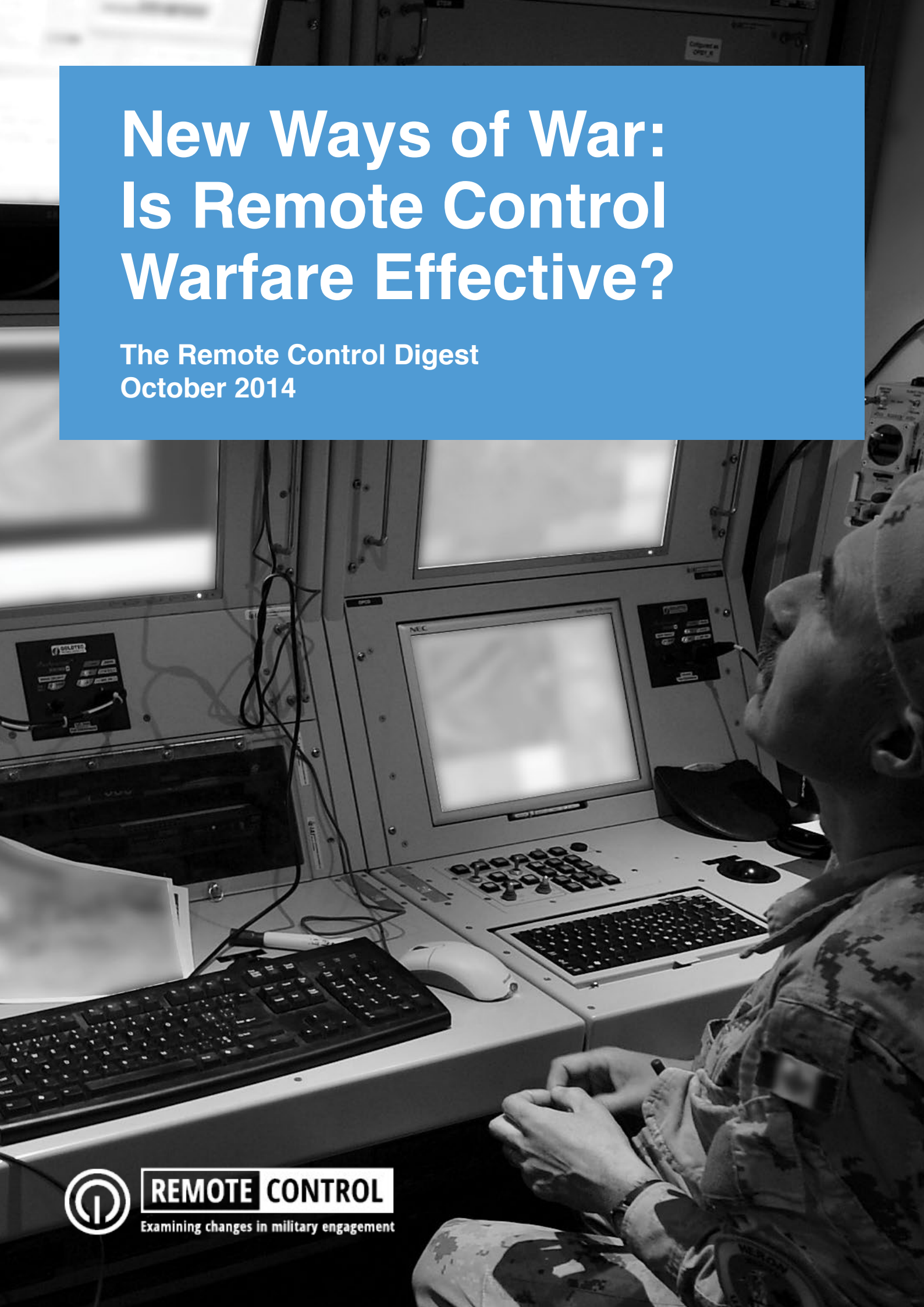
# New Ways of War: Is Remote Control Warfare Effective?

**The Remote Control Digest**
**October 2014**



REMOTE CONTROL
Examining changes in military engagement

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

# About this Digest

The last decade has seen significant developments in military technology and a rapid re-thinking of military approaches to future threats. One dominant idea now is countering threats at a distance without the deployment of large military forces, what may be termed ‘Remote Control’. This is already happening, with a heavy reliance on drones (both reconnaissance and armed variants) and a marked increase in the use of special operations forces (SOF) and private military and security companies (PMSCs). Used extensively by the United States, they are becoming much more significant in other countries too. This trend is paralleled by an increase in cyber activities, and intelligence and surveillance methods. The origins of remote warfare can be traced politically to problems that arose at the outset of what was coined as the ‘war on terror’, combined with major developments in military technology, in particular the development of armed drones, in the last decade.

The Remote Control Project, a project of the Network for Social Change hosted by Oxford Research Group, was set up to examine and challenge the long-term effects and implications of these new ways of warfare which take place ‘behind the scenes’ rather than being conducted on a traditional battlefield.

This digest compiles our first set of reports commissioned through investigative journalists, academics, think tanks and specialist research agencies, to delve deeper into the subject and examine the real impact these methods of warfare are having. It seeks to answer the question: “is remote control warfare effective in solving security problems?”

# Contributors

**Open Briefing** is the world's first civil society intelligence agency. It is a unique not-for-profit social enterprise that provides intelligence and research services to civil society organisations and concerned citizens.

**The Bureau of Investigative Journalism** is an independent not-for-profit organisation. The Bureau pursues journalism which is of public benefit, undertaking in depth research into the governance of public, private and third sector organisations and their influence.

**Dr Paul Gill** is a lecturer at University College London's (UCL) department of Security and Crime Science. Prior to joining UCL, Dr Gill was a postdoctoral research fellow at the International Center for the Study of Terrorism at Pennsylvania State University. He has previously managed projects funded by the Office for Naval Research and the Department of Homeland Security, focusing upon various aspects of terrorist behaviour. His research focuses on the behavioural underpinnings of terrorism and terrorist attacks.

**Dr Wali Aslam** is Lecturer in International Relations at the Department of Politics, Languages and International Studies, University of Bath. He is the author of *The United States and Great Power Responsibility in International Society: Drones, Rendition and Invasion* (Routledge, 2013). Dr Aslam is also co-editor of *Precision Strike Warfare and International Intervention: Strategic, Ethico-Legal and Decisional Implications* (Routledge, 2014).

**Crofton Black** is an investigator and researcher specialising in US and UK counter-terrorism activities. He has spent many years working on aspects of the CIA's "Rendition, Detention, Interrogation" programme and on military, government and corporate cooperation worldwide. He works for Reprieve's "Abuses in Counter-Terrorism Team" and is a senior investigator for One World Research. He has a doctorate from the University of London in the field of Medieval and Renaissance hermeneutics, and was formerly a Humboldt fellow at the Freie Universitaet Berlin.

**Oxford Research Group (ORG)** is a leading independent think-tank, non-governmental organisation and registered charity, based in London. ORG has been influential for thirty years in promoting the idea of sustainable approaches to global security as an alternative to violent confrontation, through original research, wide-ranging dialogue, and practical policy recommendations.

**The Verification Research, Training and Information Centre (VERTIC)** is an independent, not-for-profit charitable organization. Established in 1986, VERTIC supports the development, implementation and verification of international agreements as well as initiatives in related areas.

**Every Casualty** is committed to the principle that no individual should be killed in armed violence without his or her death being recorded, and is working to build the political will for this internationally. The programme also works on enhancing the technical and institutional capacity for casualty recording.

# Contents

# Executive Summary

Caroline Donnellan and Esther Kersley

Remote Control Project

**Remote control warfare is being expanded to new levels of complexity and intensity, yet these reports contain evidence that it is not only frequently unable to resolve conflicts, but indeed has serious repercussions well beyond the areas directly affected. The key findings include:**

## Increasing violence and radicalisation

- Drone strikes lead to an immediate 'blowback' of increased terrorist attacks, including increased civilian deaths
- In Pakistan, US drone strikes have led to an increase in radicalisation, violence and crime across the country as a result of the displacement of terrorists from affected areas
- Counter-terrorism operations in the Sahel-Sahara have increased radicalisation and undermined democracy and human rights – damaging the region's long-term stability and raising concern over the effectiveness of the operations
- The high number of civilian casualties in drone strikes places serious doubt on the supposed accuracy of this 'precision warfare'

**"Remote control warfare has now reached a critical point where policymakers need to evaluate the impact of these activities as well as their successes."**

## Lack of accountability

- The lack of information on drone strikes and the actions of special forces and private military operations severely impede the ability to record casualties; this is particularly the case in Afghanistan, the most drone-bombed country in the world
- In the US, private corporations are integrated into some of the most sensitive special operations activities including flying drones, managing surveillance technology, and running psychological operations
- Cyber attacks pose particular accountability concerns due to the ambiguous relationship between state and non-state actors, and the lack of legal clarity in this area
- Remote warfare leaves open a vacuum of responsibility, a potential abuse of power and erosion of trust between governments and those whom they govern

Remote Control methods and tactics are clearly being seen as a success by their users, demonstrated by the increase in spending on, and use of, these methods by governments across different theatres:

- Drones: Market projection suggest that the global annual export market for UAVs is likely to grow from $942 million to $2.3 billion over the decade from 2013 to 2023. By 2017, worldwide UAV production could average about 960 unmanned aircraft annually.

A broader range of states are deploying drones and developing indigenous technologies including France, Britain, Germany, Italy, Russia, Algeria and Iran

- Special operations forces (SOF): There has been a sharp increase in the use of SOF in the past decade, with the US more than doubling the size of the US Special Operations Command (SOCOM) since 2001
- Private military and security companies (PMSCs): The past decade has also seen a marked in increase in the use of PMSCs, especially in the conflicts in Afghanistan and Iraq. 69% of the $4 billion the US state department spent on reconstruction projects in Afghanistan from 2002 to March 2014 went to a single private military contractor. In 2014 it was reported that 5,000 contractors were working in Iraq
- Cyber: The US is spending $26 billion over the next five years on cyber operations and building a 6,000 strong cyber force by 2016. The UK has earmarked £650 million over four years to combat cyber threats

Remote control warfare has now reached a critical point where policymakers need to evaluate the impact of these activities as well as their successes. The evidence put forward in this report illustrates the inability of remote control warfare to resolve conflicts in the long-term and the need to tackle the root causes of conflict to ensure long-lasting global stability.

## Overview of the reports

The digest begins with a briefing paper from intelligence agency Open Briefing setting out the main trends from the past six months – and their implications – in the five key areas of remote control warfare: special forces, PMSCs, drones, cyber warfare and intelligence & surveillance. The next three papers deal with the impact of one particular aspect of remote warfare – drones – in different ways. *Drones in Afghanistan: A Scoping Study* by The Bureau of Investigative Journalism assesses the feasibility of a strike-by-strike survey of drone strikes in Afghanistan. The report finds that, despite Afghanistan being the most drone-bombed country in the world, there is a vacuum of information about where these strikes take place and who they kill. Following this is Dr Paul Gill's report, *The Impact of Drone Attacks on Terrorism: The Case of Pakistan*. The report explores whether the employment of targeted killings in counterinsurgency campaigns is an effective strategy to reduce or minimise terrorist attacks. Using data from drone strikes and terrorist attacks in Pakistan, its findings suggest that drone strikes in fact increase the risk of terrorist attacks in the country. Dr Wali Aslam's paper, *Terrorist relocation and the societal consequences of US drone strikes in Pakistan*, continues this look at the impact of drones in Pakistan by exploring their broader impact on the country. The paper finds that drones have had far-reaching negative consequences for Pakistani society, including increased radicalisation, violence and crime.

The next two papers examine other forms of remote warfare. *US Special Operations Command Contracting: Data-Mining the Public Record* by Dr Crofton Black sheds light on the activities of US military Special Operations Command contracting by analysing a US procurement database. The research reveals the extent to which private corporations are integrated into some of the most sensitive special operations activities including flying drones, managing surveillance technology, and running psychological operations. The prevalence of information and communications technology among Special Operations Command procurements and its implications are also explored. Moving on to cyber warfare, *Cyberspace: An Assessment of Current Threats, Real Consequences and Potential Solutions* by Vertic examines the role of cyber attacks in remote control warfare and the potential impact of these attacks on civilian populations and international stability, highlighting the accountability vacuum and legal ambiguities in this area.

Our final two papers look at a range of remote warfare methods in different ways. The first, *From new frontier to new normal: Counter-terrorism operation in the Sahel-Sahara*, by Oxford Research Group, is a case study of US and French counter-terrorism operations in the Sahel-Sahara that relies heavily on remote warfare, including drones, special operations forces and PMSCs. The paper examines the outcomes of these operations, raising concern over their effectiveness as a counter-terrorism strategy and their broader negative consequences on the region. Lastly, *Losing Sight of the Human Cost: Casualty Recording and Remote Control Warfare*, by Every Casualty, explores the practical challenges for recording casualty details in the context of remote warfare. The report finds that the use of drones, special operations forces and PMSCs severely reduces the ability to

scrutinise the actions of armed forces and record the casualties they cause.

Together these papers highlight troubling issues with remote control warfare in its many guises and across different theatres. The worrying developments with regard to transparency, accountability and oversight associated with these methods are echoed across the research. From Every Casualty and The Bureau of Investigative Journalism's reports we can see how the lack of information around drone strikes (in both covert and official theatres), as well as the actions of special forces and private military operations, severely impedes the ability to record casualties. Similar accountability problems were revealed in Crofton Black's research that shines a light on the outsourcing of sensitive special operations activities to private contractors, and Oxford Research Group's report, that reveals the clandestine nature of counter-terrorism campaigns being fought across North West Africa. Vertic's report shows how cyber attacks pose similar accountability concerns due to the ambiguous relationship between state and non-state actors in this field. Together these paint a worrying picture: without knowing clearly what is happening, we cannot judge the acceptability, effectiveness or legality of these operations, leaving open a vacuum of responsibility, a potential abuse of power and erosion of trust between governments and those whom they govern.

The research presented here also highlights the broader impact and implications these methods are having, raising doubts over their effectiveness. Concern over the high numbers of civilian casualties in drone strikes is emphasised in the Bureau's report, shedding doubt on the supposed accuracy of this 'precision warfare'. Dr Aslam's and Dr Gill's reports both highlight the problem of 'blowback' in Pakistan caused by drones and Oxford Research Group has identified increased radicalisation in the Sahel-Sahara as an outcome of counter-terrorism operations there. Together these reports show worrying trends of remote warfare fuelling radicalism and increasing extremism across theatres where these methods are in use. The broader impact of remote warfare is further evidenced through these reports: an increase in violence and crime across Pakistan has been an unintended consequence of drone strikes in the country and counter terrorism operations in the Sahel-Sahara have undermined democracy and human rights there, negatively impacting on the region's long-term stability. Finally, cyber attacks and the increased militarisation of cyber space have had far reaching negative implications, from increased surveillance on citizens to an erosion of trust between states.

**"Together these reports show worrying trends of remote warfare fuelling radicalism and increasing extremism across theatres where these methods are in use."**

# Trends in Remote Control Warfare

Scott Hickie, Chris Abbott and Raphaël Zaffran

Open Briefing

*"Borinqueneers" from Combined Joint Task Force-Horn of Africa opened the doors to its seventh counter-terrorism course for the Ugandan People's Defense Force. Creative Commons, Flickr / US Army Africa*

**"Over the course of the past six months, it has become apparent that in some areas there is a disconnect between civil society perception and the actual intentions and capabilities of governments and militaries."**

**Since April 2014, Open Briefing has produced a series of monthly intelligence briefings on remote-control warfare, commissioned by the Remote Control Project, focusing on five key areas of remote-control warfare: special operations forces (SOF); private military and security companies (PMSCs); unmanned vehicles and autonomous weapons systems; cyber warfare; and intelligence, surveillance and reconnaissance (ISR). Over the course of the past six months, it has become apparent that in some areas there is a disconnect between civil society perception and the actual intentions and capabilities of governments and militaries. This is due, in part, to a lack of detailed understanding of ongoing technological, political and doctrinal developments in certain key areas, including lethal autonomous weapons systems and cyber warfare. Open Briefing's monthly briefings address this by providing comprehensive but concise explanations and analysis of such developments. Conversely, in other areas, civil society is driving the debate and forcing governments to enact reforms. This is particularly so in the cases of armed drones, mercenaries and mass surveillance. In such instances, Open Briefing's monthly briefings bolster civil society efforts through the provision of timely and reliable intelligence, which allows organisations to develop more-effective advocacy strategies.**

This briefing provides a detailed overview of the key trends in remote-control warfare that have emerged during the period covered by the previous five briefings (March to September 2014). Such developments include the United States and European countries increasing their SOF footprints across

Africa, PMSCs playing increasingly important roles in Afghanistan and Iraq, the debate over unmanned aerial vehicles shifting to questions over effectiveness and developing international norms, the United States seeking international cyber-security norms while clashing with China over cyber espionage, and NSA leaks forcing Five Eyes partners to reconfigure and justify their surveillance activities. These, and the other events analysed in the following pages, are significant developments in remote-control warfare that warrant the deeper look provided in this briefing.

## Special operations forces

### United States and European countries increase special operations forces footprints across Africa

The footprint of special operation forces (SOF) across Africa, especially in the Sahel and Sahara, has received sustained attention over the last six months, even as the insecurity in Iraq and Syria has dominated security debates. Special forces from the United States and EU countries have been involved in key security developments on the continent, including operations tracking down the Lord's Resistance Army in Uganda, agreement over the continued US SOF presence in Djibouti at Camp Lemonnier, pressure for SOF assistance in freeing hostages taken by Boko Haram in Nigeria and multiple military and law enforcement counterterrorism training programmes.

The Quadrennial Defence Review 2014 provided the domestic justification for the focus of US SOF on the Maghreb, Sahel and Horn of Africa.[1] The reasons for an increased US special operations forces presence across these regions were hinted at in comments made to the New York Times in June 2014 by the commander of US Special Operations Command Africa, Brigadier General James B. Linder, who argued 'Africa is the battleground of the future' and 'the future of war is about winning people, not territory'.[2] Such sentiments are indeed consistent with the operational and tactical philosophy of US Special Operations Command (USSOCOM). This raises two key questions: why is Africa the battleground of the future, and is SOF training of indigenous, national forces sufficient preparation for this anticipated future conflict?

There are clearly regional drivers of the US preoccupation with African security hotspots that are related to the strategic desire to deny jihadist groups and insurgents operational opportunities in weak and failing states and the need to sever the connections that are likely to develop across the continent between such organisations. The US defence establishment has not forgotten Osama bin Laden's formative years in Sudan between 1991 and 1996, and is not keen to allow terrorist groups the space to develop into transnational threats.

However, a more significant driver for the United States is the opportunity countries like Kenya, Uganda, Niger and Djibouti provide in terms of more-accommodating launch pads for SOF operations in the Middle East and Southwest Asia, particularly unmanned combat air vehicle (UCAV) and intelligence, surveillance and reconnaissance (ISR) operations.

Furthermore, from a US perspective, a more geographically dispersed force projection and lighter SOF footprint serves as a salve for domestic war fatigue and accommodates pressure for defence spending austerity after more than a decade in Iraq and Afghanistan.

A number of regional partner governments are pressuring the United States, France and other special forces training partners, including Canada and the United Kingdom, to look beyond training and knowledge transfer. Algeria, Mali, Uganda, Nigeria, Niger, Djibouti and Kenya have all shown a desire for greater access to US and European military and security equipment, with Algeria's request for US unmanned aerial vehicles (UAVs) the most public. Furthermore, a number of African countries have long advocated for greater flexibility on using aid budgets for security, and have ardently rebuked critics who suggest too much national revenue is spent on military procurement and security.

However, providing equipment that creates an independent indigenous capability presents a significant risk for some US and European military planners and security policymakers; there are, after all, numerous examples of the allies of today becoming the enemies of tomorrow. For special operations forces trainers, there is also a significant difference between mission support and temporary access to technology, and the full-scale transfer of SOF equipment to partner countries.

The challenge is that even the light-footprint approach is limited by resources, and indigenous special operations forces and law enforcement agencies will be without US or European support at times. Without modern weapons, equipment and technology, many local forces will lose

any strategic advantage over domestic militant groups. The failure of US counterterrorism training for the Malian military due to problems around equipment provision and long-term engagement with SOF training is a prime example of this.

Some countries may not be in a position to demand greater support from their US and European SOF training partners, and will gladly accept any assistance on offer to confront terrorism and insurgency. Others, such as Niger, Nigeria and Uganda, will likely develop higher expectations of what their foreign partners should be delivering. These elevated expectations will come at a time when Iraq and Syria will be taking up more and more US and European SOF resources. The decisions over where to allocate limited SOF resources will clearly be taken in light of Western security concerns, not African, and will likely mean African countries will continue to struggle to adequately confront insurgent and terrorist groups within their borders.

