LSE Ideas

GLOBAL STRATEGIES

Hybrid Warfare in the Middle East

February 2017

GLOBAL STRATEGIES CONNECTS ACADEMICS WITH WHITEHALL AND BEYOND.

The aim of the project is to provide sound practical advice on how strategy can be made more effective in this complex age. The focus is on international strategic issues, often military but also political, diplomatic, economic, and business issues.

To do this, the project brings together a wide range of academics from LSE with senior practitioners past and present, from the UK and overseas. Regular discussions take place with senior officials on the strategic aspects of major issues such as ISIS, Iran, Syria, Russia, Ukraine, China, Migration, and Energy.

The project's close links with Whitehall reflect the value senior officials attach to the discussions they have with us and the quality of our research. Private Global Strategies papers have contributed to the government's work on the Strategic Defence and Security Review, and policy towards Russia and Ukraine.

GLOBAL STRATEGIES

Hybrid Warfare in the Middle East

February 2017

EXECUTIVE SUMMARY

Over the past 15 years the West has struggled against various threats from the Middle East, in particular Daesh[1], Al Qaeda (AQ), the Taleban and Iran. All of these have used Hybrid Warfare (HW) techniques which the West has found hard to counter, and which have further undermined stability in the region. Despite the setbacks Daesh has suffered in recent months we can expect to face further Hybrid threats from the Middle East for decades to come. The UK needs, therefore, to develop HW and counter-HW capabilities not just for the threats it faces today but for an unknown future.

To explore these issues further Global Strategies, the strategy group within LSE IDEAS at the London School of Economics, held a number of workshops to consider:

- The techniques of HW as practised by Daesh, AQ, the Taleban, and Iran
- How the West in general and the UK in particular could get better at countering HW.

The workshops brought together former senior British officials with long experience of dealing with Counter-Terrorism, the Middle East, Afghanistan and Iran; academics and other analysts who have followed these issues over the years; and current practitioners with experience of media, strategic communications and cyber issues. We also consulted a wide range of serving British officials and military officers.[2]

This paper reflects the overall sense of the discussions, but no participant is in any way committed to its content or expression.

THE PROBLEM

Hybrid Warfare (HW) is a military strategy that blends conventional warfare, irregular warfare, cyber warfare and subversion, and blurs the formal distinction between war and peace. It is often characterised by the use of fictitious propaganda, deniable forces, espionage, the mobilisation of ethnic, linguistic or confessional minorities, and terrorism. We explored the Russian variant of this strategy in our paper Managing the West's Relations with Russia, issued in September 2015.

The West finds it equally difficult to respond to HW in the Middle East, where education, especially for science and engineering, tends to make absolute views of the world attractive. Information and propaganda campaigns using 'facts'—be they invented or wrong—appeal to emotions more than logic, and are hard for the West to rebut.

Daesh makes the most extensive use of the internet and social media for radicalisation, recruitment and propaganda. Iran, which has a well-developed cyber capability, has mounted destructive attacks causing physical damage in the real world. To date Daesh, AQ and the Taleban have not, though they have mounted Distributed Denial Of Service (DDOS) attacks to take down temporarily websites they oppose. Whilst Daesh, AQ and the Taleban have used extreme violence as political messaging, neither they nor Iran have used Biological or Chemical weapons against the West.

Traditional deterrence, based on the threat of retaliation, is not suited for use against non-state groups as they have little to strike back at. There is, however, scope to push back by undermining their support and restricting their actions — including their propaganda, military, terrorist and financial operations.

THE RESPONSE

A key element in undermining support is through strategic communications in the Middle East. Whilst the UK cannot use 'dirty' techniques and tell outright lies like its opponents, it needs to both counter their propaganda and project a positive message, and do this 24/7 and at pace. Restricting access to extremist material on the web can be done at least in part by asking internet service providers to enforce their own terms and conditions.

Greater engagement with non-state groups in the region has risks, but regional partnerships can reduce the need for direct Western military involvement. The UK government should see non-state groups in the Middle East more as partners.

How the West uses violence sends a message: it needs to conform to Western values as well as to Western laws. Targeting the technical experts behind their cyber/social media campaigns and military operations can bring long-term benefits. Targeting the leaderships of terrorist groups has short-term impact, but may make political solutions less possible.

While the UK's criminal justice approach to terrorism demonstrates UK values, it is difficult and resource intensive. Legislation on how UK officials work against terrorism overseas needs clarification and improvement.

There is much to be gained from cooperation with the private sector, but, in the absence of an existential threat to the UK, government needs to tread cautiously. The financial sector, partly under regulatory compulsion, does on the whole cooperate well with government against terrorism and organised crime, and in support of sanctions. The tech sector is less inclined to cooperate, perhaps less influenced by the reputational considerations of financial institutions. Nevertheless, in case of National Emergency government would need to coordinate with the private sector: the planning for this should be done in advance.

For the UK to be able to counter Hybrid Warfare more effectively, ministers, officials and military officers need a shared understanding of the issues, with their reflexes developed through joint training and exercising; and the legal boundaries need to be clearly defined in advance.

RECOMMENDATIONS

The discussions generated a range of ideas on ways to enhance the co-ordination and effectiveness of HMG's policy towards Middle Eastern Hybrid Warfare. While most of these ideas will not be new to government, and some may be in hand, as ever with policy the difficulties lie not in having the ideas but in agreeing, prioritising, resourcing, and executing them. We hope that this paper will inform and stimulate a wider policy debate about what concrete steps could be taken to upgrade in UK capabilities.

1. The UK response to HW threats from the Middle East should be led at a high level and coordinate all UK government-funded effort.

2. The UK should set up multi-disciplinary teams, led at Deputy Director or Director level (1* or 2* military equivalent), to run designated HW or counter-HW campaigns, reporting via the National Security Adviser to the NSC. These teams would have control of resources and tasking, working within clear guidelines to NSC strategic direction.

3. HW and counter-HW should be taught not only on military staff courses, but to civilian officials in relevant ministries, principally FCO, MOD, Home Office, DFID and the security and intelligence agencies.

4. HMG should institute a regular cycle of HW and counter-HW exercises for senior policy-makers in order to develop doctrine and experience.

5. Strategic communication and counter-propaganda are key elements in the implementation of UK policy. They should be led at a high level, coordinate all UK-government funded effort, be coordinated with allies, and partner where possible with regional allies. Information campaigns need to be aware of what opponents and allies, including BBC language services, are saying.

6. UK should consider working with and supporting a wider range of state and non-state allies. Support could include political and media advice as well as military training and advice.

7. HMG should consider legislation on Counter-Terrorism cooperation with foreign governments, including extradition to UK.

8. UK should commit to long-term criminal justice capacity-building programmes in countries at risk of terrorism which require this.

9. As part of counter-HW planning, HMG should consult relevant non-governmental organisations and consider which, if any, non-governmental capabilities might be mobilised and under what circumstances.

