The Remote Warfare Digest

open briefing
the civil society intelligence agency

Chris Abbott
Steve Hathorn
Scott Hickie

November 2016

Published by Open Briefing and the Remote Control Project, 16 November 2016.

Open Briefing
The Workbox
4th Floor, PZ360
St Mary's Terrace
Penzance
Cornwall TR18 4DZ
United Kingdom

+44 (0)1736 800 767
info@openbriefing.org

www.openbriefing.org

Remote Control Project
Oxford Research Group
Development House
56-64 Leonard Street
London EC2A 4LT
United Kingdom

+44 (0)20 7549 0298
media@remotecontrolproject.org

remotecontrolproject.org

Chris Abbott is the founder and executive director of Open Briefing. He was previously the deputy director of the Oxford Research Group and an honorary visiting research fellow in the Department of Peace Studies at the University of Bradford.

Steve Hathorn is a senior analyst at Open Briefing. He is an intelligence analyst with over 20 years' experience in the British Army, Defence Intelligence Staff, National Criminal Intelligence Service, United Nations, International Criminal Court and the National Crime Agency.

Scott Hickie is a senior analyst at Open Briefing. He is a lawyer and former political adviser in the New South Wales parliament. He has worked on climate change adaptation for the City of Toronto, and is currently a policy officer with the New South Wales government.

Open Briefing is a groundbreaking non-profit social enterprise. It provides low-cost, high-impact intelligence, security, training and equipment services to organisations and individuals striving for social and environmental justice, particularly those working in or on fragile and conflict-affected states or under repressive regimes.

The **Remote Control Project** is a project of the Network for Social Change hosted by the Oxford Research Group. The project examines changes in military engagement, in particular the use of drones, special forces, private military companies and cyber warfare.

The Remote Warfare Digest

Chris Abbott, Steve Hathorn and Scott Hickie

Contents

Preface

The United States used special forces, covert agents, mercenaries and proxy armies in order to fight wars out of the public eye during the Cold War. Such unconventional forces were then used alongside regular coalition military units during the war on terror and the associated wars in Afghanistan and Iraq. But it is the recent and rapid development of new technologies and capabilities, such as armed drones, offensive cyber operations and mass surveillance, that has led to Western governments embracing the strategy of 'remote warfare' in today's multiple and dispersed operations against violent jihadist networks, such as Islamic State.

By adopting this approach, governments are attempting to sidestep parliamentary, congressional and public oversight of their actions. This oversight ensures better military decision-making and foreign policy strategies, and its circumvention leaves the public unable to properly engage with these issues or hold politicians and military leaders to account. Policymakers approve actions using remote warfare that they may not consider if conventional military means were to be used; however, the consequences and risks of those actions do not appear to be fully understood in advance.

Since April 2014, Open Briefing has produced a series of monthly intelligence briefings on remote warfare commissioned by the Remote Control Project. Periodically, Open Briefing undertake a more in-depth assessment of the trends in remote warfare for the project. This current report sets out the findings of the third such assessment.

The first assessment, published in October 2014, highlighted the disconnect between civil society's perception of remote warfare and the actual intentions and capabilities of governments and militaries. The second assessment, published in June 2015, explored the limits and unforeseen consequences of remote warfare. A key theme of this third assessment is the adoption of remote warfare by state and non-state actors beyond the United States and its Western allies. This includes Islamic State's external action command mimicking special forces tactics, Russia deploying special forces units and private military contractors to Syria, the proliferation of armed drones to state and non-state adversaries, North Korean offensive cyber operations acting as a testbed for other cyber powers, and the way in which jihadist networks are melding modern encrypted communications with traditional tradecraft to elude Western surveillance efforts.

Other trends in remote warfare identified and analysed in this report include the level of transparency and oversight of special forces missions being out of step with the wider risks of miscalculation in these deployments, the rise and fall (and rise again) of private military and security companies in Iraq and Afghanistan, the future of drones in RAF operations, NATO members preparing for an increase in cyber campaigns against critical infrastructure, and the potential impact of Brexit on UK and European intelligence sharing and security operations.

These, and the other trends analysed in the following pages, are significant developments in remote warfare that warrant the deeper look provided in this report.

Section I

Special operations forces

Level of transparency and oversight of special forces missions out of step with their growing use, leaving wider risks of miscalculation in these deployments

The risks of miscalculation in special operations forces (SOF) deployments are increasing as coalition forces expand their footprint and levels of engagement in counterterrorism operations. However, the level of legal authorisation, parliamentary oversight and public disclosure on SOF deployments is out of step with these risks, particularly as presented in deployments in Iraq, Syria, Yemen and Libya.

The level of disclosure surrounding SOF deployments varies considerably between countries. The high level of collaboration between coalition partners means that SOF commitments by one country may be inadvertently disclosed by a more open ally, putting governments on the back foot. Although the level of disclosure varies, there is an underlying perception across countries that the light-footprint, remote warfare made possible by special operations forces poses less political, military and diplomatic risks than conventional warfare and thus requires lower levels of public and parliamentary oversight.[1]

In the United States, the Obama administration has more readily and publicly acknowledged SOF deployments in Iraq and Syria than other partners in those conflicts. The relatively-higher level of disclosure by the US government occurs despite the fact that the deployments push the legal limits of the 2001 Authorisation for Use of Military Force (AUMF) and the War Powers Resolution[2] and that it highlights the involvement of US SOF in frontline combat. The parliaments of some European coalition partners, such as Norway,[3] Germany[4] and Denmark,[5] have authorised the recent deployments of their country's special forces for advise and assist missions in Syria. In contrast, the British government and Ministry of Defence has a longstanding policy of not commenting on special forces operations and the UK parliament has not had the opportunity to debate and vote on the deployment of UK special forces to Iraq and Syria.[6]

[1] http://www.unswlawjournal.unsw.edu.au/sites/default/files/393-14.pdf

[2] https://twq.elliott.gwu.edu/legal-legacy-light-footprint-warfare

[3] http://theiranproject.com/blog/2016/06/23/norway-send-troops-syria/

[4] http://www.nytimes.com/2015/12/05/world/europe/german-parliament-military-isis-syria.html

[5] http://www.reuters.com/article/us-mideast-crisis-danish-mission-idUSKCN0XG2AV

[6] http://remotecontrolproject.org/publications/britains-culture-of-no-comment/

Even those governments that have been relatively open about the deployment of SOF to Iraq and Syria have been less frank about such deployments to Libya.[7] The deaths of three French special forces soldiers in a helicopter crash in Libya in July removed the ability of the French president, François Hollande, to deny that French SOF are operating in Libya.[8] The UK government has tried to remain elusive on the deployment of British special forces in Libya,[9] even in the face of a leaked briefing note authored by the Jordanian king, Abdullah II bin Al-Hussein, that suggested there was a covert British presence in Libya[10]. In May, the UK defence secretary, Michael Fallon, stated in the House of Commons that there were no plans for a UK combat role in Libya,[11] despite continuing reports of SAS combat and ISR support operations for Libyan partners[12].

Events over the past year have shown that the geopolitical interests of the major powers deploying SOF can complicate an already complex field of sectarian, regional and political interests. While using SOF may make the military commitment to a conflict modest, the geopolitical consequences of a military misstep can be significant in these complex multinational and multifactional theatres.

An example of this is the Russian airstrikes on 16 June on a New Syrian Army (NSyA) camp at the al-Tanf border-crossing.[13] The New Syrian Army is trained and supported by the United States and seeks to remove Islamic State from eastern Syria. The United Kingdom and Jordan are both thought to have embedded special forces with the NSyA in the past, and the al-Tanf camp was used by British and American SOF trainers.[14] Although Western special forces were not present in the al-Tanf camp at the time of the Russian airstrikes, the attack is an example of the potential for escalating confrontation between Russia and the US and Europe because of miscalculation in a complex conflict zone. Indeed, the push for US and Russian cooperation in Syria is partly based on mitigating this risk.

[7] http://remotecontrolproject.org/publications/remote-control-project-briefing-we-need-greater-transparency-on-uk-military-operations-in-libya/

[8] http://www.longwarjournal.org/archives/2016/07/presence-of-french-special-forces-in-libya-sets-off-controversy.php?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+LongWarJournalSiteWide+%28The+Long+War+Journal+%28Site-Wide%29%29

[9] https://www.parliament.uk/documents/commons-committees/foreign-affairs/Correspondence/2015-20-Parliament/Letter-to-Foreign-Secretary-160315-Libya.pdf

[10] http://www.theguardian.com/world/2016/mar/25/sas-deployed-libya-start-year-leaked-memo-king-abdullah

[11] http://www.publications.parliament.uk/pa/cm201516/cmhansrd/cm160229/debtext/160229-0001.htm#16022911000597

[12] http://www.middleeasteye.net/news/sirte-libya-british-commandos-frontline-uk-britain-michael-fallon-islamic-state-669841059

[13] https://remotecontrolprojectblog.org/2016/08/04/the-uk-cant-stay-mum-over-russian-bombing-of-special-forces-base-in-syria/

[14] https://www.bellingcat.com/news/mena/2016/06/21/al-tanf-bombing-russia-assisted-isis-attacking-us-backed-fsa-group-cluster-bombs/

Similarly, the proposed participation of Emirati, Saudi and Jordanian special forces in Syria, announced by the US defence secretary, Ash Carter, in February, has been presented by Iran as an offensive manoeuvre that is part of a broader geopolitical campaign against the Islamic Republic.[15] The Islamic Revolutionary Guard Corps' deployment of the elite airborne unit Brigade 65 and other expeditionary forces to Syria to support the country's president, Bashar al-Assad, is well documented.[16] Iran's strategic objectives are likely to extend beyond preserving the al-Assad government, which increases the risks of miscalculation taking on a broader geopolitical dimension beyond the Syrian and Iraqi conflicts.

Another example is the US special operations forces collaboration with and training of Kurdish People's Protection Units (YPG), which included US forces wearing YPG insignia until May. This represents an ongoing risk to US-Turkey diplomatic relations beyond the direct consequences of a military coalition.[17] Washington is squarely caught between two allies: Turkey and the Kurds. Ankara's increasing deployment of special forces to Syrian border towns to support Syrian Arab fighters in confronting Islamic State and countering YPG forces that have gained a foothold creates a complex environment where blue-on-blue attacks remain a possibility.[18]

The relatively more open discussion of SOF deployments in the United States than in the UK means that the Pentagon and CIA's support and training programmes for the Syrian Democratic Force (SDF) have at least been subject to robust debate about the vetting of fighters and the supply of weapons. Considerable confusion over the allegiance and activities of proxy armies in Syria makes evaluating compliance with the US prohibition on training or funding forces accused of human rights abuses (as per the United States' Leahy Law) difficult at best. However, the open debate over the support and training provided to the SDF means the whole process is far more accountable than similar operations by British special forces, for example.