### Significant developments in special operations forces technology

The emerging technologies developed for special operations forces use provide an insight into the future force capabilities military planners desire in light of projected conflict theatre needs. In May 2014, the then commander of US Special Operations Command Europe (SOCEUR), Major General Brad Webb, gave strong indications that key areas of need for US SOF were in intelligence-gathering and communication systems that can withstand the extreme climatic conditions of Africa and the Arctic.[3]

There is an undoubtedly strong focus on intelligence collection tools. Recent examples include advanced satellite communications, improved geographic information system (GIS) data on intelligence blind spots and enhanced sensitive site exploitation (SSE) biometric and DNA testing techniques. The new capabilities are very much geared towards highly-targeted, micro-scale conflict, including targeting individuals, and are likely designed to gain advantage over non-state actors who employ non-conventional means. The expanding focus on biometrics and SSE, which have been widely used in Afghanistan, is becoming an important component of identity dominance, employed by SOF as a means to undermine the anonymity of terrorist and criminal networks.

Combat hardware has not, however, been forgotten in this rush of innovation across intelligence and communications technology. French company Vaylon is developing a combination hang glider-dune buggy for French special forces after a need for stealthier air transport was identified during missions in Somalia. The US Defence Advanced Research Projects Agency (DARPA) has funded research on a hybrid-powered motorbike to assist special operations forces to penetrate remote areas and stealthily execute rapid raids in extreme terrain conditions and contested environments. USSOCOM's $80 million Tactical Assault Light Operators Suit (TALOS) effort, colloquially referred to as the new 'Iron Man' suit, has captured the public imagination. However, questions about the programme from the US House Armed Services Committee suggest that the hype around TALOS is unjustified and that the suit will not be useful across a broad range of battlefield scenarios.

One of the most significant developments in US SOF capabilities is the conversion of the maritime support vessel MV Cragside into a special operations base for up to 200 troops. Such a maritime base, together with the increased level of training of US special operations forces commands in amphibious operations (ending the historical monopoly of this area by US Navy SEALs), will provide substantial flexibility for US SOF operations, particularly in the Middle East and North Africa. The conversion of maritime support vessels or container ships to SOF maritime bases could lessen the dependence of SOF on aircraft carriers and terrestrial bases, and therefore sidestep host country support. It would also increase the array of manned and unmanned aircraft available for SOF missions under certain circumstances, as some may previously have been inappropriate due to range limitations.

### Russia coordinates special forces operations and cyber offensives in Crimea and eastern Ukraine

Russia's annexation of Crimea and elements of their ongoing activity in eastern Ukraine has revealed the importance of Spetsnaz (special purpose forces) to Russia's force projection. Indeed, Russian President Vladimir Putin's strategy in Ukraine can be characterised as something closer to paramilitary covert action than wholesale military attack. Unconfirmed reports suggest that several hundred members of the 45th Guards Spetsnaz Regiment (a special reconnaissance unit within Russian Airborne Troops, VDV) went into Crimea without insignia and attempted to garner enough support for

a civilian-led popular uprising – or at least the appearance of it. Their activities are thought to have included bribing key institutional figureheads, activating local pro-Russian militias, covertly moving weapons and co-opting some of the 25,000 Ukrainian military personnel based in Crimea.

The tactics used in Crimea and eastern Ukraine are not dissimilar to those Russia applied somewhat more haphazardly during their 2008 war with Georgia, where they were mixed with tried and tested Soviet-style strategic operations used effectively during their conflict in Afghanistan in the 1980s. In Crimea, the principle of maskirovka – camouflage or denial and deception – allowed Russia to maintain a degree of plausible deniability and swiftly carry out the operation before NATO, the European Union and the United States could properly respond. As such, the Spetsnaz units demonstrated an ability to carry out politically-sensitive operations.

What is different in Crimea and eastern Ukraine is the coordination of special forces operations and cyber offensives. While cyber offensives by Russia and non-state actors did not involve full-scale cyber warfare, distributed denial-of-service (DDoS) attacks and the Snake malware disrupted Ukrainian communication networks and enabled significant Russian surveillance of those networks. It is not clear how Spetsnaz troops leveraged this intelligence; however, the timing of confrontations with Ukrainian soldiers and the isolating of those soldiers from Kiev via the blocking of communications would suggest a level of cooperation between Russian cyber offensives and special forces operations.

The emerging importance to Russia of coordinating special operations forces with cyber operations is evident in a June 2014 Collective Security Treaty Organisation (CSTO) announcement, which noted that the organisation was creating joint special operations force to counteract cyber attacks and use special means to intercept signals and information messages.[4] It may also involve information and psychological operations subdivisions. CTSO's preeminent member, Russia, is highly likely to have used the announcement as strategic counter response to recent NATO cyber-preparedness activities, which were reinvigorated by the Russian occupation of Crimea and its cyber campaigns against Ukraine.

*As drawdown approaches in Afghanistan, PMSCs will play an increasingly important role in the country. Creative Commons, Flickr / Marines*

## Private military and security companies

### Private military and security companies play increasingly important roles in Afghanistan and Iraq

The upcoming drawdown of international forces from Afghanistan has been challenged on several fronts during the past six months. Specifically, two major developments, namely the delayed finalisation of the bilateral security agreement (BSA) and the disputed presidential election, are likely to contribute to the creation of a political and security vacuum. As such, it is likely that private military and security companies (PMSCs) will continue to play a central and increasingly important role in Afghanistan past the December 2014 mark.

The supremacy of PMSCs in conflict and post-conflict situations is also apparent in Iraq, where security has deteriorated significantly with the advent of the Islamic State. In February 2014, the Wall Street Journal reported that 5,000 contractors were working in Iraq as intelligence analysts, security guards and military trainers or in civilian jobs, such as translators and cooks.[5] Given the current security situation and the imminent threat posed by the Islamic State, it is highly likely that defence contractors will continue to take on key security responsibilities in Iraq during the next few months. For one thing, PMSCs have the advantage of being readily available military resources, with personnel not needing to be recruited or trained.

Overall, events during the past six months suggest two key and interlinked trends. First, PMSCs are further consolidating their presence in fragile settings, where governments are unwilling or unable to provide troops and

supplies. Second, national governments, and especially the United States, have contributed to the prevalence of PMSCs by heavily relying on them for a significant proportion of their military missions abroad, including security, post-conflict reconstruction and training duties. An April report from the Special Inspector General for Afghanistan Reconstruction (SIGAR) confirmed this overreliance with the disclosure that 69% of the $4 billion the US State Department spent on reconstruction projects in Afghanistan from 2002 to March 2013 went to a single private military contractor, DynCorp.[6]

Ultimately, PMSCs prosper in countries presenting particularly weak and unstable structural conditions, including a contested government and unclear jurisdiction over foreign soldiers, and particularly fragile settings, including loyalty and desertion issues within a new national army, deeply embedded ethnic issues and security vacuums created by an outgoing intervening force.

The apparent trends that governments are increasingly relying on PMSCs and that PMSCs are successful in fragile settings suggest that Iraqis and Afghans are likely to see large numbers of private security contractors on their soils for the foreseeable future. This poses a number of issues. Given existing legislative gaps and the difficulties inherent to the task of prosecuting private security contractors, PMSCs tend to operate with impunity, which can be highly destabilising for post-conflict countries that are slowly recovering from years of fighting and the presence of foreign militaries. Politically, the predominance of PMSCs in Iraq and Afghanistan is thereby likely to undermine the democratic process and government accountability, while weakening formal security actors, such as the Afghan National Army and the national police.

From a security standpoint, leaving PMSCs as central security providers in Iraq and Afghanistan is also problematic. Given the business-oriented nature of PMSCs, security will likely become concentrated on those areas of political or financial importance where security contracts are available, such as regional capitals and the oil producing regions, thus leaving other areas completely at the mercy of armed groups driven by political, ethnic or ideological agendas, such as the returning Taliban and extremists groups like al-Qaeda and the Islamic State. This would further threaten the already fragile territorial integrity of both Iraq and Afghanistan. If the West deserts both Afghanistan and Iraq, this could leave PMSCs as the sole foreign security providers attempting to fend off extremist groups alongside host countries' militaries.

**"69% of the $4 billion the US State Department spent on reconstruction projects in Afghanistan from 2002 to March 2013 went to a single private military contractor, DynCorp."**

In Afghanistan, US President Barack Obama has declared that unless the Afghan government signs the BSA, the United States will pull all its troops out of the country by the end of 2014. US exit strategies have tended to rely heavily on private contractors in order to protect its troops during withdrawal processes. Given that it was the outgoing president, Hamid Karzai, who had refused to sign the BSA, Afghanistan's presidential election generated considerable hope for new beginnings. However, the election was contested by both second-round candidates, Abdullah Abdullah and Ashraf Ghani, amid accusations of widespread fraud. Both candidates have agreed to abide by the outcome of the internationally-supervised recount, and have promised to form something akin to a unity government. Even if a unity government were to be formed, it will have to deal with the presence of PMSCs on Afghan soil, working not only in security jobs but also contracted by diplomatic missions and for civil reconstruction efforts.

In Iraq, despite apparent unity among international actors on the need to address the spread of the Islamic State, it is likely that any intervention will only involve limited airstrikes and not troops. As a result, PMSCs are bound to play a role in on-the-ground security duties, possibly alongside limited numbers of special operations forces and CIA operatives.

Ultimately, the gradual withdrawal of international forces will undoubtedly create a security vacuum, which is likely to benefit private military and security companies. While such companies have a role to play, governments will have to mitigate their influence, especially when it comes to security provision.

### States attempt to regulate private military and security companies internationally through domestic legislation

There have been continuous efforts over the last six months to better regulate PMSCs, both nationally and internationally. The Montreux

Document of 17 September 2008 is one of the first agreements defining how international law applies to the activities of PMSCs in conflict zones.[7] Since 2008, key stakeholders, such as Switzerland and the International Committee of the Red Cross, have been attempting to strengthen the agreement by pushing states to take measures so that their national practices comply with international law. Such efforts have also taken place within UN-organised working groups and forums.

In the United States, the US House of Representatives passed the 2015 National Defense Authorisation Act (NDAA), which aims to improve the US Defense Department's use, management and oversight of private contractors in Africa. The NDAA is an attempt by US lawmakers to take measures at home in order to constrain the influence and impunity of those private security companies it contracts abroad, particularly in the Sahel and North Africa but also in Iraq and Afghanistan. In contrast, South African President Jacob Zuma has been delaying signing an amendment to his country's Private Security Industry Regulation Act (PSIRA). The amendment involves far-reaching international consequences for the regulation of PMSCs through domestic legislation, as it will compel foreign security providers to hand over 51% of their businesses to South African citizens. However, it risks jeopardising the renewal of the United States' African Growth and Opportunities Act (AGOA), designed to assist the economies of sub-Saharan Africa and to improve economic relations between the United States and the region.

In early June, a seminar was organised in Senegal in order to help increase the number of states supporting the Montreux Document while offering a platform for discussion for all concerned parties to exchange best practices in the regulation of PMSCs in sub-Saharan Africa.[8] Two major challenges in the execution of the Montreux Document appeared. First, it is crucial that a large array of states and companies be represented at such meetings for the document's provisions to apply effectively, as institutionalisation and institutional pressure are usually best at compelling states to apply international legal measures. Second, in the absence of authority above their own governments, states are otherwise likely to fail to implement the document's regulatory measures nationally, which defeats the overall document's efforts.

The trend towards attempts to regulate PMSCs internationally through domestic legislation suggests that international regulatory efforts have not been entirely satisfactory when it comes to implementation phases. The Montreux Document is a seminal agreement but is likely to become obsolete if it does not continue to increase its support from states and companies. The greatest danger to the agreement comes from the ineffective domestic implementation of the measures it promotes, due to political unwillingness or inadequate monitoring and oversight mechanisms.

**Allegations of private military and security company use by Ukraine and Russia play out in battle of narratives**

Over the past six months, there has been much controversy and accusations from both sides over the alleged presence of private military and security companies in the Ukrainian conflict. Each side uses the supposed use of PMSCs and mercenaries by the other side as propaganda to discredit one another. This suggests a very interesting dimension of PMSCs: the very essence of PMSCs seems to be at odds with the nationalistic and ethnic nature of the conflict, and their use is perceived as unpatriotic. They are seen as the last resort of cowards, and their use delegitimises each side in the eyes of the other. By and large, the alleged presence of PMSCs in Ukraine has led to a battle of narratives between Kiev and the Kremlin, in which both sides have attempted to frame the use of PMSCs as means to discredit the other side's patriotism and legitimacy.

Specifically, Kiev was accused of contracting US private military company Greystone to tackle pro-Russian dissent in eastern Ukraine. The former subsidiary of Blackwater/Xe Services (now Academi) is known to have completed contracts in Russia and Central Asia but denied deployments in Ukraine. In turn, there were suspicions that the unmarked troops who seized Sevastopol and Simferopol airports in Crimea in February 2014 were from the Vnevedomstvenaya Okhrana, a quasi-private force within the Russian interior ministry. Furthermore, the Serbian authorities have estimated that dozens of Serbian nationals have also been fighting on both sides of the conflict in Ukraine, with Serbian Prime Minister Aleksandar Vucic stressing that in most cases these fighters are mercenaries fighting for money rather than ideology.

On 17 July 2014, the European Parliament passed a resolution praising Ukrainian President Petro Poroshenko's 15-point peace plan, which included the need to withdraw mercenaries from Ukrainian territory. Poroshenko has also offered amnesty to those mercenaries who have not

committed grave crimes. Overall, the alleged presence of PMSCs within the Ukraine conflict has had a destabilising effect, and is likely to further delay resolution among the warring parties despite the peace plan.

*A Reaper MQ-9 UAV based at Creech Air Force Bace, Nevada, USA. © Crown Copyright*

## Unmanned vehicles and autonomous weapon systems

### Debate over unmanned aerial vehicles shifts to questions over effectiveness and developing international norms

A number of key government inquiries, think tank reports and civil society reviews on UAVs have underscored a potential shift in policy over 2014. The UN special rapporteur on human rights published a report on civilian deaths from US drone strikes in March;[9] the RAND Corporation published a report on unmanned aerial vehicle capabilities, arms control and proliferation in April;[10] the Stimson Centre's Task Force on US Drone Policy reported in June;[11] and the British House of Commons Defence Committee published a report on remotely piloted air systems in July.[12] Taken together, there is evidence of greater debate about proliferation, operational controls and the need for international norms. Furthermore, after their use in Afghanistan, Pakistan and Yemen, some in the security establishment are questioning whether counterterrorism objectives can actually be achieved using UAVs (as currently employed), and indeed questioning their effectiveness in a wider range of missions, including ISR.

Increased interest from the US security establishment in the creation of norms around the use of UAVs is likely driven by concerns that US national security interests are not well served by other state and non-state actors adopting the same legal, ethical and operational UAV policies as the United States has so far enacted. Criticism of US drone strike practices from the UN special rapporteur on human rights and the UN Human Rights Council has also given state opponents of such practices increased international diplomatic opportunities to pursue stricter compliance with international humanitarian law.

The RAND report highlighted that UAVs are not transformative weapons, in part because most current models have limited use against enemies with air defences. In the context of rapid military modernisation sweeping East Asia and parts of the Pacific, the current fleet of drones therefore has limited applicability, which RAND suggests will actually temper proliferation. However, this presumes state-level conflict in a multi-polar Asia Pacific as opposed to continual conflicts in hotspots where lack of rule of law, infrastructure and security allow non-state actors and insurgencies to proliferate.

The US national security community and congressional committee debates on the US Navy's requirements for the Unmanned Carrier-launched Airborne Surveillance and Strike (UCLASS) programme have typified the discussions on UAV capabilities and future conflict needs, which must balance the benefits of new technology with the cost within tightened defence budgets. One vision for UCLASS is to provide the navy with a carrier-version of non-stealthy surveillance drones instead of the navy's experimental X-47B UCAV, which over the longer term is likely to have stealth capability, longer range and more significant armament. Others argue that this vision provides no real strategic advantage for US sea power if confronted with China's Anti-Access/Area Denial (A2/AD) capabilities, specifically long-range ballistic and cruise missiles.

Market projections suggest that the global annual export market for UAVs is likely to grow from $942 million to $2.3 billion over the decade from 2013 to 2023. By 2017, worldwide UAV production could average about 960 unmanned aircraft annually. This creates proliferation concerns, which, together with Chinese advancements in military UAVs, is the likely driver behind some in the defence industry and security establishment talking more openly about international norms around UAV use. Indeed, the Stimson Centre's taskforce recommendations on a cost-benefit analysis of drone use in counterterrorism operations and improved public disclosure around UCAV use show that some in the security mainstream see the merit in greater examination and consideration of the use of drones.

**UN bodies consider implications of lethal autonomous weapons as defence industry focuses on lower-level systems automation**

A four-day meeting in May 2014 of experts from 87 countries party to the UN Convention on Certain Conventional Weapons (CCW) was the first multilateral discussion on lethal autonomous weapons systems (LAWS). The meeting provided an opportunity for key civil society groups and UN institutions to highlight the potential implications of LAWS for international humanitarian law.

Only five of the CCW delegates supported a moratorium on fully-automated weapon systems: Cuba, Ecuador, Egypt, Pakistan and the Holy See. Many delegates rejected a moratorium on the basis that it would undermine development of automation technology in civilian fields and stunt innovation in non-lethal autonomous combat and military systems, such as intelligence collection, search and rescue, logistics and transportation. Despite disagreement, comments made by UN high representative for disarmament affairs Angela Kane to the secretary-general's Advisory Board on Disarmament Matters seem to suggest that a number of UN bodies, such as the CCW, need to have ongoing discussions around lethal autonomous weapons systems.[13]

The CCW meeting demonstrated that confusion around definitions and the varied focus on different systems mean that civil society groups are possibly talking about different technologies to the defence industry and national militaries. Some civil society groups have focused on autonomous military hardware likely to replace infantry weapons and combat systems. Some precursor technology, such as the BAE Systems stealth and semiautonomous demonstrator UCAV Taranis fit this mould. However, it is likely that defence companies and militaries are more focused on system automation of ISR, transportation, communication and cyber protection rather than autonomous lethal weapon capabilities. In fact, the automation of defence and military operations much earlier in the chain of functions, such as target identification and weapon selection, should raise concerns of a similar magnitude as those related to fully-automated weapons.

The developments around building independence from human intervention appear more focused in areas of cyber defence and ISR, particularly video surveillance systems. The recent revelation by former NSA contractor Edward Snowden that the NSA has developed an automated cyber-attack programme codenamed MonsterMind is a case in point. Snowden's justification for disclosing the programme was based on the concern that as an automated counter-attack system MonsterMind posed inherent risks of miscalculation. The Defence Advanced Research Projects Agency (DARPA) has run a number of competitions seeking software that implements autonomous cyber-defence action, suggesting that the US military is particularly interested in this capability.

**Broader range of states actively deploying unmanned aerial vehicles and developing indigenous technologies**

A broader range of states are actively deploying UAVs and developing indigenous technologies, challenging the international dominance of US and Israeli UAV technology. In July 2014, the French and British defence ministers signed a £120 million feasibility study on an unmanned combat air vehicle, which is part of a broader Future Air Combat System where UCAVs will be deployed alongside F-35 Joint Strike Fighters. European defence companies, including Airbus, have made overtures to the German, Italian and French governments to develop a European UAV platform to encourage EU and potentially NATO interoperability. BAE Systems is developing the Taranis UCAV for the British Ministry of Defence, Russian defence agencies aim to test Sokol and Tranzas UCAVs in 2017 and Algeria is reportedly keen to procure Xianglong (Soaring Dragon) UAVs from the Chinese military.

There are clear political indicators that EU members are not comfortable with the level of reliance on US and Israeli UAVs but are struggling to agree partnerships for the development of European UAV platforms. Germany cancelled its Euro Hawk order with Northrop Grumman in 2013, though France was reported as moving ahead with its acquisition of General Atomics MQ-9 Reaper drones for operations in Mali in addition to UCAV development work with Britain.

Europe, Israel and the US do not have a total monopoly over UAV development as Iran has recently demonstrated. In May 2014, Iran unveiled its reverse-engineered version of the US RQ-170 Sentinel. Iran was able to reverse engineer the Sentinel after it was either compromised by Iranian cyber forces and safely landed or simply crashed in Iran.

Reports indicate that Iran's maturing drone

**"Market projections suggest that the global annual export market for UAVs is likely to grow from $942 million to $2.3 billion over the decade from 2013 to 2023."**

development programme, which includes a number of Iranian drones – the Shahed, Azem, Mohajer, Hamaseh and Sarir – is benefiting from operational use in Syria and, more recently, Iraq. This combat usage provides greater opportunity for governments to assess the true capabilities of Iran's UAV programme. For Israel in particular, it may provide some insight into the technology that Iran may make available to Hamas.


*In Iraq, significant malware distribution and network monitoring is on the rise possibly being used to disrupt Islamic State communications. Screenshot from World News Online (Youtube with Creative Commons license)*

## Cyber warfare

### United States seeks international cyber-security norms while clashing with China over cyber espionage

Espionage, crime and attacks in the cyber realm have been key diplomatic sore points in relations between China and the United States throughout 2014. At the Armed Forces Communications and Electronics Association on 24 June, the commander of US Cyber Command (USCYBERCOM), Admiral Michael Rogers, warned that the United States will likely be targeted by cyber efforts designed to damage critical US infrastructure. At the Aspen Security Forum on 24 July, the deputy director of the NSA, Richard Ledgett, advocated the need for international cyber norms, and argued that China poses the greatest cyber threat to the United States because state actors share intelligence and intellectual property with businesses.[14] In turn, China has pointed to the NSA's cyber surveillance activities and the complicity of US technology companies in NSA programmes.