INTRODUCTION

Russian use of so-called ‘Hybrid Warfare’ in its near abroad (Ukraine, Georgia, the Baltic states) has proved difficult for the West to respond to effectively. But Russia is not unique in seeking novel ways to achieve its objectives. Across the Middle East and South Asia states and non-state groups are using techniques – some new, some old, some just their societal reaction to the West – which put strategic pressure on the West in ways which the West finds hard to counter. Daesh, Al Qaeda, the Taleban, and Iran seem able to set the agenda and ‘win’ against the West and its allies despite their extreme relative economic and military weakness. While they may not pose an existential threat to the UK, they do pose an existential threat to UK allies in the Middle East which the UK currently seems unable effectively to counter. The West is reduced to using kinetic military force which may be ineffective or counter-productive.

Daesh, Al Qaeda (AQ), the Taleban and Iran are different from each other in ideology, organisation, and strategy; to analyse each of them separately would have been too broad an approach. Although Daesh emerged from Al Qaeda in Iraq (AQ-I), and has ideological similarities to AQ, its strategy is to seize and hold territory to declare as a Caliphate; whereas AQ’s strategy was to attack the US and the West to try to provoke over-reaction. Meanwhile the Taleban are essentially an old-fashioned ethnic insurgency movement, with Islamist overtones, and Iran is a fully formed state, albeit with Islamic revolutionary credentials, and is Shia; Daesh, AQ and the Taleban are Sunni. They are operating against a background of Middle Eastern governments which are perceived by many as ineffective, and where the so-called ‘Arab Spring’ replaced long-standing autocrats with less stable successor regimes.

So while taking note of which of these entities use which methods, the focus was on Hybrid Warfare methods themselves, and how the West in general and the UK in particular might counter them, rather than broader recommendations on policy towards the entities themselves.

- **Section 1** – The problem: Characteristics of Hybrid Warfare as practised by Daesh, Al Qaeda (AQ), the Taleban and Iran

- **Section 2** – Policy options for the UK and the West

SECTION 1

THE PROBLEM: CHARACTERISTICS OF HYBRID WARFARE AS PRACTISED BY DAESH, AL QAEDA (AQ), THE TALEBAN AND IRAN

WHAT IS HYBRID WARFARE?

> "Every age has its own kind of war, its own limiting conditions, and its own peculiar preconceptions."
>
> Clausewitz

The term 'Hybrid Warfare' emerged in a 2005 article[3] to describe the combining of regular, irregular and novel threats, such as cyber attack, and the use of non-state groups, and was subsequently used to describe the tactics Hizballah used against Israel during the 2006 Lebanon war, although the concept of combining regular and irregular warfare with subversion is as old as warfare itself.
In 2007 Frank Hoffman wrote that

> "Hybrid Wars can be conducted by both states and a variety of non-state actors. Hybrid Wars incorporate a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder."[4]

In 2011 US Joint Forces Command defined a hybrid threat as

> "any adversary that simultaneously and adaptively employs a tailored mix of conventional, irregular, terrorism and criminal means or activities in the operational battle space. Rather than a single entity, a hybrid threat or challenger may be a combination of state and non-state actors."

Subsequently cyber has been added: the Wikipedia definition is

> "Hybrid Warfare is a military strategy that blends conventional warfare, irregular warfare, cyber warfare and subversion."[5]

In addition, Hybrid Warfare is often characterised by the use of deniable forces, espionage, the use of ethnic minorities, and terrorism. In the case of a state such as Russia, there is a conventional and nuclear military threat in the background. Hybrid Warfare is not an ideology but a toolkit of methods. Entities conducting Hybrid Warfare choose from the toolkit according to their circumstances and strategy.

Other terms referring to essentially the same methods are Ambiguous, Asymmetric, Greyspace, New Generation, and Full Spectrum Warfare. The UK Government has recently adopted the term 'Full Spectrum Effects' to refer to measures it might deploy to achieve political goals, which if used by its opponents would be termed Hybrid Warfare. This can be seen as a logical progression from the UK military's 'Comprehensive Approach' doctrine (now known as the 'Integrated Approach') applied to stabilisation operations and counter-insurgency in Afghanistan and Iraq. The Comprehensive or Integrated Approach requires integration of military and civilian efforts into a common campaign plan, so that these efforts are mutually reinforcing.

It is worth noting that the Russian drive to develop its Hybrid Warfare capabilities initially arose because of Russian perception, and continued belief, that revolutions and unrest in countries of the former Soviet Union, such as the Orange Revolution in Ukraine, were the result of organised Western plots. These 'colour revolutions' were characterised by civil resistance, student activism, a strong role for international NGOs, and supportive Western media coverage. Russian securocrats, in a classic example of analytical 'mirroring' – that is, assuming that another government system works as your own would – assess that these elements of opposition must have been stimulated and organised by the hidden hand of the West. Western policymakers may have helped create the conditions for international NGOs, think tanks, advocacy organisations and the media to support pro-democracy movements, but know how impossible – and politically risky – it would be to organise a revolution and keep their role secret.

Hybrid Warfare campaigns tend to be long term, reflecting that we are living in a period of persistent competition, confrontation and sometimes conflict: the classical distinction between war and peace is less useful now.

INFORMATION AND PROPAGANDA

Daesh, Al Qaeda (AQ), the Taleban and Iran all have in common the use of propaganda to spread an integrated narrative. All make use of 'facts' which are made up or wrong – there is no acceptance of a western concept of objective truth, either as the basis for a rules-based system of international relations, nor as useful for the audiences which they address. They also interpret genuine facts in ways which support their narrative; the prevalence of conspiracy theories (e.g. that the US and Israel founded Daesh) shows that their interpretations are often more believable that the West's, and illustrates the difficulties of producing a compelling Western counter-narrative.

However, facts are not the most important elements of their narratives – the appeal is largely emotional. Such a communication strategy is not unique; many Western political campaigns are explicitly based more on emotion than fact. But it is normally difficult for Western governments to appeal emotionally to people in the Middle East.

Sympathisers and supporters of Daesh, Al Qaeda (AQ), the Taleban and Iran make use of 'lawfare', i.e. the use of domestic or international law, especially human rights law, with the intention of damaging an opponent, winning a public relations victory, financially crippling an opponent, or tying up the opponent's time, so accomplishing purposes other than, or contrary to, those for which the laws were originally enacted (based on Wikipedia definitions[6]). UK law firms specialising in human rights law which have mounted a series of challenges to the conduct of military operations in Iraq and Afghanistan have been accused of lawfare, in that their motivation appears to some to be as much political as driven by the individual interests of their clients[7].

A key element of all narratives is success and the inevitability of victory. When the facts go against this the narrative becomes less effective, e.g. Boko Haram shifting allegiance from AQ after the death of Osama Bin Ladin to Daesh, which was by then a stronger, more successful, brand.