The continued expansion in the number and scope of SOF deployments suggests that the strategy of supporting proxy forces to confront Islamic State at a local level (a key tenet of remote warfare) is having the effect of scattering militants from one ungovernable safe haven to the next.[19] A lack of transparency hinders proper public and parliamentary oversight of SOF strategies and their effectiveness. Disclosure of even limited SOF deployments would allow informed debate about the effectiveness and benefits, or not, of special forces missions.

[15] http://nationalinterest.org/blog/the-buzz/iran-isnt-sweating-saudi-intervention-syria-15262

[16] http://www.al-monitor.com/pulse/originals/2016/04/iran-army-brigade-65-green-berets-syria-deployment.html

[17] http://www.theatlantic.com/international/archive/2016/05/turkey-us-ypg/484631/

[18] http://www.cbc.ca/news/world/turkey-cross-border-operation-syria-1.3733464?cmp=rss

[19] https://www.ctc.usma.edu/posts/how-realistic-is-libya-as-an-islamic-state-fallback and http://remotecontrolproject.org/publications/british-war-terror/

Counterterrorism efforts of US special operations forces shifting beyond advise and assist missions

The increasing diversity of counterterrorism tactics employed by Western special operations forces across the Middle East and North Africa is a natural reflection of the varying threats, capabilities of adversaries and political constraints. However, the shifting emphasis between different tactics may also be underpinned by divergent philosophies among allies on broader counterterrorism objectives.

In late February 2016, the United States deployed an Expeditionary Targeting Force (ETF) to Iraq for high-value target (HVT) kill/capture missions in Iraq and Syria. Between February and May 2016, the ETF killed or captured several high-ranking IS officials and captured Sleiman Daoud al-Afari, who was the head of Islamic State's chemical weapons programme and had previously worked for Saddam Hussein's regime.[20] The ETF reflected a shift from advise and assist missions to a high-tempo, kill/capture team operating more in line with the operational function of the Joint Special Operations Command (JSOC) in the Iraq and Afghanistan insurgencies.

The authorisation and deployment of the ETF was announced by the US defence secretary, Ash Carter, less than three weeks after the November 2015 IS-led attacks on Paris and the day before the IS-inspired attack in San Bernardino, California. Against this backdrop, the ETF was most likely deployed to attack Islamic State's leadership and inhibit its ability to direct external forces to attack Western targets. However, high-tempo ETF missions carry the risk that disrupting the leadership hierarchies drives organisations to build redundancy across global jihadist networks, thereby encouraging 'aggregation of conflict' and the unification of disparate networks.[21] This may create a disjuncture with local advise and assist missions, which fundamentally seek to localise the conflict, interdict jihadist networks through a disaggregation strategy and allow indigenous forces to confront rank and file IS fighters in local battlefields rather than push jihadist networks to other safe havens. Targeting the IS leadership in kill/capture missions also risks displacing those leaders who escape US forces, who may become 'organisational heirs' with the ability to direct local militants from afar.[22]

[20] http://www.thedailybeast.com/articles/2016/05/28/special-ops-rule-in-war-on-terror.html

[21] http://www.tandfonline.com/doi/abs/10.1080/01402390500300956 and http://www.smallwarsjournal.com/documents/kilcullen.pdf

[22] https://www.researchgate.net/profile/Aaron_Mannes/publication/242187440_Testing_The_Snake_Head_Strategy_Does_Killing_or_Capturing_its_Leaders_Reduce_a_Terrorist_Group's_Activity/links/54bfdc9f0cf21674ce9c96a6.pdf

Chasing key leadership figures across multiple conflict theatres based on the belief that killing or capturing those leaders will destroy the functioning of Islamic State may create the conditions under which local conflicts can be aggregated into a global jihadist narrative. Alternatively, confronting rank and file IS members and reclaiming territory using local indigenous forces (even if supported by Western SOF) is less likely to encourage the upper echelons of Islamic State to disperse to other safe havens and reconstitute organisational structures outside Iraq and Syria. However, shifting the focus of US SOF from advise/assist to kill/capture may also disrupt the ongoing training of and support for those local forces, undermining the ability of groups, such as the Iraqi Army, to secure definitive battlefield victories.

Even in purely advise and assist missions, there is always the risk of mission creep. Reports that Canadian,[23] British[24] and US[25] special forces have been involved in defensive combat operations during reconnaissance and forward air control missions suggest that SOF operators on advise and assist missions risk taking on frontline combat roles. This may encourage US SOF to reconsider the rules of engagement for such missions, which risks creating diverging rules of engagement between coalition partners and challenges for interoperability and cooperation, which in turn may reveal differences in the underlying counterterrorism theories various partners are basing their strategies on. There is also the danger that if the rules of engagement for advise and assist missions are loosened, SOF operators will end up in a halfway house between advise/assist and kill/capture missions, which on the surface may seem like a compromise, but in reality would only embrace the disadvantages of both approaches.

Islamic State's external action forces mimicking special operations forces tactics

In January 2016, the European Union's law enforcement agency, Europol, released a report on the modus operandi of Islamic State attacks.[26] The report indicated that Europol had intelligence suggesting that Islamic State had set up small training camps in EU and Balkans countries and had developed an 'external actions command' trained for special forces-style attacks in Europe. In the report, Europol drew heavily on its examination of the tactics and tradecraft employed by the attackers in the 13 November 2015 attacks in Paris, in particular the mass shooting at the Bataclan theatre, in which 89 people were killed and over 200 injured.

[23] https://ipolitics.ca/2015/12/17/canadian-forces-involved-in-firefight-with-isis-near-mosul/

[24] http://en.alalam.ir/news/1786758

[25] http://www.theatlantic.com/national/archive/2016/05/american-death-toll-isis/481206/ and https://www.theguardian.com/us-news/2016/may/04/charles-keating-iv-navy-seal-isis-battle-video

[26] https://www.europol.europa.eu/content/changes-modus-operandi-islamic-state-terrorist-attacks

The November 2015 Paris attacks and the attacks in Brussels in March 2016 and at Istanbul's Ataturk airport in June 2016 are held up as examples of Islamic State's external actions command employing tactics that emulate those used by special operation forces.[27] Such tactics included swarming, diversionary attacks and environment containment, and showed a sophisticated level of pre-attack reconnaissance and training and an advanced logistics capability. The planning of these attacks was likely supported by open source tools and secure communication channels that are difficult for Western security services to identify and monitor.[28] The devastating power of such tactics was demonstrated in the 2008 Mumbai attacks in which militants from Lashkar-e-Taiba (LeT) used an array of diversionary, swarming and urban siege tactics synchronously employed by small, mobile tactical units to create mass casualty attacks.

There are further interesting parallels between the targeting strategies of special operations forces and Islamic State and other violent jihadist groups. At first glance, SOF kill/capture missions or SOF-led drone strikes against high-value targets would seem the opposite of the indiscriminate attacks on civilian, soft targets preferred by Islamic State and its ilk. However, this overlooks the idea that the selection of targets by Islamic State's external actions command and returning foreign fighters is embedded with substantial social, cultural and political meaning in addition to consideration of attack opportunities. What the targeting philosophies have in common is that they seek operational and system dysfunction through remote, light-footprint attacks and are based on the idea that a specific attack can engender internal disorientation and conflict.

However, significant barriers may make it impossible for the IS external actions command to emulate SOF tactics more fully in future, including limited access to advanced intelligence, surveillance and reconnaissance (ISR) technologies and a limited arsenal of primarily small arms and IEDs to draw from. Indeed, the level and standard of training and equipment available to Islamic States means that it is highly unlikely that its external action command will ever be able to completely emulate the skills of Western special operations forces operators; however, the nature of the missions that members of the command will be tasked with – primarily suicide attacks against soft targets – means that they do not need to reach that high standard. Instead, it may be that the lessons learned from fighting Western SOF in Iraq and Syria will be used by Islamic State to plan and execute more effective attacks in Europe.

[27] https://www.europol.europa.eu/content/changes-modus-operandi-islamic-state-terrorist-attacks and http://www.thedailybeast.com/articles/2016/06/29/istanbul-ataturk-airport-attack-shows-sophisticated-planning-by-terrorists.html

[28] https://www.europol.europa.eu/content/changes-modus-operandi-islamic-state-terrorist-attacks and http://www.wsj.com/articles/islamic-state-teaches-tech-savvy-1447720824

While light-footprint SOF missions provide countries such as France, the United Kingdom and the United States with military advantages and battlefield victories, this type of combat shapes adversaries and drives evolution in counter-tactics and therefore possibly catalyses the proliferation of SOF tactics to non-state actors. IS militants have had to develop counter-SOF tactics in order to survive in Iraq, Syria and elsewhere. SOF counterterrorism missions can be 'reverse-engineered' to provide militants with an understanding of the fundamentals of SOF tactics.[29] Furthermore, SOF advice and assistance to indigenous forces or local proxies carries the risk that SOF tactics will be disseminated to groups outside those allies or taught to fighters who may one day become adversaries if the geopolitical winds change (as eventually happened with many of the Mujahideen who were trained and supported by the CIA and SAS during the Soviet occupation of Afghanistan).

In July 2016, al-Qaeda in the Arabian Peninsula (AQAP) released a video showing a training camp most likely located in southern Yemen where it trains its 'special forces'.[30] Former Guantanamo Bay detainee Ibrahim al Qosi appears in the video and states that the facility trains fighters from different tribes without requiring them to work with AQAP. This suggests that SOF-like tactics are being exchanged across different jihadist networks, despite the level of political or ideological disunity. If correct, this suggests that SOF tactics may also be deployed by jihadist groups without any direct combat experience against Western special forces.

[29] http://www.popsci.com.au/robots/drones/ied-drone-kills-kurdish-soldiers-french-commandos,439261

[30] http://www.longwarjournal.org/archives/2016/07/aqap-details-special-forces-training-camp.php

Section II

Private military and security companies

The rise and fall (and rise again) of private military and security companies in Iraq and Afghanistan

The private military and security company (PMSC) sector underwent a significant transformation in 2003-04 with the highly-lucrative government contracts being offered in post-invasion Iraq.[31] The outsourcing of military roles – such as protecting diplomats, providing convoy security and training local forces – to the private sector in both Iraq and Afghanistan prompted the rapid growth of hitherto relatively-small companies in the United States and United Kingdom, in particular, through expansion and acquisition. However, instead of driving up professionalism in the sector, the dramatically increased demand for security advisers to provide protective security services in hostile environments encouraged PMSCs to employ unsuitable contractors with limited relevant military or close protection experience in order to meet their contractual obligations to their clients.[32]

The bubble had burst by 2005, and unscrupulous companies attempted to protect their profits by driving down wages and cutting costs, including by withholding ballistic protection, suitable weapons and armoured vehicles – with even highly-experienced former special forces operators unable to attract the previously-high day rates that had been enjoyed across 'The Circuit' (as the international commercial security circuit is known). At the same time, though, the risks to private security contractors had greatly increased, particularly in Iraq, with an unknown number losing their lives or being seriously injured.[33] Contractor wages have since been further undercut by PMSCs recruiting increasing numbers of host-country nationals (HCNs) and third-country nationals (TCNs) from African and Asian countries, rather than employing the former soldiers from Western elite units and special forces that were previously preferred.[34] Some PMSCs were also able to adapt by accepting controversial but lucrative contracts from Middle Eastern governments accused of human rights abuses, such as Saudi Arabia and Israel, or in the emerging maritime and African markets.[35]

[31] See *The Circuit* by Bob Shepherd and *Licensed to Kill* by Robert Young Pelton.