In April, US defence secretary Chuck Hagel sought to open dialogue with People's Liberation Army (PLA) commanders during a visit to China in which he provided some details of US cyber capabilities and emerging cyber doctrines. The stated aim of this diplomatic candour was to ensure that China understood US cyber red lines. However, this approach changed in the following months.

A stream of reports from private information security companies on alleged Chinese cyber units and 'bad actors' have pointed to PLA units targeting US and Israeli companies and government agencies to obtain confidential business and government information. US targets have included Westinghouse Electric, Alcoa, Allegheny Technologies, the United Steelworkers Union, SolarWorld and the United States Steel Corporation; while Israeli targets included defence contractors involved with Israel's Iron Dome air defence system. Other operations have focused on US targets with specific Asian geopolitical expertise and subject matter knowledge and more recently US think tank specialists on Iraq. The shift in hacking targets is likely to stem from extensive Sino interests in Iraqi oil production, with China being the largest foreign investor in Iraq's oil sector.

In May 2014, the US justice department named five members of a Chinese People's Liberation Army advanced persistent threat (APT) unit known as Unit 61398 in an indictment for cyber espionage, which has put a diplomatic chill on continuing negotiations between the two countries over cyber issues. This is the first criminal hacking charge that the United States has filed against specific foreign officials.

There is no extradition treaty between China and the United States, which makes it highly unlikely indeed that the Unit 61398 members will face a US court. Instead, the indictment seems in part designed to symbolically shame China in international forums. In light of extensive revelations about NSA interception and surveillance activities, particularly the installation of backdoors in routers scheduled for foreign export, a range of commentators and the Chinese Communist Party have suggested that the US indictment is hypocritical. Others speculate that the indictment is a US strategy to deflect attention from Edward Snowden's leaks on US cyber spying and intelligence-gathering activities.

Another motivation for the indictment may be internal pressure within the US administration to pursue international norms for cyber warfare and offensives, and the indictment is part of developing legitimacy around cyber activities. This requires the US administration to craft a convincing and easily understandable distinction between cyber activity for national security purposes (the supposed NSA approach) and cyber espionage

for the purposes of intellectual property theft and commercial advantage (the focus of Chinese efforts). Otherwise, Beijing needs do no more than highlight the controversial NSA activities revealed by Snowden and the complicity of US technology companies in NSA surveillance programmes.

Beijing cancelling its participation in a US-China working group on cyber-security after the US indictments raised very little public criticism. With countries such as India, Brazil and Russia harbouring significant grievances over NSA activities, BRICS countries are unlikely to give any significant consideration to US pressure for international cyber norms. China's agreement to work closely with the EU on cyber-security issues through enhancing the work of the China-EU Cyber Taskforce is likely to further isolate the United States and Five Eye partners from open dialogue and cyber-security confidence building with China. Furthermore, there is little strategic incentive for less-developed cyber powers, such as China, to disclose their current capabilities to a more dominant cyber power, such as the United States.

The July 2014 report of the State Department's International Security Advisory Board recommended that the US administration use bilateral dialogues and multilateral discussions to establish a broad multinational cooperative response mechanism to promote cyber stability.[15] However, the limited capacity of the United States to influence or catalyse the setting of cyber norms is likely to reinforce efforts to increase Pentagon spending on cyber operations – earmarked at $26 billion over the next five years – and to build a 6,000 strong cyber force by 2016, making USCYBERCOM one of the largest cyber forces in the world. As such, the United States is likely to continue to pursue both a norm-setting agenda and offensive and defensive cyber capabilities.

### Cyber attacks being deployed in conflicts in Israel, Syria and Iraq

Recent conflicts in Israel, Syria and Iraq have witnessed the cyber dimension being more effectively integrated into kinetic warfare, insurgency and terrorism operations. Claims such as those made by US Assistant Attorney General John Carlin that al-Qaeda have developed cyber capabilities, adopted cyber warfare as a strategy and tested the feasibility of such operations have captured media attention.[16] The threat of non-state actors initiating full-scale cyber warfare on the critical infrastructure of modern economies supports political justifications for increased cyber defences. However, on-the-ground reports indicate that the cyber dimension of the major Middle East conflicts is more akin to cyber guerrilla warfare than sophisticated advanced persistent threats (APTs) and signals interception by non-state groups.

In the context of Israel's Operation Protective Edge, cyber attacks and counter-attacks have spiked during the conflict between Hamas and the Israeli Defence Force. Distributed denial-of-service (DDoS) and Domain Name System (DNS) attacks were launched against Israeli government agencies, financial services and military websites, including Mossad and the Prime Minister's Office, with 70% of attacks appearing to originate or have been routed through Qatar. Despite the scale and alleged involvement of the Iranian Cyber Army and Turkey's cyber forces in attacks, the actual level of intrusion, disruption and damage to Israeli operations appears limited. Israel's cyber defence capabilities are currently much more advanced than those of Hamas or non-state hacking collectives. More capable actors, such as Iran and Turkey, may have shown strategic restraint in not wanting to raise the stakes by seriously attacking Israel, a country with mature cyber offensive capabilities.

In Iraq, significant malware distribution and network monitoring is on the rise. Specifically, the popular remote access tool njRAT, commonly used against Syrian opposition rebels, appears to be widely used across Iraqi internet service provider (ISP) networks. The trojans and malware are distributed via malicious web links, most likely embedded in political material on social media, and are likely being used to execute screen grabbing and key-logging activities. In addition to the remote access tools, analysts have noted a surge in use of the TOR anonymity network in Iraq over the last few weeks, with internet users trying to hide their ISP addresses when undertaking malicious activities.

The increase in malware and the broad distribution of njRAT in Iraq raises the question of whether state-sponsored actors are involved, using cyber tools to either disrupt Islamic State communications or gather intelligence on the militant jihadist group's movements. There is the possibility of Syrian Electronic Army involvement in cyber attacks on the Islamic State for the purpose of gathering intelligence on behalf of the Syrian and Iranian governments.

### Cyber confrontation in Ukraine pushes NATO to consider cyber mutual defence doctrines

Cyber attacks between Russia and Ukraine, which encompassed broad scale DDoS attacks and malware distribution for surveillance and sabotage, have spilt over into cyber offensive

against NATO. CyberBerkut, a group of pro-Russia hackers, were attributed with DDoS attacks on NATO websites in March 2014 as well as malware distribution using variations of Snake for cyber-espionage campaigns. At this point, Russian President Vladimir Putin has not launched a full-scale cyber offensive against Ukraine and, while it is unlikely in the short term, NATO members are now much more cognisant of the need for formal cyber-defence doctrines.

The recently-approved NATO cyber polygon base in Estonia and the existing NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) were given new relevance by cyber operations between Russia and Ukraine. Exercises, including the Locked Shields cyber-warfare drill in March 2014, also enabled NATO to test its cyber defences. However, such NATO activities are unlikely to have a significant deterrent effect on the intended target, Russia, for a number of reasons. Firstly, Russia has no need to intensify the level of cyber attack or push the offensive to a level that would endanger human life. Secondly, challenges around attributing attacks still provide a temporary period of plausible deniability.

NATO members are also considering cyber offensives in relation to Article 5 of the North Atlantic Treaty, the collective defence clause. In light of Russia's annexation of Crimea and previous cyber attacks on Eastern European countries, NATO has been updating its cyber defence policy to clarify the implications of major cyber attacks on member states. This update builds upon the work of approximately 20 experts who, at the behest of the CCDCOE, examined the application of the laws of armed conflict to cyber warfare.[17] The key principle to be established in the policy is that a certain intensity of cyber attack and malicious intention could be treated as the equivalent of an armed attack. At the NATO summit in Wales on 4 September 2014, members indicated support for an enhanced cyber defence policy and made key announcements on cyber defence, including enhancing the cyber security of national networks upon which NATO depends.[18]

The policy is, however, beset by a number of political challenges, and does not detract from the fact that many NATO partners are not necessarily comfortable with sharing information on their cyber capabilities. Key Western European countries and the United States are likely to be concerned about the cyber vulnerabilities of NATO partners in Eastern Europe who have developing economies and reduced levels of cyber maturity. The US Department of Defense announced in June 2014 that the United States and specific allies are working to bolster the cyber offensive and defensive capabilities of vulnerable US allies, which is a clear indication that there is a fear opponents may focus their attacks on cyber-vulnerable and strategically important partners in Eastern Europe, including Latvia and Lithuania.

*The United Kingdom's Government Communications Headquarters (GCHQ) was forced to reveal its policy on mass surveillance. Creative Commons, Flickr / UK Ministry of Defence*

## Intelligence, surveillance and reconnaissance

### NSA leaks force Five Eyes partners to reconfigure and justify surveillance activities

The release of information about NSA operations by Edward Snowden has required many Five Eyes partners to publicly defend and clarify the nature of government surveillance activities. Snowden and media outlets holding his trove of NSA documents have revealed a wide-spanning intelligence-collection network spanning multiple communication modes and countries. NSA programmes, such as PRISM, MYSTIC, RETRO, RAMPART-A and SOMALGET, have allowed the agency to collect vast volumes of communications intelligence and metadata, despite pushing the legal envelope.

The international debate over the NSA's activities forced the United Kingdom's signals intelligence agency, GCHQ, to reveal its policy on mass surveillance, which due to an interpretation loophole defines communications via social media networking sites and search engines outside of the United Kingdom as 'external communication' because the servers are based outside Britain, usually in the United States. The implication is that GCHQ can apply the surveillance standard for foreign communications

in a domestic context, enabling a form of mass surveillance. An Australian constitutional affairs committee inquiry into telecommunication data storage and interception has showed a number of Australian agencies collecting personal telecommunications information without a warrant. Canada is also experiencing an emerging debate over collection, storage and access to personal telecommunications metadata. In response the British, Australian and Canadian governments have needed to formulate clear public policy on mass surveillance.

The NSA's intelligence, surveillance and reconnaissance (ISR) activities have raised the ire of national governments, including Germany, Brazil, China and India, international telecommunication providers, such as Verizon, US IT companies and service providers and civil libertarians. The US House Intelligence Committee chairman, Mike Rogers, accused the companies of putting business profits from European markets ahead of US national security.[19] However, the political and economic implications of the NSA's activities are starting to become more tangible for the US administration, including direct economic costs to US businesses, the loss of credibility for the US internet freedom agenda and serious damage to internet security through the weakening of key encryption standards, stockpiling information about software security vulnerabilities and the insertion of surveillance back-doors into widely-used software and hardware.[20]

Legislatures in Five Eye jurisdictions are urgently considering regulatory reforms to address public concerns over mass surveillance while still maintaining existing ISR capability and ensuring harmonisation and interoperability between Five Eye partners. The US Congress has already seen two iterations of the USA Freedom Act aimed at regulating NSA activities. The bill initially passed the House of Representatives by a margin of nearly three to one, but the Democrat senator and chair of the US Senate judiciary committee, Patrick Leahy, introduced a revised USA Freedom Act. The new version is hailed as strengthening privacy provision where the original House version of the bill was too weak.

In the United Kingdom the three major political parties have supported legislation that requires telecommunication companies to retain customer metadata for 12 months and reasserts the application of data interception obligations on overseas communication services providers delivering services to British citizens. The British government argued that the Data Retention and Investigatory Powers Bill is an emergency response to the European Court of Justice (ECJ) ruling in April 2014 that invalidated a 2006 EU directive allowing telecommunication companies to store customer metadata for up to two years. The ECJ held that the directive disproportionately interfered with the fundamental rights of privacy and protection of personal data.

Australia's and Canada's political establishments are also contending with contentious reforms to surveillance and data-retention activities. In Australia, the director-general of the Australian Security and Intelligence Organisation, David Irvine, made a rare media appearance to explain proposed legislation.[21] Irvine also told the Australian senate's legal and constitutional affairs references committee that it is appropriate that telecommunication companies retain metadata upwards of two years. In Canada, a Globe and Mail article revealed that reforms to Canada's electronic intelligence agency, the Communications Security Establishment Canada (CSEC), flagged as a critical legislative priority by then defence minister Peter MacKay, were derailed in 2009.[22]

The New Zealand parliament already passed reform to the Government Communications Security Bureau Act in 2013. However, revelations on the eve of the New Zealand election by the Intercept show a degree of cooperation between New Zealand and the United States to establish a level of public communications surveillance in 2012 and 2013.[23]

In all jurisdictions, the current concerns around the threat of fighters returning from Syria and Iraq are proving an important catalyst for governments to push ahead with reforms. In the case of the United Kingdom, reforms were concurrent with the announcement of a £1.1 billion package to equip the armed forces for modern conflicts, which includes an over £800 million boost to British intelligence, surveillance and cyber capabilities. Such moves are likely to be repeated across other jurisdictions, despite any pledges for defence budget austerity, to potentially offset any operational inefficiency introduced by political-acceptable ISR reforms. Furthermore, there is likely a level of coordination between the Five Eye jurisdictions in order to ensure interoperability and retain existing surveillance capabilities, even if those capabilities are distributed across the alliance.

### Defence ministries building capabilities for information operations across social media

Defence ministries are increasingly interested in open source intelligence (OSINT) collectable from social media networks. Recent examples where OSINT has provided critical evidence to explain important global events include YouTube videos of a Buk missile launcher in eastern Ukraine after the downing of Malaysia Airlines Flight 17 and Eliot Higgins' work under the pseudonym Brown Moses on barrel bombs and other weapons used in the Syrian civil war.

Governments, the private sector and NGOs are developing complex research programmes that use big data for conflict prediction and prevention. These include the US defence department's Information Volume and Velocity (IV2) programme, the CIA's Open Source Indicators programme and the United Nation's Global Pulse initiative. Most intelligence services monitor social media networks. The German foreign intelligence service, the Bundesnachrichtendienst (BND), recently committed €300 million to support real-time social media monitoring to bring it in-line with the United States' NSA and Britain's GCHQ.

However, more recent announcements and revelations about NSA activities indicate that governments are also interested in social media networks as a social terrain on which information operations and propaganda campaigns can be carried out with the aim of influencing audience responses. For example, BAE Systems are expected to receive a total of £30 million from the UK Ministry of Defence for projects to explore ways for the military to use social media and psychological techniques to influence people's beliefs. Documents leaked by Edward Snowden show that GCHQ's Joint Threat Research Intelligence Group (JTRIG) has already developed a number of information operation applications. The applications provide GCHQ with the ability to manipulate and alter information presentation across social media platforms, block email and website access, covertly record real-time Skype conversations and retrieve private Facebook photos.

The US Department of Defense's military research arm, the Defence Advanced Research Projects Agency (DARPA), pre-emptively released information on its Social Media in Strategic Communication (SMISC) programme after revelations about Facebook's emotional contagion news feed experiment and the JTRIG applications. The Australian Defence Force (ADF) has also revealed that it has developed offensive information operation doctrines. Media reports suggest that the Russian government recruits an army of 'online patriots' who consistently post pro-Russian sentiment on Western media websites, such as Fox News, Huffington Post and Politico.

Such social terrain activities are most likely going to be deployed by militaries during combat operations or civil unrest to manage the social dynamics of conflict, and will be more advanced and sophisticated than historical propaganda campaigns. Consistent with trends in other areas of remote-control warfare, these information operations are likely to be highly targeted and based on detailed intelligence on social network structures, including key decision makers and people of influence.

**"The current concerns around the threat of fighters returning from Syria and Iraq are proving an important catalyst for governments to push ahead with reforms. In the case of the United Kingdom, reforms were concurrent with the announcement of a £1.1 billion package to equip the armed forces for modern conflicts, which includes an over £800 million boost to British intelligence, surveillance and cyber capabilities."**

### Subversion of encryption standards part of intelligence toolkit

Documents leaked by Edward Snowden in September 2013 implicated the NSA in the covert undermining of encryption standards through a $250 million signals intelligence (SIGINT) enabling programme. In December 2013, information came to light that revealed the NSA's encouragement of and support for tech-security company RSA in making a now-discredited cryptography system used by a wide range of companies and services. After the fallout from the Heartbleed OpenSSL bug discovered in April 2014 and the discontinuation of the freeware encryption tool TrueCrypt in May 2014 left consumers and businesses concerned about encryption security, pressure has built on the US Congress to address NSA exploitation

of encryption backdoors for surveillance and intelligence collection.

Despite the director of national intelligence, James Clapper, making it clear in budget requests that US agencies need cryptanalytic capabilities to defeat enemy cryptography and exploit internet traffic, more recent deliberations of the US House Science and Technology Committee adopted an amendment from Florida Democrat Alan Grayson to remove the mandatory requirement for the National Institute of Standards and Technology (NIST) to consult with the NSA when developing security standards. The aim of the amendment is to prevent the NSA from influencing the peer review process for encryption standards developed by the NIST. The amendment, which is now part of the NIST Reauthorisation Act of 2014, was passed by the House of Representatives on 22 July 2014.

The subversion of encryption standards poses a vexing challenge for many governments. Recent analysis by Recorded Future showed that a number of mujahideen fighters and operatives are using open-source, off-the-shelf encryption tools, which may have in-built vulnerabilities that can be exploited by intelligence agencies.[24] However, leaving in-built vulnerabilities may allow them to be exploited by non-state actors and cyber criminals. Both legitimate multinational companies and terrorist groups such as al-Qaeda use encryption tools for communication. As such, in-built vulnerabilities and backdoors can be exploited for unauthorised surveillance, cyber espionage and intelligence, or can be used to target terrorist or criminal groups.

**END NOTES**

1 http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf

2 http://www.nytimes.com/2014/06/15/magazine/can-general-linders-special-operations-forces-stop-the-next-terrorist-threat.html

3 http://www.executivegov.com/2014/05/special-ops-leaders-outline-troop-requirements-for-intell-gathering/

4 http://www.eurasianet.org/node/68751

5 http://online.wsj.com/news/articles/SB10001424052702304851104579361170141705420

6 http://www.sigar.mil/pdf/special%20projects/SIGAR-14-49-SP.pdf

7 https://www.icrc.org/eng/assets/files/other/icrc_002_0996.pdf

8 https://www.icrc.org/eng/resources/documents/news-release/2014/06-04-senegal-seminaire-entreprises-militaires-securite-privees.htm

9 http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G14/119/49/PDF/G1411949.pdf?OpenElement

10 http://www.rand.org/pubs/research_reports/RR449.html

11 http://www.stimson.org/images/uploads/research-pdfs/task_force_report_FINAL_WEB_062414.pdf 12 http://www.publications.parliament.uk/pa/cm201415/cmselect/cmdfence/611/61102.htm

13 https://s3.amazonaws.com/unoda-web/wp-content/uploads/2014/07/FINAL_HR_Remarks_ABDM_62_2-July-2014.pdf

14 http://www.aspendailynews.com/section/home/163200

15 http://www.state.gov/documents/organization/229235.pdf

16 http://www.justice.gov/nsd/pr/remarks-assistant-attorney-general-john-p-carlin-cyber-crime-carnegie-mellon-university

17 http://www.cambridge.org/gb/academic/subjects/law/humanitarian-law/tallinn-manual-international-law-applicable-cyber-warfare

18 http://www.nato.int/cps/en/natohq/official_texts_112964.htm

19 http://www.politico.com/blogs/under-the-radar/2014/06/rogers-lashes-out-at-google-on-surveillance-stance-190199.html

20 http://oti.newamerica.net/sites/newamerica.net/files/policydocs/Surveilance_Costs_Final.pdf

21 http://www.abc.net.au/news/2014-08-08/asio-chief-says-security-plan-not-mass-surveillance-exercise/5658526

22 http://www.theglobeandmail.com/news/politics/wiretap-oversight-bill-derailed-in-2009/article20054907/

23 https://firstlook.org/theintercept/2014/09/15/new-zealand-gcsb-speargun-mass-surveillance/

24 https://www.recordedfuture.com/al-qaeda-encryption-technology-part-2/

# Drones in Afghanistan: A Scoping Study

Alice K Ross, Jack Serle and Tom Wills

The Bureau of Investigative Journalism

*MQ-9 Reaper drone from the 62nd Expeditionary Reconnaissance Squadron at Kandahar Airfied, Afghanistan. Creative Commons, Flickr / David Axe*

**This report assesses the feasibility of a strike-by-strike survey of drone strikes in Afghanistan, modelled on the Bureau's existing databases of drone strikes in Pakistan, Yemen and Somalia. Armed drones (remotely piloted aircraft) are an important weapon in the Afghan conflict. The country has seen more than 1,000 drone strikes, carried out by both US and UK forces, making it the most heavily drone-bombed country in the world. As full-scale operations wind down, and an expected slimmed-down US force takes on counter-terrorism operations, drones are likely to be a prominent aspect of the continuing US presence. Yet, little is currently known about where the drones strike, or who they kill in Afghanistan.**

We know from our previous experience tracking drone strikes that each country presents its own research challenges and has its own unique set of sources. In order to explore what these might be in Afghanistan, we have created a database compiling what has been reported in the media and other open sources about drone and air strikes that reportedly took place in September 2013. We have also interviewed journalists and human rights researchers to gather their views on the challenges of carrying out such work in Afghanistan. This report also provides an overview of current drone operations in Afghanistan and examines how these are likely to develop as the drawdown by international troops approaches. It also surveys the existing casualty counting and explores how this may be accessed.

