The Evolution of Unconventional Warfare

David Kilcullen
University of New South Wales Canberra, AU
davidjkilcullen@gmail.com

While Unconventional Warfare (UW) remains a viable, low-cost method of indirect warfare, some of the assumptions underpinning traditional UW have diverged from reality in the last two decades. These include the idea that UW occurs mostly within denied areas; the categorisation of resistance movements into underground, auxiliary and guerrilla components; the model of a pyramid of resistance activities becoming larger in scale, more violent and less covert until they emerge ‘above ground’ into overt combat; and the assumption that the external (non-indigenous) component of UW primarily consists of infiltrated Special Forces elements, or support from governments-in-exile. Arguably these assumptions were always theoretical attempts to model a messy reality. But since the start of this century the evolution of resistance warfare within a rapidly changing environment has prompted the UW community to reconsider their relevance. This article examines that evolution and its implications. It begins with a historical overview, examines how drivers of evolutionary change are manifested in modern resistance warfare and considers the implications for future UW.

Keywords: Unconventional Warfare; Guerrilla; Resistance; Underground; Evolution

Introduction

As used by Western Special Operations Forces (SOF) the terms special warfare, guerrilla warfare or unconventional warfare (UW) all mean roughly the same thing: operations by specialised forces to advise, assist and accompany local partners conducting resistance warfare against a hostile state or occupying force. Current United States doctrine considers UW a subset of irregular warfare (IW), a category that includes counterinsurgency, stability operations, foreign internal defence (FID) and counterterrorism. It defines UW as ‘activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area’ (Joint Chiefs of Staff 2016: 249).

While UW remains a viable, low-cost method of indirect warfare, some of the assumptions underpinning traditional UW have diverged from reality in the last two decades. These include the idea that UW occurs mostly within denied areas; the categorisation of resistance movements into underground, auxiliary and guerrilla components; the model of a pyramid of resistance activities becoming larger in scale, more violent and less covert until they emerge ‘above ground’ into overt warfare; and the assumption that the external (non-indigenous) component of UW primarily consists of infiltrated SOF or support from governments-in-exile. Arguably these were always theoretical attempts to model a messy reality. But since the start of this century the evolution of resistance warfare within a rapidly changing environment has prompted the UW community to reconsider their relevance. This article examines that evolution and its implications. It begins with a historical overview, examines how drivers of evolutionary change are manifested in modern resistance warfare and considers the implications for future UW.

A Brief History of Unconventional Warfare

Though state sponsorship of irregulars is one of the oldest and commonest forms of warfare, its modern western iteration dates to the work of the American Office of Strategic Services (OSS) and British Special Operations Executive (SOE) with resistance movements in Nazi-occupied Europe during the Second World War. This, in turn, drew on First World War efforts like those of the Arab Bureau (including T.E. Lawrence in
the Ottoman-occupied Hejaz), 19th-century irregular campaigns in the European colonies of Asia and Africa and the Anglo-Russian ‘Great Game’ in Afghanistan and Central Asia.

**Origins of classical UW**

In its Second World War manifestation, the raw material for UW was the spontaneous resistance (including nationalist, royalist, separatist and communist movements) that sprang up in territories occupied by Germany and its allies. European governments-in-exile provided personnel for infiltration or trained their own UW organisations to work with SOE and OSS, while the Soviets infiltrated teams from intelligence agencies (principally GRU, the main intelligence directorate of the Soviet general staff) to work with partisans and Red Army stragglers behind German lines. In the Pacific, Special Operations Australia (SOA), the Services Reconnaissance Department (SRD) and the Allied Intelligence Bureau (AIB) attempted initially to apply European methods over vastly longer distances, with fewer local partners and correspondingly lower rates of success. While each organisation eventually developed its own style, in general there were five components of classical UW:

- **Espionage** by services such as Britain’s Secret Intelligence Service (SIS), involving clandestine collection of military, political and economic information and other ‘silent’ activities often in tension with the noisy operations of other elements.

- **Political warfare** by organisations such as the U.S. Office of War Information (part of OSS) or the British Political Warfare Executive (PWE) involving remote (radio) propaganda and deception or close-access agitation and subversion. Such activity was normally intended as clandestine (where the existence of the operation remained undetected) or covert (where the sponsor remained unknown, though the operation itself was detected).1

- **Sabotage** and economic warfare, by local networks trained and equipped by UW teams, exile governments or political parties, and (by definition) covert rather than clandestine. Indeed, at times sponsors overtly acknowledged operations in an effort to deter reprisals against local civilians, usually with little success.