[32] Op. cit.

[33] See *Highway to Hell* by John Geddes and *The Circuit* by Bob Shepherd.

[34] Personal communication with various contractors during 2016.

[35] See *The Circuit* by Bob Shepherd.

The lowering of standards, the absorption of companies into several behemoths and the fulfilment of controversial contracts has protected the profits of the larger security corporations, such as G4S (which acquired ArmorGroup) and GardaWorld (which acquired Aegis), over the last decade. Today, though, these companies look set to benefit from new developments in Iraq and Afghanistan. The US president-elect, Donald Trump, appears to be in favour of continuing the withdrawal of US military forces from the two countries begun by the current president, Barack Obama. In Afghanistan, US troop levels have dropped markedly from 99,000 in June 2011 to around 9,800 today.[36] The intention is to reduce this further to 5,500 by early 2017. Replacing these conventional military forces are the private security contractors. There are now 28,626 contractors in Afghanistan, three times as many as US troops.[37] In Iraq, there are 7,773 contractors working alongside 4,087 US troops.[38] There was an eight-fold increase in the number of contractors in Iraq between January 2015 and January 2016.[39] The demand for private military and security companies looks set to increase if the long-term drawdown in US forces in both theatres continues under the next US president at the same time as the intensity of the conflicts show no signs of reducing.

Fundamentally, as with the more-widespread use of special operations forces rather than conventional forces, the use of PMSCs removes the state one step further from a conflict and sidesteps public and parliamentary oversight. This may be one reason why the British government, for example, has dragged its heels for so long over effectively regulating PMSCs.

There are important *security* roles that the private sector can and should fulfil, from protecting journalists reporting in war zones to training executives before they travel to hostile environments. However, when PMSCs are allowed to fulfil *military* roles, it may tempt governments to shirk their responsibilities to acknowledge the true security situation in countries they have intervened in and commit the troop numbers necessary to secure the ground so that post-conflict reconstruction and development can take place.

[36] http://thewire.in/42132/is-the-world-ready-for-private-military-companies-as-peacekeepers/ and http://edition.cnn.com/2016/07/06/politics/obama-to-speak-on-afghanistan-wednesday-morning/

[37] http://thewire.in/42132/is-the-world-ready-for-private-military-companies-as-peacekeepers/

[38] http://thewire.in/42132/is-the-world-ready-for-private-military-companies-as-peacekeepers/

[39] http://www.defenseone.com/threats/2016/02/back-iraq-us-military-contractors-return-droves/126095/

The use and abuse of third country nationals by private military and security companies

Contractors fulfil many roles in modern wars, including logistics, communications support, construction, training, translation and drivers. A smaller number of contractors provide security services in conflict theatres, and an even smaller number are armed private security contractors.[40] In addition, the CIA and other intelligence agencies employ an unknown number of contractors and PMSCs to provide paramilitary services.

Although not technically employed for frontline combat roles, security contractors working in hostile environments, such as Iraq and Afghanistan, frequently find themselves in high-risk situations of close quarters combat without the numbers or air support and other backup that state military personnel can call upon. There are no official contractor casualty figures available, as neither the companies nor the governments employing them wish to draw attention to the deaths of contractors (one of the roles contractors serve is to deflect attention from military casualties, which damage public support for a given conflict). However, according to a paper by researchers at the George Washington University Law School published in 2011, more than 2,300 contractors were killed and 51,000 injured in Iraq and Afghanistan in the decade from 2001.[41] As both the numbers of contractors and the dangers they face increases, so too does the proportion of the casualty rate borne by contractors: in 2003, Defense Base Act fatality claims by the families of contractors represented only 4% of all fatalities in Iraq and Afghanistan; in 2010, such claims represented 47% of all fatalities.[42]

Statistics like this mask an important nuance: many contractors are not nationals of the country employing them and may not even be citizens of a country involved in the conflict theatre they are working in. Overall, of the 43,781 contractors that the US Department of Defense (DoD) reported as employed in the US Central Command (USCENTCOM) area of responsibility (AOR) in January 2016, only 36% were US citizens – 43% were host country nationals (HCNs) and 21% were third country nationals (TCNs).[43] Of the 1,083 *armed* private security contractors that employed by the DoD in Afghanistan, only 16% were US citizens – 53% were host country nationals and 31% were third country nationals.[44]

[40] http://www.acq.osd.mil/log/PS/.CENTCOM_reports.html/5A_January_2016_Final.pdf

[41] https://cybercemetery.unt.edu/archive/cwc/20110929221203/http://www.wartimecontracting.gov/docs/forum2011-05-02_statement-Schooner.pdf

[42] http://www.huffingtonpost.com/david-isenberg/the-uncounted-contractor-_b_859206.html

[43] http://www.acq.osd.mil/log/PS/.CENTCOM_reports.html/5A_January_2016_Final.pdf

[44] http://www.acq.osd.mil/log/PS/.CENTCOM_reports.html/5A_January_2016_Final.pdf

The involvement of third country nationals was highlighted by the deaths of 14 Nepalese security guards in a suicide attack on a Canadian embassy bus in the Afghan capital, Kabul, on 20 June 2016.[45] Around 9,000 Nepalis officially work in Afghanistan, mostly as security guards at foreign military or diplomatic compounds, but some estimates place the total figure at over 20,000 when those who have entered the country illegally are included. Nepal has stopped providing work permits for its citizens for Afghanistan, Iraq, Libya and Syria in the aftermath of the Canadian embassy bus attack.[46]

The reliance on host- and third-country nationals – mainly from Asia and Africa – raises an important question: is it ethical for Western governments to be using individuals from poorer regions of the world as proxy soldiers in place of conventional forces? After all, European and North American governments are essentially exchanging, for example, Nepalese lives for Western lives by hiring contractors to undertake military tasks in conflict zones.

As if the risk of death or injury is not enough, TCNs are also suffering abuse at the hands of their employers. In an article for Canada's *Globe and Mail* newspaper, the political anthropologist Noah Coburn outlined his findings from interviewing over 200 security contractors in Nepal, India and Turkey who worked for various private security companies in Afghanistan that were funded by Canada, the United States and other Western donors.[47] He found that a large number of these TCNs were subject to a variety of abuses by their employers. Many reported being trafficked into the country and then forced to take lower wages than they had been promised. The contractors risk being sent to prison if they reported these abuses, as they are brought into the country illegally and do not have proper visas. The situation is compounded for some contractors, as Nepal, for example, does not have an embassy in Afghanistan. During his 12-month investigation, Coburn also found many instances of injured contractors being provided only a small amount of cash and immediately shipped back home then abandoned by their employer.

TCNs working in other roles for Western militaries are not immune to abuse. Cooks, cleaners, construction workers, beauticians and shop assistants from the Philippines, Kenya, Bosnia, India and elsewhere can be forced to take lower wages than promised, subjected to sexual assault with little hope of any law enforcement action, and made to live in squalid conditions. Some TCNs have been trafficked into the country after being promised well-paid jobs in Dubai and elsewhere before being processed and sent to work on military bases in Iraq and Afghanistan.[48] Widespread mistreatment even led to a series of riots in 2010 in DoD subcontractor camps.[49]

[45] https://www.thestar.com/news/world/2016/06/20/suicide-bombing-in-kabul-kills-14-canadian-embassy-security-guards.html

[46] http://news.trust.org/item/20160624142846-nzez4/

[47] http://www.theglobeandmail.com/opinion/reliance-on-private-contractors-is-changing-the-human-cost-of-war/article30575141/

[48] http://www.newyorker.com/magazine/2011/06/06/the-invisible-army

[49] http://www.newyorker.com/magazine/2011/06/06/the-invisible-army

There has been some intervention by the US government in abuses by PMSCs in their employ. Raids have been carried out on contractor camps where reports of abuses have been received, trafficked staff have been transported home and, occasionally, contracts have been terminated.[50] But Western governments must do more to ensure the safety of the contractors they employ to support their fighting machines, wherever those contractors come from.

Russia adopting remote warfare with deployment of special forces and private military contractors in Syria

In a mirroring of the West's predilection for remote warfare over the deployment of conventional forces, Russia appears to be extending its strategy of hybrid warfare in Syria beyond the special forces (Spetsnaz) and forward air controllers that are long thought to have been fulfilling reconnaissance and strike roles in the country. More information has come to light about a shadowy Russian private military company called Wagner that is reportedly fighting alongside Spetsnaz units in Syria. Wagner is the informal name for a private group called OSM, led by a former Spetsnaz officer and current reservist called Dmitry Utkin.[51] The Russian defence ministry has previously dismissed reports about the Wagner's operations in Syria as an 'information attack'; however, sources at the FSB and the Russian defence ministry have unofficially revealed Wagner forces are in theatre.[52] Unlike their Western counterparts, the Russian private military contractors appear to be heavily armed and engaged in frontline combat operations.[53]

The independent Russian newspaper *Fontanka* reported in March 2016 that an undisclosed number of military contractors working for Wagner were operating alongside the Spetsnaz units that had remained in Syria when the bulk of the Russian military operation was first wound down.[54] An investigation by the newspaper found that the Kremlin had contracted Wagner for operations in Syria and had previously used the company in Ukraine (the latter was corroborated by a UN Working Group on 18 March 2016[55]). *Fontanka* also claimed that Wagner is also building a formidable arsenal of hardware, some issued by the Kremlin, including armoured combat vehicles, portable anti-aircraft systems and mortars.[56]

[50] http://www.mcclatchydc.com/news/nation-world/world/article24512842.html

[51] http://www.wsj.com/articles/up-to-nine-russian-contractors-die-in-syria-experts-say-1450467757 and http://www.interpretermag.com/fontanka-investigates-russian-mercenaries-dying-for-putin-in-syria-and-ukraine/

[52] http://www.russia-direct.org/russian-media/russian-private-military-company-detected-syria

[53] http://www.wsj.com/articles/up-to-nine-russian-contractors-die-in-syria-experts-say-1450467757

[54] http://www.fontanka.ru/2016/03/28/171/

[55] http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=18492&LangID=E

[56] https://lobelog.com/russia-leads-the-way-to-a-pmc-future/

Then in August 2016, Sky News published an exclusive report on Wagner based on interviews with a group of young men who claimed to be working for the company.[57] According to the broadcaster, prior to their deployment to Syria the contractors had been stationed in Molkino, the small Black Sea village in southern Russia that is home to the 10th Detached Special-Purpose Brigade (Spetsnaz) of the Russian defence ministry's Main Intelligence Directorate (GRU).[58] Part of the Spetsnaz base has been set aside for Wagner, and contractors are housed in a barracks built to the southwest of the main base sometime around 2015 (according to imagery from Google Earth).[59] Here, new recruits undergo one to two months of selection and training, during which inexperience recruits receive basic infantry training and ex-military personnel receive more-advanced training in multiple skills. However, former contractors have complained that the training given at the Molkino camp is too basic, with insufficient fieldcraft training.[60]

After training, the contractors that Sky News spoke to were flown to Khmeimim, a Russian military airbase adjacent to Bassel Al-Assad International Airport to the southeast of Latakia in Syria. There, they joined their unit, which one source described as having 564 soldiers with '…two reconnaissance companies, one air defence company, two assault groups and foot troops, plus heavy artillery, tanks and so on.'[61] This suggests that Wagner is being used to provide small-scale but flexible battlegroup formations. Estimates of Wagner's current deployed strength vary widely, ranging from between 1,000 and 1,600 Wagner employees overall[62] to nearly 2,500 deployed near Latakia and Aleppo alone.[63] Such numbers would indicate the presence of two to four battalion-sized Wagner battlegroups in Syria.