**"Afghanistan is the most heavily drone-bombed country in the world... over 1,000 drone strikes conducted by British and US-operated drones have hit the country – more than in Pakistan, Yemen and Somalia combined."**

## Why it matters

The use of drones in warfare is a relatively new phenomenon. At present only three nations – the US, the UK and Israel – are known to have carried out armed drone strikes. But a recent report by the

Council on Foreign Relations noted that other nations including China and Iran are believed to have deployed armed drones without firing missiles. It also found that countries including India, Pakistan, Turkey and a collaboration between Switzerland and EU member states including France, Italy, Spain, Greece and Sweden have all announced that they are developing armed drones of their own.

Drones, it is claimed, offer a forensic level of accuracy due to their ability to loiter for lengthy periods of time, gathering intelligence and tracking a target before an attack with minimal civilian casualties. However, there are concerns in practice over their accuracy. The armed forces that operate drones publish no data on casualties to corroborate these claims. The Bureau, which has tracked drone attacks on a strike-by-strike basis in Pakistan and Yemen, has found evidence that suggests hundreds of civilians have been killed in drone attacks.

Amassing and analysing data on a strike-by-strike basis is important for a number of reasons. Not only does it reveal important trends and tactics (such as the controversial tactic of carrying out 'follow-up' strikes targeting rescuers, labelled as a potential war crime by a UN special rapporteur), it also allows for analysis and comparison of the use of drones between different theatres and greatly informs public debate. So far this debate has focused on covert conflicts, such as Pakistan and Yemen, with much less known about the use of drones in an official theatre of war. A lack of transparent data with regard to drones in Afghanistan stifles wider debate and creates an accountability vacuum around civilian casualties.

## Drones in Afghanistan

Afghanistan is the most heavily drone-bombed country in the world. Data released to the Bureau in 2012 by the US military showed that over 1,000 drone strikes conducted by British and US-operated drones have hit the country – more than in Pakistan, Yemen and Somalia combined. Drones are playing an increasingly important role in Afghan air campaigns in recent years. In 2011 drones fired 5% of all missiles fired in air strikes, by 2012 this had risen to 18%. Drones also accounted for a third of all civilian deaths in Afghan air strikes, this is a greater proportion than any other type of air strike. Both US and British drones operate in Afghanistan. The US's fleet includes both the MQ-1 Predator and the more advanced MQ-9 Reaper drone. Britain operates a small fleet of 10 armed Reaper drones. Britain's drone fleet is small but highly active, having carried out over 300 drone strikes between 2008 and 2013. Figures released to the British parliament in July 2014 show the central role occupied by drones in the UK's air campaign: remotely piloted aircraft fired more than 80% of the precision-guided munitions fired by UK aircraft between 2011 and 2014. However, we know markedly little about the details of these strikes and there is no data released on the overall casualties caused by them.

For our report we approached Afghan and international journalists, as well as human rights organisations, to understand the context in which strikes take place, the challenges of reporting strikes in Afghanistan, and the possible future of drone strikes in the country. We found that the number of air strikes carried out across the country has fallen steeply in the past year: the number of munitions fired by all aircraft in 2013 was half that of the peak, in 2011. The data does not disaggregate between drone strikes and those carried out by other aircraft. Several sources agreed that with the Coalition forces' drawdown approaching and key eastern provinces almost completely under Taliban control, there is an increasing reliance on drone strikes and other air operations in the provinces bordering Pakistan.

With drawdown approaching and almost all Coalition troops leaving Afghanistan at the end of this year, a look ahead to the role of drones in the future of Afghanistan is essential. A US force will remain in Afghanistan next year engaging in counter-terrorism missions which will focus on tracking al-Qaeda rather than tackling other Afghan militant groups. The analysts and reporters the Bureau spoke to agreed overwhelmingly that the counter-terrorism section of the US mission is likely to rely strongly on drone surveillance and strikes.

## Who's counting the casualties?

After 13 years of continuous combat there are a number of national and international organisations that count casualties, particularly civilian casualties, in Afghanistan. These include UNAMA, ISAF, and the Afghanistan Independent Human Rights Commission (AIHRC). But there is no organisation that systematically counts, and makes publicly available, the specific casualties of drone attacks, both civilian and insurgent.

### Challenges to information-gathering

The poor security situation in many parts of the country severely hinders reporting of drone strikes and other incidents. Some areas are entirely controlled by the Taliban and so are extremely dangerous for journalists, who often find themselves confined to the provincial capitals. This has become more problematic as international forces have started to pull out of Afghanistan as the media has lost an important level of protection and has been forced to pull back its operations too.

Gathering information from those affected by drone strikes can also be complicated. In Afghanistan's more remote districts, people are commonly illiterate and poorly educated, which impedes the level of detail they can provide about the attack. A further challenge to gathering information from eyewitnesses lies in the Taliban's suspicion of communication with the outside world and fear amongst Afghans of lodging complaints about drone strikes. Because of such challenges, it is quite common for strikes to go entirely unreported in the media.

### Official reporting

Official record keeping is often incomplete and there are large discrepancies between ISAF's estimates of civilian casualties and UNAMA's. Data collected by NATO and other organisations is also starting to look a bit messier as these institutions lose their eyes on the ground as international forces disengage. There are records kept by various branches of local and central government, but it is unclear whether they keep records of past events.

While casualty recording is often better in areas that have had extensive exposure to NGOs and other international organisations, such improvements are likely to have limited penetration into the rural areas, where many of the drone strikes have occurred. Furthermore, even if some official choose to keep records, the fact that large areas are off-limits to the government means that they are unlikely to have comprehensive access to information about the dead.

### Distinguishing drone strikes from other violence

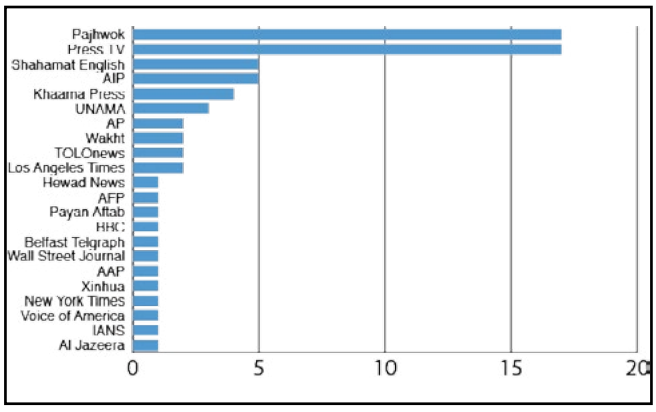
Drones are not the only form of aerial attack that occurs in Afghanistan and it is often unclear from available reporting whether a particular attack was carried out by a drone. Furthermore, both the UK and US operate armed drones, so establishing whether a strike was carried out by drone does not reveal conclusively who carried out the attack. Moreover, US drone strikes could be carried out by the Air Force on behalf of conventional forces, Special Forces or the CIA, making it impossible to say conclusively which force carried out which attack.

## September 2013: An exercise in casualty recording

We conducted a 'sample month' exercise to examine how comprehensively drone strikes are reported and to establish the scope of difficulties that might arise in gathering strike-by-strike data on drone strikes in Afghanistan. The team gathered media reports and other open-source data on all the strikes occurring in September 2013, using techniques developed through our previous casualty recording experience. As it is hard to distinguish drone strikes from other air strikes on the basis of open-source reports, we have gathered reports on both.

This exercise identified reports describing 34 incidents of air strikes or drone strikes occurring in Afghanistan in September 2013. Ten of these incidents were specifically described as drone strikes. The chart below shows which publications reported on air strikes, including drone strikes, most frequently:

**Figure 1: Air strikes (including drone strikes) reported per publication/agency**




Pajhwok, a private news agency based in Kabul, and Press TV, an Iranian news station, report air strikes more frequently than any other outlets. The Bureau has frequently used Pajhwok's reporting in its research on drone strikes in Pakistan, and has found it a reliable source that often corroborates reporting by other outlets, while adding details. However, the Bureau has previously identified dozens of Press TV reports relating to drone strikes in Somalia that have not

been corroborated by any other source, and so regards its reports as potentially unreliable. Press TV's reports on drone strikes in Afghanistan should therefore be treated with caution.

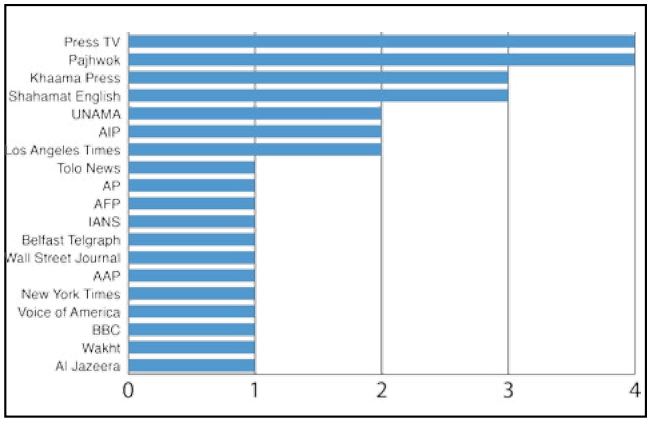
The sample month revealed that reporting of air strikes is far less comprehensive than in other theatres: almost 60% of reported air strikes are effectively reported by a single source, and many strikes appear to go unreported. The table below shows how frequently strikes in the sample month were reported by multiple sources:

**Figure 2: Number of outlets reporting air strikes, including drone strikes**

| Number of reports | Number of strikes |
|---|---|
| 1 | 17 |
| 2 | 10 |
| 3 | 4 |
| 4+ | 3 |

We found reports of 10 drone strikes taking place during September 2013. These included one incident that was reported by more than a dozen sources: the Kunar province strike of September 7, which reportedly killed at least 10 people, including at least eight reported civilians. A further 24 incidents were reported as air strikes. Five drone strikes were reported in Kunar; two in Helmand and one each in Uruzagan, Paktia, and Ghazni provinces. The chart below illustrates how frequently news outlets reported drone strikes.

**Figure 3: Outlets reporting drone strikes**




Given the concerns relating to Press TV's reporting, outlined above, this finding should again be regarded with caution, particularly where Press TV is a sole source. Based on available reporting, it appears that drone strikes are significantly more likely to kill civilians than conventional air strikes. However, the single-sourced and uncorroborated nature of most reports means that these figures cannot be considered comprehensive or conclusive. According to available reporting, 54-71 people were killed in incidents described as drone strikes, of whom 11-33 were described as civilians. Air strikes killed a further 82-96 people, of whom 4-10 were reportedly civilians. Six of the 10 reported drone strikes reportedly killed civilians (60%), while five of the 24 air strikes were reported to have killed civilians (21%).

**For the full data set see Appendix 1 in the full report.**

## Conclusion

The study concludes that media reports would not be sufficient as a primary source for developing a full record of drone strikes in Afghanistan. Instead, this would require a network of local contacts who could gather data such as eyewitness reports where possible, and data compiled by local sources.

However, owing to the safety risks and the difficulty in distinguishing drone strikes from air strikes, even these steps are likely to be incomplete. Instead, any such effort would also require a sustained engagement with the military forces involved to encourage them to release their own data for public scrutiny. Partnering with academics or NGOs could help facilitate this process.

Recording of drone strikes in Afghanistan is crucially important if we are to develop the fullest possible understanding of how armed drones are being used internationally at this early phase in their evolution. Despite the considerable difficulties involved, it is clear that developing a strike-by-strike database of attacks in Afghanistan is vitally needed. Over the past three years the Bureau and others have pieced together a detailed picture of drone usage in secret wars, revealing controversial tactics and questionable strategies. Without similar efforts for Afghanistan, this picture remains frustratingly incomplete.

**This is a summary of *Tracking drone strikes in Afghanistan: A scoping study* by the Bureau of Investigative Journalism. For the full report, including citations, visit remotecontrolproject.org/our-reports**

# The Impact of Drone Attacks on Terrorism: The Case of Pakistan

Dr Paul Gill

*The ruins of a building in Karachi after a bomb exploded outside a Shiite mosque in Abbas Town. Creative Commons, Flickr / Nadir Burney*

**Countering terrorism with punitive enforcement measures like targeted assassinations has a long history. In the aftermath of 9/11, the merits of 'war' approaches to countering terrorist groups became highly salient within public discourse. Proponents claimed that such measures promise to reduce subsequent terrorism by degrading terrorist group capacity in a number of ways. First, it reduces the pool of cadres and recruits. Second, by imposing costs on those who provide financial and other forms of support for terrorists. Third, it has the potential to remove terrorist group leaders and other skilled members. Fourth, it serves as a deterrent for would-be terrorists and supporters. Fifth, it imposes costs on terrorist group members who have to spend more time and finances in changing locations and avoiding detection. This lessens their ability to commit terrorist attacks. Sixth, it reduces the flow of internal communications within the terrorist groups. Seventh, these policies are often popular within a country's domestic constituency. Finally, compared to other forms of counter-terrorism (like full-scale insurgencies), single strikes are far more proportional (Lotriionte 2003; Luft 2003; Yoo 2006; Wilner 2010).**

"In the aftermath of 9/11, the merits of 'war' approaches to countering terrorist groups became highly salient within public discourse."

Critics suggested otherwise and made a number of compelling arguments. First, it violates basic democratic and human rights. Second, other initiatives such as arresting terrorists may prove more effective. Third, it may in fact prompt a backlash from the terrorist group. Fourth, it may erode public support for state counterterrorism officials. Fifth, it may kill non-combatants. Sixth, it may enhance sympathy for terrorists. Finally, it provides the targeted terrorist movement with propaganda fodder (see Byman 2006; Jordan, 2009; Hafez 2006; Walsh and Piazza 2010).

While these theoretical debates grew in number, there was a striking lack of empirical approaches that actually tested these assumptions. In 2006, Lum et al analysed the effectiveness of counter-terrorism

strategies from the available social science research literature. Their main finding was that "there is almost a complete absence of high quality scientific evaluation evidence on counter-terrorism strategies" (2006:1). Amongst the handful of studies they could find, there was a suggestion that "retaliatory attacks (for example, the U.S. attack on Libya in 1986 or attacks by Israel on the PLO) have significantly increased the number of terrorist attacks in the short run" (2006:1). In the eight years that have passed since, empirical approaches to understanding this question have flourished. In particular, these studies have tested whether punitive counter-terrorism measures downgrade or foster future terrorist attacks. Aided by parallel major data, collection efforts have allowed analyses to be carried out on conflicts such as Northern Ireland, Palestine, Chechnya, Afghanistan, Iraq, Spain and Pakistan. In a relatively short period of time, we have gone from very few analyses to many, of which there have been very quick improvements in terms of the methodological rigour and theoretical nuance.

The table below provides an overview of these analyses. How 'effectiveness' is measured differs widely.

**Figure 1: An overview of empirical analyses of 'deterrence' vs.'backlash'**

| Authors | Case Study | Tested | Finding |
|---|---|---|---|
| Kaplan et al (2005) | Israel/ Palestine | Do targeted assassinations reduce level of violence? | 1. Israeli targeted killings of terrorists led to a subsequent increase in suicide bombings<br>2. Preventive arrests rather than targeted killings led to a decrease in attacks over time |
| Hafez & Hatfield (2006) | Israel/ Palestine | Do targeted assassinations reduce level of violence and success rate of operations? | No Impact |
| Cronin (2011) | Various qualitative cases | Does killing a group's leader lead to the death of the group? | "Cases where a group has halted a campaign following the killing of the leader are difficult to find, and those examined here do not support the conclusion that assassination ends terrorism" |
| Jordan (2009) | 298 incidents of terrorist leaders being killed from 1945-2004 | Does killing a group's leader (a) lead to a group becoming inactive (b) decrease its frequency of attacks (c) decrease the number of people the group kills? | "Decapitation is actually counterproductive, particularly for larger, older, religious, or separatist organizations" |
| Mannes (2008) | 81 Examples of Terrorist Groups Losing their Top Leadership from 1970+ | Does killing a group's leader (a) decrease its frequency of attacks (b) decrease the number of people the group kills? | 1. General decline in no. of incidents but not on fatal attacks<br>2. "decapitation strikes…cause religious organizations to become substantially more deadly" |
| LaFree et al (2009) | Northern Ireland | How did 6 high-profile British CT operations impact subsequent PIRA terrorism? | "Strong support" for the backlash argument |
| Dugan & Chenoweth (2012) | Israel/ Palestine | Test effects of repressive (or punishing) and conciliatory (or rewarding) actions on terrorist behavior | 1. Repressive actions by the Israeli state sometimes led to increases in Palestinian terrorism<br>2. Conciliatory actions are generally related to decreases in terrorist attacks |
| Fielding & Shortland (2010) | Egypt | Impact of repressive actions on subsequent terrorism | Repressive actions by Egypt sometimes led to increases in Egyptian terrorism |
| Moaz (2007) | Israel/ Palestine | Tests the temporal effects of when reprisal attacks occur after a targeted assassination. | While violent actions by Israel often lead to a short-term decrease in Palestinian terrorist activity, there is a corresponding long-term increase in terrorism. |

| | | | |
|---|---|---|---|
| Phillips (2013) | Mexico (organised crime groups) | Impact of killing or arresting leaders of Mexican drug cartels | 1. Killing leaders -> No significant impact on violence in short-term, increase in long-term<br>2. Arresting leaders -> Significant decrease in short-term, increase in long-term |
| Benmelech, Berrebi & Klor (2010) | Israel/ Palestine | Examines whether house demolitions are an effective counterterrorism tactic against suicide terrorism. | 1. House demolitions targeting the dwellings of Palestinian terrorists were deemed to cause "an immediate, significant decrease in the number of suicide attacks"<br>2. House demolitions that were indiscriminately targeted against the Palestinian community at large caused a significant increase in subsequent suicide attacks. |
| Condra & Shapiro (2012) | Iraq | Impact of 'collateral damage' on subsequent insurgent violence. | 1. Iraqi insurgent attacks significantly increased following civilian deaths attributed to coalition forces.<br>2. Attacks significantly decrease following coalition force activities that kill insurgents. |
| Braithwaite & Johnson (2012) | Iraq | Analyzed the sequential relationship between Iraqi insurgent attacks and Coalition counterinsurgency (COIN) operations. | 1. Indiscriminate COIN operations in a particular geographic area elevated the likelihood of subsequent insurgent attacks in the same area in the medium- to long-term,<br>2. The opposite was true for discriminatory and capacity-reducing COIN operations. |
| Gill, Horgan & Piazza (In Press) | Northern Ireland | Did the occurrence of killing PIRA members or members of the Catholic community impact PIRA bombing activities (a) in general and (b) against particular targets. | Both indiscriminate and discriminate CT killings caused a significant increase in PIRA bombing activities (Particularly bombings that targeted civilians) |
| Asal, Gill, Rethemeyer & Horgan (2014) | Northern Ireland | Did the occurrence of killing PIRA members or members of the Catholic community impact PIRA's ability to kill? | 1. Killing PIRA members significantly decreases IED fatalities<br>2. Killing innocent Catholics in a Brigade's county significantly increases total and civilian IED fatalities & shooting fatalities |

The American political scientist Joseph K. Young succinctly expresses the aggregate impression that one generates from this wealth of studies:

"In social science, there aren't really laws like gravity. There are always exceptions. Most theories are probabilistic. We expect something on average to go up whenever another thing goes down (or up). We look at trends and note the exceptions and hope to get it right more than we get it wrong. One process, from my observation, seems nearly law-like. Violence begets violence…Sometimes violence is necessary, sometimes it is unavoidable, sometimes it may be the moral decision, but I think whatever the justification for its use, it will (almost) always generate more of itself"

## Drone strikes in Pakistan

This particular study is interested in the impact of US drone strikes in Pakistan on subsequent terrorist activity there. The analyses depicted below are based on data from two sources. Data related to drones was kindly supplied by the Bureau of Investigative Journalism. This data provides accurate data on drone attacks within Pakistan's borders between 2004 and 2013. The variables include locational and temporal details and fatality metrics disaggregated across civilian and children lines. The terrorism event data comes from the Global Terrorism Database, a free resource provided by the START Center at the University of Maryland. This data also encompasses locational and temporal details and fatality metrics as well as details regarding target type.

## Analysis 1: Impact at the monthly level

The first analysis aggregated the drone and terrorism data into monthly amounts. For example, March 2008 witnessed 1 drone attack, 18 deaths by drones (at least 4 of which are civilian and at least 1 of which was a child). It also witnessed 28 terrorist attacks (of which 14 targeted the military, religious figures or government – in other words 'High Value Targets') and a total of 109 were killed. In total, the sums for 120 months were calculated. A correlational matrix was run and the results are displayed in Table 1. Significant associations are shaded.

**The results indicate that:**

1. The more drone attacks in a given month, the higher the number of terrorist attacks and fatalities attributed to terrorist attacks. It also appears that this spike in terrorist activity is disproportionately aimed against civilians and not high-value targets.

2. The more people killed in drone attacks, doesn't have any significant impact on terrorist attacks in a given month. However, there does appear to be some tit-for-tat aspects. The more people killed in drone attacks in a given month is significantly associated with more people being killed by terrorist attacks and this could be a function of more terrorist attacks targeting civilians.