Daesh have the most developed propaganda messaging, and the most developed use of social media. They are more sophisticated in terms of quality and quantity, up to the standards of Western media organisations. They integrate their use of propaganda with military or terrorist attacks, mounting such attacks to distract or seize the headlines after a setback. Daesh take a segmented and targeted approach to specific audiences just as Western media organisations do – they are 'customer-focused'. They have a strong religious appeal despite not having recruited many serious Islamic scholars.

Daesh themes include:

- The West vs. the Islamic world
- Western democracies are hypocritical, degenerate, oppress the weak, and support undemocratic regimes in the region
- Democracy does not deliver moral outcomes
- Daesh allow you to live a righteous family life in the Caliphate
- Their version of Islam is right, everyone else is wrong. The *takfiri* approach, i.e. to accuse your opponents of unbelief or heresy, justifies killing anyone who disagrees with their version of Islam.
- Joining the Caliphate is a romantic, heroic adventure.

ADMINISTRATION

Although Hybrid Warfare practitioners may operate in what appears to be a decentralised way, there is generally an organisational framework behind them, though with different models. At one end of the spectrum Iran is obviously an established state and performs all the functions of a state. In Lebanon Hezbollah, supported by Iran, provide social services, and run cultural and educational programmes parallel to the state, but at the same time are pursuing a policy of entryism into the Lebanese government. Hizbollah teach this approach to allied Shia militia groups within the Popular Mobilisation Forces in Iraq. In Afghanistan the Taleban set up courts and have shadow governors for every province in the country. They offer a prospect of administrative stability and justice as part of their narrative (and ran Afghanistan as an Islamic Emirate when they were in power 1996-2001). Daesh makes claims to statehood and promotes the possibility of living well, both materially and morally, within the Caliphate.

Both Daesh and the Taleban rely on taxation as a source of revenue and as emblematic of statehood. It is a source of control, by creating debt. Increasingly taxation (and payments more generally) will be done by mobile phone app.

The outlier is Al Qaeda, which has historically sought a host state (Sudan, Afghanistan) and has not tried to set up parallel structures or its own state. AQ is not particularly strong at Hybrid Warfare, in contrast to their ideological partners Daesh. This may reflect generational differences in leadership and experience, but may also indicate that to be an effective Hybrid Warfare practitioner requires more organisation and stability than old-fashioned violent terrorism.

EDUCATION

Education in the Middle East has more rote learning than modern Western practice. It tends not to reward challenging or enquiring, questioning students. There may be the risk therefore that it generates expectations of certainty – that there is a 'right answer' to every issue – and that this makes absolute views of the world more attractive. This is particularly the case for science students[8]. Recent research[9] suggests that engineering graduates are disproportionately more likely to become terrorists than are social science graduates. The West does try to drive education reform in the Middle East (and elsewhere in the world) but this runs the risk of being seen by many in the region, correctly, as an attempt to spread Western values.

USE OF THE INTERNET AND CYBER

The internet (both open and the dark web) is obviously a key enabler for Hybrid Warfare. In particular, the internet enables any group, however small or otherwise weak, to project threat internationally. This empowers individuals and minorities in novel ways. The Taleban and AQ make less use of cyber and the internet generally than Daesh or Iran. One reason for this may be that their leadership is emotionally tied to the theatrics, violence and heroism (in their terms) of conventional terrorist attacks. In the case of the Taleban, it may also reflect low levels of literacy and education, and limited access to the internet in Afghanistan[10]. The Taleban media effort is therefore outward facing, aiming to promote wider support, funding and recruitment. For AQ, it may be a reflection of the age of their leadership, and of the vulnerability of their international network to Sigint monitoring, which has largely marked the AQ leadership out of the game. By the end of his life Osama bin Laden had insulated himself entirely from electronic contact with the internet, and because AQ do not have a secure territory from which to operate they are not as active in the cyber sphere as Daesh.

Daesh make particular use of social media, not just for propaganda but for radicalisation and recruitment, grooming potential recruits from anywhere in the world. Targets often self-select by connecting with wider Daesh propaganda, so that Daesh does not have to be pushy. Once contact is made Daesh establish one-to-one connections, creating a dialogue designed to make the individual feel special. Young people who are alienated from social institutions and citizenship are particularly susceptible to this messaging and grooming, apparently joining the Caliphate as their means of rebellion. Why this is the case will require further study. The speed at which whims can be actualised is a factor. It is not uncommon for individuals to buy a plane ticket and travel to Syria within a week of first making contact with Daesh online. Daesh's online operations do not require sophisticated technology, just motivated individuals skilled in building and instrumentalising online relationships.

Daesh also run an information campaign aimed at the fighting forces of the Caliphate in order to retain and motivate the membership.

Using cyber/digital means to cause damage requires far more training and expense than using it for propaganda, radicalisation and recruitment. Iran uses cyber to attack and to produce effects, e.g. the Shamoon attack on Saudi Aramco computer infrastructure in 2012, which brought down 30,000 computers, and occasional Distributed Denial Of Service (DDOS) attacks, for example on the BBC and some US financial institutions, also in 2012.

Daesh, AQ and the Taleban have used DDOS to attack or vandalise websites they oppose, but do not appear to use cyber means to try to cause physical damage in the real world. To develop and mount physically destructive cyber attacks requires territory as a safe haven. Without this, local or Western intelligence and security services can monitor and close down attacks. And, contrary to alarmist opinion, developing cyber attack tools that will cause serious physical damage is expensive and highly skilled work that is probably beyond Daesh, AQ and the Taleban – though not beyond Iran. However, so long as Daesh control territory, and have cyber-capable people living within the Caliphate, there must be the possibility that they try to develop destructive cyber-attack capability.

Besides the costs and technical difficulty, Daesh, AQ and the Taleban may not have taken up cyber warfare because it doesn't fit their aims or narrative. They may judge that 'cyber terrorism' is not effective as terrorism, since cyber attacks cannot produce the kinetic damage and threats to human life that IEDs and guns can. The narratives of Daesh, AQ and the Taleban are centred on violence – 'cyber' is perhaps not violent enough for them. Cyber attacks are also expensive and have long lead times. More traditional terrorist techniques – e.g. decapitation – are cheap, require less skill, are easily videoed and publicised, and are genuinely frightening. Cyber attacks are expensive to counter, so in a broad Hybrid Warfare strategy you may want your opponents to believe you are pursuing a cyber attack capability even if you are not.

PROXIES

In conventional western analysis we often categorise hostile non-state groups as proxies of states or as subordinate branches or affiliates of other non-state groups, e.g. Iran's relationship with Hezbollah, with Popular Mobilisation Forces (PMF) in Iraq, or with the Houthi in Yemen; Daesh's relationship with Boko Haram (where they now manage BH's digital campaigning); AQ's with Al Qaeda in the Islamic Maghreb (AQ-IM); and so on. There is considerable variety in these relationships. Some proxies/affiliates are funded or given material support by their sponsor, to a greater or lesser extent, while some share only a loose ideological relationship with their sponsor. There is also great variation in the extent of direction that sponsors have over their proxies/affiliates, which is not directly related to the level of support they provide.