- **Guerrilla warfare** by irregulars such as the French Forces of the Interior (FFI) and other maquis groups, the Polish home army (AK) and Albanian, Italian, Greek, Yugoslav or Russian partisans, supported by advisors infiltrated from OSS or SOE, resupplied by air and sea and directed to coordinate uprisings intended to support conventional invasions of their territories. This component was epitomised by the ‘Jedburgh’ missions around D-Day 1944, in which teams of British, American and local advisors, instructors and radio operators parachuted into occupied Europe to link up with local guerrillas, train them, receive airdropped weapons and supplies, then support the allied invasion. Jedburghs became the archetype for later UW teams. In the Pacific, the activities of Z Special Unit (part of Australia’s SRD) with indigenous peoples in Borneo, SOE’s Force 136 with Communist guerrillas in Malaya and the Independent Companies (later Commandos) in Timor and New Guinea influenced Australian SOF thinking.2

- **Direct action**, ranging from small assassination teams like the SOE cell that killed senior SS officer Reinhard Heydrich in occupied Czechoslovakia, to raids by OSS Operational Groups or SOE detachments in France, Yugoslavia, Greece and Norway, to desert- and sea-based raiding by the Special Air Service (SAS) and the Small-Scale Raiding Force (later Special Boat Service, SBS) to airborne operations such as the company-sized Bruneval raid and the ‘Grand Raids’ by Commando brigades at Dieppe and St. Nazaire. Again, variants emerged from the war against Japan, including the ultra-long-range maritime raid (Operation Jaywick) by Special Operations Australia against Japanese shipping in Singapore in 1943, division-sized long-range penetration operations by Orde Wingate’s Chindits and Merrill’s Marauders in Burma, and operations by United States Marine Corps Raiders from Makin Island to Bougainville.3

---

1 These definitions follow traditional British Commonwealth usage, rather than current SOF doctrine, but are preferred in this article because they are useful in examining the concept of liminal warfare described below. For current US definitions of clandestine, covert and overt operations see United States Department of Defense (2010).

2 For Agas and Semut see Harrisson (1959) and Gin (2002). For Force 136 see Chapman (1950). Harrisson, T. (1959). *World within: A Borneo story*. London, United Kingdom: Cresset Press. Gin, O. K. (2002). *Prelude to invasion: Covert operations before the recapture of Northwest Borneo, 1944–45*, *Journal of the Australian War Memorial*, 37. Retrieved from https://www.awm.gov.au/articles/journal/37/borneo#84. Chapman, F. S. (1950). *The jungle is neutral*. London, United Kingdom: Chatto and Windus.

3 Note that Axis powers had their own variants of special operations, but these translated poorly to UW since the raw material, i.e. local resistance movements, was lacking. While some operations – particularly airborne and maritime raiding and underwater
Much as the ‘Jeds’ became the template for future UW, the raiding forces shaped subsequent SOF direct action units such as Britain’s post-war SAS, Australia’s SASR, the British Royal Marine Commandos, United States Rangers and U.S. Special Forces. Others (including the British Long-Range Desert Group and M Special Unit, part of Australia’s AIB, became the progenitors of later special reconnaissance organisations. But after 1945, direct action and special reconnaissance missions (which we might call ‘elite conventional’ rather than unconventional operations) diverged from UW in its guerrilla support and resistance warfare manifestation and were increasingly performed by different organisations.

During the Cold War, starting in the late 1940s with operations into Ukraine, the Baltic states and Albania, successors to OSS and SOE (both SOF and intelligence services) continued UW seamlessly, treating Soviet-dominated Eastern Europe and Communist-controlled Latin American and Asian countries much as their predecessors had treated Nazi-occupied Europe. Most of these operations failed due to factionalism among émigrés, Soviet penetration of Western intelligence services or because the raw material—a motivated indigenous resistance willing and able to accept external UW support—did not exist or was crushed by the extremely capable Communist repressive apparatus in these regions. More fundamentally, classical UW, designed for operational preparation of the environment (OPE) ahead of an invasion, was less successful during the Cold War where such invasions were not contemplated, leaving resistance groups with no immediate objective beyond survival.

The 1960s, with Soviet Premier Nikita Khrushchev’s ‘wars of national liberation’ and a series of campaigns of decolonisation in Africa, Asia and Latin America, saw the retooling of Western SOF (and of UW) into counter-revolutionary warfare support for governments facing Communist insurrections. Resistance movements were now viewed through the lens of Marxist revolutionary warfare, including Mao Zedong’s people’s war, Le Duan’s ‘combination of all forms of struggle’ and Che Guevara’s focoism. Counterinsurgency and FID missions followed, drawing on many of the same concepts and lessons as classical UW.

**Pyramids of resistance**

As can be seen, the set of wartime UW components listed earlier resembles a pyramid of increasingly overt and violent actions at progressively larger scale, with increasing lethality, and in rough chronological sequence. Under the influence of the wars of national liberation, the early 1960s saw this progression solidify into doctrine. The ‘Resistance Pyramid’ developed by the Special Operations Research Office (SORO) in 1966 represents an effort to codify the experience of the preceding 20 years into a unitary model (see Hasler 2017).