3. Who is killed in drone attacks doesn't appear to have any correlation with terrorist behaviour.

In sum, there appears to be a relationship between the proliferation of drone attacks and terrorist attacks within a given month. The content of the drone attack (in terms of how many are killed or who is killed) doesn't appear to change the frequency of terrorist attacks significantly. What matters is that these drone strikes occur; and not necessarily what they do.

**Table 1: Correlation between drone and terrorist behaviour in the same month**

| | | Drones | DeathBy Drone | Civilian DBdD | Children DBD | TTAttack | HVT | Civilian | Fatalities |
|---|---|---|---|---|---|---|---|---|---|
| Drones | Pearson Correlation | 1 | .846** | .260** | .053 | .265** | .131 | .349** | .350** |
| | Sig. (2-tailed) | | .000 | .004 | .562 | .003 | .153 | .000 | .000 |
| DeathByDrone | Pearson Correlation | .846** | 1 | .545** | .355** | .125 | -.020 | .229* | .211* |
| | Sig. (2-tailed) | .000 | | .000 | .000 | .172 | .825 | .012 | .021 |
| CivilianDBdD | Pearson Correlation | .260** | .545** | 1 | .902** | -.074 | -.120 | -.034 | -.045 |
| | Sig. (2-tailed) | .004 | .000 | | .000 | .420 | .193 | .712 | .628 |
| ChildrenDBD | Pearson Correlation | .053 | .355** | .902** | 1 | -.107 | -.118 | -.091 | -.105 |
| | Sig. (2-tailed) | .562 | .000 | .000 | | .244 | .201 | .321 | .252 |
| TTAttack | Pearson Correlation | .265** | .125 | -.074 | -.107 | 1 | .947** | .969** | .750** |
| | Sig. (2-tailed) | .003 | .172 | .420 | .244 | | .000 | .000 | .000 |
| HVT | Pearson Correlation | .131 | -.020 | -.120 | -.118 | .947** | 1 | .839** | .769** |
| | Sig. (2-tailed) | .153 | .825 | .193 | .201 | .000 | | .000 | .000 |
| Civilian | Pearson Correlation | .349** | .229* | -.034 | -.091 | .969** | .839** | 1 | .682** |
| | Sig. (2-tailed) | .000 | .012 | .712 | .321 | .000 | .000 | | .000 |
| Fatalities | Pearson Correlation | .350** | .211* | -.045 | -.105 | .750** | .769** | .682** | 1 |
| | Sig. (2-tailed) | .000 | .021 | .628 | .252 | .000 | .000 | .000 | |

## Analysis 2: Lagged effects at the monthly level

A major problem with the above analysis is that it does not take the sequencing of attacks into account. By aggregating the counts it doesn't take account of when the drones and terrorist attacks happened within that month. The above findings are related to correlations, not causation. The March 2008 example shows 1 drone attack and 28 terrorist attacks. Our understanding of the relationship between the two factors would be very different if the 28 attacks preceded, not proceeded, the 1 drone attack. In that case, the correlation appears to be a result of drone strikes responding to a spike in terrorist attacks. If the drone strike preceded, not followed, the 28 terrorist attacks, our reading of the situation would be different. To overcome this problem, analysis 2 lags the terrorist attack counts by one month. In other words, we are now looking at the correlation, for example, between drone related behaviours in month 1 and terrorist related behaviours in month 2. Analysis 1 on the other hand, looks at the correlation of both within the same month. Table 2 outlines the results.

The same significant findings as analysis 1 are found. We can now say with a little more confidence that terrorist attacks (particularly ones targeting civilians) and fatalities spike in the aftermath of a drone strike.

**Table 2: Correlation between drone and terrorist behaviour lagged effects**

| | | Drones | DeathBy Drone | Civilian DBdD | Children DBD | TTAttack | HVT | Civilian | Fatalities |
|---|---|---|---|---|---|---|---|---|---|
| Drones | Pearson Correlation | 1 | .846** | .260** | .053 | .207* | .075 | .294** | .285** |
| | Sig. (2-tailed) | | .000 | .004 | .562 | .024 | .419 | .001 | .002 |
| DeathByDrone | Pearson Correlation | .846** | 1 | .545** | .355** | .099 | -.043 | .201* | .185* |
| | Sig. (2-tailed) | .000 | | .000 | .000 | .285 | .646 | .028 | .044 |
| CivilianDBdD | Pearson Correlation | .260** | .545** | 1 | .902** | -.091 | -.149 | -.039 | -.052 |
| | Sig. (2-tailed) | .004 | .000 | | .000 | .326 | .105 | .674 | .576 |
| ChildrenDBD | Pearson Correlation | .053 | .355** | .902** | 1 | -.096 | -.123 | -.068 | -.094 |
| | Sig. (2-tailed) | .562 | .000 | .000 | | .297 | .181 | .459 | .311 |
| TTAttack | Pearson Correlation | .265** | .125 | -.074 | -.107 | 1 | .947** | .968** | .758** |
| | Sig. (2-tailed) | .003 | .172 | .420 | .244 | | .000 | .000 | .000 |
| HVT | Pearson Correlation | .131 | -.020 | -.120 | -.118 | .947** | 1 | .836** | .774** |
| | Sig. (2-tailed) | .153 | .825 | .193 | .201 | .000 | | .000 | .000 |
| Civilian | Pearson Correlation | .349** | .229* | -.034 | -.091 | .969** | .839** | 1 | .689** |
| | Sig. (2-tailed) | .000 | .012 | .712 | .321 | .000 | .000 | | .000 |
| Fatalities | Pearson Correlation | .350** | .211* | -.045 | -.105 | .750** | .769** | .682** | 1 |
| | Sig. (2-tailed) | .000 | .021 | .628 | .252 | .000 | .000 | .000 | |

## Analysis 3: Weekly analysis

Analyses 1 and 2 find a relationship at the monthly level. Next, we drill down on our unit of analysis to the weekly level in a couple of ways. A series of independent t-tests were conducted that compared (a) the number of terrorist attacks in total (b) the number of terrorist attacks on civilians (c) the number of terrorist attacks on high value targets and (d) the number of fatalities in the 7 days prior and after every drone strike. Table 3 outlines the results. It indicates that there is no discernible shift in behaviours in the week immediately after a drone strike in either direction. It is actually strikingly similar. While analyses 1 and 2 note a spike in terrorism at the monthly level, it certainly appears that this spike is not immediate, but rather appears gradually over weeks 2-4 for example.

**Table 3: Before and after a drone strike comparisons**

| | When | N | Mean | Std. Deviation | Std. Error Mean |
|---|---|---|---|---|---|
| Attacks | Before | 383 | 21.1514 | 13.51974 | .69083 |
| | After | 383 | 21.0183 | 12.51354 | .63941 |
| Civilian | Before | 383 | 14.2533 | 8.02653 | .41014 |
| | After | 383 | 14.0418 | 7.42455 | .37938 |
| HVT | Before | 383 | 6.8982 | 7.01737 | .35857 |
| | After | 383 | 6.9765 | 6.70250 | .34248 |
| Fatalities | Before | 383 | 40.3238 | 34.53770 | 1.76479 |
| | After | 383 | 40.5379 | 39.68064 | 2.02759 |

A potential problem with the above analysis is the level of overlap between the drone attacks which were themselves clustered in space and time. Perhaps this clustering effect has caused some double counting and has thrown off the findings somewhat. The same test was therefore run that only included drone strikes that appeared in isolation within a given week. This narrowed down the sample substantially (by 70%). The results however stayed the same although there does appear to be a (non-significant) widening of the number of fatalities caused in the aftermath of an isolated drone attack.

**Table 4: Before and after a drone strike comparisons II**

| | When | N | Mean | Std. Deviation | Std. Error Mean |
|---|---|---|---|---|---|
| Attacks | Before | 109 | 22.8716 | 16.37020 | 1.56798 |
| | After | 109 | 22.5780 | 14.71287 | 1.40924 |
| Civilian | Before | 109 | 14.3119 | 9.52355 | .91219 |
| | After | 109 | 14.0418 | 7.42455 | .37938 |
| HVT | Before | 109 | 8.5596 | 8.51190 | .81529 |
| | After | 109 | 8.1927 | 7.89571 | .75627 |
| Fatalities | Before | 109 | 37.9450 | 31.76734 | 3.04276 |
| | After | 109 | 42.9083 | 37.79882 | 3.62047 |

Next, we broke this analysis down by region and found that this fatality divergence is largely attributable to drone attacks that occur in Bajaur, Kurram and South Waziristan.

## Analysis 4: Disaggregating drone impacts & weekly behaviour

Analysis 3 simply tested the impact of drones on terrorist behaviour at a weekly level and found no significant impact. Next, we tested whether what occurred in the drone attack matters (Remember, this was not the case at the monthly level). The results suggest that it does impact behaviour but possibly not in the direction we expect. Particularly deadly drone attacks ease the number of subsequent attacks across all categories of targets. However, this downgrading in activity has no significant impact upon the numbers killed by terrorist groups. So while their capacity to operate lessens, they are just as lethal when they choose to do so. We also tested whether these effects are made stronger by the presence of multiple drone attacks and it appears that the results stay consistent.

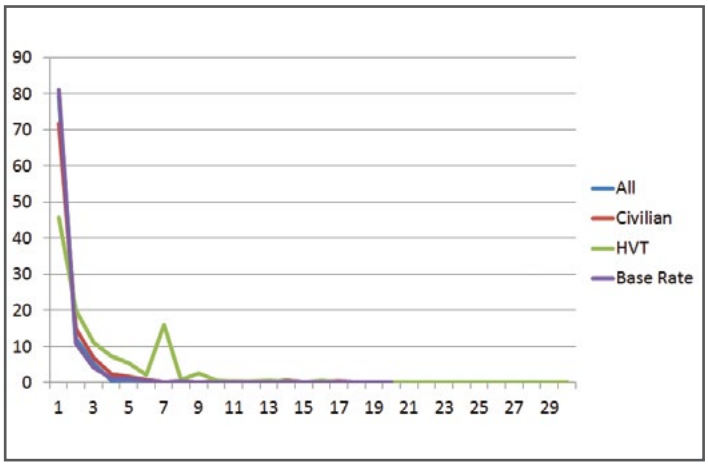
**Table 5: Correlation between drone and terrorist behaviour in the subsequent week**

| | | DeathByDrone | CivDeathByDrone | InjByDrone | ChildByDrone | TActsPW | TActsCPW | DronePW | TActsHVTPW | FatalitiesOW | TActsFW | TActsCFW | TActsHVTFW | FatalitiesFW |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DeathByDrone | Pearson Correlation | 1 | .693** | .380** | .638** | -.149** | -.119* | -.043 | -.151** | -.118* | -.179** | -.176** | -.139** | -.099 |
| | Sig. (2-tailed) | | .000 | .000 | .000 | .004 | .020 | .406 | .003 | .021 | .000 | .001 | .006 | .053 |
| | N | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 |
| CivDeathByDrone | Pearson Correlation | .693** | 1 | .129* | .924** | -.118* | -.117* | -.088 | -.094 | -.090 | -.148** | -.139** | -.122* | -.082 |
| | Sig. (2-tailed) | .000 | | .011 | .000 | .021 | .022 | .087 | .068 | .077 | .004 | .006 | .017 | .108 |
| | N | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 |
| InjByDrone | Pearson Correlation | .380** | .129* | 1 | .076 | -.127* | -.090 | -.032 | -.142** | -.112* | -.111* | -.085 | -.114* | -.059 |
| | Sig. (2-tailed) | .000 | .011 | | .139 | .013 | .079 | .537 | .005 | .028 | .029 | .096 | .026 | .249 |
| | N | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 |
| ChildByDrone | Pearson Correlation | .638** | .924** | .076 | 1 | -.113* | -.121* | -.084 | -.080 | -.084 | -.120* | -.126* | -.085 | -.062 |
| | Sig. (2-tailed) | .000 | .000 | .139 | | .027 | .018 | .101 | .116 | .102 | .019 | .013 | .098 | .229 |
| | N | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 | 383 |

## Analysis 5: Daily analysis

In relation to each drone incident i, the time elapsed until the subsequent incident i+1 was calculated (The smallest unit of time available was the date on which the incident occurred, therefore excluding the possibility of determining the order of multiple incidents taking place on the same day. However, in relation to the present analysis it was necessary only to measure the frequency of time delays between incidents so this was not problematic. For example, were four incidents to occur on the same date, three of these would be considered to be followed by a further incident on the same day with i+1 in relation to the final incident occurring on the nth day; it is not necessary to determine the order of these incidents). The data was then aggregated to indicate in how many instances the subsequent incident i+1 occurred on the same day, in how many instances it occurred one day later, two days later and so forth. These frequencies were subsequently used to estimate the hazard rate at each time interval with the denominator defined by how many incidents in the sample had not yet experienced i+1, effectively, in how many instances districts remained at risk after their initial incident.

The analysis indicated that in approximately 80% of drone attacks, a terrorist attack is likely to follow within a day. The hazard rate then begins to decline dramatically, but remains at a relatively elevated level until day three before decaying. This figure appears remarkably high but when compared against the base rate, it actually remains quite consistent with normal day-to-day affairs where no drone attack is present. When we disaggregate across who is targeted by these terrorist attacks, a slightly different pattern emerges. Just over 40% of drone strikes are followed the next day by an attack against high value targets. This elevated level of risk lasts longer than those targeting civilians and spikes again around days 7 and 8. This second spike may account for some of the disparities found between the monthly and weekly levels of analysis. The findings are also indicative of the ease with which civilians can be targeted in the direct aftermath of a drone strike, compared to high-value targets (75% vs. 43%).




## Conclusion

These analyses collectively show the complex relationship between targeted killings by drones and terrorist attacks. The answer is not as easy as the traditional deterrence vs. backlash argument. Both are apparent in these analyses but their prevalence changes dependent upon where the measure of 'effectiveness' occurs. The rate of attacks remain consistent for the first day compared to the base rate but this then ebbs away significantly in the week that follows before returning stronger again over the course of the subsequent 3 weeks. This is particularly the case in relation to the terrorist group targeting civilians.

**This is a summary of *The Impact of Drone Attacks on Terrorism: The Case of Pakistan* by Dr Paul Gill.**

# Terrorist Relocation and the Societal Consequences of US Drone Strikes in Pakistan

Dr Wali Aslam

**The US drone programme in the Federally Administered Tribal Areas (FATA) of Pakistan seems to be coming to an end. Supporters of drones have argued that they work because they have been successful in killing key terrorist leaders and their deployment has led to 'denying terrorists sanctuaries in Pakistan' and elsewhere. It is true that the number of terrorists operating in FATA is likely falling. Drones have indeed pursued some high-value targets, which has led to other terrorists' plans being disrupted. However, drone strikes have also had serious negative consequences for Pakistani society, and these effects remain under-examined. This report examines 'on-the-ground,' negative consequences of drone attacks. It looks at the consequences of terrorists' relocation from heavily targeted tribal territories to avoid being attacked by US drones. The relocation has had a serious impact on their new host societies. It is important to acknowledge that drones are just one of the factors that have forced the relocation of terrorists to the rest of the country. The Pakistani army also conducted a number of operations in parts of FATA and northwest Pakistan, including South Waziristan and Swat, starting in 2008 and, for balance, it is crucial to remember that these military operations have also dislocated terrorists in the country's northwest, causing them to move to other parts of Pakistan. However, an examination of all relocations is beyond the scope of this study.**

"Drones have indeed pursued some high-value targets, which has led to other terrorists' plans being disrupted. However, drone strikes have also had serious negative consequences for Pakistani society, and these effects remain under-examined."

## Method

This research will only concern itself with studying the relocation caused by US drones. For that purpose, it will examine four destinations within Pakistan where terrorists are settling once they are displaced from FATA, in order to avoid being targeted by

drones. These include the southern megacity of Karachi in Sindh province, a relatively safe tribal agency of Kurram (within FATA) and Punjab and Baluchistan provinces of Pakistan. The study focuses on the activities of militants once they reach their new refuges and it argues that those fleeing the tribal areas engage in different activities in different locations. These activities include participating in organised crime, committing sectarian and jihadi violence and perpetrating other petty crimes. The consequences of the move take different forms depending on the destination. The next section of the report (see 'Findings' below) conducts a case study on the city of Karachi. It will look at the terrorist movement and its consequences for the mega-city. I will then examine the case of Kurram agency, one of the tribal territories of FATA, where the drone strikes have indirectly caused an increase in sectarian strife and a number of casualties. This will be followed by the cases of the provinces of Punjab and Baluchistan. I will then critically evaluate the policy of the use of drone strikes in Pakistan and show how the UK government can learn valuable lessons from the US drone programme in Pakistan given increasing UK investment in its own drone programme. In closing, the report will argue that the policy of conducting drone strikes in FATA has some flaws. The problems will reappear in the area once drone strikes have stopped. Various other measures will have to be adopted if the government of Pakistan, the United States and the broader international community are genuinely interested in eliminating militancy from FATA for good. The conclusion will conduct a brief overview of those measures.

**Figure 1: Map of Pakistan (FATA highlighted)**


*© CIA World Factbook*

# Findings

## Karachi

Karachi, the capital of Sindh province is Pakistan's largest city and the ninth largest in the world by population. It is the biggest Pashtun city in the world. It generates approximately 70% of Pakistan's GDP. Since early 2010, it has been experiencing some of the worst violence in its history resulting in death and injury to thousands of civilians. Some have argued that, with the Pakistani army starting major military operations in Swat in May 2009, and in South Waziristan in November 2009, migrants were pushed to the south and Pashtuns from these areas joined their brethren to find safe havens in the city, thereby destabilising the ethnic balance in Karachi and leading to conflict over scarce resources. However this ethnic explanation is inadequate as the city witnessed a large influx of migrants as a result of the Afghanistan jihad in the 1980s without such a wave of violence. A number of militants fleeing drone strikes in FATA (similar to those dislocated by Pakistan's military operations in the northwest of the country) have chosen to relocate to Karachi. The city's existing Pashtun networks have facilitated the move by making room for new arrivals. Karachi provides ample opportunities for these new residents to engage in petty crime such as kidnapping for ransom and land-grabbing. The proceeds generated by these crimes are often channelled back to various militant groups in FATA and elsewhere. Some of the new arrivals have also joined the ranks of those seeking to undermine secular political parties. An increase in attacks on secular political parties, kidnapping and petty crime occurred after 2010, coinciding with a dramatic increase in drone attacks in the same year (122, compared with 36 and 54 in 2008 and 2009, respectively).

## Kurram Agency

While some terrorists fleeing drone strikes have chosen to leave FATA, others have tried to take refuge in relatively safer agencies of FATA, one of which is the Kurram agency, surrounded by Afghan territory on the north and the west and bordering the North Waziristan agency to the south. The tribal agency of Kurram has attracted a number of terrorists fleeing the heavily targeted parts of FATA, such as the North Waziristan agency which has been the prime target of drones. Kurram is home to the largest population of Shia Muslims in FATA and has endured only a limited number of strikes, making it an attractive place to hide for those trying to escape US drones. The territory is also a suitable

destination for a number of Taliban fighters given its location and proximity to major urban hubs in Afghanistan, including Kabul and Jalalabad. For these reasons, a number of fighters want to use its routes to attack international forces based in Afghanistan. The move by terrorists to relocate to Kurram and use its access routes has been resisted by the locals who understandably fear US drones. This has, in turn, resulted in anti-Shia violence in Parachinar, Kurram agency's capital, leaving hundreds of casualties. It has been estimated that since 2007 the Turi Shia tribe of Kurram has lost an estimated 2,000 members to violence.

**Figure 2: Movement within the FATA**


*Source: TerrorismWatch.com*

### Punjab and Baluchistan

Militants fleeing from FATA, and other parts of northwest Pakistan due to US drone action and Pakistan army operations, have also taken up residence in the Pakistani provinces of Punjab and Baluchistan. Punjab, the most populous province in Pakistan has been attracting a number of terrorists relocating from northwest Pakistan. In Punjab, these individuals preach a more violent interpretation of Islam than many locals, bringing negative consequences for those incumbent groups – such as Shias and Barelvis. The latter of these follow a milder, Sufi-like version of Islam and constitute the largest proportion of Muslims in Punjab. A number of Sufi shrines have recently been targeted by suicide bombers, killing hundreds. There have also been attacks on Punjab's Ahmadi, Shia and Christian communities since 2007, leaving hundreds dead. The terrorists relocating to Punjab strengthen the ranks of militants already there. The long-term impact of this relocation on the sectarian landscape of Pakistan is set to be particularly negative. The terrorist relocation to Punjab has led to radicalisation of usually tolerant Sunni Muslims of Punjab who, until recently, have lived peacefully with other sects and religions.

Baluchistan province provides lucrative opportunities for drugs and arms smuggling given its location on the border with Iran and its land links with Europe. The most recent incidents of terrorist attacks have been blamed on sectarian and separatist groups in the province. Those relocating to Baluchistan have so far refrained from engaging in violent activities for the fear of attracting US drones. The United States has often hinted that it may expand the drone attacks within Baluchistan, in which case there is a risk of major disruption for the leadership of the Taliban and al-Qaeda militants living there. Should the leadership move to Karachi, a status until now enjoyed by Quetta (the capital of Baluchistan), the Taliban will not have any need to keep peace in Baluchistan and are likely to become involved in terrorist activities and criminality.