According to an extensive report published by the Russian news service RBC on 25 August, the Wagner contractors are commanded by officers from Russia's GRU and FSB;[64] however, contractors have complained that they are not respected by the Russian and Syrian military leaderships. They claimed that they would often be used as first-wave troops, deployed on suicide missions to soften up hardened defences before Syrian forces were sent in.[65]

[57] http://news.sky.com/story/revealed-russias-secret-syria-mercenaries-10529248

[58] http://www.russia-direct.org/russian-media/russian-private-military-company-detected-syria

[59] http://www.interpretermag.com/russia-update-august-26-2016/

[60] https://lobelog.com/russia-leads-the-way-to-a-pmc-future/

[61] http://news.sky.com/story/revealed-russias-secret-syria-mercenaries-10529248

[62] http://www.russia-direct.org/russian-media/russian-private-military-company-detected-syria

[63] http://www.interpretermag.com/russia-update-august-26-2016/

[64] http://www.rbc.ru/magazine/2016/09/57bac4309a79476d978e850d

[65] http://www.russia-direct.org/russian-media/russian-private-military-company-detected-syria

Officially, only 19 Russians have been killed in Syria;[66] however, RBC cited a Russian defence ministry source who claimed that 27 private military contractors had been killed in the Middle East, and a former private military officer said that at least 100 had been killed.[67] The contractors interviewed by Sky News claimed that as many as 500-600 Wagner employees had been killed in Syria.[68] Whatever the actual number of Russian private military contractors killed, there is no official recognition of their employment, let alone their deaths. The families of dead contractors do reportedly receive compensation of up to 5 million roubles (about $80,000 at the current exchange rate), but it comes with non-disclosure conditions.[69]

The Russian constitution currently outlaws private military companies, and participating in mercenary activity is punishable by a prison term of up to 15 years. However, there are reports that this legislation is going to be withdrawn,[70] and the Russian leadership is showing increasing official support for companies such as Wagner, as well as unofficially using their services. In 2012, the then Russian prime minister, Vladimir Putin, made public statements describing PMSCs as a 'tool for the implementation of national interests with direct participation of the state', and has since authorised the Kremlin to use these companies for deniable operations.[71] In 2013, Russia's deputy prime minister, Dmitri Rogozin, suggested that it was worth formalising the sector and that companies should be established with state backing, though he met considerable opposition from the defence ministry at the time.[72]

Opposition to PMSCs from the Russian military hierarchy began to soften during the Ukraine operation with the deployment of independent Crimean militias to carry out combat operations that could not officially be carried out by the Russian Army. These militias were often created from organised criminal gangs and right-wing groups and, while they offered a degree of deniability at the time, their lack of training and experience often saw them requiring considerable support from Russian military assets, which somewhat undermined the value of their unofficial status.[73] Many of the people now involved with Wagner – including its leader, Utkin – were previously employed by the short-lived Slavonic Corps, which was based in Hong Kong and briefly operated in Syria before being dissolved at the end of 2013.[74] Wagner itself is registered in Argentina in order to bypass the current constitutional ban on its existence and activities.

[66] http://news.sky.com/story/revealed-russias-secret-syria-mercenaries-10529248

[67] http://www.rbc.ru/magazine/2016/09/57bac4309a79476d978e850d

[68] http://news.sky.com/story/revealed-russias-secret-syria-mercenaries-10529248

[69] http://rbth.com/defence/2016/08/26/russian-private-military-company-spotted-in-syria_624521 and http://www.russia-direct.org/russian-media/russian-private-military-company-detected-syria

[70] http://www.interpretermag.com/russia-update-august-26-2016/.

[71] http://www.telegraph.co.uk/news/2016/03/30/vladimir-putin-sent-russian-mercenaries-to-fight-in-syria-and-uk/

[72] http://warontherocks.com/2016/04/moscows-mercenaries-in-syria/

[73] http://www.rferl.org/content/ukraine-luhansk-bednov-plotnitsky-assassination-russia-torture-arrest/26775163.html

[74] https://lobelog.com/russia-leads-the-way-to-a-pmc-future/

As the Syrian president, Bashar al-Assad, remains firmly in power, ceasefire agreements in the country disintegrate and cooperation between the United States and Russia over the conflict falters, it is highly likely that Russia will continue to rely on private military contractors to supplement its special forces operations in Syria. While official support for the PMSC sector is increasing in Russian political and military circles, the Kremlin is likely to wish to maintain unofficial links with Wagner and similar organisations as it expands its hybrid warfare operations in Syria and potentially elsewhere.

Section III

Unmanned vehicles and lethal autonomous weapons systems

The future of drones in RAF operations

Between 8 August 2014 and 10 September 2016, the US-led coalition conducted 9,818 airstrikes in Iraq and 5,189 in Syria.[75] The United Kingdom conducted 936 of those airstrikes in Iraq and around 100 in Syria.[76] The UK Ministry of Defence claims that the British missions have resulted in the death of over 1,000 members of Islamic State and questionably claims that no civilians have been killed in UK airstrikes.[77]

Up-to-date figures on the proportion of these strikes that were made by the RAF's MQ9A Reaper drone fleet are not available; however, a tally made in July 2016 from MoD figures revealed that 27% of all RAF airstrikes in Iraq and Syria were by drones (448 drone airstrikes out of a total 1,875 airstrikes).[78] Once surveillance missions are also included, then drones were responsible for 49% of all RAF missions in Iraq and Syria (1,427 drone missions out of a total 2,895 strike and reconnaissance missions).[79] The majority of the RAF's drone missions in the Iraq/Syria theatre are therefore in a reconnaissance and strike-support role, utilising high-definition cameras to locate, identify and track IS assets, with conventional manned aircraft then being deployed for an airstrike.[80]

The RAF's fleet of MQ9A Reapers has performed remarkably well – denying IS fighters sanctuaries, targeting key leaders and providing high-quality surveillance and post-strike imagery. This has been accomplished without direct risk to UK military personnel and at less financial cost and (at least according to the government) fewer civilian casualties than conventional air platforms would have caused. However, opponents of drone warfare have their own assessments. They claim that

[75] https://airwars.org/data/

[76] https://dronewars.net/2016/03/04/500-days-of-british-drone-operations-in-iraq-and-syria/ and https://airwars.org/data/

[77] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/520366/PJHQ_FOI2016_03806___Number_of_enemy_combatants_killed_in_RAF_airstrikes_in_Iraq_from_2014_to_2016.pdf

[78] https://dronewars.net/uk-drone-strike-list-2/

[79] https://dronewars.net/uk-drone-strike-list-2/

[80] https://dronewars.net/uk-drone-strike-list-2/

innocent civilians have been killed during drone strikes on both legitimate targets and in incorrectly-targeted strikes, that drones have alienated allied governments who oppose their use, such as Pakistan, and that using them to kill British and American citizens is illegal.[81]

There is no doubt that drones – or remotely piloted aircraft systems (RPAS) in the MoD's lexicon – are going to increase as a proportion of the RAF's combat fleet and continue to play a significant role in the RAF's combat reconnaissance and ground strike capabilities. While the MQ9A Reapers were initially procured as part of an Urgent Operational Requirement (allowing the MoD to sidestep formal procurement policies, which would have delayed purchase and deployment), the next generation of drones are deep in development, allowing us a detailed forewarning of the shape of warfare in the coming years.

In the near term, the £415 million Protector programme is lined up to replace the Reaper by the end of the decade. This is a medium-altitude, long-endurance (MALE) platform based around the next-generation version of General Atomics' Predator-B/MQ-9 Reaper,[82] fitted with extended wings and a larger fuel tank for greater endurance. The United Kingdom is currently planning to procure 20 Protectors to replace the 10 Reapers currently in service. The United Kingdom has also ordered four QinetiQ/Airbus Zephyr platforms. These are a high-altitude, ultra-endurance aircraft that will loiter at 70,000ft, at the edge of the atmosphere, providing surveillance and communications capabilities. With a planned three-month endurance, the Zephyr will act as a pseudo-satellite, able to be deployed faster and at far-lower cost than conventional satellites.[83]

Longer term, the United Kingdom is developing the £1.5 billion Future Combat Air System (FCAS) to be in service by 2030. This is central to the RAF's desire to have drones make up a third of the combat fleet by that year. This will be a home-grown project, underlining the prolonged development periods for this technology. FCAS is currently expected to be a jet-propelled stealth design based on the BAE Systems Taranis and Dassault nEUROn demonstrators.[84] Other capabilities that have been mentioned include increased autonomy – planning routes, avoiding defences and selecting viable targets without human input – and a possible ability to be integrated into a manned aircraft, possibly to allow for longer-range and/or 'swarm' missions involving multiple drones attacking single targets. Concurrent with these developments, the UK government must improve its policies governing the use of drones – as is being demanded of the United States.[85]

[81] https://www.brookings.edu/articles/why-drones-work-the-case-for-washingtons-weapon-of-choice and https://airwars.org/civilian-casualty-claims/ and https://www.thebureauinvestigates.com/category/projects/drones/drones-graphs/

[82] https://www.contractsfinder.service.gov.uk/Notice/75acf2ae-7f58-4c9f-98d3-2bd7b1828f1b

[83] http://www.janes.com/article/56204/sdsr-2015-uk-prime-minister-confirms-plans-to-field-near-space-uav-likely-zephyr

[84] https://www.flightglobal.com/news/articles/analysis-anglo-french-fcas-feasibility-study-kicks-405711/

[85] http://berkeleytravaux.com/drones-looking-legitimizing-violence-international-law/

