Trends in remote-control warfare

March-September 2014

open briefing
the civil society intelligence agency

Scott Hickie
Chris Abbott
Raphaël Zaffran

October 2014

Published by Open Briefing, 13 October 2014

Open Briefing
27 Old Gloucester Street
Bloomsbury
London WC1N 3AX
United Kingdom

Tel +44 (0)20 7193 9805
info@openbriefing.org

www.openbriefing.org

Commissioned by the Remote Control project
remotecontrolproject.org

REMOTE CONTROL
Examining changes in military engagement

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

Chris Abbott is the founder and Executive Director of Open Briefing. He is an Honorary Visiting Research Fellow in the School of Social and International Studies at the University of Bradford and was the Deputy Director of Oxford Research Group until 2009.

Raphaël Zaffran is an associate researcher at Open Briefing. He is an analyst and political scientist researching and teaching international security issues. He is currently pursuing a PhD at the Graduate Institute of International and Development Studies in Geneva.

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

Open Briefing Ltd is a **not-for-profit social enterprise** run nearly entirely by volunteers.
Registered in England & Wales as a company limited by guarantee, No. 07649656.

Trends in remote-control warfare

March-September 2014

Scott Hickie, Chris Abbott and Raphaël Zaffran

Contents

Preface

Remote-control warfare is an emerging military and political framework that allows for warfare to be actioned at a distance by relying on 'smart' technologies and light-footprint deployments, such as armed drones and special forces. While in some respects it is more attractive than traditional military approaches, it has two significant disadvantages. Firstly, it allows actions to be approved that would never be considered using conventional military means, yet the consequences and risks of those actions are not being adequately considered. Secondly, it removes policymakers and military planners one step further from the realities of war fighting for both the military operators and civilian casualties. However, these downsides are being ignored as policymakers struggle to respond to multiple conflicts and security threats around the world.

Since April 2014, Open Briefing has produced a series of monthly intelligence briefings on remote-control warfare. These briefings were commissioned by the Remote Control project, which was initiated by the Network for Social Change and is hosted by Oxford Research Group. These briefings focus 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). These are the areas that Open Briefing considers central to the development and application of remote-control warfare.

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 publication differs from the usual monthly format in that it 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.

London

22 September 2014

Section I

Special operations forces

United States and European countries increases 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 precise 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 begs two key questions: why is Africa the battleground of the future, and is SOF training of indigenous, national forces sufficient preparation for this perceived 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 severe 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.

[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

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 local 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 special operations forces 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 special operations forces 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.

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

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.

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

Section II

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 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 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 those 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.

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

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

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.

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 Defence Authorisation Act (NDAA), which aims to improve the US defence 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.

[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

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.

Section III

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 increasing 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 current employed), and indeed questioning their effectiveness in a wider range of missions, including ISR.

Increased interest from the US security establishment 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.

[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

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 focusses 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]

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

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 Air Bus, 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 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 all-important 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.

Section IV

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 Peoples' 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.

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

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 cybersecurity 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 cybersecurity 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 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.

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

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 at this point in time 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 being 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.

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

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

Cyber attacks between Russian 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 defence 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.

[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

Section V

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 publically 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]

[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

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 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.

[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/

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 defence'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.

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.

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

open briefing
the civil society intelligence agency

Open Briefing
27 Old Gloucester Street
Bloomsbury
London WC1N 3AX

t 020 7193 9805
info@openbriefing.org
www.openbriefing.org