**Figure 3: A map of Pakistan (arrows mark the relocation of militants out of FATA)**


## Drones strikes – policy flaws and lessons for the UK government

Pakistan has suffered brutal violence since 2007 with an estimated 50,000 deaths due to a combination of suicide bombings, improvised explosive devices (IEDs) and gun attacks. Although there are other dislocating factors at work concurrently, the negative societal consequences of US drone action in Pakistan show that a policy that changes the focus of terrorists from Western forces to local targets could be unethical. If drone strikes are to have an element of legitimacy as key instruments of remote-control warfare, they must be employed after a thorough assessment of their

consequences at the receiving end. The British government can learn from the US experience in Pakistan. The research has shown how the use of drones can have profound societal consequences for communities. The question arises who is responsible for the harm to civilians perpetrated by terrorists who relocate due to drones. In the end, the aim of the strikes cannot be just to protect Western forces in conflict zones but also innocent civilians from harm.

## Conclusion

FATA has one of the world's worst education systems and a virtually non-existent rule of law. Such conditions are the nurseries in which violent extremism thrives. Without a proper education system young children have no option but to go to madrassas, which act as stepping stones for violent extremism, and the lack of rule of law forces people to turn to jihadi militant leaders to seek security. The demand for these services will not decrease unless underlying problems in FATA are addressed. There is a need to bring the territory into the mainstream of Pakistani politics. In the current situation, once the focus of the international community moves away from the region, the problem could very well reappear in that area. The US also needs to re-evaluate its relations with Pakistan which is nominally a US 'ally' in the campaign against terrorism and deal with the Pakistani army's policy of playing 'double games' by allying also with terrorists to achieve its aims.

The study recognises that US drones alone are not responsible for terrorist relocation and that various operations by the Pakistani army have also contributed. The study has primarily focused on the relocation caused by drones and the sources examined in this report have asserted that these drones, in addition to Pakistan's military operations, are playing a role in causing relocations. These relocated individuals have gone on to inflict harm on Pakistani civilians as asserted by various sources examined. The report acknowledges that members of Pakistan's decision-making elite have by far the most blame to carry for the situation in which Pakistan finds itself today and that the problems caused by US drones are miniscule compared to certain steps taken by Pakistan's political and military elite. However, the scope of the research endeavours to highlight only the relocation caused by drones.

The report concludes that the US should be held accountable for the effects of its drone policy. The report also suggests that a more comprehensive analysis of the efficacy of drone strikes cannot be conducted without looking at the bigger picture highlighted here. The idea that the drones policy should be characterised as a 'success' on the basis that it has sharply reduced the threat of terrorism in the short run against US targets needs re-evaluation.

**This is a summary of *Terrorist relocation and the societal consequences of US drone strikes in Pakistan* by Dr Wali Aslam. For the full report, including citations, visit remotecontrolproject.org/our-reports**

# US Special Operations Command Contracting: Data-Mining the Public Record

Crofton Black

*U.S. Army Soldiers from Alpha Company, 4th Battalion, 10th Special Forces Group, Fort Carson, Colo., prepare to call for close air support. Creative Commons, Flickr / US Air Force*

**This report examines federal spending by the US Special Operations Command (USSOCOM) via the medium of the Federal Procurement Data System – an open access database which gives researchers a window into US government procurement. USSOCOM has existed since 1987 and is headquartered at MacDill Air Force Base, Florida. It has about 57,000 active duty troops and civilians and includes four commands (Army Special Operations Command, Naval Special Warfare Command, Air Force Special Operations Command, Marine Corps Forces Special Operations Command) and one sub-unified command (the Joint Special Operations Command). Its mission statement is to "provide fully capable Special Operations Forces to defend the United States and its interests" and to "synchronize planning of global operations against terrorist networks".**

This report looks at unclassified records of procurement by USSOCOM over a five-year period, starting in January 2009, approximately at the inauguration of Barack Obama's presidency. Transactions listed over this period amount to a sum of nearly $13 billion. The dataset analysed here gives us a detailed snapshot of activities carried out by the "military industrial complex" and points to ways in which these activities connect to remote warfare.

**"USSOCOM outsourcing has been dominated by a relatively small group of companies. Although over 3,000 companies provided services as Global Vendors, eight of these companies accounted for over 50% of total transaction value."**

## Method

Given the context of this report I have chosen not to focus on more traditional military hardware (e.g. purchase of helicopters and bullets) although these too are represented in the dataset. Investigative journalists have long been aware of the value of federal contracting data in uncovering or filling out stories. On their own, such data are fairly dry: to make a story they usually need to be complemented with interviews, FOIA requests, congressional

notifications and other material. Nonetheless there is an intrinsic value to the initial quantitative analysis.

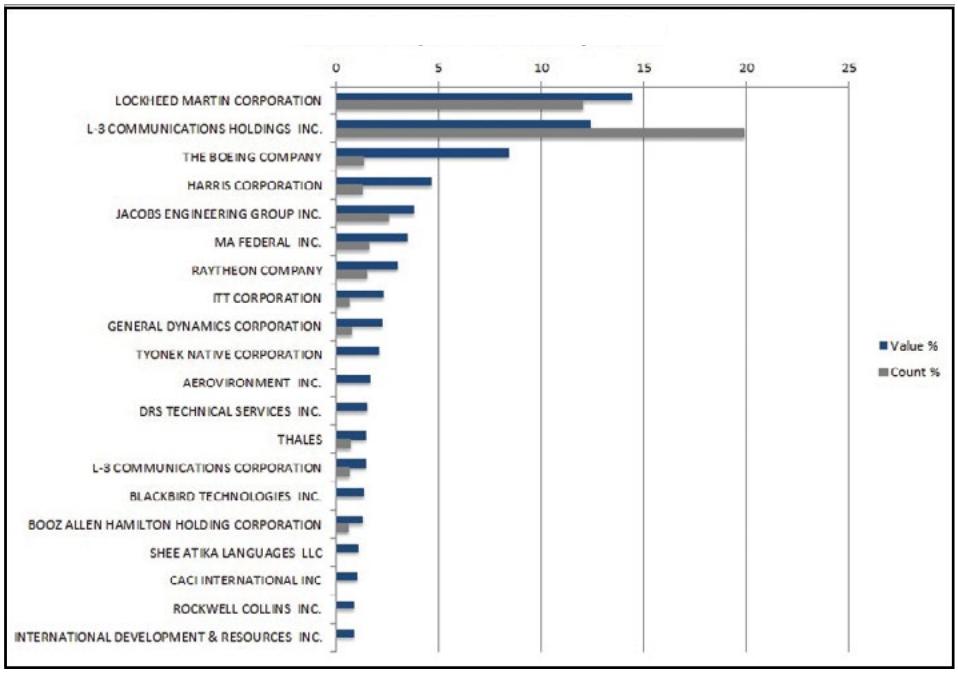
The purpose of this research is to provide an insight into the activities of USSOCOM via its unclassified procurements. It is not intended to provide absolutely reliable accounting data. While I have tried to remain aware of possible inconsistencies and mitigate them where possible, I have not attempted to clean up the entire dataset. As a result, inaccuracies may be present, although I hope that these will be quite small.

## Findings

The dataset covers many types of purchases, from computer systems to bullets. After an initial analysis, the report focuses on purchases relating to remote warfare.

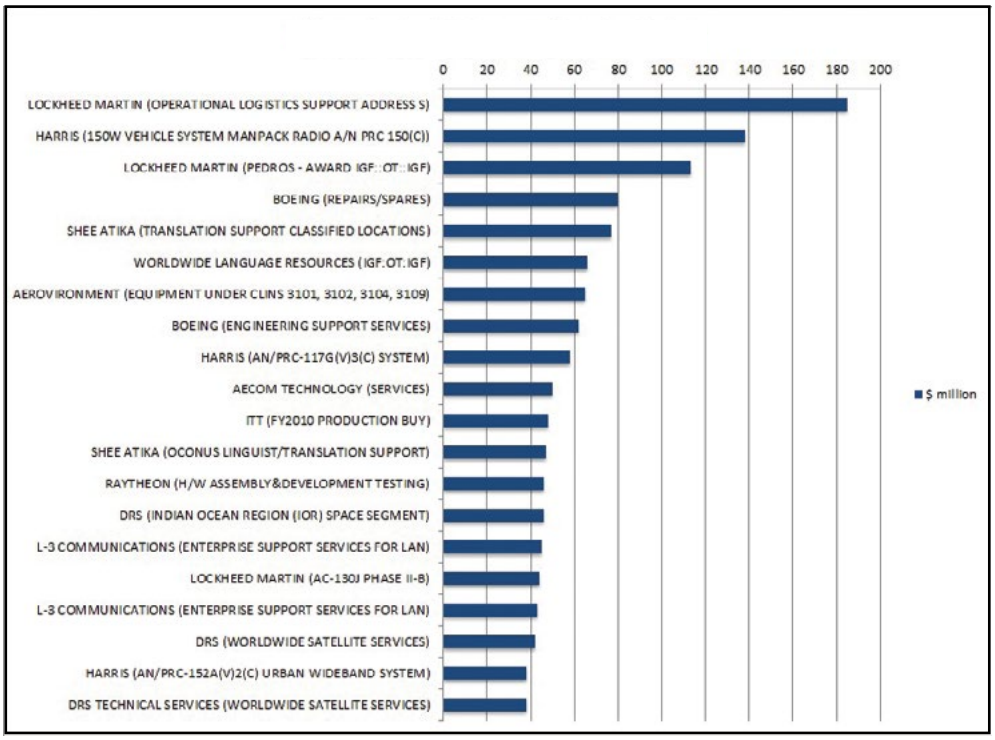
USSOCOM outsourcing has been dominated by a relatively small group of companies. Although over 3,000 companies provided services as Global Vendors, eight of these companies accounted for over 50% of total transaction value. These eight were Lockheed Martin, L-3 Communications, Boeing, Harris Corporation, Jacobs Engineering Group, MA Federal, Raytheon and ITT Corporation. The top 20 companies account for nearly 70% of the total expenditure (see chart below).

**Figure 1: Top 20 vendors by value**



Among the most expensive individual transactions were: radio communications from Harris Corporation; translation support in classified locations from Shee Atika LLC; procurement of drones equipment from Aerovironment Inc.; worldwide and Indian Ocean satellite services from DRS Technical Services Inc.; and IT Services from L-3 (see chart below).

**Figure 2: Top 20 transactions by value**




## Case Studies

The report contains four case studies.

### Information Activities in Africa: Magharebia and Native Prospector

The first examines information-related purchases by the Africa Command (AFRICOM), whose theatre of operations has seen a significant expansion of counter-terrorism activity in the past years. The Special Operations Command has contracted General Dynamics to run a website (Magharebia) as part of its information operations initiative in the region. There is no reference to General Dynamics in the Magharebia website but it admits its affiliation with USSOCOM, stating that it is a central source of news and information about the Maghreb in three languages: Arabic, French and English and that its goal is to offer accurate, balanced and forward-looking coverage of developments in the Maghreb. A 2012 Stimson Center report contextualised Magharebia within “Clearly Public Diplomacy-Like Activities” as one of USSOCOM’s “Trans Regional Web and Magazine Initiatives” noting that the Senate Armed Services Committee described it as an initiative under which USSOCOM establishes websites to counter violent extremism objectives. In setting out the requirements for interested contractors, it was stated that the content should “provide open and unbiased analyses of major events in the targeted regions” but it also outlined that content should be strongly drawn from contributors with a particular background on various aspects of the “Global War on Terror”.

Navanti Group, a subcontractor for Jacobs Technology, also provides intelligence and information support to the Special Operations Command in Africa, the military command responsible for supporting and enhancing US efforts to promote stability, co-operation and prosperity in the region. A programme (Native Prospector) was developed by Navanti with the purpose of providing research and analyses focusing on al-Qa’ida and affiliates in North Africa (Libya and Tunisia), West Africa (Northern Mali and Northern Nigeria) and East Africa (Somalia and Horn of Africa).

options is anticipated to be put in place under Navanti Group, LLC's GSA Advertising & Integrated Marketing Solutions (AIMS) - Schedule 541, GS-07F-0412Y from the current end date of 9/21/2012 of an existing task order (H92222-10-D-0018 Task Order 004) through 4/20/2013. This bridge order is necessary to prevent a break-in-service for SOCAFRICA and SOCEUR's need for continued marketing services support and to allow sufficient time to smoothly compete for a follow-on order.

**(c)(2)(iii) Description of Services.**

This task order will continue to provide U.S. Special Operations Command-Europe with target audience analysis and market research in support of J39 communications and engagement. Activities under this contract will support J3 strategic communications and information operations to engage local populations and counter nefarious influences within AFRICOM and EUCOM area of responsibility (AOR) and which may be emanating from United States Central Command (CENTCOM), or other AORs. The contractor shall provide research, assessments,

[redacted]

This contracted activity will be for Native Prospector research and analysis in the following SOCAFRICA AORs:

North Africa: Focusing on al-Qa'ida & affiliates in Libya, with additional / cursory coverage of AQ in Tunisia
West Africa: Focusing on al-Qa'ida & affiliates in northern Mali and Northern Nigeria
East Africa: Focusing on al-Qa'ida & affiliates in Somalia and Horn of Africa

[redacted]

**(c)(2)(iv) Justification Rationale.**

This acquisition is being conducted under the authority of the Multiple Award Schedule program. The statutory authority permitting other than full and open competition is Section 201

### Intelligence, Surveillance, Reconnaissance: Afghanistan and the Philippines

The second case study looks at ISR services. Around 156 transactions in the dataset are stated as involving “ISR” in some capacity. Over two-thirds of these were with Boeing, often via its subsidiary McDonnell Douglas. Performance for these transactions was divided between Afghanistan (most frequently), Iraq, the Philippines and the USA. The case study looks at key references in the dataset to drone use in Afghanistan and in the Philippines, where the US has conducted a low-level campaign against the Abu Sayyaf group. Although it is reported that the US is phasing out its counterterrorism unit in the Philippines, it is phasing in a new ten-year agreement with the Philippines that will provide greater access to bases there, providing the first presence of US troops in the Philippines since 1992 at a time of increased tension with China and its neighbours over claims in the East and South China Seas.

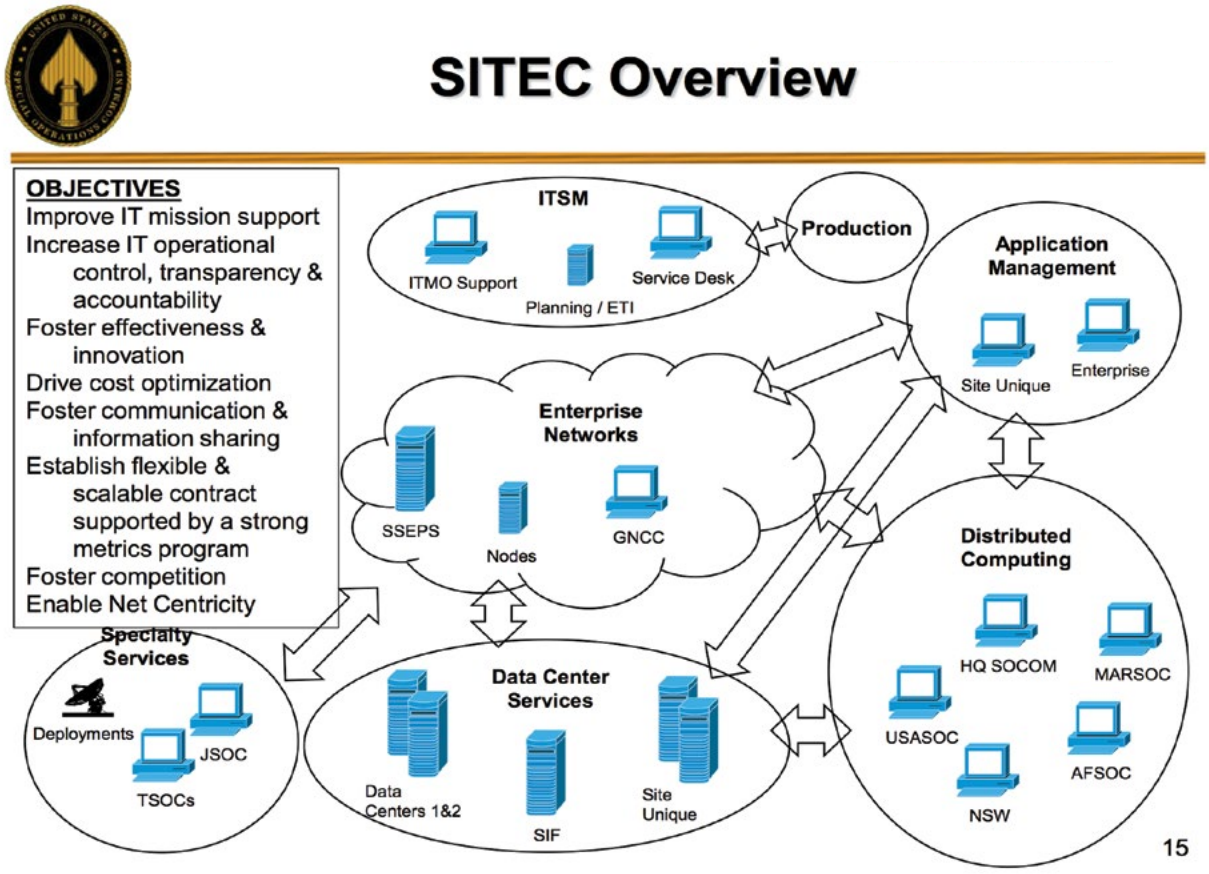


*http://batchgeo.com/map/052d6226d5fafd65e8afb0074357ab2f*

### Distributed Computing and Communications: SITEC

The third case study uncovers some of the activities taking place under the umbrella of the Special Operations Forces Information Technology Enterprise Contracts (SITEC). The SITEC framework is intended to provide a wide range of integrated enterprise IT services for USSOCOM, including planning, management and operation, and maintenance for all Wide Area Networks (WANs), Metropolitan Area Networks (MANs), and Local Area Networks (LANs). It also includes network and communication infrastructure for voice, video and data as well as information assurance, transmission, communication security, disaster recovery and help desk support. While it aims to integrate disparate systems across Special Operations Support into a single enterprise-wide network with global capability, it is spread over multiple contractors in so far as it aims “to move IT services support at USSOCOM from a single service provider to multiple providers in multiple capability areas called Towers”. Firms with major involvement in this overall project include L-3, General Dynamics, Science Applications International, and Arma Global, working alongside Hewlett-Packard, Pragmatics, Booz Allen Hamilton, Sterling Parent, Dell, Berico Technologies, DRS Technical Services, BAE Systems, CACI International, Gartner and Jacobs Engineering Group. The SITEC

framework demonstrates the US military's increasing commitment to networked information sharing – a "netcentric operating environment" which can provide IT services in support of global special operations "anywhere, anytime"




*A diagram from a 2012 presentation on USSOCOM's policy for "acquiring IT services". Annex 18, slide 15*

### Translation and Interrogation Services: Shee Atika

The fourth case study shows how translation services provided by Shee Atika accounted for one of the largest single transactions in the dataset ($77 million). As documents relating to this contract show, Shee Atika provided interrogation services as well as more general translation and role-play assistance for USSOCOM across the globe. Apart from this transaction, the dataset includes a further 131 transactions with three Shee Atika subsidiaries. Together they total $153.6 million. A redacted copy of the original contract, awarded in May 2007, shows that Shee Atika agreed to provide "foreign language interpretation, transcription, reporting and translation services to support various units and troops for USSOCOM". As well as military personnel, this included "any Government agency providing direct support to the SOF mission" which would allow contractors to work alongside CIA and FBI officials. In addition to providing translation and transcription (of local periodicals, foreign government publications and "captured enemy documents"), Shee Atika was also to provide "interrogation support".

**"In addition to providing translation and transcription, Shee Atika was also to provide "interrogation support"."**

Section C - Descriptions and Specifications

PERFORMANCE-BASED WORK STATEMENT (PWS)
LINGUIST AND TRANSLATION SERVICES
31 May 2007

1.0 **BACKGROUND.** The United States Special Operations Command (USSOCOM) is a Unified Command of the Department of Defense (DoD). USSOCOM is responsible for all Special Operations Forces (SOF) in DoD. USSOCOM leads, plans, synchronizes, and as directed, executes global operations against terrorist networks. USSOCOM trains, organizes, equips and deploys combat ready special operations forces to combatant commands.

2.0 **SCOPE.** The Contractor shall provide all labor, equipment, tools, materials, travel, and other items and services necessary to provide foreign language interpretation, transcription, reporting, and translation services to support various units and troops for USSOCOM. For the purposes of this PWS, USSOCOM includes all personnel in the USSOCOM Headquarters, the Naval Special Warfare Command (NAVSPECWARCOM), the U.S. Army Special Operations Command (USASOC), the Air Force Special Operations Command (AFSOC), the U.S. Marine Corps Forces Special Operations Command (MARSOC), the Joint Special Operations Command (JSOC), the Theater Special Operations Commands (TSOCs), and any Government agency providing direct support to the SOF mission.

