinance leads to a globalisation of battlespace and a perception that a networked response to a networked enemy comprises a form of omnipresence. While drones cannot be everywhere at all times, they can both give the impression of ubiquity through the capability of covering vast amounts of terrain. As recent comments on the drone war in the AFPAK theatre has shown, drones are a constant presence leading to anxiety on the ground as to the omnipresent possibility of targeting. This extension of battlespace combined with a perception that a networked enemy demands an agile and swift response whose recombinance outpaces that of the enemy drives a temptation to interdiction evidenced by the inexorable expansion of the theatre of operations for drones.

Conclusion: the temptations of interdiction

---

11 Also referred to as Remotely Piloted Aircraft (RPA) or colloquially as drones.
12 For example see the Washington Post database Tracking America's Drone War (http://apps.washingtonpost.com/foreign/drones/ accessed 26.11.12)
13 A good example of the ‘air conditioning’ (Adey, 2010, pp. 170–176) by ever present drones in the skies above North West Pakistan and the fear and anxiety it induces can be found in the report Living Under Drones (International Human Rights And Conflict Resolution Clinic at Stanford Law School and Global Justice Clinic at NYU School Of Law, 2012)
Network thinking thus gives rise to an expansive imaginary of warfighting that is constantly tempted towards interdiction. It is this temptation to interdiction that links the urbanisation of conflict and the drone war currently being waged across Somalia, Yemen and the AFPAK theatre. Each is guided by a notion of resilience that values adaptive embrace of disruption over conservative gestures designed to restore the status quo. This adaptive security is driven by a perception that the enemy is resilient precisely because of its recombinant potential. In return this drives a perception that attempts to combat that enemy must be similarly recombinant, ultimately seeking to outperform the enemy’s kinetic velocity. Guided by the notions of promiscuous recombinance and the disavowal of contiguity – the twin onto-epistemological principles underpinning network thinking – the war on terror has succumbed to a temptation to interdiction. The disavowal of contiguity reinforces a fantasy of precision that argues one can remove nodal targets from a social-political network without damaging anything surrounding it. Once this fantasy for precision – or, more correctly, blindness to civilian risk – has taken root, the notion of promiscuous recombinance encourages increasingly wide ranging nodal targeting.

Indeed, as a state of war, global counterinsurgency is characterised by ceaseless movement from one perceived node to the next, regardless of traditional normative or legal boundaries or proscriptions.

The temptation to interdiction can be quite clearly seen in the escalation of the use of UAVs: a strategy that is gaining not losing pace as the ground campaigns in Iraq and Afghanistan are wound down. UAVs are assemblages (Grayson, 2012, p. 123; Williams, 2011) that, in delivering guided munitions, feed a fantasy of precision. Leveraging information technology and surveillance networks (both human and machine) in order to identify and remove singular nodes in complex socio-politico-military networks, UAVs represent the translation of network thinking into military doctrine. The Use of UAVs is a logical conclusion of the temptation to interdiction inherent to that network thinking. This temptation towards an escalating, widening set of targets can be seen in the plans to use UAVs to grasp the twin problems of complexity and networked enemies posed by the urban environment.
The largest potential growth area for UAVs is domestic law enforcement (Wall and Monahan, 2011, pp. 243–245). While some of these drones will be used for surveillance of large rural areas hard to access through ground based means, a significant number will be used to patrol the skies above urban areas.\footnote{14} The drone and the city are, when seen through the lens of networking thinking, ideally suited for each other. The city is a complex assemblage of critical nodes and relationships: it’s dense infrastructure and social relationships have been perceived as both vulnerability and strength. Indeed, the networked nature of the urban has led to an ambivalence about the deployment of force in its environs.\footnote{15} In particular the collateral damage associated with using force in urban environments has been uppermost in the mind of military planners. And yet the fantasy of precision and the disavowal of contiguity central to network thinking has re-vivified the idea of urban intervention. Selective, nodal targeting of infrastructures and individuals is seen as a legitimate deployment of violence in the war on terror. Network thinking is thus legitimating the idea of the city as an arena of combat. Conceived through, and subject to, network thinking, the urban is the ideal complement to strategies of networked force. Indeed, insofar as it gives rise to the idea that networked threats are expansive, contagious and resilient due to their recombinant potential, the global interconnection of cities simply multiplies the sense that urban problems require nodal responses. The contemporary city is thus deeply imbricated with networked thinking, the two intertwined in what I have elsewhere referred to as the ‘urbanisation of security’ (Coward, 2009).