The threat of global proliferation of unmanned technology

Experts have long predicted that drone technology will lead to a fundamental transformation in the conduct of warfare, and this appears to be coming to pass with the deployment of (mostly-US) unmanned platforms in operations against terrorist groups around the world. With the palpable advantages of these assets, it was inevitable that the take-up by other countries would be swift. The leading countries have moved on significantly from the early era of short-range reconnaissance drones to long-range strike platforms, but some of the newcomers are catching up. Over 80 countries around the world are now adding drones to their military arsenals,[86] with around 35 owning major systems,[87] though less than that possess weaponised versions (which are limited to the United States, the United Kingdom, France, China, Russia, India, Israel, Pakistan, Iran, Iraq, Nigeria, Somalia and South Africa).[88] Israel has long eclipsed the United States as the world's leading manufacturer of unmanned aircraft, supplying over 60% of the world's needs.[89]

Pakistan, rebuffed by the United States when it looked to obtain armed Predator platforms, quickly developed and unveiled its own Burraq combat drones,[90] which it used to kill three senior militants on 7 September 2015. Analysts assess that these are based on China's CH-3 drone, one of which had previously been obtained by Pakistan. The CH-3 is an all-weather medium-altitude, long-endurance (MALE) drone with an 8 metre wingspan, a range of 2,400 km and a maximum payload of 80 kg.[91] In February 2016, Nigeria announced its first successful combat drone strike, using a drone based on the Chinese CH-3 to target a Boko Haram group.[92]

China is currently actively exporting the CH-4 armed drone, which looks almost identical to the MQ-9 Reaper, with sales across the Middle East.[93] The CH-4 has a range of 5,000 km and an endurance of up to 40 hours, making it a very capable platform (the MQ-9 has an 1,800 km range and 40-hour endurance).[94] Iraq, Saudi Arabia, the United Arab Emirates and Egypt currently use the CH-4, while Jordan has been linked to further purchases.[95]

[86] http://foreignpolicy.com/2013/03/11/the-global-swarm/ and http://securitydata.newamerica.net/world-drones.html

[87] https://www.theguardian.com/news/datablog/2015/mar/16/numbers-behind-worldwide-trade-in-drones-uk-israel

[88] http://fortune.com/2016/02/12/these-countries-have-armed-drones/ and http://securitydata.newamerica.net/world-drones.html

[89] https://www.theguardian.com/news/datablog/2015/mar/16/numbers-behind-worldwide-trade-in-drones-uk-israel

[90] http://thediplomat.com/2016/07/the-consequences-of-global-armed-drone-proliferation/

[91] http://defence-blog.com/news/chinas-armed-ch-3-drone-spotted-in-myanmar.html

[92] http://www.dailysabah.com/africa/2016/02/03/for-the-first-time-nigeria-hits-boko-haram-targets-with-drones

[93] http://www.defensenews.com/story/defense/show-daily/dubai-air-show/2015/11/06/dubai-airshow-china-ucav-drone-market-fighter/74051236/ and http://www.middleeasteye.net/news/china-drones-1492124367

[94] http://www.globalsecurity.org/military/world/china/ch-4.htm

[95] http://thediplomat.com/2016/07/the-consequences-of-global-armed-drone-proliferation/

But it is not just states that are acquiring armed drones. Hezbollah reportedly used one to bomb an al-Nusra base in north-eastern Lebanon in September 2014.[96] Hezbollah claims to manufacturer its own drones, but intelligence agencies have linked the aircraft to Iran, with Iranian support units stationed close by to provide assistance.[97] Islamic State are relative newcomers to armed drones, but are using adapted commercially-available quadcopters to carry small (less than 25 kg) explosive devices.[98] Both Hezbollah and Islamic State also use drone for reconnaissance, as does Hamas. Hamas has released video footage purporting to show a drone fitted with air-to-ground missiles.[99] If true, this would be a significant achievement for a militant group with limited resources and little outside assistance; however, there is no firm evidence that the drones have been used or are even capable of launching the missiles.

The technological genie is out of the metaphorical bottle. But it is important to remember that the level of sophistication of drones varies widely. The drones possessed by the United States, United Kingdom, Israel and other leading players are fast, capable of long-endurance and high-altitude and increasing autonomous and stealthy. At the other end of the spectrum, the small, fragile, line-of-sight and mostly civilian models that Islamic State uses pose little effective offensive threat. Many have sensors that are little more sophisticated than an off-the-shelf camera sending line-of-sight imagery to a laptop. The armed versions are only capable of carrying 'dumb' unguided improvised explosive devices strapped to the underside of the airframe, which requires the drone to hover openly over the target at low altitude.

This comparatively low level of sophistication means that such aircraft are also highly vulnerable to basic countermeasures, including being shot down. If hostile states or non-state actors do acquire more capable drones, they will also need more sophisticated support systems, such as launch and command vehicles, and access to secure communications to control aircraft over longer ranges. If the drone itself becomes difficult to tackle, then this infrastructure can be an alternative target for countermeasures.

United States proposes new multilateral controls on armed drones

The United States has initiated a drive to establish an international control regime on the proliferation and use of armed drones.[100] The US state department drafted a proposal, entitled *Proposed Joint Declaration of Principles for the Export and Subsequent Use of Armed or Strike-Enabled Unmanned Aerial Systems (UAS)*, and presented it to international export control officials at the UN Arms Trade Treaty conference in Geneva in September 2016.

[96] http://edition.cnn.com/2014/09/22/opinion/bergen-schneider-armed-drone-hezbollah/ and https://www.youtube.com/watch?v=mo9yIxiWDnA

[97] http://thediplomat.com/2016/07/the-consequences-of-global-armed-drone-proliferation/

[98] http://www.bloomberg.com/news/articles/2016-07-07/armed-drones-used-by-islamic-state-posing-new-threat-in-iraq

[99] https://theaviationist.com/2014/07/14/ababil-over-israel/

[100] http://www.defensenews.com/articles/us-seeking-global-armed-drone-export-rules

Defense News obtained a copy of the one-page document and confirmed its authenticity with an anonymous state department official; however, the full content of the draft guidelines has not been publicly released. The United States' proposal is known to state five core principles for international norms:

- the applicability of international law and human rights when using armed drones;
- a dedication to follow existing arms control agreements when considering the sale of weaponised unmanned systems;
- that sales of armed drone exports should take into account the recipient country's history regarding adherence to human rights, international obligations and commitments;
- that exporting countries should demonstrate appropriate transparency measures when required; and
- a resolution to continue to ensure these capabilities are transferred and used responsibly by all states.[101]

The United States is pushing for as many countries as possible to sign the draft declaration as part of a two-stage process. Once a viable number of signatories has been obtained, an international working group of the signatories will be created to draw up a voluntary code of conduct for exporting and importing unmanned military vehicles.[102] It is believed that up to 40 countries have now signed the draft declaration, including the United Kingdom, Germany, Italy, the Netherlands, Japan, South Korea and Singapore, with a summit now possible next year to create a standard-setting treaty organisation.[103]

The US state department's efforts follow the release in February of its *US Export Policy for Military Unmanned Aerial Systems*.[104] This policy is limited to drones manufactured by US companies, and was designed to loosen restrictions on exports of armed drones; however, it forms part of the broader US review of unmanned systems. As such, it is likely that the US position in negotiations around achieving consensus on the draft declaration will be consistent with this domestic policy.

This effort is thought to be primarily motivated by concerns in Washington over the rapid proliferation of armed drones in Africa, the Middle East and Asia, many developed from drones originally obtained from China. However, there are other factors possibly involved in this uncharacteristic push for international regulation from a country that is often at odds with similar moves to regulate the international sale and use of military hardware.

[101] http://www.defensenews.com/articles/us-seeking-global-armed-drone-export-rules

[102] http://www.globalresearch.ca/the-globalization-of-drone-warfare-towards-a-us-led-international-control-regime-on-armed-drones/5544813

[103] http://www.bloomberg.com/news/articles/2016-10-05/armed-drone-export-standards-sought-by-u-s-and-dozens-of-allies

[104] http://www.state.gov/r/pa/prs/ps/2015/02/237541.htm

One possible reason is Barack Obama's desire for a positive legacy at the end of a presidency that has suffered from the repeated blocking of flagship legislation by a hostile Congress. The United States may also be seeking to deflect some of the criticism it has received over the years for its widespread use of armed drones in targeted killings around the world. Another consideration is that the US arms industry has been restricted by the country's membership of the Missile Technology Control Regime (MCTR), a multilateral agreement of 35 countries established in 1987 to control the proliferation of unmanned delivery systems; however, many significant states are not signatories, including China and Israel.[105] The proposed joint declaration would go some way to levelling the playing field and apply restrictions across the global marketplace.[106]

However, it is highly unlikely that all the major drone-producing countries will sign up to the United States' new initiative. Russia and China will be unenthusiastic about restricting lucrative sales that also play a significant role in solidifying military alliances. Israel, the world's leading manufacturer, has also shown some hesitation over signing the declaration, believing any restrictions could not be effectively enforced, would have a sizeable impact on its own exports, and may weaken the war on terror by restricting the use of what it considers a highly-effective tool.[107] Furthermore, with Iran also unlikely to sign the declaration, the supply of drones to Hezbollah for it to use in its ongoing conflict with Israel will continue unhindered.

Campaign groups may also need convincing that the United States is genuinely interested in developing and implementing controls and are not just seeking to hamstring competition in this profitable and rapidly-developing field. Campaigners also fear that the language of the final joint declaration will fall substantially short of what is necessary and will end up being only a shallow layer of regulation that will be regularly breached with minimal sanction.