We are uncomfortable describing non-state groups the West supports (morally or materially) as proxies, e.g. the Kurds in Northern Iraq, or NGOs in Iran, Afghanistan, Pakistan, because 'proxy' implies subordination. We are more inclined to see such groups as allies (albeit loose ones) or partners, i.e. organisations which share some of the West's aims and/or values, although in general the West has less shared identity with them than Iran/Daesh/AQ/Taleban have with their proxies/affiliates. Further, in many of these relationships it is not clear whom the relationship benefits most – the sponsor or the proxy/affiliate.

It would be clearer – and avoid double standards – to consider all these relationships as loose alliances or partnerships rather than as sponsor/proxy relationships between a dominant party and a subordinate. This re-definition is uncomfortable for our preferred Westphalian principles of international relations in that it does not differentiate between state and non-state actors. However, it should be a more useful way of looking at how the politics of the Middle East and South Asia work, certainly from the viewpoint of regional actors.

PHYSICAL VIOLENCE

Daesh have used extreme violence as political messaging, which they amplified by broadcasting, e.g. through beheading videos, in a more extreme way than even AQ. Daesh seem particularly good at linking violence ('terrorism') to their broader propaganda effort, although this has decreased dramatically, possibly because Daesh assessed this sort of messaging as counter-productive. Unlike Russia's use of violence, which seems generally to be part of a central plan, when Daesh use violence it may not be centrally planned, for example the bombing of the Russian tourist flight from Sharm el-Sheikh was carried out by Daesh in Sinai, not coordinated centrally. For Russia, Hybrid Warfare is a set of carefully formulated tactics, to create a conflict that can be escalated at will (e.g. in Ukraine), whilst for Daesh it is more their instinctive method of waging war.

In attacks in the West, Daesh and AQ have inspired the use of particular kinds of violence – beheadings, IEDs and marauding gun attacks – but so far not Biological or Chemical Weapons (BW/CW), nor targeted assassinations against political leaders. The consensus of workshop participants was that security measures are generally already in place to protect likely assassination targets in the West, which make them unattractive targets for the relatively unsophisticated capabilities Daesh have in the West. It is mass casualty attacks that would change the everyday life of ordinary westerners, and which are easier to plan and execute, so this is what Daesh focus on.

BW and CW are in principle available to Iran, the Taleban, AQ and Daesh, but they have not used them, possibly because there are religious objections, particularly to BW – authoritative religious dispensation would be required. Another possibility is fear of retaliation or escalation, though this would be more of a consideration for states and non-state groups which control territory. Given that Western media reaction is a key driver for the use of violence by AQ and Daesh, and that conventional violence and beheadings are less and less newsworthy, it is surprising that neither group has yet mounted a BW or CW attack in the West. Such an attack would seize headlines and dominate policy.

Daesh, AQ and the Taleban have an asymmetric advantage over the West in their use of violence in terms of their ferocity, readiness to kill innocents, and tolerance of casualties. It is hard to see the West matching this unless it felt existentially threatened.

IS DETERRENCE POSSIBLE FOR HYBRID WARFARE?

States generally assess their policies in cost/benefit rather than ideological terms. They have targetable assets they do not want to put at risk, and however aggressive they may be, generally accepting the status quo is better than losing a confrontation. So deterrence can work against states.

Non-state actors such as terrorist groups generally do not have targetable assets, and for a non-state actor to tolerate the status quo would be to accept defeat. Highly ideological groups do not change their beliefs in response to physical pressure. Furthermore, the terrorist aim is generally to provoke the state into overreaction, so terrorist groups often welcome attacks by states as this strengthens their support. So deterrence against non-state groups is difficult. Another factor is that deterrence implies mutual recognition. States are generally reluctant to recognise their terrorist opponents, for fear that this will to some extent legitimise them, and so states may be reluctant explicitly to use deterrence in campaigns against terrorist groups (although they could perhaps deter whilst seeking to destroy).

An exception might be non-state groups with clear state backers, where the state backer could be deterred into constraining its proxy group. E.g. deterrence against Iran might serve to constrain Iranian-backed Shia militia groups in Iraq. The more a non-state group tries to operate like a state and hold territory, as Daesh is doing, the more vulnerable they become to deterrence. Air strikes on Daesh fighters clearly disrupt them and may also deter.

Deterrence includes more than the threat of response to aggression, such as the nuclear deterrence of the Cold War. Measures which have deterrent effect are also forms of deterrence if they alter the cost-benefit analysis of opponents. For example, hardening targets to make them more difficult to attack is a form of deterrence. Similarly, in addition to disruption operations, the intense global intelligence collection effort against AQ made it so difficult for them to communicate without being caught that it significantly reduced their effectiveness.

A key part of deterrence of HW is the ability to identify it is happening and call it out, in order to reduce ambiguity and counter 'plausible deniability'. There then needs to be the will and the capability to push back in areas that will hurt the opponent. ■

SECTION 2

POLICY OPTIONS FOR THE UK AND THE WEST

WHAT CAPABILITIES SHOULD THE UK TRY TO DEVELOP? WHAT COMMAND AND CONTROL (C2) ARRANGEMENTS COULD/SHOULD THE WEST/UK ADOPT TO CONDUCT EFFECTIVE HYBRID WARFARE AND COUNTER-HYBRID WARFARE?

The UK's military, intelligence, security, technical, economic and political capabilities are all stronger than those of Daesh, AQ, Iran or the Taleban. But somehow the UK finds it difficult to counter the Hybrid campaigns these groups are running. Whilst there are some specific capabilities that should be improved (e.g. counter-propaganda), more important is how the executive arms of government involved are organised, and what self-imposed legal and political constraints they work under.

Following the 2015 Strategic Defence and Security Review (SDSR) there is broad agreement that full spectrum, integrated approaches to National Security issues are required. But this has always proved difficult to deliver in the past, and there is no reason to think that it will not be at least as difficult in the future. There are regular calls for 'stronger leadership', but it is unclear whether this 'stronger leadership' is required from officials and senior military officers at Director/Director-General level (2*/3* if military officers), or from politicians. This is a reflection that the systems, structures and processes currently in place cannot deliver the integrated approach. If these were right, leadership would merely complement them.

There are several structural blockers. Firstly, departments work to their own ministers/secretaries of state, with their own budgets, their own knowledge assets, their own cultures, and their own policy officials. There are few incentives to work collectively, so departments' default position is to develop a departmental plan and work in a departmental silo. Secondly, the nature of any bureaucratic organisation is to resist reduction in its power or resources – and the same applies for most ministers. Coordination tends therefore to be by persuasion and consensus. This is time-consuming, and can be too slow when it comes to running a dynamic campaign. Departmental caution and instinctive need to argue for their policy ideas often leads not only to delay but to inaction. Our opponents get inside our OODA[11] loop to seize and hold the initiative.