The original SORO pyramid is reproduced in Figure 1. It incorporates several assumptions inherent in modern UW doctrine, including the categorisation of resistance into underground, auxiliary and guerrilla components, the covert/overt dichotomy, and the notion that successful resistance must be built from the underground upward, progressing from psychological and political operations by clandestine underground cells, through auxiliary networks and increasingly violent covert activities, toward open warfare by mobile guerrilla forces. The pyramid was updated in 2013 under the Assessing Revolutionary and Insurgent Strategies (ARIS) project to include a ‘public component’ that operates openly alongside the underground, auxiliary and guerrilla force (Figure 2) (Tompkins 2013: 6).

The updated model added the underground/armed component labels implicit in the 1966 version, changed the original ‘underground/above ground’ dichotomy to ‘clandestine/overt’ and replaced ‘preparation of parallel hierarchies for taking over government institutions’ (on the right of the old pyramid) with ‘preparation of revolutionary cadres and masses for revolution’ (now on both sides). Other than these changes, the classical pyramid remained largely unaltered as late as 2016 (United States Army Special Operations Command 2016: 9).

As the statistician George Box pointed out (Box, Hunter, & Hunter 2005) all models are wrong, but some are useful. The SORO pyramid is no exception: it has been hugely influential for a generation of resistance warfare operators, suggesting that it captures something meaningful about the range of potential activities that can occur within a resistance movement and how they might relate to each other. At the same time, the pyramid was cogently critiqued in a 2017 Special Warfare paper by Jeffrey Hasler. Hasler’s analysis is worth reading in full: he questions many assumptions in the pyramid, pointing out that, rather than moving sequentially through a series of increasingly overt, vertically-stacked horizontal layers of activity, real resistance movements operate on a continuum of actions and can go forwards or backwards depending on...
Figure 1: Original version of the SORO pyramid. 1966 (Molnar, Tinker, & LeNoir 1966: 29).

Figure 2: Updated version of the SORO pyramid (Tompkins 2013: 6).
circumstances, while individuals and cells within a movement can take on multiple roles traditionally associated with guerrilla, underground and auxiliary components or can transition among roles over time. And he critiques the centrality of undergrounds in resistance movements, suggesting that different movements can grow from a variety of starting points along the continuum.

Beyond Hasler’s critique, a couple of other observations are worth making. The first is to note that the pyramid, in its post-2013 form, incorporates elements of Second World War and Cold War resistance warfare, blended with social movement theory and Maoist insurgency theory along with elements (such as leaderless resistance, implicit in the notion of a ‘public component’) derived from recent terrorist and militia thinking. While it is easy to conceive of resistance movements where some or all of these elements might apply, there are clearly others—global jihadist insurgency or national resistance movements against occupation, for example—where they might not. Far more importantly, the notion of a clandestine/overt dichotomy is increasingly questionable, given the pervasiveness of social media and deep penetration of electronic surveillance and connectivity tools within modern societies.

The seven-phase model of UW

As an adjunct to this pyramidal concept of a resistance movement—and, again, codifying one particular sequence from Jedburgh-type operations—UW doctrine had solidified, by the 1970s, into a seven-phase model with stages as follows:

1. **Phase 1: Preparation.** Psychological preparation to unify the population against a government or occupying power and ready them to accept external assistance.
2. **Phase 2: Initial contact.** UW teams or sponsoring agencies contact resistance groups or governments-in-exile to develop joint plans and agree on support arrangements.
3. **Phase 3: Infiltration.** UW teams infiltrate the area of operations (AO), contact local resistance groups and establish communication links back to the external sponsor.
4. **Phase 4: Organisation.** UW teams organise, train and equip local resistance cadres, focussing on developing resistance infrastructure and building the underground, then auxiliary networks and ultimately a guerrilla force.
5. **Phase 5: Build-up.** UW teams help cadres expand into an effective resistance movement, focussing on organisational development of the resistance and conducting limited combat operations only.
6. **Phase 6: Employment.** UW teams support the resistance as it conducts combat operations, either until a conventional allied force arrives or hostilities end.
7. **Phase 7: Transition.** UW teams assist as the resistance movement and its guerrilla forces demobilise or are absorbed into a post-war regular government structure and armed forces.¹

In effect, this phasing takes the typical progression of a Jedburgh mission, aligns it with the SORO pyramid and plugs UW teams into the pyramid in a sequential bottom-to-top fashion. The goal is to enable a resistance movement to move quickly through an organic growth process from a clandestine underground to covert auxiliary networks, then overt guerrilla groups and eventually mobile forces, before demobilisation. Obviously enough, since the sole function of a UW team in this model is to enable the resistance movement, the approach hinges on various assumptions about how such movements develop, grow and operate. But are these assumptions valid for modern resistance warfare, as it has evolved over the half-century since classical UW doctrine was codified?