[105] http://truepublica.org.uk/global/us-wants-restrict-international-use-drones-loses-market-share/

[106] http://www.globalresearch.ca/the-globalization-of-drone-warfare-towards-a-us-led-international-control-regime-on-armed-drones/5544813

[107] http://www.defensenews.com/articles/israel-wary-of-us-armed-drone-initiative, http://www.defensenews.com/articles/experts-question-new-armed-drone-export-policy and http://www.defensenews.com/articles/us-seeking-global-armed-drone-export-rules

Section IV

Cyber conflict

NATO members prepare for increase in cyber campaigns against critical infrastructure

NATO's designation of cyberspace as an operational domain and inclusion of cyber-attacks in Article 5 at the Warsaw Summit on 8 July is the culmination of increasing concerns over offensive cyber operations against Western critical infrastructure.[108] Since the December 2015 cyber intrusion on Ukraine's electricity distribution network, which disrupted power to approximately 80,000 customers, a number of NATO members have expressed concern over the potential for an increase in the frequency and scope of cyber operations against critical infrastructure.[109]

The US intelligence community's 2016 worldwide threat assessment ranked cyber-attacks as the highest threat to US security and identified Russia, Iran, China and North Korea as leading threat actors.[110] The key US concern is likely to be that the United States and its allies may face significant disruption to critical infrastructure. In response to the general heightened awareness of cyber risks, bills have been put before the US Congress that grant the energy secretary emergency powers to take control of the country's power grid in the event of a cyber-attack. In March 2016, the US and UK governments announced that mock cyber-attack exercises against nuclear power plants[111] would be carried out to improve emergency readiness and cyber security.[112]

While a particular threat actor was not identified as the catalyst for NATO's new policy, the comment at a 14 June press conference from the alliance's secretary general, Jen Stoltenberg, that it is hard to imagine conventional military attacks without blended cyber tactics is possibly a reference to Russia's hybrid warfare.[113] Russia-based hackers have been linked to a number of cyber-attacks, including against a French television network,[114] a Kiev airport,[115] a German steelmaker,[116]

[108] http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf and https://ccdcoe.org/sites/default/files/multimedia/pdf/NATO%20CCD%20COE%20policy%20paper.pdf

[109] http://www.huffingtonpost.com/daniel-wagner/the-growing-threat-of-cyb_b_10114374.html

[110] http://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf

[111] http://ntiindex.org/news-items/beyond-technology-addressing-nuclear-cyber-threat/ and http://www.ntiindex.org/wpcontent/uploads/2013/12/NTI_2016-Index_FINAL.pdf

[112] http://www.theguardian.com/uk-news/2016/mar/31/uk-us-simulate-cyber-attack-nuclear-plants-test-resilience

[113] http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en

[114] http://www.bbc.com/news/technology-37590375

the Polish stock market[117] and, more recently, the Dutch Safety Board,[118] the NSA[119] and the Democratic National Committee[120]. In contrast to other cyber threat actors, Russian cyber operations appear more focused on intelligence-gathering and reconnaissance of critical infrastructure networks rather than on commercially-orientated cyber espionage or network disruption.[121] These cyber operations are occurring at a time of increased Russian military activities and mobilisation.

NATO's designation of cyberspace as an operational domain means that member states that are subject to major cyber-attacks can invoke Article 5, the alliance's collective defence clause. The move is likely intended to be a deterrence signal to Russia, and as such is a shift from the status quo, in which alleged Russian state and non-state threat actors have not faced sanctions or indictments for their various cyber operations. However, the threshold at which cyber-attacks on critical infrastructure would trigger Article 5 remains unclear, and this ambiguity limits the intended deterrence effect. British and American politicians have raised questions over defining cyber acts of war,[122] but in both cases the response has been evasive or limited to suggesting that a cyber-attack is an act of war if the consequences are essentially the same as those of a conventional kinetic attack.

Furthermore, NATO's move to collective defence in the face of major cyber-attack may prompt Russia to centralise significant or high-risk cyber operations within state apparatuses. Centralisation may result in a smaller number of larger, more-professional attacks rather than a multitude of lower-intensity scale attacks carried out with the involvement of Russian organised crime networks and completed with the knowledge or endorsement of state institutions. Although the latter provides a greater degree of deniability, both the sophistication required for and the possible ramifications of cyber attacks against a more-alert NATO alliance suggests a move towards centralisation is likely.

[115] http://www.reuters.com/article/us-ukraine-cybersecurity-malware-idUSKCN0UW0R0

[116] http://www.bbc.com/news/technology-30575104

[117] http://thehill.com/policy/cybersecurity/221806-hackers-breach-the-warsaw-stock-exchange

[118] http://www.nltimes.nl/2016/06/10/report-russia-behind-cyberattacks-mh17-investigation-team/

[119] http://www.ibtimes.co.uk/cyberwar-begins-us-believed-hack-back-russia-following-democratic-party-email-leaks-1573640

[120] http://www.ibtimes.co.uk/cyberwar-begins-us-believed-hack-back-russia-following-democratic-party-email-leaks-1573640

[121] http://www.defenseone.com/ideas/2016/06/west-must-respond-russias-increasing-cyber-aggression/129090/

[122] http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2016-05-18/37120 and http://www.wsj.com/articles/defining-a-cyber-act-of-war-1462738124

In addition to cyber defence collaboration within NATO, the UK government announced a new cyber security strategy and the establishment of the National Cyber Security Centre (NCSC) in May 2016.[123] It is expected that the NCSC will build on the expertise of the Centre for the Protection of National Infrastructure, CERT UK (the national computer emergency response team), the Centre for Cyber Assessment based at GCHQ and GCHQ's information security arm, CESG. A month earlier, the UK Ministry of Defence announced the establishment of the Cyber Security Operations Centre (CSOC) to lead defensive cyber operations and secure defence networks against cyber threats.[124] CSOC will primarily focus on military networks, whereas the civilian National Cyber Security Centre will support cyber security for both public and private institutions.

Despite advancing cyber offensive capabilities and the rising risks of cyber miscalculation there is limited diplomatic rapprochement between perceived adversaries. US and Russian cyber security officials met in Geneva, Switzerland, in mid-April 2016 to review and discuss confidence-building measure (CBM) agreements signed by the two countries in 2013.[125] However, US officials emphasised that the latest talks were not a resumption of the US-Russia Bilateral Presidential Commission working group on cyber issues, which had been suspended, along with the rest of the commission's activities, following Russia's annexation of Crimea.[126]

US Cyber Command pitched as force multiplier in counterterrorism operations

In March 2016, the US defence secretary, Ash Carter, took the unprecedented step of announcing at the RSA Conference in San Francisco that US Cyber Command (CYBERCOM) was undertaking operations against Islamic State.[127] The following month, the US deputy defence secretary, Robert Work, suggested that the United States was dropping 'cyber bombs' on the jihadist group.[128] CYBERCOM's operations against Islamic State have allowed the US administration to claim that a full spectrum counterterrorism operation has been launched against the jihadist group without committing additional 'boots on the ground'. However, the openness with which the US administration acknowledges the cyber operations against Islamic State stands in stark contrast to other cyber operations against, for example, Iran and North Korea, which begs the question of whether cyber operations are actually functioning as a force multiplier or if the announcement is more about shoring up support for the Obama administration's light-footprint SOF-led doctrine.

[123] https://www.gov.uk/government/publications/national-cyber-security-centre-prospectus

[124] https://www.gov.uk/government/news/defence-secretary-announces-40m-cyber-security-operations-centre

[125] https://southfront.org/us-and-russia-meet-on-cybersecurity-in-geneva/

[126] https://southfront.org/us-and-russia-meet-on-cybersecurity-in-geneva/

[127] http://www.baltimoresun.com/news/maryland/bs-md-secret-cyber-campaign-20160306-story.html

[128] http://www.reuters.com/article/us-mideast-crisis-usa-idUSKCN0X92A6

The US administration has provided only minimal details on the nature of the CYBERCOM offensives against Islamic State, generally focusing on overall strategic objectives. The message from military and government officials is that CYBERCOM is disrupting Islamic State's command and control capability by degrading and compromising information and communications technology (ICT) infrastructure and networks. Islamic State's command structures and social networks are likely to be significantly disrupted by CYBERCOM's attempts to block its use of encrypted communications, which will force militants onto less-secure communication channels or to use human couriers. Spear phishing and watering hole attacks that implant malicious code on IS networks would possibly provide new intelligence sources and interrupt the financial transactions used to pay IS fighters and receive income. Indeed, the US defence secretary's advocacy for splitting CYBERCOM and its functions from the NSA and its functions – offensive cyber operations from intelligence – could be interpreted as a strong sign of CYBERCOM's success against Islamic State.[129]

The cyber strategy against Islamic State is broadly consistent with the special operations forces strategy, which seeks to disrupt organisational functions by attacking key nodes in the network or hierarchy. The disruption impacts and intelligence dividends from cyber operations could in some cases mirror the results of kill/capture missions. However, it would appear that the United States is using cyber offensives as a force multiplier rather than a substitute for kinetic operations. For example, degrading Islamic State's trust in its communication networks and isolating it in Mosul was most likely intended to lay the foundations for kinetic offensives to recapture the city. Another possible scenario is that CYBERCOM could issue falsified commands to IS militants that would redirect them to areas of the battlefield vulnerable to attack by airstrikes or local ground forces.

What is not explicitly discussed in relation to CYBERCOM's offensives are the proliferation risks and threats to existing intelligence sources. The White House's national security adviser, Susan Rice, hinted at tensions between the NSA and CYBERCOM over the potential for cyber offensives to compromise surveillance assets, despite the two organisations sharing the same head, Admiral Michael Rogers.[130] The potential compromise comes from the use of particular attack vectors or entry points for cyber offensives that would likely highlight network vulnerabilities used for surveillance access.[131]

Similarly, cyber offensives against a non-state actor risks provoking an evolution in countermeasures, which may be transferred to other US cyber adversaries, such as Iran, who have significant cyber offence arsenals. The United States' cyber offensive against Islamic State may also influence its cyber diplomacy and norm-building efforts, with the campaign against IS building precedent.

[129] https://techcrunch.com/2016/09/13/ashton-carter-talks-equation-group-hack-encryption-debate-and-military-innovation-at-disrupt-sf/

[130] http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?_r=0

[131] http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?_r=0

The US Institute for Critical Infrastructure Technology released a report in June 2016 suggesting that Islamic State does not possess significant cyber capabilities on a par with more sophisticated state and non-state actors and is probably only positioned to launch very low-intensity and unsophisticated cyber-attacks.[132] However, the report argues that the group appears to have ambition to procure external cyber capabilities from the dark web to support its information warfare strategies. In addition, there is a high level of uncertainty as to how Islamic State may respond to losing territory in Iraq and Syria and whether a 'cyber caliphate' could arise to direct global jihadist networks from the cyber realm. The uptick in recent lone wolf attacks may give Islamic State cause to consider how more-sophisticated online communities could preserve or translate its lost physical territory and networks into a purely online socio-religious network, rending interdiction and disaggregation of the global jihadist movement challenging.

North Korean cyber incursions against South Korea template for asymmetrical operations against advanced, ICT-dependent adversaries

As political and military tensions have continued to rise between North and South Korea under Kim Jong-un's leadership of the North, South Korea's public and private sector ICT networks and infrastructure have been subjected to repeated and persistent cyber offensives allegedly launched by their northern neighbour. North Korea has completed multiple tests of nuclear bombs and long-range ballistic missiles and flown surveillance drones across central and western regions of the demilitarised zone between the two countries.[133] South Korea has responded with special operations forces training exercises with the United States (Key Resolve and Foal Eagle), which also flew two B-1B bombers with fighter escorts over South Korea on 13 September. Below the surface of these shows of kinetic force, North Korea has launched a multipronged and staged cyber campaign.