When new bodies are formed, often in a hurry in response to a crisis, it is important to define their mission correctly. For example, the decision to set up a counter-Daesh taskforce instead of a 'stability of Syria' taskforce had immediate implications for UK policy.

The problem is how to achieve better executive leadership between and across departments once the strategy and overall objectives have been set at the political level. Giving control of (or at least, significant influence over) budgets and expertise/knowledge to a single campaign coordinator might give them enough leverage to run a Hybrid Warfare campaign (or an anti-HW campaign).

There is a view that changes in Whitehall culture have made inter-departmental coordination more difficult. Officials' departmental identity has strengthened as their Civil Service identity has declined. Some argued that the abolition of the National School of Government (Sunningdale) had been a factor in this.

There is also a view that the UK has become worse at delivering coordinated or integrated plans because the problems the UK is facing have become much more complex, because the UK is almost always working within a coalition, and because UK is held to higher standards than in the past. The world has become more inter-connected, and the technological and military options for the UK's enemies have become broader (e.g. cyber, CW, 'dirty bombs', suicide bombers).

Whitehall also has a structural problem with knowledge management. There is an abundance of information, but there is a need to harness what is known, retain people with deep knowledge, and engage further with academia.

The UK is not currently agile and adaptive enough to be effective at Hybrid Warfare or Counter-HW. Hybrid Warfare itself is not complicated, but UK organisations and processes are complicated, which makes it complicated and slow for them to counter HW. The Full Spectrum Effects (FSE) initiative is trying to address this problem, but has not yet delivered. UK needs greater agility; current interdepartmental structures are too slow. Small teams are needed, working within clearly defined parameters, but disconnected from day-to-day departmental business, and in small enough numbers to avoid bureaucratic friction. Opponent HW practitioners are effective because they have clear and simple goals, and do not appear to need much coordination. UK needs to find a way to mirror this.

Key questions are who will command and control UK Hybrid Warfare operations, and how; and to distinguish between the strategic and tactical levels of command. The strategic level, i.e. designing HW and counter-HW strategy, is a long-term, conventional policy issue for Whitehall. The tactical level, i.e. running HW and Counter-HW campaigns and operations on a daily basis, is a task that needs to be delegated to a defined and med body.

The UK has been remarkably effective at domestic Counter-Terrorism (CT) since 2005. A significant factor in this has been that the policy lead has rested clearly with the Home Office, and, within the Home Office, with OSCT. By contrast, no one department has the clear policy lead for countering Hybrid Warfare threats, at home or overseas, nor for running FSE campaigns.

For example, in the case of the current campaign against Daesh, there is no lead department and no lead cabinet minister, perhaps reflecting an underlying lack of enthusiasm for the task. There is, however, a great deal of coordination: there are around 25 different regular inter-departmental meetings which deal with some aspect of the campaign. But there is little sense that the UK is running an effective campaign. There was an attempt during the Afghanistan campaign to achieve unity of command, when John Reid, then Secretary of State for Defence, was appointed to lead the campaign. This was not regarded as a success.

Although the Home Office is a key driver for policies to reduce the UK domestic security threat, it is not set up to deliver effect and operations overseas. The obvious potential lead departments for HW are the Cabinet Office, FCO or MOD.

Cabinet Office is staffed and configured to develop policy, but not to deliver detailed programmes or campaigns. The National Security Council (NSC) is the body which would naturally oversee HW and counter-HW campaigns, but its role is to bring departments together, not to do their work for them.

Within the MOD, 77 Brigade is aiming to develop a range of FSE capability, and to promote understanding of this with senior military commanders and ministers, but will not have the expertise or authority to 'command' the many different ministries involved in HW. For serving military officers to 'command' a range of almost entirely civilian capabilities, of which they had little or no direct experience, would be unprecedented, and the MOD do not want this. It may be that civilian MOD officials take the lead.

The FCO has a wide range of functions, but is not culturally attuned to thinking in terms of effect or being an executive delivery organisation. Overseas, embassies and ambassadors could be focal points for coordination of FSE, just as they are for much programme work. But in a crisis this depends heavily on the quality, training, experience and capacity of ambassadors and their immediate staffs. If this option were adopted there would need to be heavy investment in posts and heads of mission, not least to free them from administrative burdens. And it would be undermined if departments in London tried to interfere with decisions made in theatre.

The Security Service (MI5) is the key focus for work against terrorist and covert threats to the UK. The Security Service and the other security and intelligence agencies are likely to be essential partners in any HW or counter-HW campaigns, but are not configured to coordinate and deliver those campaigns, not least because the existence of the campaigns should be public and subject to conventional parliamentary scrutiny.

An option would be to accept US leadership and integrate more fully with US efforts, as the UK latterly did in the campaigns in Iraq and Afghanistan, so avoiding the duplication and lack of coherence that characterised early UK efforts in Afghanistan. However, the US tends to focus more on military responses than the UK does, has more inter-departmental friction than the UK, and works in a different legal framework to differing political objectives. UK has distinct non-military capabilities for HW that can only be fully developed and utilised under UK leadership. UK is better at mounting an integrated campaign when the UK is operating alone and the campaign is not widely publicised. But if the political willpower to run the campaign is lacking then it will not succeed. Evidently the UK does not yet feel the threat of HW strongly enough to mobilise as a Government and as a nation against it. Even if it did mobilise more resources, it is not clear that government would create the operational permissions and command structure necessary to prosecute an effective HW or counter-HW campaign. The nature of HW is that the threat tends to be persistent and make incremental progress, without the clear decision points of explicit, conventional warfare. There is thus the risk that the HW threat is not given the necessary focus from government early enough.

RECOMMENDATIONS

1. The UK response to threats from the Middle East should be led at a high level and coordinate all UK government-funded effort.

2. The UK should set up multi-disciplinary teams, led at Deputy Director or Director level (1* or 2* military equivalent), to run designated HW or counter-HW campaigns, reporting via the National Security Adviser to the NSC. These teams would have control of resources and tasking, working within clear guidelines to NSC strategic direction.

HOW SHOULD THE WEST TRAIN AND PREPARE FOR HYBRID WARFARE? WHAT WOULD BE THE MAIN POLITICAL AND LEGAL ISSUES?

Ministers, officials and military officers must contribute to HW on the basis of shared understanding and common expertise. This requires common education and training, supported by joint exercising. The UK military has been thinking about Hybrid Warfare and how UK should respond for some time, and training to play its role in this response. This level of effort is not matched across the other government departments which could also play a role. The military can be over-trained, and come to HW with a lot of capability but limited authority; the civilian side tends to be under-trained and approach HW with authority but limited capability.