Evolution and Modern Resistance Warfare

In general, evolution is a process of change among organisms or populations in response to stimuli (‘selective pressure’) from an ecosystem. These pressures punish certain behaviours (based on particular combinations of traits and characteristics) while rewarding others. Variation in particular characteristics confers selective advantage, with some variants performing better in a given state of the environment than others. Better performers have a higher probability of surviving to pass their characteristics on to others, and thus over time such characteristics are replicated among a wider population. The combination of selection, variation and replication allows those best adapted to a particular environment to dominate. Several theorists—notably Dominic D.P. Johnson and Rafe Sagarin—have applied these concepts to irregular and asymmetric warfare (Johnson 2009; Sagarin & Taylor 2008).

¹ Adapted from Box, Hunter, & Hunter (2005: 11–15).
Long-standing trends in the environment

Because changes in the environment—and hence in selective pressures acting on resistance movements—are continuous and ongoing, the character of resistance warfare continuously evolves. Long-term changes (which I have described elsewhere as ‘mega-trends’) include population growth, urbanisation, littoralisation (the tendency for population, infrastructure and settlement to cluster on coastlines) and globalisation (increasing ease of transnational flows of people, goods, money and information). These trends, dating back to the start of the European industrial revolution around 1750, are long-standing background factors. Arguably, a fourth megatrend—climate change—is equally long-standing, but has emerged as a military factor only in recent years with the opening of ice-free Arctic sea routes, great-power competition in the high North and changes in maritime and land access to polar settlements. Similar effects are likely to appear in the future in Antarctica, while across the globe populations in low-elevation coastal zones are increasingly subject to flooding and extreme weather events.

Another new trend is the return of great-power conflict in the 21st century. In the first decade after the Cold War most Western militaries were mainly concerned with threats posed by non-state actors and weak or failing states, focussing on peacekeeping, humanitarian assistance and disaster relief. After the 9/11 terrorist attacks of 2001, another decade was spent on large-scale counterinsurgency, counterterrorism and stabilisation operations, again in weak and failing (or occupied) states. By 2011, however, competition between Western powers and revisionist or rising states such as Russia, China, Iran and North Korea was increasing, and by 2014 this had broken into military confrontation (though mostly short of war) in Ukraine, the Baltic, the Middle East, the South China Sea and parts of Africa.

There had been notable instances of UW since the Cold War—in particular, during the invasion of Afghanistan in 2001, the Sunni ‘awakening’ in Iraq in 2006–8 and the Libyan uprising in 2011. However, none of these campaigns involved support to a classic pyramidal resistance; rather, in each case the primary purpose of UW teams was to liaise with an existing, established guerrilla force, provide access to fire support from western air forces and ensure a smooth flow of enablers such as money, equipment and intelligence. Indeed, in the eyes of their local partners, it was often the UW teams’ ability to access coalition airstrikes and thereby help a partner overcome obstacles or defend bases that arguably became the critical contribution of such teams—making the role of the Special Forces Joint Terminal Attack Controller (SFJTAC) the critical one. The return of great-power competition created new opportunities for UW. But the new era of UW was taking place in a transformed environment, due to the most significant trend of recent decades: the explosion of electronic connectivity.

The connectivity explosion

Electronic connectivity began a massive expansion in the 1980s, initially in the industrialised world. This spread to the global south around the turn of the century, with rapid increases after 2000 in Internet penetration, mobile phone usage, access to satellite and cable television and (later) the emergence of smartphones and other smart handheld devices. By 2017, the number of Global Navigation System Satellite (GNSS) devices in use worldwide—including the American GPS, Russia’s GLONASS, China’s Beidou network and the European Galileo system—was more than 5 billion and was expected to grow to 8 billion by 2020 (European Global Navigation Satellite System Agency 2017: 5). The ubiquity of GNSS created new opportunities for communications, command, control, communications and intelligence (C3I), precision engagement, weaponisation of consumer technologies like drones and smartphones, and collaborative or remote engagement. Shooters, sensors and targets no longer had to be in the same geographical area. Virtual theatres (with actors physically separated from their effects) along with increasing connectivity between diasporas and countries-of-origin, decoupled resistance AOs from sources of support.