In March 2016, South Korea's National Intelligence Service told a parliamentary committee that North Korean intelligence agencies had launched a cyber offensive against critical infrastructure companies, key government agencies and major financial institutions in the South.[134] The following month, Seoul accused Bureau 121, North Korea's cyberwarfare agency within its Reconnaissance General Bureau, of trying to hack Hanjin Heavy Industries & Construction Co, an attack likely aimed at understanding South Korea's rapid amphibious special operations forces resources.[135]

[132] http://icitech.org/wp-content/uploads/2016/06/ICIT-Brief-The-Anatomy-of-Cyber-Jihad1.pdf

[133] http://thediplomat.com/2015/09/north-korea-flew-a-spy-drone-across-the-dmz/

[134] http://www.usnews.com/news/world/articles/2016-03-11/seoul-number-of-north-korean-cyberattacks-doubles

[135] http://securityaffairs.co/wordpress/47202/cyber-warfare-2/north-korea-defense-contractor.html

On 13 June, the cyber division of South Korea's National Police Agency released information about a large-scale cyber operation that had compromised over 140,000 computers across 160 government institutions and private sector companies.[136] The campaign was likely in preparation for a hybrid large-scale cyber-attack designed to cause cascading ICT failure across critical infrastructure in conjunction with cyber espionage actions.[137] Defence companies were significant targets of the preparatory operation, and there are suspicions that sensitive documents on the F-15 fighter jet were accessed in the attacks.[138]

North Korea is likely to continue low-intensity cyber disruption operations and increasingly coordinate them with other activities, such as military exercises, missile tests and diplomatic provocations.

The broader implications of North Korea's alleged persistent cyber operation are that elements of its cyber tactics and strategy may inform the cyber doctrines of emerging cyber powers. A number of potentially-hostile cyber powers, such as Russia, China and Iran, have cooperated with North Korea in cyber training exercises and educational exchanges, and are likely to have played some role in developing the capabilities of Pyongyang's estimated 6,000-strong cyber army.[139] North Korea's lower-intensity cyber operations against South Korea may form part of a proving or testing ground for asymmetrical cyber operations that will be useful to those other cyber powers.

The dynamics of the tensions on the Korean Peninsula provide an ideal environment for examining how a country with less conventional military power, limited economic dependence on ICT and networked infrastructure and experience in asymmetrical operations can degrade the capabilities or expose the vulnerabilities of a militarily-superior adversary with a high level of economic and social dependence on advanced ICT infrastructure. To this extent, the cyber conflict between North and South Korea is the canary in the coalmine in terms of emerging cyber doctrine and operations.

Multinational professional services company Deloitte highlighted this archetypal dynamic in their report *Asia-Pacific Defence Outlook 2016*.[140] Countries with comparatively lower levels of dependency on internet-based interactions and connectivity to drive domestic economies and productivity will have greater incentives to develop low entry-cost offensive cyber capabilities that target the e-commerce, highly-connected infrastructure and knowledge sectors of advanced economies. Challenges in attributing attacks will continue to give cyber offensives the additional benefit of plausible deniability. In extremis, the costs to those advanced economies targeted by advanced persistent threat (APT) cyber offensives – whether loss of competitive advantage, economic disruption or physical damage to infrastructure – may even trigger strategic retreats from digital dependence or technological regression as a lesser of two evils.[141]

[136] http://www.reuters.com/article/us-northkorea-southkorea-cyber-idUSKCN0YZ0BE

[137] http://www.reuters.com/article/us-northkorea-southkorea-cyber-idUSKCN0YZ0BE

[138] http://www.thedailybeast.com/articles/2016/06/17/north-korea-steals-u-s-fighter-blueprints.html

[139] https://jsis.washington.edu/news/north-korea-cyber-attacks-new-asymmetrical-military-strategy/

[140] http://www2.deloitte.com/sg/en/pages/public-sector/articles/deloitte-2016-asia-pacific-defense-outlook.html

[141] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2790630

This cyber conflict dynamic exists beyond the Korean Peninsula and could equally apply to other existing conflict theatres. Acquiring cyber capabilities that expose the vulnerabilities of economically and technologically advanced adversaries with low entry costs and limited probability of successful attribution will be an attractive proposition for other countries with a low dependency on ICT, comparatively limited conventional military power and weak regulatory and institutional environments, such as countries in Central America, sub-Sahara Africa and Southeast Asia.

The expansion of this dynamic would have significant implications for the effectiveness of sanctions regimes. While advanced ICT countries can employ sanctions on export-orientated activities focused on natural resources, manufacturing and physical goods, cyber-attacks on the financial systems of those countries imposing sanctions could offset these losses. The alleged involvement of Pyongyang in recent cyber heists related to the SWIFT interbank payment system may suggest the use of cyber operations to counter sanctions.[142] This has also been the case where US sanctions against Iran inspired and generated a campaign of attacks on US financial institutions in 2012 and 2013 with the intention of dissuading the US administration from extending sanctions.[143]

[142] http://money.cnn.com/2016/05/26/technology/swift-bank-hack-philippines-lazarus/

[143] http://www.reuters.com/article/us-usa-iran-cyber-idUSKCN0WQ1JF

Section V

Intelligence, surveillance and reconnaissance

Future-proofing the United Kingdom's Investigatory Powers Bill

In August, the independent reviewer of terrorism legislation in the United Kingdom, David Anderson QC, concluded that the proposed laws included in the Investigatory Powers Bill that give Britain's intelligence agencies the power to gather large volumes of data from members of the public had a 'clear operational purpose'.[144] In his review, Anderson concluded that bulk interception is of 'vital utility' to the security services and that alternative methods did not provide the same results. He also claimed that data collection is important for a range of intelligence operations, including counter-terrorism, counter-espionage and counter-proliferation, and that there are likely to be cases where no 'effective alternative is available'.[145]

Anderson's findings were welcomed by the prime minister, Theresa May, who had championed the Bill while home secretary, but prompted concerns from opposition parties and privacy campaigners, who have described it as a 'snooper's charter'. Labour MPs want to know why several key recommendations in Anderson's review, including the creation of an advisory panel on technology, tougher restrictions on the use of internet connection records (ICRs) and stronger protections for journalists and lawyers, were not accepted by the UK government.[146]

The human rights organisation Liberty argued that the review had not convincingly supported the government's position that bulk surveillance powers were required. It concluded that the review amounted to little more than a 'trust your government' attitude at a time when public confidence in government transparency is low following the finding of the Iraq Inquiry that Tony Blair's government had exaggerated intelligence in the lead up to the invasion and occupation of Iraq in 2003.[147]

[144] https://www.gov.uk/government/publications/investigatory-powers-bill-bulk-powers-review and https://www.theguardian.com/world/2016/aug/19/bulk-data-collection-vital-to-prevent-terrorism-in-uk-report-finds

[145] Ibid.

[146] https://www.theguardian.com/world/2016/aug/19/bulk-data-collection-vital-to-prevent-terrorism-in-uk-report-finds

[147] https://www.theguardian.com/world/2016/aug/19/bulk-data-collection-vital-to-prevent-terrorism-in-uk-report-finds

The Investigatory Powers Bill is currently at the report stage in the House of Lords, having already passed through the House of Commons in June 2015.[148] If passed, it would require telecommunication service providers to retain and handover to UK law enforcement and intelligence agencies communications data – including for the first time internet connection records – that reveal which websites internet users have visited, though it would not detail the pages on those websites that were viewed. The Bill also sets out new rules to govern the interception of communications and the use of 'equipment interference' powers (or hacking). It also outlines the qualified right of UK intelligence agencies to obtain bulk personal datasets for national security reasons under warrants that would be issued by government ministers.

In July, the House of Lords tabled amendments to the Bill that provide further safeguards on the gathering of ICRs, ensuring that they are only obtained by the security services for offences that are sufficiently serious that an offender can be sentenced to at least six months' imprisonment.[149]

Given the highly-fraught path of this Bill through parliament and the dynamic nature of counter-terrorism efforts (particularly in the cyber and mass surveillance spheres), it is essential that the final version of the legislation that eventually makes it onto the statute books is future-proof. This is not an easy task, as it involves convincing legislators and the electorate that powers that are not necessary now may become extremely useful in the future as the strategies of different terrorist groups evolve over time. For example, as terrorist groups develop and improve their encryption capabilities, intelligence agencies will have to rely more heavily on metadata as they seek to exploit as much as possible from the available communications data. If such future-proofing is not included within the Bill, the final Act could quickly become obsolete, necessitating another drawn-out process to push amendments through parliament. However, attempts to future-proof the legislation must also respect the need for individual privacy.

In an attempt to address concerns over future-proofing, the government has included provision for review of the Act after five and a half years and has also taken more care to avoiding overly abstract drafting. Future-proofing is extremely important, but as the Investigatory Powers Bill continues its path through parliament, it is essential that the need to future-proof the legislation does not grant the government sweeping powers and is balanced with the rights of the individual to privacy.

[148] http://services.parliament.uk/bills/2015-16/investigatorypowers.html

[149] http://www.out-law.com/en/articles/2016/july/restrictions-on-access-to-internet-connection-records-agreed-by-uk-peers/

Terrorist networks melding modern encrypted communications with traditional tradecraft to elude surveillance

The landscape of international communications has changed immeasurably in the last 30 years. As always, the fruits of this technological development can be used for good or ill, and global terrorist organisations have greatly benefitted from the improved command and control, fundraising and recruitment links that have brought their networks closer together. Indeed, it could be argued that cohesive global terrorist networks have only been able to truly develop in the electronic communications age. The ability of groups to spread their propaganda was greatly limited before the internet. Today, jihadists can record footage on a mobile phone in Syria, Iraq, Yemen or Libya and post it on a closed internet forum or open social media platform within minutes, reaching thousands of followers and inspiring potential new recruits.

Combined with the much-treasured social norms of civil rights, especially around freedom of speech, freedom of religion and privacy from state surveillance, terrorist networks have considerable freedom of communications. This combination of terrorists and law-abiding citizens sharing the same communications networks has led to a significant minefield for law enforcement and intelligence agencies to navigate as they attempt to protect democratic principles while conducting effective security operations.

One of the most significant developments across Western counter-terrorist operations in the past several years has been in the expansion of technical capabilities to monitor communications between suspects. However, these have still not kept pace with the resultant countermeasures and tactical evolution by terrorist groups.[150]

In the period leading up to the IS attacks in Paris on 13 November 2015, Western intelligence agencies believed the leader of the attack, Abdelhamid Abaaoud, was in northern Syria being tracked using phone geolocation data and other electronic sources.[151] In fact, Abaaoud had slipped through the surveillance net and made his way to Paris. It is now believed that elements within Islamic State were aware of the West's surveillance techniques and manipulated the data and used false social media accounts to provide cover for Abaaoud and his group as they crossed Europe. As in all conflict, terrorist groups and others engaged in irregular and unconventional warfare will always attempt to turn an adversary's strengths against them. In this case, Western intelligence agencies were over confident in their electronic communications surveillance capabilities and lost sight of the basics of tradecraft.[152]

[150] http://foreignpolicyblogs.com/2016/08/29/law-enforcement-modern-counterterrorism/

[151] http://www.wsj.com/articles/new-tricks-make-isis-once-easily-tracked-a-sophisticated-opponent-1473613106

[152] http://www.wsj.com/articles/new-tricks-make-isis-once-easily-tracked-a-sophisticated-opponent-1473613106

Terrorist organisations, such as Islamic State, are rapidly evolving to counter the West's superior surveillance capabilities. Until relatively recently, terrorists and their supporters communicated via mobile phones and social media accounts that were easily monitored by the authorities; however, terrorist networks have evolved their approach into a complex mix of encrypted electronic communications using chat apps, such as WhatsApp and Telegram, combined with prolonged periods of silence and old-fashioned face-to-face meetings and written notes couriered by person.[153] Groups will also engage in misdirection, creating noticeable activity to pull intelligence agencies' focus away from other actions elsewhere.[154] Attackers are also communicating sparingly with commanders and operating more autonomously as the attack day approaches in order to reduce their exposure to possible surveillance.