3.0 **REQUIREMENTS.** The Contractor shall provide on-site linguist support elements during emerging military operations in various locations worldwide. Precise locations will be coordinated through the Contracting Officer's Representative (COR). The contractor is responsible to provide language interpretation when and where needed. This may or may not require movement of personnel. Specific requirements will be delineated by individual task orders at the start of the performance period.

3.1 **Translation Support.** The Contractor shall provide linguists for foreign language translation and interpretation support operations in other areas and/or countries and exercises and/or rehearsal events conducted prior to the start of military operations. Linguists may be required to travel from the Continental United States (CONUS) to the operational area via commercial transport or via travel conveyance arranged and directed by the Government. When Government provided travel is directed, the linguists will be provided with a departure location, date, and time. In all cases, regardless of mode of travel, forward elements will be made aware of, in advance of travel, the name, social security number, and exact travel information of all linguists traveling in support of this PWS. The personnel and/or language pool for the period of performance will be identified in the individual task orders and any modifications to the task orders issued by the Contracting Officer.

3.1.1 **Interrogation Support.** The Contractor shall provide interrogation support to USSOCOM. This support shall include linguist support to USSOCOM in the interrogation and debriefing of sources who are captured and/or detained and/or persons of interest being questioned. All interrogation support will be conducted in accordance with DoD Directive 3115.09 and all applicable DoD, USSOCOM, and organizational level detainee interrogation policies.

3.1.2 **Transcription Support.** The Contractor shall provide written conversions of source texts, including but not limited to local periodicals, magazines, foreign government publications, and captured enemy documents (CEDs) from one language into a target language, while keeping the meaning and intent of the original source. All translation documents shall be word processed in a standard text format and a hard and/or soft copy will be provided to the requiring activity as delineated in individual task orders.

3.2 **Hours of Operation.** The Contractor shall provide interpretation, transcription, reporting, and translation services as required by the supported elements up to 24 hours per day, 7 days per week. Hours of operation for linguists will be delineated by individual task orders. During off hours, linguists will remain on-call for emergency situations. The supported element leadership, normally the senior U.S. Government intelligence officer or designated representative, will notify the Contractor of work schedules for linguists based on specific mission requirements.

## Conclusion

The first product of this study is the dataset itself. Findings there have been discussed and include overall transaction totals, a breakdown of key vendors and product/service categories, a map of expenditure outside the continental US and a list of major individual transactions. Part Two has shown how fields in the FBDS-NG dataset can provide entry points to broader qualitative research. This report shows how corporations are integrated into some of the most sensitive aspects of special operations activities: flying drones and overseeing target acquisition, facilitating communications between forward operating locations and central command hubs, interrogating prisoners and translating captured material, and managing the flow of information from regional populations to the US military presence and back again. These examples are indicative of a broader finding which is the prevalence of information and communications technology among special operations command procurements. Drawing on this finding, each of the case studies illustrates facets of the role of information in modern warfare.

Information has been important in warfare since time immemorial but, as quantities of available information grow and, as information technology becomes increasingly embedded in warfare systems, corporations are relied upon to create, store and move this information. Nowadays, knowledge is still gained from people (via human intelligence collection, "subject matter experts" or the interrogation of prisoners and "people of interest") but the military has devoted an increasing portion of its budget to attempts to infer knowledge from phenomena which can include such "unstructured" sources as social media feeds and open source text (as analysed by Navanti). More typically, they are the physical landscapes and human activities overseen by "persistent" surveillance drones as seen in the case studies on Afghanistan and the Philippines. The greater the volume of phenomena surveyed, the greater the burden of transporting and analysing the observations; and thus the greater need for a robust and networked IT infrastructure (this being the overall goal of the SITEC framework). Though not discussed much in the case studies, human analysts can no longer keep pace with the inward flow of full motion video from drone sensor feeds and the quantum increase in data threatens to undermine rather than facilitate the emergence of knowledge. The US military has therefore recently solicited proposals for a variety of automated "processing and exploitation" techniques to identify and track targets within its video feeds. The procurement activities of the Special Operations Command – the "tip of the spear" – offer a snapshot of some prominent roles of information in modern warfare. The dataset points to the sharp end of US military activity and force projection in the recent past and near future. A central part of this activity lies in receiving, transferring and production of information and the processing of this information to produce knowledge with corporations integrated into every stage of the activity.

The dataset examined here, and the methods employed to analyse it, offer a rich source for investigators, academics, journalists and policy makers. More detailed work will enhance knowledge of the significant role that the private sector plays in remote warfare. This report offers a framework for interpreting the dataset and points to companies, products and services that will be of interest to other researchers. It also shows how public records can be interpreted to give a glimpse of the usually classified world of special operations.

**This is a summary of *US Special Operations Command Contracting: Data-Mining the Public Record* by Crofton Black. For the full report, including citations and annexes, visit remotecontrolproject.org/our-reports**

# Cyberspace: An Assessment of Current Threats, Real Consequences and Potential Solutions

Alberto Muti and Katherine Tajer with Larry Macfaul

Vertic

*The Ministry of Defence badge on a computer chip. The UK is building a dedicated capability to counter cyberspace attacks. © Crown Copyright*

**Leaders across the globe have identified cyber-attacks as one of the greatest threats facing developed nations. The rising importance of cyber security issues is also part of a global trend of moving towards 'remote control' warfare that minimises engagement and risk while extending its reach beyond conflict zones. This paper seeks to examine the role of cyber-attacks in remote control warfare, and considers the potential impact of cyber-attacks on civilian populations and on future international stability. It aims to provide a comprehensive overview of the main talking points in the cyber security field and to identify trends that may have an impact on future developments.**

"The rising importance of cyber security issues is also part of a global trend of moving towards 'remote control' warfare that minimises engagement and risk while extending its reach beyond conflict zones."

This report is divided into four sections: the first section will examine how the rise of potential threats and vulnerabilities in cyberspace is being addressed in state-to-state relations, and will present some important cases of cyber-attacks that have had an impact on foreign policy. The second section will look at the use of cyber-attacks during conflicts and at the potential of 'cyber weapons' to cause destruction and casualties on the scale of conventional weaponry. The third section will assess the impact of cyber-attacks on everyday life for civilians. Finally, the fourth section will look at current trends in the debate and implementation of cyber security, focusing especially on the potential for future instability caused by present policies, and will outline proposals to mitigate threats.

## Cyber-attacks in international relations

Developed nations like the US and UK have adopted a multi-pronged approach for targeting cyber threats and have integrated cyber security programs across several levels of defence and law-enforcement. The prevention of cybercrime, cyber warfare

and cyber-facilitated espionage has become a major objective of a nation's police, military, and government to ensure a minimal cyber disruption within their jurisdiction. The UK's Cyber Security strategy, for example, launched in 2011, earmarked £650 million over four years to combat cyber threats suggesting that the UK sees issues of cyber security as issues of national security. For many experts this is still a questionable association and to date the majority of cyber incidents that make the news or affect our daily lives do not impact a state's sovereignty. It is, therefore, important to define what types of attacks may have a real impact on national security. For this paper we have used a narrow set of criteria to define what constitutes a cyber threat to national security, these are as follows: a threat to critical infrastructure (such as targeting power lines or water sources), an attack on government internet infrastructure (websites or interactive online platforms for government initiatives) or the use of any cyber-attack during a physical war between states.

### Stuxnet

An oft-cited example of cyber sabotage entering the realm of national security is the 2010 case of Stuxnet. The attack, widely thought to have been developed by American and Israeli governments to set back Iranian progress on the development of a nuclear capability, targeted Iranian uranium centrifuges that were controlled by a network of in-house computers. Current estimates suggest that the worm successfully destroyed around 110 centrifuges. Stuxnet was a watershed moment for the use of cyber-attacks as a political tool. It is perhaps the first time in US history that an administration turned to cyber-sabotage to promote a foreign policy goal. Furthermore, as it has now set a precedent for the use of cyber sabotage by one state against another, it seems plausible to consider that it may be used for a variety of foreign policy and security objectives – either secretly or openly – in the future. Lastly, it demonstrates the paradox that nations face regarding the weaponisation of technology. The militarisation of cyberspace, as demonstrated in the Stuxnet attack, is ultimately at odds with the goals of many governments that support the internet as a conflict free and consumer maintained space.

### Current international dialogue on cyber security

The differing opinions held by states about the role of the internet may be a significant factor behind the lack of international legislation in the field of cyber security. The only existing international attempt has been the Budapest Convention, or the Convention on Cybercrime. This treaty targets the important issue of cybercrime but does not tackle any further issues, such as military use of cyberspace. The Budapest Convention, although signed by 50 states, does not have the necessary support within or outside of it to provide seamless enforcement of its objectives, nor does it have any sort of monitoring regime and crucially has not been signed by Russia or China. There has also been extensive UN-level debate on cyber security, which although harnessed a lot of discussion, has not necessarily produced concrete results.

The most fully formed attempt to consider the international legal implications of cyber-attacks is the Tallinn Manual on the International Law Applicable to Cyber Warfare. Developed over a three year period by 20 international legal scholars, the manual sets out 95 'rules' covering the legal implications of cyber war on state responsibility, sovereignty, and role in warfare and attempts to identify in which situations existing international law can apply directly to the cyber realm. However, the manual reveals many instances where the complexities of cyber conflict do not easily adhere to current legislative standards, demonstrating that these inconsistencies may have to be negotiated on a case-by-case basis. Finally, the speed of technology advancement in this area has further hampered the drafting of laws and international legislation.

### Estonian or 'Nashi' attack

The 2007 attack on Estonian government and private sector websites and web-based services is often referred to as a cyberwar and offers an example of a cyber-attack that significantly affected international relations. After authorities announced plans to remove a Soviet-era memorial to World War II in Tallinn, low-tech cyber-attacks were launched on governmental website and the banking system, eventually causing the largest bank of Estonia to cease web operations for over three hours across two days. The three-week attack on the Baltic republic warranted a substantial national response, altered the relationship between Estonia and Russia, and caused Estonia to call on NATO for assistance.

A key feature of this cyber incident was the inability of the target, in this case the Estonian government and companies, to identify the perpetrators, making it difficult for the Estonian government to develop an effective response to the attacks and take action against the perpetrators once the attacks had ended. Another issue these attacks highlighted were the blurring between state and non-state actors in cyber-attacks. About a year after the event, a pro-Putin Youth group called Nashi claimed that they had orchestrated the attacks. The legitimacy of Nashi as an independent youth movement has been heavily questioned, however, as sources suggest Putin's government funds their activities. Nashi's relationship with the government echoes the ambiguity surrounding the place of non-State actors in many realms of modern warfare.

### The 'Cool' war

Alternative styles of attack that also have the capability to impact on a nation and its citizens are smaller, repeated infiltrations such as a barrage of attacks to banks or financial systems that may challenge international trust in a currency or economic system. The term 'Cool War' has been coined to describe this type of attack: a locked in constant escalation of small-scale, damaging events taking place regularly over an extended period of time that never breaks out into actual conflict. The strongest example of this is currently taking place between China and the US. Industrial espionage also plays an important role in this process and raises similar problems as it is widespread and unnoticed so there is a difficulty of attribution.

## Cyber-attacks as a weapon of war

There have been at least two occasions in which cyber-attacks were used in conjunction with conventional military operations. The first was during the Russo-Georgian conflict in 2008. Here a wave of cyber-attacks, consisting mostly of the defacement of websites and disruption of web-based services, hit full force on the same day as the main military offensive started on August 8th. The second example was during the Israeli air raid against a nuclear reactor facility in Syria in 2007. To strike the reactor, Israeli air forces had to fly over Iraq and most importantly, surpass Syrian air defense positions. To avoid being targeted with anti-radar weapons a cyber-attack was used by Israel to disable the air defence positions and allow the Israeli planes to enter the Syrian airspace undisturbed. This was desirable as it disabled infrastructure without the need for violent action.

**"The securitisation of cyber security issues has fostered the 'Cool War' dynamic whereby states engage in continuous attrition and escalation, which can lead to a 'cyber arms race' between nations."**

The debate on cyber security has, however, often focused on the opposite type of scenario: one in which cyber-attacks are unleashed against critical infrastructures in a catastrophic way, resulting in mass casualties and destruction. No cyber-attack to date, however, has ever demonstrated the ability to inflict physical damage on the scale of a military or terrorist attack and many have suggested this is unlikely because of the great technological expertise, significant resources and knowledge of the target that is required. As well as this, there are also political reasons that make this unlikely, such as a state's concern for the far reaching consequences - in particular the response an attack could prompt. The situation may change if, for example, different actors gain access to sophisticated cyber-attack capabilities, meaning it is likely in the future that a cyber-attack will cause real damage and casualties.

## Civilian consequences of cyber threats

Although cyber-attacks have not yet been used to cause direct, physical destruction and loss of life on the scale of drone attacks, evidence has shown how cyber-attacks could infiltrate civilian life, for example by targeting critical infrastructure in a time of war or conflict. The impact of cyber war and other militarised uses of cyber instruments on civilian life are not, however, limited to large-scale sabotage or terrorism. Extensive surveillance – exposed by the Edward Snowdon NSA leaks - is an example of the impact of cyber warfare entering the civilian realm. These widespread surveillance networks raise important concerns about the loss of civil liberties.

## Main concerns and moving forward

For many countries, cyber war is already a reality: cyber security is discussed in the national security strategies of many nations, and states have identified cyber-attacks as a relevant and credible threat to their national security. The United Kingdom has listed cyber-attacks, conducted by other nations, terrorist organisations or organised crime, as the second highest priority threat for the coming years. In addition, countries have started integrating cyber security operations in their military doctrine.

### The securitisation of cyber space

Given the importance cyber warfare has assumed in the strategic outlook of many nations, it seems fitting that its effectiveness at achieving security and stability is analysed. However, trying to assess different cases of cyber-attacks with the same lens may be misleading as not all cyber-attacks are created equal. Attacks vary in their targets and level of success, from small-scale 'vandalism' and espionage attacks to destructive sabotage of important national security infrastructures. This highlights the diverse and multidisciplinary nature of cyber security, cutting across most sectors and sections of society and government and affecting individuals, governments, large utilities and service providers alike.

The current debate on cyber security has often ignored the diverse range of issues inherent in the field, conflating vastly different problems and repeatedly aiming for hyperbolic statements regarding the potential dangers posed by cyber-attacks. A useful instrument to understand this process is the concept of securitisation: the creation of a narrative that casts a specific object (often the state) as subject to an existential threat, and thus in need of urgent protection. A highly securitised debate around cyber security issues could have destabilising effects. The securitisation of cyber security issues has fostered the 'Cool War' dynamic whereby states engage in continuous attrition and escalation, which can lead to a 'cyber arms race' between nations. Securitisation in this field has also had an impact on civilians' day to day lives as greater government control has led to increased surveillance on citizens.

### Looking forward: maintaining stability in cyberspace

One way to counter the rampant securitisation of the issue is to ensure that accurate information is available. Especially when a new cyber threat is discovered, disseminating factual information on real risks and possible mitigation strategies can help users to defend themselves more effectively and avoid the panic brought on by sensational reporting. To this end, it seems that Computer Emergency Response Teams (CERTs) might have an important role to play. CERTs are expert groups and emergency response centres that analyse and, in some cases, counter cyber security threats. Furthermore, cooperation at the expert level, such as between CERTs and other track two initiatives, seem particularly promising for the field of cyber security, as international legislation and other forms of official intergovernmental action on the matter have progressed slowly. By helping the spread of best practices at a dynamic pace that keeps up with technological developments, cooperation between CERTs and similar bodies can lay the groundwork for nascent norms and more elaborate international arrangements in the future.

Increased cooperation and information sharing at both the technical and political level could also help to solve one of the most challenging issues in the cyber security realm, namely the problem of attribution. Over time, these measures could help foster a safer cyber security environment. If states manage to establish a sustained practice of cooperating against cyber-attacks and routinely sharing information, the decision by a state not to release forensic data after an attack might prove as telling as the data itself, and provide the international community with a modicum of leverage against the alleged offender.

**This is a summary of *Cyberspace: An Assessment of Current Threats, Real Consequences and Potential Solutions* by Vertic. For the full report, including citations, visit remotecontrolproject.org/our-reports**

# From New Frontier to New Normal: Counter-terrorism Operation in the Sahel-Sahara

Richard Reeve and Zoë Pelter

Oxford Research Group

*A US Navy SEAL advisor watches a Malian special operations vehicle run through counter-terrorism mission training drills near Gao, Mali. © Max R. Blumenfeld, Joint Special Operations Task Force-Trans Sahara*

**"AFRICOM represents something new in US strategy... the Sahel-Sahara is the laboratory for experiments in US "light-touch" counter-terrorism."**

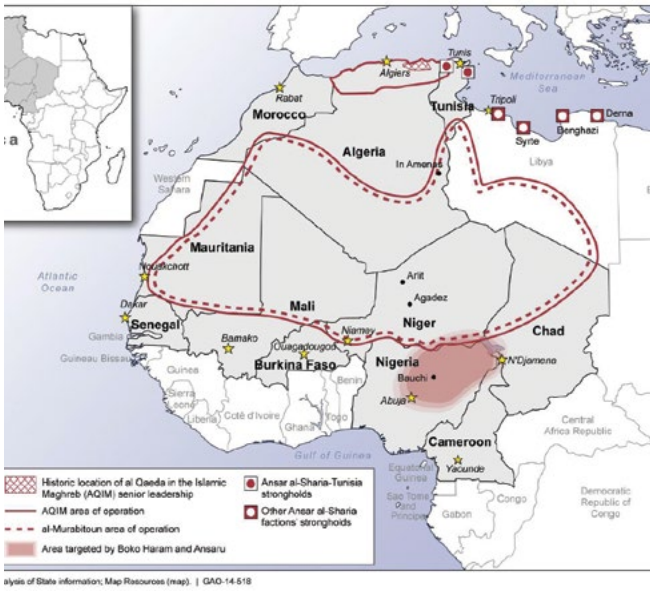
**This report documents the evolving importance of the Sahel-Sahara in French and US counter-terrorism strategy and the means with which they and their allies are waging overt and covert war against jihadist groups in the region, defined by an increased reliance on "remote-control" methods. It is the first attempt to provide a comprehensive overview of the character and scope of all counter-terrorism operations being conducted by external security actors along this new frontline. The report examines the various local and external security actors in the region before analysing the nature of counter-terrorism operations and deployments and, finally, evaluating their effectiveness against their stated objectives.**

The Sahel-Sahara is increasingly seen as the "new frontier" in global counter-terrorism operations. Recurrent security crises since the 2011 Arab uprisings and the NATO-led overthrow of Libya's Gaddafi regime have radically changed international perceptions of northwest Africa as a focus of activities by jihadist groups. It is now the priority area for French external counter-terrorism operations and for the US it ranks behind only Syria, Iraq and Afghanistan. In mid-July France formally initiated its redeployment of military forces under Opération Barkhane and the US is increasing its presence more steadily in line with the maturation of its newest combatant command, Africa Command (AFRICOM) and the rolling out of a crisis response concept known as the "New Normal" which could see US marines establish bases across the continent with the capacity to deploy within hours to anywhere that US citizens and interests are threatened. AFRICOM represents something new in US strategy, with only a few thousand assigned troops, no conventional armoured forces and barely any fighter aircraft or combat vessels, the Sahel-Sahara is the laboratory for experiments in US "light-touch" counter-terrorism.

## Context

The Sahel-Sahara is a vast territory the size of the USA or China. Its 12 countries touch on the arid Sahara desert and semi-arid Sahel strip to its south. Covering 10 million km, it is home to over 200 million people. Broadly speaking, it is the area in which three jihadist groups and their splinter factions operate: Al-Qaida in the Islamic Maghreb (AQIM), an Algerian-origin group; Boko Haram, a Nigerian group; and Ansar al-Shari'a, a newer North African group.

**Figure 1: Key Terrorist Groups in Northwest Africa and their Regions of Operation, 2009-2014.**




*Source: GAO analysis of State information; Map Resources (map). I GAO-14-518*

### Regional actors

Algeria and Nigeria are the only regional states that have sufficient capacity to play a unilateral role in regional counter-terrorism operations. Although both have waged counter-terrorism operations on their own territory, both lack the will and/or resources to use their armed forces to be a significant security actor in the wider Sahel-Sahara. The most powerful remaining regional state actors are Morocco and Chad. Morocco, however, is geographically isolated from the more unstable regions of the Sahel-Sahara and is economically oriented towards Europe and the Atlantic. Chad is a very minor country economically but has used its recent oil revenues to build up the most powerful armed forces in the Sahel, increasingly used to assert a greater regional and international role for Chad. There are also regional security organisations, in particular the Economic Community of West African States (ECOWAS) that are of some importance. However, this is limited by ECOWAS's military dependence on Nigerian leadership and assets as well as on external funding and logistics. Furthermore, most of its 15 member states lack the experience and equipment needed for counter-terrorism or desert-fighting operations.

### External actors

France has been the dominant external security actor in the region for over a century and sees a direct threat to its citizens and territory from regional terrorist groups. French interests in the region are shaped by economic and security concerns. Most significant economically are the French-owned uranium mines in northern Niger that are central to the French energy sector, providing around 30% of French uranium imports, and thereby about a quarter of its electricity. French security perceptions of the Sahel-Sahara are shaped by threats to the homeland and the many thousands of French citizens who live, work or visit the region. Other European states, and increasingly some Asian states, have strong interests in Saharan energy exports (oil, gas, uranium) and trade, including arms sales.