\footnote{14}{It is hard to gauge the extent of drone use by the police and other agencies. In the case of the US the Electronic Frontier Foundation has been using Freedom of Information Requests to try and gather such information: https://www.eff.org/foia/faa-drone-authorizations. In the UK The Guardian has also made (more limited) Freedom of Information Requests (cf. Lewis, 2010; for a response see, Kent Police, 2010) The Federal Aviation Administration is responsible for approving the use of UAVs in US airspace and has gathered public documentation here: http://www.faa.gov/about/initiatives/uas/. A recent United States Government Accountability Office report summarises the state of domestic UAV use (United States Government Accountability Office, 2012).}

\footnote{15}{The various military perspectives on the deployment of organised force in cities are summarised by Evans (2007).}
The urbanisation of security is one aspect of the long term trend in global counterinsurgency towards networked interdiction. As such, it epitomises the ethical and political problems of networked thinking: the expansive temptations it poses and the selective blindness it encourages. As those who have sought to counter the use of UAVs have found, international law has not been fully equipped to respond to the challenges of network thinking (Grayson, 2012, pp. 121–122). Designed to limit the ambitions of states and regulate their warfighting, international law – especially with its emphasis on proportionality and the protection of civilians – is rooted in the territorial thought that network thinking contests. Proportionality, for example, is predicated on the notion of contiguity – proscribing force where its effects would spill out in a disproportionate manner from the intended target to adjacent individuals or materiel. Similarly, the protection of civilians is predicated on the proscription of particular zones on the battlefield: areas with no obvious military target. Network thinking’s disavowal of contiguity surpasses such conceptions viewing anything regarded to be a node in a threatening network as a legitimate target. Targets are not selected despite possible spillover to individuals or materiel contiguous to the target. Rather the contiguous is simply elided from the purview of networking thinking. Orthodox military thought can disregard damage to things and individuals contiguous to targets insofar as the rule of proportionality is observed; network thinking simply does not factor them into calculations, focusing instead on the nodes and relationships that define the network. As such, novel forms of contestation will be required. Appeals to human rights, that would apply despite the deterritorialising effect of network thinking and the attempt to invoke universal jurisdiction in domestic courts provide one nascent route to contesting and potentially disrupting network thinking. However, as Marieke de Goede notes (2012, p. 14), network thinking entails a greater danger: the seductive lure of the network as a supposed descriptive category for the social sciences and humanities. Fields as diverse as the sociology of globalisation, urban studies, political science

16 It is worth noting that this is despite military targeting becoming increasingly tied to legal protocols and advisers. That said, much of the discussion in targeting focuses on the status of the target not that which is contiguous. That this is the case is revealed in discussions of civilian casualties which often focus on whether they were the mistaken target of strikes, not a consequence of contiguous spillover.

17 See for example the attempts by Reprieve to document the drone assemblage and trace political – and ultimately legal – accountability: http://www.reprieve.org.uk/investigations/drones/
and international relations have all taken the network as a descriptive term rather than an epistemological prism through which life is performatively constituted as networked (e.g., Castells, 2000; Sassen, 2001; Taylor, 2004). This has led to a valorisation of networked social movements as offering transformative potential in an era of globalisation (Keck and Sikkink, 1999, p. 100). And yet if the temptation to interdiction identified above is inherent to network thinking, there will have to be a reconsideration of the utility of the network as either descriptive term or critical tool in contesting established social orders. Ultimately, if we are to delineate and contest the current state of war, we will need to see the deleterious impact of the network as an onto-epistemological trope and find a politics that contests it.

Acknowledgements

This paper has benefitted from comments and suggestions from a number of colleagues in a number of fora. Thanks to Alex Houen, Kyle Grayson and Simon Philpott for helpful pointers on the final text as well as to audiences at Warwick University and the Institute of Contemporary Arts. As ever, any remaining obscurities and errors are my own.

References


Available from:
[Accessed 19 November 2012]