A first step would be a cross-government view of UK vulnerabilities. Thereafter UK needs to develop doctrine (i.e. training and teaching) and Standard Operating Procedures (SOPs) so that departments can react semi-automatically to Hybrid Warfare threats. For example, led by MoD the UK reacts in pre-planned and pre-practised ways to incursions by long range Russian aircraft; and the Police and Security Services similarly follow SOPs in reacting to terrorist incidents and threats. Such SOPs for Hybrid Warfare situations like cyber-attack do not yet exist. Nor is there an obvious lead department. The Full Spectrum Effects initiative needs to include a Training Needs Analysis and to develop doctrine, which will develop further through running exercises and training courses. An option would be to outsource aspects of this to think-tanks and contractors. HW is now on the syllabus of the Diplomatic Academy. HW and counter-HW techniques will not be stable but will be constantly changing.

There is currently a lack of clarity over the legal position of HW and counter-HW work. Civil servants tend to think there are more barriers than there probably are. Fear of personal liability limits willingness to take decisions and causes risk-averse policy decisions Reporting to ministers, and to bigger allies (i.e. the US) also has this effect. An alternative would be to first institutionalise innovative thinking and develop HW and counter-HW capability, and apply the constraint of legality at a later stage, when the context is clear. An activity which would not be proportionate and necessary against a minor threat, and so would be illegal, might be legal against a more major threat. UK should not self-censor in developing national capabilities to counter Hybrid Warfare. If the UK were to face more serious HW threats than today then the legal boundaries of what would be 'necessary and proportionate' would expand.

Legal measures could both constrain or enhance UK responses to Hybrid Warfare. Whilst UK's likely opponents won't be constrained by the laws that constrain the UK, the fact that UK is constrained by law can function in UK's favour as a form of soft power.

RECOMMENDATIONS

3. HW and counter-HW should be taught not only on military staff courses, but to civilian officials in relevant ministries, principally FCO, MOD, Home Office, DFID and the security and intelligence agencies.

4. HMG should institute a regular cycle of HW and counter-HW exercises for senior policy-makers in order to develop doctrine and experience.

STRATEGIC COMMUNICATIONS, CYBER AND COUNTER-PROPAGANDA

Whilst much effort is being put into countering the messaging and propaganda of hostile groups, workshop participants agreed that the West is not winning this struggle. This may be because the effort is not yet big enough, or prioritised enough relative to military and security policies, or because the West has not fully developed the expertise required.

Any strategic communications effort needs to have a common core narrative or message, but differentiate how and in what form it is communicated to a range of different audiences, both domestic and international. Messaging to the Middle East will be different to messaging to the UK, and messaging to the leadership in Tehran will be different to messaging to the population of Raqqa: language and culture vary across the Middle East. The means of delivery may also be different (radio, social media, etc). Repetition with variation is an important feature of an effective communications strategy: the more often the same basic thing is said to the greatest variety of people then the more likely it will become the eventual 'received truth'. There should be clarity about the aims: about overall strategy for the Middle East, and the role of communications within that. During the Cold War, Western information campaigning had a clear aim – to distinguish Soviet propaganda from reality. The West needs a similarly clear aim for any communications effort in the Middle East. International messaging could focus on defeating insurgency, persuading Muslim states and their populations to ally with the West against jihadism, the global ideological battle, or counter terrorism: but it cannot do all at the same time.

Domestically, should effort be directed at preventing people joining Daesh, or more broadly at putting across a positive Western alternative, or both? Nothing in terms of tactical communications should contradict or undermine the broader Western democratic ideological narrative.

The UK has a large and influential global media presence. However, for obvious political and legal reasons, this is independent of government. The BBC Arabic radio service is influential. However, anecdotally the quality is variable, and the language used about terrorism is neutral. It is often seen in the Middle East as under HMG control (not least because it was and will be funded by HMG), although paradoxically HMG policy departments know little about what it broadcasts – BBC Monitoring covers foreign broadcasts, not the BBC language services. To run a dynamic, adaptive communications campaign in real time officials need to be aware of the content of UK and allies' communications and actions as well as those of their enemies. London is a major centre for foreign media organisations. To what extent should the UK Government act against bad or hostile behaviour by these organisations? Should reporting of foreign funding for UK-based media be made mandatory?

The UK's strategic communications effort is both constrained and supported through working within the US-led coalition against Daesh, and within the EU.

Whilst the Iranians and Russians will use 'dirty' techniques (e.g. telling outright lies, trolling), the West is limited by its cultural values and rules. We cannot tell a story we do not believe.

During the Cold War, Information Research Department (IRD) in the Foreign Office employed many Eastern European émigrés to counter Soviet propaganda, primarily by highlighting uncomfortable facts. It was controversial, and was closed in 1977. Given the scale of the information effort against the West, the UK needs a similar sized effort now, though it would need to operate more transparently than IRD did. The Research, Information and Communications Unit (RICU) within the Office of Security and Counter-Terrorism (OSCT) at the Home Office, fulfils some of the same functions today in the CT arena, and has made great strides over the past few years. But just as IRD was criticised for its clandestinity, so RICU has been criticised in the press for failing openly to acknowledge its sponsorship of strategic communications content.

The UK government regional Arabic spokesman plays a key role in communicating UK policy to the people of the Middle East.

Messaging by religious and state authorities within the Middle East is influential. In principle, UK could try to find ways to work with and influence these bodies, emphasising respect for Islam as one of the world's great religions and its shared values with other faiths. However, past experience of trying to work with authentic voices in the Middle East to put the counter-narrative has been relatively unsuccessful.

There are two main avenues for counter-propaganda work: to seek **technical solutions,** or to engage with and try to **counter the content**. Any counter-propaganda strategy will probably be a combination of the two.

The aim of technical solutions is to take down or limit access to propaganda outlets (such as websites which host extreme jihadi material or bombmaking instructions) through the use of legal and political measures, or by cyber counter-attack. Internet norms are still developing. Legal regulation of the internet is limited, and internet pioneer culture has been ultra free speech. However the terms and conditions of most internet service providers (ISPs) forbid violent extreme content, and ISPs will take action against such material if alerted to it, whether by government or by user pressure through 'report content' buttons. Cyber counter-attack would be a demonstration of power, but whilst Anonymous and other non-state groups can mount cyber attacks on their opponents in cyber-space, Western governments face legal and policy problems in doing so, for example free speech issues in the USA (first amendment rights). The UK is less legally restricted than the US in this respect, but law and policy on the use of cyber attack is not yet clarified.

Engaging with the content, for example by having anti-Daesh/AQ Arabic speakers contributing to extremist forums, is also difficult to do. It might be worth working jointly with regional allies to deliver this: they would find it easier to contextualise extremist content and to respond to it convincingly. The UK does not currently have enough understanding of the huge regional processes taking place in the Middle East to engage effectively with enemy propaganda. And if the start point is that communications effort should be based on fact, there is an irreducible lead time associated with making sure this is the case. That said, a dedicated team rebutting rumours and conspiracy theories about the UK and its role, whether historical or contemporary, could react immediately and not lose the argument by default.