In May, the head of the French General Directorate for Internal Security, Patrick Calvar, told French parliament investigators that Islamic State has studied Western intelligence techniques and learnt from experienced Jihadists and veterans of the Iraqi armed forces.[155] Islamic State and its sympathisers have posted numerous guides online to provide jihadists with instructions in high- and low-tech methods to thwart surveillance. These include regularly switching mobile phones, signing up for online accounts using temporary phone numbers, switching frequently between chat apps and using throwaway codes in communications.[156] Islamic State further tightened its security following repeated airstrikes by the US-led coalition on its forces in Syria and Iraq. According to documents seized by US special operations forces, the organisation banned the use of GPS devices by its fighters in order to avoid coalition forces detecting and using the data to track the movements of specific individuals and groups.[157]

Intelligence agencies are increasingly concerned that the so-called 'flash to bang' ratio – between the moment that counter-terrorism officials detect a plot and the time that an attack is launched – has dangerously shrunk. This is in part because the online radicalisation of 'lone wolf' attackers is nearly impossible to detect, but also because the intelligence community is forever struggling to intercept encrypted directions between the Islamic State leadership and the rest of its network.[158] By melding modern communication technologies with traditional tradecraft, Islamic State and the like are making intelligence agencies' jobs even harder. Of course, in the cat-and-mouse world of counter-terrorism, Western intelligence and law enforcement agencies are also adapting their tactics and pushing the technological boundaries in order to adapt to Islamic State's surveillance countermeasures.

[153] http://www.ibtimes.co.uk/paris-terrorists-used-whatsapp-telegram-plot-attacks-according-investigators-1533880 and http://dailycaller.com/2016/09/12/isis-controlling-low-level-terrorists-from-afar-to-potentially-distract-from-larger-plot/

[154] http://www.wsj.com/articles/new-tricks-make-isis-once-easily-tracked-a-sophisticated-opponent-1473613106 and http://dailycaller.com/2016/09/12/isis-controlling-low-level-terrorists-from-afar-to-potentially-distract-from-larger-plot/

[155] http://www.wsj.com/articles/new-tricks-make-isis-once-easily-tracked-a-sophisticated-opponent-1473613106

[156] http://www.wsj.com/articles/new-tricks-make-isis-once-easily-tracked-a-sophisticated-opponent-1473613106

[157] http://www.wsj.com/articles/new-tricks-make-isis-once-easily-tracked-a-sophisticated-opponent-1473613106

[158] http://jewishnews.com/2016/09/12/the-terrorist-threat-has-evolved/

The potential impact of Brexit on UK and European intelligence sharing

On 23 June, the United Kingdom narrowly voted to leave the European Union in a deeply divisive referendum.[159] When the British government takes the country out of the EU ('Brexit'), among the many serious economic and security consequences will be the potential loss of the intelligence-sharing benefits that the United Kingdom both gains from and brings to the union.

As a member of the European Union, the United Kingdom is currently part of a complex law enforcement, intelligence and defence partnership – sharing intelligence, manpower and procurement on a wide variety of multilateral projects and initiatives. Much of this work is facilitated through the EU's law enforcement agency, Europol, and its constituent European Counter Terrorism Centre (ECTC). Europol enables the sharing of intelligence on terrorists and other criminals across jurisdictions and assists in the pan-European investigation and analysis of serious crime. For example, the agency made 60 officers available to investigate the attacks in Paris in November 2015.[160] One of the ECTC's goals is to tackle the related threats of jihadist propaganda and foreign fighters, both of which are major threats to the United Kingdom, as over 800 British citizens have so far thought to have travelled to Iraq and Syria to fight for Islamic State and al-Nusra Front.[161] The United Kingdom is a major participant in European intelligence and law enforcement cooperation and uses Europol more than almost any other country,[162] with UK agencies involved in approximately 40% of Europol cases.[163]

The UK International Crime Bureau within the National Crime Agency (NCA) provides the UK Europol National Unit and is the UK Central Authority for European Arrest Warrants (EAWs). European Arrest Warrants require another member state to arrest and transfer a criminal suspect to the issuing state. They were used by the NCA and its predecessors 1,424 times between 2010 and 2015, including 10 requests related to terrorism, 11 related to human trafficking and 232 related to drug trafficking.[164]

[159] https://infacts.org/sin-bin/ and https://infacts.org/category/ins-sins/

[160] https://www.europol.europa.eu/content/ectc

[161] http://www.bbc.co.uk/news/uk-32026985 and https://www.mi5.gov.uk/news/director-general-speaks-on-terrorism-technology-and-oversight

[162] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521926/The_UK_s_cooperation_with_the_EU_on_justice_and_home_affairs__and_on_foreign_policy_and_security_issues.pdf

[163] http://www.politico.eu/article/europol-first-in-line-for-life-after-brexitvb-law-enforcement-rob-wainwright/ and https://www.quilliamfoundation.org/wp/wp-content/uploads/2016/05/The-EU-and-Terrorism_Maajid-Nawaz-and-Julia-Ebner.pdf

[164] http://www.nationalcrimeagency.gov.uk/publications/european-arrest-warrant-statistics/wanted-by-the-uk-european-arrest-warrant-statistics/690-wanted-by-the-uk-european-arrest-warrant-statistics-2009-may-2016-calendar-year

It is possible that the 916 arrests that occurred between 2010 and 2015 in response to British EAW requests would not have happened in a timely manner if the United Kingdom was not in the EU and therefore unable to use the European Arrest Warrant system. For example, the British police were able to extradite the 21/7 suspect Hussain Osman from Italy in only eight weeks using the EAW system as opposed to the average 10 months it takes from non-EU countries.[165] This significantly aided the authorities' investigation into the terrorist threat facing the United Kingdom at that time.

Membership of the EU also gives the United Kingdom access to data-sharing mechanisms that are of significant assistance to British law enforcement and intelligence agencies. These include the Visa Information System (VIS), which collects information from consulates in non-EU countries and external border crossing points; the Schengen Information System (SIS II), which allows police and border guards to enter and consult alerts on wanted or missing persons (the National Crime Agency is the UK SIRENE Bureau for SIS II); and EURODAC, which is a fingerprint database for identifying asylum seekers and irregular border-crossers. The EU also facilitates the sharing of criminal records across all member states. Lastly, the Prüm Convention, which the United Kingdom has now opted in to, facilitates the exchange of DNA, fingerprint and vehicle registration data of suspects. It takes up to 143 days to gain access to DNA profiles via Interpol; the Prüm Convention grants access within 15 minutes.[166]

There is also a myriad of small ad-hoc bi-lateral and multi-lateral agreements set up for individual law enforcement investigations and intelligence operations, in processes greatly eased by the parties all being EU members. If the United Kingdom leaves the European Union it will have to reconfigure its national security machine, scoping out new bilateral agreements with the key EU members, which will be costly, time consuming and, potentially, less effective. A weakened Europe and an isolated United Kingdom is a dangerous prospect.

Although the EU is not a military alliance per se, the European Union Military Staff (EUMS) does operate European Union Force (EUFOR) rapid reaction forces as part of the Common Security and Defence Policy. EUFOR has supervised operations in Macedonia, Bosnia and Herzegovina, the Democratic Republic of the Congo, Chad and the Central African Republic. The United Kingdom has contributed to several of these missions. The United Kingdom has also contributed to the stand-by EU battlegroups, which can be deployed within 10 days to carry out military tasks of a humanitarian, peacekeeping and peacemaking nature for up to 30 days or longer if resupplied.[167] Britain is also party to the European Air Group (EAG), the Movement Coordination Centre Europe (MCCE) and the European Amphibious Initiative (EAI) and benefits from the security of supply ensured by the European Defence Agency (EDA).[168] If it chose to, the United Kingdom could also cooperate as part of the European Corps (Eurocorp), European Gendarmerie Force (EUROGENDFOR), European Maritime Force (EUROMARFOR) and European Air Transport Command (EATC), extending the security benefits of EU membership even further.

[165] http://infacts.org/briefings/european-arrest-warrant-pros-outweigh-cons/

[166] https://www.gov.uk/government/news/government-sets-out-case-for-joining-prum

[167] https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/esdp/91624.pdf

[168] http://www.openbriefing.org/thinktank/publications/the-united-kingdom-needs-the-eu-not-nato-to-ensure-its-security/

Despite all this, the military force that matters most in Europe is the US-led NATO alliance. It is the same in the intelligence world: the alliance that matters most is Five Eyes (FVEY), the long-standing and wide-ranging intelligence network consisting of the United Kingdom, the United States, Australia, New Zealand and Canada. This evolved out of the close ties between Britain and the United States during and after the second world war, and now sees the five countries working hand in glove, closely sharing signals intelligence with each other. Other European countries rely on the United Kingdom sharing at least some of this intelligence, and the need for Britain to occasionally share such intelligence with its EU partners is understood by the other Five Eyes members. If the United Kingdom leaves the EU, then such sharing may no longer be tolerated by the Five Eyes members, and the union's security and intelligence infrastructure would almost certainly be significantly weakened.[169]

The flip side to this is that as a member of the EU the United Kingdom is subject to strict rules on the transfer of private data from EU to non-EU countries, such as the United States and the other members of Five Eyes. Brexit is the new – uncertain – factor in this dynamic. If the United Kingdom is not going to be part of the EU, then upcoming European reforms of data protection laws would no longer directly apply to the United Kingdom, which will be able to more openly share 'unsanitised' data with its Five Eyes partners. However, if the British government decides in the end that it wants to remain part of the European single market, which is seen by most in parliament and industry as vital to the country's economy, it may have to prove 'adequacy' by committing to keep British data protection standards equal to the EU's General Data Protection Regulations.[170]

[169] http://www.aspistrategist.org.au/brexit-security-sleeper-issue/

[170] https://www.openrightsgroup.org/blog/2016/what-does-brexit-mean-for-the-ip-bill

open briefing
the civil society intelligence agency

Open Briefing
The Workbox
4th Floor, PZ360
St Mary's Terrace
Penzance
Cornwall TR18 4DZ
United Kingdom

t +44 (0)1736 800 767
info@openbriefing.org
www.openbriefing.org

Certified Member of Social Enterprise UK.
Company number 07649656. Registered in England and Wales.
VAT Reg. No. 247 9028 83.