Remote-control warfare briefing | #15

16 May 2016

Remote-control warfare is an emerging strategy that allows for conflict to be actioned at a distance. It incorporates technologies and light-footprint deployments that enable policymakers and military planners to approve actions that would unlikely be considered if using conventional means.

These monthly briefings are produced by **Open Briefing** and commissioned by the **Remote Control** project, a project of the Network for Social Change, hosted by Oxford Research Group.

Special operations forces: Deployment of foreign special operations forces in Syria may complicate conflict and increase risks.

Private military and security companies: Shadowy Russian private military company fighting alongside Spetsnaz special forces in Syria.

Unmanned vehicles and autonomous weapons systems: US officials explore scenarios for Islamic State 'dirty bomb' attacks using drones.

Cyber conflict: US Cyber Command operations against Islamic State becoming important force multiplier.

Intelligence, surveillance and reconnaissance: Studies find mass surveillance having negative impact on democracy and informed debate.

Special operations forces

Deployment of foreign special operations forces in Syria may complicate conflict and increase risks

The US president, Barack Obama, announced in Germany on 25 April that an additional 250 US special operations forces (SOF) soldiers would be deployed to Syria to complement the existing contingent of 50 soldiers from Joint Special Operations Command (JSOC). The US administration sees the additional commitment as necessary to capitalise on recent territorial gains in Syria.

Obama used the announcement to try to leverage greater NATO and EU involvement in Syria, as regional and local allies, including the Gulf States and the Syrian Democratic Forces, are concerned that Western countries are making insufficient military contributions to combating Islamic State and other violent jihadist groups, such as the Al-Nusra Front. On 19 April, the Danish parliament approved the deployment of approximately 60 SOF personnel to Syria after direct requests from the United States and France.

Open Briefing
27 Old Gloucester Street
Bloomsbury
London WC1N 3AX

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

The US administration intends to build on existing momentum to lay the groundwork for local forces to retake both Raqqa in Syria and Mosul in Iraq. This would remove Islamic State from its main strongholds and deny it crucial income and relatively safe spaces to plan external attacks. The existing momentum has depended on territorial gains made by local allied forces with the support of Western airstrikes, cyber operations and SOF kill or capture missions. Special operations forces are also guiding the movements of local forces, sharing intelligence and calling in airstrikes. Increasing SOF numbers may require greater logistical and transport support, impeding the ability of those soldiers to maintain a low profile.

The expansion of US SOF participation in Syria may become more problematic as Turkey, Iran and Russia all increase their own SOF presences in Syria. In early April, over 100 Turkish special forces soldiers crossed into Syria's northern Idlib province, likely concerned about the expansion of Kurdish forces along the Syria-Turkey border. In late March, an Iranian army commander publicly stated that Iranian special forces from the country's Rapid Response Battalions (65th Airborne Special Forces Brigade) are deployed in Syria for advisory and assistance missions.[1,2] Russian officials also highlighted the involvement of their special forces (Komandovaniye Sil Spetsial'nykh Operatsiy) working alongside Syrian, Iranian and Hezbollah forces to retake the historic city of Palmyra from Islamic State.[3]

The common element for all foreign special operations forces operating in Syria is that they are supposedly limited to advisory and assistance missions to support local forces; however, assistance missions are creeping into kill or capture missions and combat. Indeed, foreign special operations forces are likely to be increasingly pulled into combat missions involving a complex array of groups participating in a civil war and terrorist insurgency. As such, the increasingly diverse deployment of special operations forces in Syria is intensifying the risk of miscalculation and conflict escalation.

Other developments

Vice News published an investigative report on 7 April describing the participation of British intelligence and special forces in US counterterrorism operations in Yemen.[4] The report reveals that the Secret Intelligence Service (MI6) and UK Special Forces counterterrorism teams collaborated with the CIA and US special operations forces to degrade al-Qaeda in the Arabian Peninsula (AQAP). A number of sources cited in the report note tensions between the British and US teams due to different rules of engagement for drone strikes and the critical role of UK special forces facilitating intelligence sharing to support drone strikes. Rules of engagement and compliance with the European Convention on Human Rights were partially circumvented by British special forces soldiers being seconded from the Ministry of Defence to MI6, which is subject to different rules.