UK responses are too slow for social media. To compete on social media at high tempo – 24/7 with a response time of perhaps 20 minutes – requires high level language and media skills. This might be achieved by using contractors and NGOs. The counter-propaganda effort would not then be directly run by government officials, but it would be hard to conceal HMG funding so HMG would still bear some political responsibility. It is unknown whether the UK is politically ready to run an explicit anti-propaganda campaign. Times have changed since the Cold War and it might be. An approach often used by Russia is to bombard forums and social media with irrelevancies to create doubt rather than spending time on specific messages or trying to win the argument. Could the UK adopt the same approach?

We need evidence of what works, including by engaging with former supporters of these groups.

RECOMMENDATION

5. Strategic communication and counter-propaganda are key elements in the implementation of UK policy. They should be led at a high level, coordinate all UK-government funded effort, be coordinated with allies, and partner where possible with regional allies. Information campaigns need to be aware of what opponents and allies, including BBC language services, are saying.

PROXIES/ALLIES

Should UK consider working with more non-state groups with which it shares some interests, for example in Iran where there are many minorities, each with a 'liberation organisation', many previously funded by Saddam Hussein? There would be many risks in such a policy. If UK supports groups with very different values to its own, it risks compromising its narrative and strategic communications plan. It would be hard to guarantee that any group would act in accordance with UK values, in particular on human rights. There may also be longer term geopolitical implications, particularly when UK interests and those of the group diverge at some point in the future. The risk of unintended consequences is high. The long-term impact of supporting non-state groups for short-term effects is hard to assess. For example, support for the Afghan mujahidin in the 1980s has led to jihadi blowback. Support for the Iraqi Kurds has encouraged them to become more independent of Baghdad. Support for minority ethnic groups in Iran seeking minority rights or autonomy (e.g. Arabs, Kurds, Azeris, Baluch, Turkmen) might stimulate some domestic unrest, but the Iranian government would respond, in its own way, against those it considered their sponsors. The overall effect would be regionally destabilising.

Establishing lines of communication to actors in the region may seem an obvious move, but even meeting representatives of non-state groups may have strategic impact and be open to misinterpretation, both by them and their enemies. The rules are clearly different for Middle Eastern governments, which, being less transparent and more authoritarian than Western liberal democracies, seem able to maintain links to any number of non-state groups without this being controversial, either domestically or with their allies, even when publicised.

There is an argument that the UK should be engaged with non-state groups because if it isn't others will be, and that over time UK can influence and nudge them towards UK values. While the political risks of working with non-state groups are high, it is clearly much cheaper than having to deploy conventional Western military forces, and presentationally avoids the criticism that 'Western Crusaders' are imposing their will through the use of military force.

RECOMMENDATION

6. UK should consider working with and supporting a wider range of state and non-state allies. Support could include political and media advice as well as military training and advice.

VIOLENCE

Daesh integrates its violence with its propaganda. It uses conventional violence to seize territory, but also uses iconic, symbolic and performative violence as a means of communication. Could the West deliberately use violence in the same way? We need to consider the types of violence used as well as the targets of that violence. Some Western commentators suggest that use of drones is somehow unfair, even illegitimate. The message drone strikes are intended to send is that enemies of the US can never be safe, wherever they are, and that the US government wants to minimise collateral casualties. But if this is not how they are being perceived then in some circumstances they may have a negative political effect. Carpet bombing, as used by the Russians in Syria, sends a different message, but from the West's point of view is unacceptable for moral, legal and political reasons, as well as making the task of post-conflict reconstruction more difficult, in terms of political reconciliation, human and financial cost. It is unclear whether the Arab 'street' makes this distinction between US and Russian policy on violence.

A consistent theme of both US and UK counter-terrorism campaigns since 2001 has been the targeting of the leaderships of terrorist and insurgent groups, so-called decapitation strategy. Academic research on the efficacy of this is mixed.[12] Killing leaders of terrorist groups may reduce their operational effectiveness in the short term but make them more extreme ideologically and reduce the chances of any sort of negotiated end to their violence; in general only long-established leaders of 'terrorist' groups have been able to negotiate political solutions and deliver their membership.

Using violence in ways which conflict with Western values or laws would undermine Western communications; for the West, the use of violence requires a moral purpose. The West must also operate within legal constraints which may not apply to other actors. For example the responses of non-Western navies to Somali piracy have often been more violent than Western rules of engagement would have allowed (and have arguably been more effective). Clarity about the law and how it will be applied is needed. Legislation may be required to define the parameters for UK officials to cooperate with foreign governments on terrorism investigations and in particular on extradition of terrorist suspects to the UK.

The full criminal justice approach (detaining terrorists and putting them on trial) allows the UK to demonstrate its values, and treats terrorism as crime rather than as war, both of which have potential political benefit. However, it is difficult and resource-intensive to implement, and can be unpopular with those who have to implement it on the ground if they perceive that it adds to their risks and the effort required to remove a terrorist from the struggle. An example would be the 'catch and release' policy the UK military pursued in Afghanistan, when they normally had no legal means of detaining suspected members of the Taleban for more than 96 hours. A different approach is to improve (i.e. make fairer, more effective, and speedier) the criminal justice systems of countries at risk of terrorism, though this is difficult and long term work. This would undermine one strength of insurgent groups such as Daesh and the Taleban, which is that they deliver security and justice, of a sort.

RECOMMENDATIONS

7. HMG should consider legislation on Counter-Terrorism cooperation with foreign governments, including extradition to UK.

8. UK should commit to long-term criminal justice capacity-building programmes in countries at risk of terrorism which require this.

HOW COULD/SHOULD THE WEST/UK MOBILISE NON-GOVERNMENT CAPABILITIES?

Western opponents mobilise non-government capabilities, but it is unclear how much the West/UK should and could do the same in response. In principle, a wide range of non-government capabilities could be mobilised, from soft power (e.g. press, communications, advocacy NGOs) through harder options (e.g. voluntary financial boycotts, cooperation by tech companies) to hard power (e.g. support for armed insurgency groups). The non-government actors/organisation are varied and have varied goals, and will differ in how far they are prepared to cooperate with government.

However, direct government involvement with non-government actors/organisations could compromise them politically, and so be counter-productive. They might be stronger and more effective left alone. We are therefore cautious about trying to mobilise non-government capabilities for Hybrid Warfare. It is probably better to demonstrate confidence in the virtues of liberal democracy and the free market by not trying to direct non-government actors. This reflects that the UK is not fighting an existential struggle. During WW2 and the Cold War government made more use of non-government actors.

In the case of media and communications, although most media organisations support Western ideological standpoints (against Daesh, for example), they do not want to compromise their independence. Daesh propaganda targets different groups with different emotional narratives – to respond to these separately would require a level of coordination that the media and communications sectors could not agree to. In addition, messaging which is too obviously government-inspired tends to be less effective.