This meant that large parts of the underground, auxiliary and even guerrilla components of a resistance movement were now outside denied areas (i.e. regions controlled by hostile governments or occupying forces) and could act as a sort of strategic hinterland or virtual safe haven, giving resistance actors greater freedom of action and better access to funding and political support. It also meant that UW teams—or extremist groups—wishing to work with a resistance movement were able to access it without infiltration or covert insertion, either by engaging members online or accessing them indirectly through diaspora networks. And it meant that at least the first four phases of the classic seven-stage UW model (preparation, initial contact, infiltration and organisation)—and possibly the fifth and sixth (build-up and employment)—could now be done remotely by online UW teams (or extremist sponsors) engaging many resistance groups simultaneously across multiple AOs without ever leaving their home locations. And physical infiltration of UW teams could now build on this ‘virtual infiltration’, taking advantage of much deeper prior OPE than in traditional
UW doctrine. The same tools allowed UW organisations to maintain ‘virtual persistent presence’ in between episodic physical operations in a given AO.

Likewise, the proliferation of social media transformed both sources of support and available audiences for propaganda and political warfare, while reducing the resources needed for information operations. Just in the period since 9/11, new tools emerged including the BlackBerry (whose first email-capable version appeared in 2002), Facebook (2004), YouTube (2005) and Twitter in 2006 (which between them created social media), the iPhone and Android smartphones (2007 and 2008), WhatsApp (2009), Instagram (2010), Snapchat (2011) and Telegram—the messaging app of choice for Islamic State—in 2013. Resistance actors could now plan, reconnoitre, radicalise, recruit, pass target information, collect and collate intelligence, perform battle damage assessment, synchronise supporters, conduct political and information warfare operations, mount cyberattacks (including lethal attacks on infrastructure connected to the ‘Internet of things’) and publicise their operations, all online and on the move, via handheld smart devices.

The new environment for resistance actors
The environment for modern resistance warfare is thus characterised by:

- Increasing urbanisation and littoralisation of conflict, so that an increasing proportion of resistance warfare action takes place in crowded, cluttered, highly connected urban and coastal areas where resistance actors can hide in complex human, physical and informational terrain.
- Increasing public perception of connectivity as an essential service, so that resistance actors (or their opponents) who disable or manipulate connectivity can achieve significant leverage over a population.
- US or allied air superiority, but with a limited weight of allied air power, less-than-capable local ground (partner) forces and extremely tight legal and political constraints on the use of air power.
- Pervasive electronic surveillance, so that resistance actors must expect all their communications to be intercepted, and all activities to be eventually compromised, though this is offset by traffic volumes so massive that intercepted communications may not be analysed in time for opponents to act on them.

This environment favours (and therefore encourages the replication of) resistance actors with the following characteristics:

- **Stealth**: the ability to blend into the physical, social and electronic or informational background, to disappear when threatened;
- **Dispersion**: the ability to move and fight dispersed, either without ever having to concentrate at all (leveraging connectivity and remote warfare tools) or only concentrating for specific operations before dispersing again to avoid retaliation;
- **Modularity**: the ability to operate in a distributed matrix of many small, multi-role combat groups that can perform multiple tasks simultaneously, transition among tasks quickly, survive the destruction of other groups and create self-healing (ad hoc or mesh-like) networks to regenerate as necessary;
- **Autonomy**: the ability to operate for long periods without orders or communication with other groups, thereby reducing the electronic signature of the group and improving its survivability (albeit also increasing the risk of error);
- **Infestation**: the ability to disappear into urban environments or other complex terrain, by melding with the physical fabric of built environments, moving entirely within the hollow spaces and covered routes afforded by cities;
- **Hiding in electronic plain sight**: the ability to exploit the clutter created by gigantic volumes of electronic traffic, adopting low-profile behaviour to avoid attracting analysts' attention or triggering a response, even while accepting the reality of pervasive surveillance and thus the presumption of eventual compromise;
- **Technological ‘Hugging’**: the ability to get close to protected populations or sites or to piggy-back onto systems (GPS, Google Earth, smartphones, the Internet) that opponents cannot disable without harming themselves;
- **Media manipulation**: the ability to goad, provoke or trick an adversary into inflicting disproportionate civilian casualties or property damage, and then to exploit errors or over-reactions through a media backlash;
• **Political warfare**: the ability to manipulate and mobilise supporters through mass communication, social networks, weaponised diasporas and online networks, using protest movements, industrial strike action or agents of influence to undermine an opponent's unity and legitimacy;

• **Technology hacking**: the ability to rapidly repurpose consumer systems, use civilian devices in combat settings and develop precision or collaborative-engagement systems better than those available to state opponents (using both hardware and software skills);

• **Connectivity hacking**: the ability (correlated with urban, technically-educated populations) to exploit electronic systems to access data, technical know-how and collaborative tools in order to repurpose consumer technologies or integrate military hardware into improvised systems; and

• **Reach-back/Reach-forward**: the ability to mobilise remote capabilities (diaspora populations, online knowledge, partners and networks of global or regional extent) in order to generate local effects or retaliate against an expeditionary opponent in the opponent's homeland.