[1] http://www.longwarjournal.org/archives/2016/03/iran-deploys-army-special-forces-to-syria-and-iraq.php and http://offiziere.ch/?p=27077

[2] The announcement has been interpreted as a potentially-adverse reflection on the effectiveness of the Islamic Revolutionary Guard Corps (IRGC) operating in Syria, which has recently lost a number of high-ranking soldiers. It is also significant because Iranian special forces are constitutionally assigned with protecting the country's territorial integrity not conduction expeditionary missions.

[3] https://www.washingtonpost.com/news/checkpoint/wp/2016/03/29/how-russian-special-forces-are-shaping-the-fight-in-syria/ and http://warontherocks.com/2016/03/the-three-faces-of-russian-spetsnaz-in-syria/

[4] https://news.vice.com/article/britains-covert-war-in-yemen-a-vice-news-investigation

A leaked briefing note reveals that Jordan's King Abdullah provided a confidential briefing to US congressional leaders on the deployment of Jordanian special operations forces together with British SAS soldiers in Somalia, Syria and Libya.[5] The briefing, which occurred in January 2016, revealed Jordan's dissatisfaction with US action against Islamic State and its belief that East Africa remains a critical blindspot for the US administration. Material leaked from the briefing was reported to highlight King Abdullah's concern over the lack of coordination between special operations forces working across multiple jurisdictions and the limitations of training indigenous special operations forces without appropriate technology transfer. The leak, in conjunction with recent reports, has raised political concerns in the United Kingdom about the need for parliamentary oversight of special forces deployments. The Scottish National Party's leader in Westminster, Angus Robertson, has called for the SAS to be subject to parliamentary oversight.[6]

The US defence secretary, Ashton Carter, discussed SOF cooperation with his Gulf State counterparts in Riyadh, Saudi Arabia, on 20 April. The following day, the US president, Barack Obama, joined a summit with the monarchs of the six Gulf Cooperation Council states. AFP reported that an unidentified senior US official had indicated the talks would likely focus on the concerns the Gulf States have over rising Iranian influence and interference in the region.[7] The United States likely highlighted the importance of special operations forces cooperation, training and assistance, rather than the export of conventional US military hardware.[8] The US administration likely harbours some concerns over the use of conventional weapons and conventional warfare tactics by Gulf States in Yemen and Egypt, which result in higher numbers of civilian casualties compared to unconventional warfare efforts. The US administration would likely point to recent joint campaigns by UAE and Saudi special operations forces in Yemen as evidence that collaborative SOF campaigns can be effective against al-Qaeda in the Arabian Peninsula (AQAP).

Also of note

- **Bulgarian and US naval special operations forces held an 18-day joint drill in the Black Sea during mid-April.** Bulgaria and the United States signed a defence cooperation agreement in 2006 and conducted over 80 military training sessions and drills in 2015.
- **US and Tunisian special operations forces (Groupement des Forces) completed joint training exercises between 21 March and 8 April.** The counterterrorism training focused on improving operational mobility using High Mobility Multipurpose Wheeled Vehicles (HMMWVs).
- **The head of the Australian Army, Lieutenant-General Angus Campbell, confirmed in April that the country's special forces are the subject of a broad ranging review into culture and operations in response to unsubstantiated reports of breaches of rules of engagement and unethical behaviour.** The review, which has been progressing over the last year, is also looking into training and selection, administration, technology and future direction.