Government funds NGOs to deliver particular programmes in order to achieve certain outcomes; however while there is overlap, often the overall aims of government and NGOs differ. A second issue with NGOs is that they may resist government direction of their work if it leads to a loss of perceived independence and neutrality. In the 1990s there was a strong focus on appearing neutral, and NGOs set up mechanisms to ensure this. This has been changing, for example in Syria, but a question of the extent of political motivation (whether overt or covert) behind the humanitarian work of NGOs is one that needs to be considered. UK policymakers also need to be mindful that cultural differences mean that what they may not consider a political (or partisan) goal, such as improving the position of women, may be received as political on the ground, even if UK is explicitly trying to avoid supporting any party in domestic politics.

The financial sector has on the whole developed a cooperative model with government. The US Treasury, admittedly making good use of the threat of investigation and regulation, has influence on any major bank as they all need to be able to clear dollars through the US. However, countering the financing of Hybrid Warfare actors is not straightforward. For example, privacy laws often stop banks discussing transactions with each other or with governments, except under a legal warrant. Foreign policy and international financial policy ought to be more closely aligned. Tech companies are hesitant to get involved with government, particularly after Snowden, for a combination of business and ideological reasons. Tech companies seem less influenced by the reputational issues that cause banks and other financial institutions to be more cooperative with government. It is possible that the public may get used to the idea of tech companies becoming closer partners with government in counter-Hybrid Warfare operations, particularly if trust in institutions and regulation in this area develops.

Non-government capabilities used to counter Hybrid Warfare may undermine each other if not coordinated and part of an overall strategy; but if coordination reduces tempo, agility and the level of activity then it may be best not to attempt it. The struggle against Islamic terrorism is however a societal challenge requiring a societal response. Government leadership is needed to consider which non-government capabilities might be harnessed, under what circumstances, and how. At a minimum government should consult civil society and draw on its expertise, especially in the financial, tech and media sectors.

RECOMMENDATION

9. As part of counter-HW planning, HMG should consult relevant non-governmental organisations and consider which, if any, non-governmental capabilities might be mobilised and under what circumstances. ■

LIST OF ABBREVIATIONS

AQ	Al Qaeda
AQ-IM	Al Qaeda in the Islamic Maghreb
BH	Boko Haram
BW	Biological Warfare/Weapons
C2	Command and Control
CW	Chemical Warfare/Weapons
DDOS	Distributed Denial of Service
FSE	Full Spectrum Effects
HW	Hybrid Warfare
IED	Improvised Explosive Device
NGO	Non-Governmental Organisation
NSC	National Security Council
NSA	National Security Adviser
OSCT	Office of Security and Counter-Terrorism, Home Office
PMF	Popular Mobilisation Forces (Shia militia in Iraq)
RICU	Research, Information and Communications Unit, Home Office
SOE	Special Operations Executive

ENDNOTES

[1] Daesh is an acronym for the Arabic phrase al-Dawla al-Islamiya al-Iraq al-Sham (Islamic State of Iraq and the Levant). Essentially, it is another word for ISIS, the English language acronym for the Islamic State in Iraq and Syria, which Daesh militants do not favour.

[2] Those who took part in the discussions or commented on the draft included: Sir Mark Allen, former FCO official; Prof. Gordon Barrass, co-leader of Global Strategies; General (ret) Sir Richard Barrons, former Commander, Joint Forces Command; Prof. Christopher Coker, LSE International Relations Dept. and co-leader of Global Strategies; Prof Toby Dodge, Director, LSE Middle East Centre; Mr Tom McKane, former DG Security Policy, MOD; Mr Clovis Meath Baker, former Director of intelligence production, GCHQ; Mr Julian Miller, former Deputy National Security Adviser; Mr Stephen Mitchell, former Deputy Director News, BBC; Mr Gerard Russell, former FCO Arabic Spokesman; Mr Bernard Siman, Geopolitical Information Service AG; Maj-Gen (ret) Jonathan Shaw, former Director Special Forces; and serving officials from the Cabinet Office, FCO, MOD, DFID, British Council, and the Armed Forces.

[3] Hoffman, Frank G; Mattis, James N 'Future Warfare: The Rise of Hybrid Wars', Proceedings (November 2005)

[4] Hoffman, Frank G 'The Rise of Hybrid Wars', Potomac Institute for Policy Studies (December 2007) p. 14

[5] Wikipedia 'Hybrid Warfare', accessed February 2016

[6] Wikipedia, 'Lawfare', accessed February 2016

[7] For example see article 'Lawyers to right of them, lawyers to left of them', The Economist, 9 August 2014

[8] See for example G. Almond, R. Appleby and E. Sivan, *Strong Religion: The Rise of Fundamentalisms around the World,* University of Chicago Press, 2003, on the connection between the prescriptive/axiomatic characteristics of science teaching and Islamist intolerance.

[9] D. Gambetta and S. Hertog, *Engineers of Jihad: The Curious Connection between Violent Extremism and Education,* Princeton University Press, 2016.

[10] During the period before 2002 when the Taleban were in power in Kabul the internet was officially banned in Afghanistan on the grounds that it broadcast undesirable material.

[11] The phrase 'OODA loop' refers to the decision cycle of *observe, orient, decide, act*, developed by US Air Force Colonel John Boyd.

[12] e.g. Bryan C. Price, *Targeting Top Terrorists: How Leadership Decaptitation Contributes to Counterterrorism,* in International Security, Vol 4, issue 36

THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

EXECUTIVE MASTERS PROGRAMME

INTERNATIONAL STRATEGY AND DIPLOMACY

LSE IDEAS, a Centre for the study of international affairs, brings together academics and policy-makers to think strategically about world events.

This one year **EXECUTIVE MASTERS PROGRAMME** is at the heart of that endeavour. While studying in a world-leading university you will be able to learn from top LSE academics and senior policy practitioners.

The programme will sharpen your ability to challenge conventional thinking, explore new techniques for addressing risk and threats, and coach you in devising effective strategies to address them.

The course has been especially tailored so that you can accelerate your career while holding a demanding position in the public or private sector.

"Right from the first week
I was able to apply the lessons
I had learnt to our operational
and policy work and to coach
my teams to look at
issues differently."

- **Karen Pierce**
UK's Permanent Representative
to the UN and WTO in Geneva

CONTACT US

Email: **ideas.strategy@lse.ac.uk**
Phone: **+44 (0)20 7955 6526**
lse.ac.uk/ideas/strategy

LSE IDEAS is LSE's foreign policy think tank. We connect academic knowledge of diplomacy and strategy with the people who use it through our projects, publications, events, and executive education.

ADDRESS

LSE IDEAS
9th floor, Towers 1 & 3
Clement's Inn, London
WC2A 2AZ

lse.ac.uk/IDEAS

FOLLOW US ON TWITTER
@lseideas

facebook/lseideas