### Implications for Unconventional Warfare

Obviously enough, this evolution has several implications for the traditional UW construct. The first relates to the structure of resistance movements. If multi-role cells can perform several functions simultaneously and transition rapidly among combat/support, information/kinetic and political/tactical tasks, then the notion of distinct clandestine underground, covert auxiliary and guerrilla force components plus an overt public component needs rethinking. As noted, Jeffrey Hasler (2017) addresses this issue very well in his critique of the SORO pyramid. Earlier work on netwar by John Arquilla and David Ronfeldt also supports the notion of a mesh of multi-role cells that self-synchronise and swarm to support each other across multiple functional areas (Arquilla & Ronfeldt 1996; Brose 2017).

Ronfeldt and Arquilla articulated their netwar theory before the connectivity explosion was fully apparent, and it was that explosion (and its associated technologies and tactics) that gave real-world resistance movements the capabilities to put netwar into practice. But operations in Syria, Africa and Europe by state-backed UW actors, as well as patterns of insurgency and terrorism globally, suggest that netwar is now at least as prevalent a model as the classic resistance pyramid. Notions derived from terrorist and militia movements—including leaderless resistance, remote radicalisation and ad-hoc direct action by self-motivated (but remotely mobilised) individuals—also suggest other models beyond the pyramid or netwar. Indeed, the archetypal underground, auxiliary and guerrilla labels might better be considered as functional descriptors of roles within a mesh of multi-role resistance cells, rather than organisational components. This does not imply that the traditional model is outdated; it still clearly applies in multiple theatres. It merely suggests that the traditional model should be considered as one possible type of resistance movement, and UW teams should assess its relevance during preparation.

A second implication is the need to move beyond a simple overt/clandestine dichotomy, recognising that the zone of ambiguity between overt and clandestine activity is a manoeuvre space in its own right, where resistance actors (and their sponsors) can operate in the gap between detection, attribution and response. We might call this the ‘liminal warfare’ space, from the Latin word for ‘threshold’.

Liminal Warfare is illustrated in [Figure 3](#). In the bottom (clandestine or subliminal) layer of this liminal space, the existence of resistance operations and the identity of sponsors remains undetected. The ‘detection threshold’ – defined by an adversary’s intelligence, surveillance and reconnaissance (ISR) capabilities – is reached when the size or intensity of resistance activities reaches the level at which an adversary detects the operation, but cannot identify its sponsor. The next layer up, between detection and attribution, is that of covert operations in which an adversary cannot attribute responsibility, despite detecting the existence of an activity. The ‘attribution threshold’ – again determined by ISR capabilities – is the level at which the adversary suspects (or knows, but cannot prove) the sponsor’s identity, and this is the realm of ambiguous action. The upper boundary of this layer is the ‘response threshold’ at which an adversary has enough certainty to convince policy-makers to approve a response and enough proof to ensure domestic or international legitimacy for that response. Of critical importance, unlike the two lower thresholds, the response threshold is determined not by ISR capability, but by political decision-making.

Democratic countries constrained by domestic and international opinion or high regard for international norms and the rule of law, alliances such as NATO that require consensus before initiating collective action or countries with publicly-stated response criteria (‘red lines’) have high, and very predictable, response thresholds, creating significant vulnerabilities and expanding the liminal warfare space for resistance actors. Even improvements in ISR capability, which push the attribution and detection thresholds down, only open up greater manoeuvre space for liminal warfare. Conversely, countries whose leaders act unpredictably, do
not publish red lines or respond promptly and unilaterally to threats (Israel being one obvious example) can collapse the liminal space by lowering or obfuscating response thresholds regardless of ISR capacity. In the most extreme case, political leaders who are prepared to issue bald-faced denials of blatantly obvious action by their own forces, or by irregular actors they sponsor, can create a zone of ‘implausible deniability’ whereby international pressure loses much of its impact.

The fact that the response threshold is politically-driven rather than capability-dependent emphasises the reality — recognised in UW doctrine all along — that resistance warfare is fundamentally a form of political warfare. The explosion of connectivity and social media during the last two decades has changed the methods available to resistance actors, but not their target: the legitimacy, cohesion and effectiveness of political institutions and leaders. Understanding an adversary’s political limits—in terms of response time, range and nature of likely responses and constraints on leaders—thus helps to create space for liminal manoeuvre.

Further, in an environment of pervasive surveillance and omnipresent social media, there is no such thing as a permanently clandestine operation. All operations will eventually be compromised, and sponsor identities will out. But at the same time, the very pervasiveness of social media increases opportunities for deception, enabling resistance actors to hide in plain sight, mimic others, create and exploit ‘fake news’ or manipulate their physical and electronic signatures. Further, if all operations are eventually, but not immediately compromised, there is a temporal dimension to liminal manoeuvre: Resistance actors do not need to create permanent deniability, just temporary ambiguity. Once an adversary’s response threshold and reaction time are identified, a resistance actor can calculate the time window available to achieve objectives before a response, render a response ineffective or prevent it altogether.