The US has historically been a minor player in the Sahel-Sahara, having few regional interests in the region before 2002. Threats against or attacks on US interests, firms and citizens in the Sahel-Sahara or by terrorists based in this region were very limited up to 2012. The deadly attacks on US diplomatic facilities between 11-14th September 2012 in Benghazi (Libya) and Tunis radically changed the perception of the threat to US interests in the region, in particular by activating Congressional enquiries and inter-party competition for a robust response. The great majority of foreign terrorist organisations designated by the US since then have been located in the Sahel-Sahara.

## Counter-terrorism operations in the Sahel-Sahara

### Major conventional military interventions

The military operation launched in January 2013 against AQIM and its allies in northern Mali was one of at least seven such French-led interventions in the region since 1968. However, it was the first major overt operation by an external power to target jihadist groups and it was the most multinational. At least 22 other countries provided direct support for Opération Serval and the associated African-led International Support

Mission to Mali (AFISMA). Opération Barkhane and the UN Multidimensional Integrated Stabilization Mission in Mali (MINUSMA) entrench the presence of over 9,000 external security forces in the Sahel-Sahara with mission and mandate to combat terrorist groups.

### Special forces operations

Compared to conventional counter-insurgency operations that need to gain and hold territory, counter-terrorism operations make disproportionate use of special forces troops. In the Sahel-Sahara region it is not clear how many special forces operations or operatives the US has. AFRICOM has established a Special Operations Command Africa (SOCAFRICA) based in Stuttgart, operations include overt CT training programmes with most of the states of the region and it is clear from US tendering documents that small teams of special forces operatives are deployed across a wide area of the Sahel.

Since at least 2013, French, UK, Canadian and Dutch special forces also operate in Mali, Niger and Nigeria. France relies increasingly on special forces in its operations in the Sahel-Sahara, especially in its search and destroy operations in northern Mali. Indeed, its repositioning to many smaller bases or forts under Opération Barkhane relies on small units of air-mobile special forces that can be rapidly and flexibly redeployed. They also have special forces covertly around Arlit, northern Niger, guarding the French-owned uranium mines and foreign workers, and in Mauritania, French special forces have a robust partnership with elite units of Mauritania's military. Air-mobile US Marines task forces are increasingly deployed to Africa from bases in Spain and Italy and are known to be seeking at least one "Intermediate Staging Base" in coastal West Africa.

### UAVs and other ISR assets

The Sahel-Sahara region has seen a major increase in aerial surveillance in the last decade. France and the US have been increasing their manned intelligence, surveillance and reconnaissance (ISR) capabilities in the Sahel-Sahara, as well as deploying unmanned aerial vehicles (UAVs, or drones) since 2013. Locally, Algeria, the most capable regional actor, has immediate plans to acquire longer endurance and possible armed UAVs for use in the Sahara. Morocco has purchased four MQ-1 Predator drones from the US and three shorter range IAI Heron drones from Israel via France. These are unarmed versions of the drone.

There are currently two known UAV bases for external operators in the Sahel and both are used jointly by France and the US. A third base in Italy is used to monitor Libya and the northern Sahara. The first, Niamey airport in Niger, their main ISR base in the Sahel, began its development as a drone base in October 2012, where each operates two unarmed versions of the MQ-9 Reaper "hunter-killer" unmanned aerial vehicle (UAV). The second active drone base is N'Djamena in Chad, which was used most notably during the current US response to the Chibok abductions in northeast Nigeria. The third, and probably most potent, drone base for surveillance of the Sahara is located off-shore at Sigonella in Sicily. This is a NATO base and was used by French Harfang and US MQ-1 Predator UAVs during the 2011 Libya campaign, when US UAVs (some operated remotely by UK pilots) launched at least 105 strikes. Given gaps in its UAV coverage from Niamey, Sigonella and Djibouti, the US is likely to seek further long-term UAV and ISR basing facilities, possibly in Senegal and Chad in the future.

**Figure 2: Map of US and French bases in and around the Sahel-Sahara.**


*Key: Red = French bases; Pink = French rotational deployments; Blue = US bases. © ZeeMaps*

### Private military and security contractors

The practice of hiring private military and security contractors (PMSCs) to undertake ISR and infiltration/exfiltration activities across West and East Africa has been a cornerstone of US covert operations on the continent since at least 2007. Although PMSCs are a small part of French operations in the Sahel-Sahara, they have run key parts of AFRICOM's covert counter-terrorism operations in the region.

These include running a post-2007 ISR operation using light aircraft (Operation Creek Sand). A call for contractors issued in May 2010 by AFRICOM for Africa Command ISR initiatives Operations

show that contractors were expected to have a minimum 150 airborne hours per month, supply their own concealed surveillance equipment, and take on further roles as pilots, intelligence analysts and linguists. Other activities private contractors are used for include transporting special operations forces, providing medical evacuation and search and rescue capacities, and to stockpile aviation fuel at regional airports. Furthermore, the UN Multidimensional Integrated Stabilization Mission in Mali (MINUSMA) will contract PMSCs to operate its unarmed UAVs from Mali.

### Counter-terrorism training and doctrine

Counter-terrorism training to regional security forces has become ubiquitous under AFRICOM's multifaceted Trans-Sahara Counterterrorism Partnership (TSCTP) and is likely to be expanded significantly under the Counterterrorism Partnerships Fund announced in mid-2014. In addition to France, a range of second-tier external actors also play a role in regional counter-terrorism training, including the European Union, Canada, Israel, Colombia and Japan.

### Abductions and renditions

The use of abduction and illegal rendition of terrorism suspects appears to have been a minor aspect of recent counter-terrorism operations in the Sahel-Sahara. However, there were numerous such cases documented between 2001 and 2004 implicating Algeria, The Gambia, Libya, Mauritania and Morocco. Morocco, the US's primary regional ally, was accused of hosting secret detention and torture facilities. Since October 2013 US special forces have twice abducted terrorist suspects from Libya and taken them for trial in the US without the consent of the Libyan government.

## Counter-terrorism outcomes

Over its 18 months, Opération Serval (January 2013 to July 2014) achieved tactical successes within major strategic limitations. The (overstated) advance south of jihadist groups was repelled and control of much of the north was returned to the Malian government. However, French, African and UN intervention has not addressed the political and social nature of the northern rebellion and has limited ability to protect civilians against a terrorist rather than insurgent threat. Moreover, intervention in Mali appears to have displaced AQIM and its allies into Libya, Niger and possibly Nigeria. UN mandates for ongoing French operations in parallel to MINUSMA effectively authorise an indefinite right of deadly pursuit of groups that France may define as terrorists. This is a dangerous precedent that goes beyond the normal understanding of peace support operations and UN accountability.

The US has set many more strategic objectives for its TSCTP but so far has seen marginal success. While AFRICOM and Washington have established a regular military presence in all regional countries and thus a close knowledge of its local partners' capabilities, there is little recognition of the often toxic nature of these partnerships. Successes in building capacities of Mauritanian and Chadian elite units is balanced by dismal failures in Mali and Libya and the disruption caused by repeated political interventions, mutinies and coups by elements of allied regional militaries.

There is also wider concern that these operations considerably undermine governance and human rights in the region. France, and to a lesser extent the US, relies hugely on the support of Chad's authoritarian government for basing and combat support. Undemocratic governments in Algeria and Mauritania have also been able to normalise their international relations, including arms imports, as crucial partners in Saharan counter-terrorism operations. Perceived international protection may discourage some regional governments from seeking internal political settlements. The elected Malian government seems to have interpreted the post-2013 French military spearhead and UN shield as a reason not to pursue a peace process with northern separatists.

Lastly, there is concern that rather than discrediting terrorist ideology as planned, the heightened visibility of US and French forces in the Sahel-Sahara and the strengthening of Islamist militia during the Libyan civil war appears to have significantly increased the profile and activity of jihadist groups. The threat posed to the US, France and Europe from Sahel-Saharan jihadist groups is still largely assumed; neither AQIM, Boko Haram nor Ansar al-Shari'a has yet launched an attack outside its home region. While some disruption of such groups has been effected since 2013, at least the motivation for retaliatory attacks is likely to increase as the militarisation of the Sahel-Sahara continues.

## Conclusion

While French-led operations in Mali, US "snatch" and evacuation operations in Libya, and the international response to the Chibok abductions have garnered headlines on counter-terrorist operations in northwest Africa, a far-reaching reorganisation and entrenchment of US, French and other NATO militaries' presence in the Sahel-Sahara has been underway. US and French counter-terrorism operations have seen a "pivot to Africa" with increasing reliance on "remote-control" methods including special forces, drones and private military and security companies for these operations.

This overt and covert build-up of foreign forces in and around the Sahel-Sahara has not gone unnoticed in the region. Although these counter-terrorism operations do not yet appear to have caused large numbers of civilian casualties, it is the alliances that Washington and Paris have made and must maintain with local strongmen – politicians, military, secret police and, at times, rebel leaders – that are likely to undermine local confidence in counter-terrorism operations.

Looking to the future, it is likely to be the implosion of Libya that increasingly concerns local and external security actors. Jihadist ideology has not been countered effectively there and armed Islamist groups have been major beneficiaries of the post-Gaddafi vacuum. Weapons supplies from Libya's looted arsenals and the payment of millions of euros in ransoms by European governments has further reinforced the appeal of jihadist groups across the region. Intervention in Mali has restored some stability to parts of that country but at the expense of Libya at an extremely vulnerable point in its consolidation. At best, the new configuration of foreign forces in Sahel-Sahara may partially contain the security challenges displaced from Mali to Libya but its presence, actions and compromising alliances are more likely to exacerbate than to mitigate the appeal of jihadist and nationalist groups. These foreign legions may not be coming home soon.

**This is a summary of *From New Frontier to New Normal: Counter -terrorism operation in the Sahel-Sahara* by Oxford Research Group. For the full report, including citations, visit remotecontrolproject.org/our-reports**


# Losing Sight of the Human Cost: Casualty Recording and Remote Control Warfare

Kate Hofstra and Elizabeth Minor

Every Casualty

*Protestors from US non-governmental organisation Code Pink read the names of children killed in drone strikes. Creative Commons, Flickr / Steve Rhodes*

**To understand the human costs of conflict, knowing the specifics about the casualties of violence – including where, when, and how people have been killed and injured, and who they were – is very important. Where there is a lack of data on casualties, the impact and acceptability of certain tactics cannot be assessed, with consequent negative repercussions for victims, communities and policy-makers. Casualty recording is a practice that strives to achieve the comprehensive, systematic and continuous documentation of individual deaths or injuries from armed violence and the incidents in which they occur. It involves documenting as much information as possible about incidents or individuals. Good casualty recording practice also includes the transparent publication of this information as soon as possible, so long as this does not threaten the safety of casualty recorders, their witnesses or affected communities. This paper explores the challenges remote control warfare pose to transparent casualty recording by states or other organisations. The tactics examined include the use of armed drones; the potential development of lethal autonomous weapons; the use of special operations forces (SOF); and the use of private military and security companies (PMSCs).**

**“Where there is a lack of data on casualties, the impact and acceptability of certain tactics cannot be assessed, with consequent negative repercussions for victims, communities and policy-makers.”**

## Method

This briefing paper is based primarily on a review of key literature on the four remote control tactics examined and the application of Every Casualty programme’s understanding of casualty recording’s methodologies, benefits, and challenges. This includes review of materials published by casualty recording practitioners who document casualties caused by remote control tactics. Our research also involves reviewing data collected during previous Every Casualty programme investigations into casualty recording

practice and its challenges – primarily semi-structured qualitative interviews with practitioners about their work – for material specific to the use of remote control tactics. Lastly, we gathered, through informal interviews and email exchanges, further or updated experiences and data samples on relevant topics from a small number of members of the International Practitioner Network (IPN) of casualty recording practitioners, to enhance the examples and operational understanding given in the paper. This briefing paper intends to give an introductory or scoping overview based on a systematic review of the materials available.

## Findings

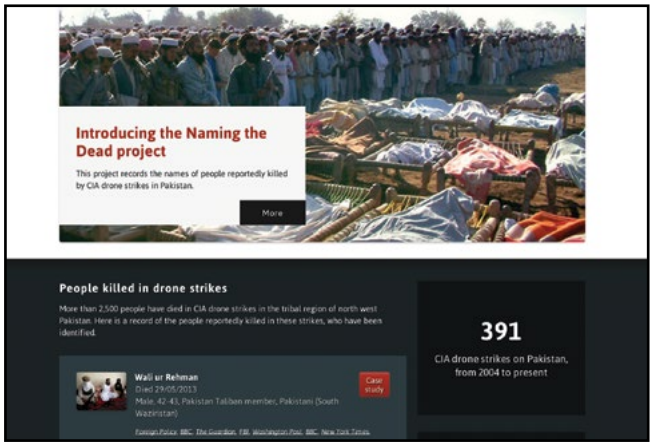
### Drone strikes

State-led casualty recording:

No public, systematic, comprehensive casualty records, produced by any of the states involved in launching or hosting drone strikes, were identified from the limited survey and review that was possible for this paper. However, the state-led recording of drone strike casualties is undertaken to various extents in different contexts. Academic, UN, and civil society analysis has drawn attention to the obligation on states to investigate possible civilian casualties as a result of drone strikes, and also proposed or recommended that all casualties should be recorded and reported upon.

Casualty recording by other actors:

Given the lack of adequate, transparent state-produced casualty records across the contexts in which armed drone strikes are currently conducted, non-governmental organisations currently provide the predominant source of information about drone-strike casualties. These organisations operate remotely, with the capacity to conduct on-the-ground investigations limited to a minority of cases. Their data and methodologies have sometimes been criticised but, in the absence of state data, and the challenges to comprehensive on-the-ground investigation, the organisations which apply most rigour and transparency in their methodologies provide vital baseline information in what would otherwise be a data vacuum.




*Naming the Dead, a project of the Bureau for Investigative Journalism, hosts an online database of people identified killed by drone strikes in Pakistan. Screen shot of Naming the Dead website © The Bureau of Investigative Journalism*

### Lethal autonomous weapons

Several countries have indicated their intentions to increase autonomy in the weapons systems they use. Incentives might include force multiplication (carrying out more tasks using fewer people) and force protection (reducing possibilities of military casualties on the side deploying the technology). Lethal autonomous weapons may be able to retain a digital trail that would assist investigators but it can only be conjectured what information about casualties this would be able to provide. Whatever information a weapon could provide about its actions, independent corroboration of any given source is a key good practice in casualty recording, and the weapon's own assessments of who had been killed would need critical evaluation to achieve an accurate record of casualties. Using data collected by the weapon alone to investigate and determine the profile and identities of casualties would not be sufficient. Obligations would have to be put in place to ensure the systematic review of a weapon's digital trail, given that there would by definition be no human involvement or supervision of the lethal actions of the autonomous weapon at the time they occurred.

### Special operations forces

The past decade has seen a sharp increase in the use of SOF. As the appetite for large-scale military interventions continues to diminish, many nations, particularly the US and the UK, have begun to prioritise the use of low profile, small, and highly trained combat units over traditional military interventions. The US has been at the forefront of this rapid expansion – more than doubling the size of the US Special Operations Command (SOCOM) since 2001. With SOCOM personnel levels expected to reach 69,700 in

2014, and a general shift in US strategy from large counter-insurgency operations to discreet counter-terrorism measures, this trend is likely to continue. The reliance of SOF on classified intelligence to carry out missions, coupled with their clandestine nature, presents a new and less accountable form of warfare. The increased opacity of SOF missions, coupled with the dangerous environments in which they take place, presents an even greater challenge to casualty recording. The hostile nature of such areas means that casualty recorders may have limited access to sites, or may lack the networks or safe modes of access to witnesses required to gather details about casualties in the field. The combined lack of transparency and access greatly constrains efforts to record casualties, and raises serious concerns about the accountability of SOF. While SOF may conduct their own post-attack assessments and collect data on casualties, this is likely to remain classified. It is therefore essential that states and other actors ensure that all casualties of SOF are recorded and recognised.

### Private military and security companies

The widespread outsourcing of military and security functions to private companies marks another phenomenon of modern warfare. The outsourcing of military functions previously considered the domain of states – including combat and the use of direct force – marks a fundamental shift with regard to state monopoly on the legitimate use of force. The past decade has seen a marked increase in the use of PMSCs, due in large part to the conflicts in Iraq and Afghanistan. The rapid proliferation of PMSCs has not, however, been matched by an adequate increase in oversight mechanisms to monitor their activities. The lack of coherent regulatory frameworks for PMSC activities as well as a general lack of transparency surrounding the actions of PMSCs and their subcontractors hinders attempts to accurately record casualties. International efforts to improve the regulation of PMSCs have been developed, including the 2008 Montreux Document and the 2012 International Code of Conduct for Private Security Service Providers (ICoC), both of which are non-binding. While the ICoC has been signed by 58 companies, attempts by states or others to conduct accurate or transparent casualty recording currently continue to face the challenges presented by limited oversight and implementation. The opacity with which PMSCs operate is increased by their use of further subcontractors, for whom oversight is even more severely limited. States contracting with PMSCs may not have any knowledge of consequent subcontractors, creating a further barrier to the collection of accurate and transparent data on PMSC-related casualties.

The literature review undertaken for this paper did not reveal any intergovernmental body, civil society organisation, or state conducting comprehensive casualty recording in relation to PMSCs. The media have often captured information on civilian deaths from PMSCs – particularly for high-profile instances of contractor abuse, such as the killing of 17 civilians by private security contractor Blackwater in the Nisour Square incident in Iraq in 2007.

## Conclusion

Each of the remote control tactics described have the effect of decreasing the possibilities for scrutiny of how military activities, or political objectives pursued through armed force, are carried out – including the human costs they incur. Delegating to forces or organisations whose activities are classified or secretive, as with SOF and the use of armed drones by special forces or covert agencies; subcontracting the use of force to private companies without clear lines of accountability and little regulation; developing new technologies to remove military personnel of one party to the conflict from the battlefield, and even from life and death decisions completely: all potentially pose crucial challenges to casualty recording. Transparent casualty recording can make a crucial contribution to bringing the impacts of these specific tactics into public debate and to accountability. It is essential to call for states to take ultimate responsibility for casualty recording in all situations where they use or contract force, and to release the information they collect as soon as it is safe to do so without undue delay. It is essential also that robust, independent casualty recording is undertaken. Our recommendations (synopsised) are:

1. *The independent recording of casualties from remote control tactics should be enhanced:*
    a. Impartial actors such as civil society and UN entities should engage in casualty recording, and their work should be supported. Where UN entities, civil society groups, academics, or other entities such as regional organisations can impartially engage in casualty recording, this can complement and may often provide greater value than a state-run casualty

recording mechanism alone.

b. Casualty recorders should apply common standards including transparency, and ensure that they use a robust methodology.

c. The structure of casualty recorders' records should assist the evaluation of different tactics and deployments of force. A description of the violence that has caused casualties, where possible by documenting the tactics or weapons used, is one of the fundamental elements of casualty data.

d. Independent casualty recording should be commenced as soon as possible, and followed up with more detailed investigations as necessary.

e. Where possible, casualty recorders should act in alliance and with other independent actors to bring the meaning of their data to policy-makers and those who can assist victims.

*2. State casualty recording, accountability, transparency, and oversight of remote control tactics should be enhanced:*

a. States should transparently record the casualties of the remote control tactics they use or host. States should ensure the recording of every casualty of armed violence within their territory or where they undertake or commission operations elsewhere.

b. States should not obstruct the work of independent casualty recorders, and should engage in evidence-based dialogue with them.

c. Whether operated from near or far from the target or battlefield, casualties from drone strikes must be properly investigated. The transparent recording of casualties from drone strikes by states should always include detailed on-the-ground investigation to ensure that the most accurate information about who has been killed is gathered. This should be conducted in partnership with the host state if possible.

d. The potential challenges posed by lethal autonomous weapons to the transparent recording and recognition of every casualty should be considered.

e. States must ensure that casualties caused by special operations forces are recorded, recognised, and assisted. States must ensure that the increased use of clandestine forces does not prevent robust investigation and collection of data on all casualties.

f. State contracts with PMSCs should include provisions to ensure that casualty recording is conducted by PMSCs.

g. States should provide adequate resources to ensure effective management and oversight of PMSCs' serious incident and casualty recording practices. States that engage the services of PMSCs should ensure that they have planned for the thorough and continuous management and oversight of these companies' incident reporting and casualty recording practices.

**This is a summary of *Losing Sight of the Human Cost: Casualty Recording and Remote Control Warfare* by Every Casualty. For the full report, including citations, visit remotecontrolproject.org/our-reports**

**Editor:** Esther Kersley

**Design:** Allan Bailey

**Cover photo:** Payload Vehicle Operators man their post in the Ground Control Station (GCS) for Canada's new Heron Unmanned Aerial Vehicle (UAV) at Kandahar Airfield, Afghanistan. Creative Commons, Flickr / Pierre Gazzola

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

+44 (0)207 549 0298
media@remotecontrolproject.org
www.remotecontrolproject.org