This temporal aspect underlines a further implication: the primacy of OPE (or Phase Zero) shaping operations. Ideally, in resistance or hybrid warfare the resistance acts an adjunct to conventional shaping (or strategic posturing) in such a way that campaign objectives are achieved before the first assault troops hit landing zones or the first tank crosses the line of departure. But if objectives are already achieved before conventional operations begin—if the purpose of combat becomes merely to consolidate gains already won by a resistance campaign coordinated with conventional shaping—then major combat operations are no longer decisive and may never occur. An enemy may be beaten before the first tank rolls, and thus the tanks may never roll at all. Likewise, if shaping plus resistance can achieve goals without conventional combat, the pyramid may never break the surface: resistance actors may remain below the threshold of combat, or engage only in very limited, small-scale acts of violence, yet still achieve their military goals.

**Into the Future**

As noted earlier, evolution is a continuous process that affects all actors in the resistance warfare ecosystem—adversary states, sponsors, domestic and international populations, resistance movements, neutral states and international institutions. Likewise, the technological, demographic and geographical trends

![Figure 3: Liminal warfare: layers between clandestine and overt action.](image-url)
noted earlier are certain to continue, but highly unlikely to be linear. Thus, there is little chance that future UW will represent a straightforward projection of current conditions. That said, in the existing environment there are already discernible indications of possible future developments.

One such development is the emergence of offset command nodes (possibly to be replaced with Artificial Intelligence [AI] in the future). Several military AI projects already exist. Resistance actors, including terrorists and insurgent groups, have already mastered the use of offset command nodes, where control of elements in the field is exercised by cells offshore, hidden in major cities or inside adversary nations themselves. The application of AI may enable resistance groups to do away with command nodes altogether, creating instead a distributed C3I system that exists in multiple locations at the cell group level, sits on nets of hijacked computers or floats within the smart city systems of modern urban areas. The possibility, in the next decade, of an AI-controlled resistance movement fighting an AI-enabled state adversary is entirely feasible.

In a less extreme version of the same scenario, the current trend towards remote UW by resistance warfare actors engaging in virtual infiltration, offshore shaping and collaborative engagement may develop to the point where kinetic resistance activities, political warfare and ordinary politics merge. The liminal manoeuvre space for newwar could thus expand to cover most of the planet, with every location potentially acting as a virtual hinterland, support base or AO for a resistance warfare campaign somewhere on the globe. SOF teams working remotely with resistance partners may look very different; physical infiltration teams would still be needed, at least some of the time, but UW operators would increasingly be cyberwarriors operating on their own or supporting physical infiltration teams.

When such teams do need to physically infiltrate a denied area, the ability to access data online and draw on technically-skilled populations with advanced manufacturing capabilities might enable a ‘naked man infiltration’ approach. In this method, individuals or teams would be infiltrated in plain sight with no military equipment, weapons or other compromising material, simply a memorised URL allowing them to download a cache of 3D printing data to manufacture weapons and devices on site. Likewise, the ability to access targeting data, intelligence, propaganda support and other enablers online might allow individuals or teams to operate in near-complete electronic blackout conditions between periodic downloads. The use of satellites, Radio Frequency Identification (RFID) tags and burst transmission might allow downloads via space systems communicating periodically with ground assets who would never need to access the Internet or pick up a radio handset.

In a related development, resistance movements in the future environment seem increasingly likely to field multi-domain capabilities (including land, air, sea, cyber and space-based systems) rather than being primarily ground forces. Resistance movements are already employing swarms of drones and small boats; CubeSats and other small-scale, low-cost satellite systems may bring space capabilities to future resistance groups, even those not sponsored by a major nation-state. This in turn would mean that SOF organisations supporting resistance movements would need a more complete range of joint capabilities to include non-standard maritime, non-standard aviation, cyber, space and other capabilities as well as advanced ground capabilities.

**Conclusion**

As noted, UW is one of the oldest, most cost-effective and historically most successful forms of warfare. In its modern form it derives from Second World War resistance movements and organisations such as OSS and SOE who sponsored them. This model was updated during the Cold War, incorporating theories of Communist revolutionary warfare, conditions behind the Iron Curtain and wars of decolonisation in Asia and Africa. By the late 1960s, this classic model had solidified into the SORO pyramid framework, the seven-stage sequence of a UW mission, the overt/clandestine dichotomy and the underground/auxiliary/guerrilla structure. Despite recent updates and critiques, this model remains extant in current doctrine.

Yet, as we have seen, the evolution of modern resistance movements—against a background of urbanisation, littoralisation, the explosion of connectivity, the return of great-power military competition, the development of precision systems and social media—has encouraged the development of resistance actors who look different, and operate differently, from the classic pyramidal model. Likewise, the ubiquity of electronic surveillance and social media has made clandestine operations impossible to sustain for any length of time, while simultaneously creating a ‘liminal warfare’ space for actors able to operate in the gap between detection, attribution and response.

Technologies for remote UW, offset command and control, repurposing of consumer systems and connectivity tools have made infiltration into denied areas an option, rather than a necessity, and opened up the possibility that SOF units could engage in a continuous process of preparation, initial contact, organisation and build-up (phases one to four of the doctrinal UW sequence) across their entire area of responsibility, with multiple potential resistance partners, from their home locations, all the time. They might never need to infiltrate a field team into denied areas, or if they did, would never have to infiltrate
‘blind’, but could always work with vetted, developed and organised groups based on thorough and deep OPE. Virtual persistent presence could be achieved through a combination of periodic visits or short-term infiltrations, combined with permanent online remote support to resisters. Teams might infiltrate to locations—say, a diaspora community in a country remote from the AO, but connected to it through electronic means—to engage in organisational development and political warfare.

In the future, the trends we can currently identify are likely to continue, but are highly unlikely to be linear. Indeed, if this analysis suggests anything, it is that we should be extremely sceptical about our ability to predict future UW. Instead, today’s techniques, doctrine and concepts should serve as tools to be critically evaluated, updated and (if necessary) discarded as we continue keeping pace with the evolution of unconventional warfare.

Competing Interests
The author has no competing interests to declare.

References
Arquilla, J., & Ronfeldt, D. (1996). The advent of netwar. Santa Monica, CA: RAND Corporation. Retrieved from https://www.rand.org/pubs/monograph_reports/MR789.html
Box, G. E. P., Hunter, J. S., & Hunter, W. G. (2005). Statistics for experimenters, (2nd edition). London, United Kingdom: John Wiley & Sons.
Brose, R. (2017). Cyber war, netwar, and the future of cyberdefence. Retrieved from https://www.dni.gov/files/documents/atf/Cyber%20War%20Netwar%20and%20the%20Future%20of%20Cyberdefense_Header.pdf
European Global Navigation Satellite System Agency. (2017). GNSS market report: Issue 5. Luxembourg: European Union Publications Office.
Hasler, J. (2017). The SORO resistance pyramid challenged: Critical observations and questions on a classic. Special Warfare, 30(3), 10–27. Retrieved from https://www.soc.mil/SWCS/SWmag/archive/SW3003/SoroResistanceChallenged.pdf
Johnson, D. (2009). Darwinian selection in asymmetric warfare: The natural advantage of insurgents and terrorists. Journal of the Washington Academy of Sciences, 95(3), 89–112. Retrieved from https://www.jstor.org/stable/24536315
Joint Chiefs of Staff Washington DC. (2016). Department of Defense dictionary of military and associated terms. Joint publication 1-02. Retrieved from https://apps.dtic.mil/dos/citations/AD1004650
Molnar, A., Tinker, J., & LeNoir, J. (1966). Human factors considerations of undergrounds in insurgencies. Department of the Army Pamphlet No. 550-104, September 1966. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a592949.pdf. DOI: https://doi.org/10.21236/AD0645518
Sagarin, R., & Taylor, T. (Eds.) (2008). Natural security: A Darwinian approach to a dangerous world. Berkeley and Los Angeles, CA: University of California Press. DOI: https://doi.org/10.1525/california/9780520253476.001.0001
Tompkins, P., Jr., & Bos, N. (Eds.), & United States Army Special Operations Command. (2013). Human factors considerations of undergrounds in insurgencies, (2nd edition). Fort Bragg, NC: United States Army Special Operations Command. Retrieved from https://www.soc.mil/ARIS/books/pdf/HumanFactors3.pdf
United States Army Special Operations Command. (2016). Unconventional warfare pocket guide. Fort Bragg, NC: United States Army Special Operations Command. Retrieved from https://www.soc.mil/ARIS/books/pdf/Unconventional%20Warfare%20Pocket%20Guide_v1%200_Final_6%20April%202016.pdf

How to cite this article: Kilcullen, D. (2019). The Evolution of Unconventional Warfare. Scandinavian Journal of Military Studies, 2(1), pp. 61–71. DOI: https://doi.org/10.31374/sjms.35
Submitted: 15 December 2018 Accepted: 10 January 2019 Published: 20 May 2019
Copyright: © 2019 The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC-BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited. See http://creativecommons.org/licenses/by/4.0/.
Scandinavian Journal of Military Studies is a peer-reviewed open access journal published by Scandinavian Military Studies.