[5] http://www.middleeasteye.net/news/revealed-britain-and-jordan-s-covert-military-operations-against-al-shabab-1322093760

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

[7] https://www.yahoo.com/news/washington-seeks-gulf-special-force-naval-cooperation-164601321.html

[8] http://www.defenseone.com/ideas/2016/04/what-us-gives-its-mideast-partners-isnt-always-what-they-need/127613/

- **The French government announced in late March the deployment of a paramilitary police special forces battalion to Ouagadougou, Burkina Faso,** to provide a rapid response team for terrorist attacks.
- **The Indonesian Air Force is making plans to deploy special operations forces from the Korps Pasukan Khas (PASKHAS) to the Natuna Islands cluster in the South China Sea to test medium-range air-defence systems.** The move is likely to be interpreted as part of ongoing militarisation of the contested maritime space.
- **On 12 April, three French SOF soldiers involved in Operation Barkhane in Mali were killed by an IED.** The attack came after al-Qaeda in the Islamic Maghreb (AQIM) launched a series of attacks on UN forces operating in the country's north.

Private military and security companies

Shadowy Russian private military company fighting alongside Spetsnaz special forces in Syria

Private contractors are being used in Syria following the recent withdrawal of the best part of Russia's military deployment from the country. According to the independent Russian newspaper *Fontanka*, an undisclosed number of contractors working for a shadowy company called Wagner are operating alongside the Spetsnaz special forces units that remained in Syria when the bulk of the Russian operation was wound down.[9] An investigation by the newspaper has found that the Kremlin had contracted Wagner for operations in Syria and also previously in Ukraine (the latter was corroborated by a UN Working Group on 18 March[10]). Wagner is the informal name for a private group called OSM, led by a former GRU Spetsnaz officer and current reservist called Dmitry Utkin.[11]

Russian law currently prohibits the existence of private military companies, but the Russian leadership is showing increasing official support for these type of companies as well as unofficially using their services. In 2012, the then Russian prime minister, Vladimir Putin, made public statements describing them as a 'tool for the implementation of national interests with direct participation of the state', and has since authorised the Kremlin to use these companies for deniable operations.[12] In 2013, Russia's deputy prime minister, Dmitri Rogozin, suggested that it was worth formalising the sector and that companies should be established with state backing, though he met considerable opposition from the defence ministry at the time.[13]

This opposition from the military hierarchy started to soften during the Ukraine operation with the deployment of independent Crimean militias to carry out combat operations that could not officially be carried out by the Russian Army. These militias were often created from organised crime gangs and right-wing groups and, while they offered a degree of deniability at the time, their lack of training and experience often saw them requiring considerable support and rescue by Russian military assets, which somewhat undermined the value of them not being connected officially to the state. Furthermore, these groups were sometimes led by maverick commanders and proved difficult to control, conducting operations without informing the Russian military and reportedly committing atrocities, such as torture and executions.[14]

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

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

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

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

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

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

So while Wagner is currently not allowed to officially exist, and is consequently registered in Argentina, the company is believed to have around 1,000 active contractors on their books.[15] Many of these were previously employed by the short-lived Slavonic Corps, which briefly operated in Syria before being dissolved at the end of 2013.[16] Wagner also operates a training camp near the Russian town of Molkino, around 100 km east of Crimea. It is probably not coincidental that this town also hosts a training camp for the 10th Spetsnaz Brigade of the GRU military intelligence agency. *Fontanka* claim that Wagner is also building a formidable arsenal of hardware, some issued by the Kremlin, including armoured combat vehicles, portable anti-aircraft systems and mortars.[17]

One former soldier claimed the Wagner had deployed 600 men to Syria and described the company's operation in the country as consisting of three reconnaissance/assault companies each of 90-100 men, a fire support company with three platoons operating recoilless rifles and automatic grenade launchers, an air-defence company equipped with SA-24 Igla-S man-portable surface-to-air missiles, a communications company, a Guard company and a medical unit.[18] *Fontanka* claims that Wagner has suffered dozens of casualties in Syria, with reports of only one-third of one particular company ending its tour alive and uninjured. There are also indications that the group suffers from poor leadership that lacks tactical awareness. Former contractors have complained that the training given at the Molkino camp is too basic, with insufficient fieldcraft training.[19]

While it appears that Wagner is still suffering considerable teething problems, it should not be readily dismissed. While Western private military companies, such as DynCorp and G4S, are often restricted to roles such as base security and convoy protection, Wagner is clearly intended for frontline combat deployments.

Other developments

An evolutionary development that could potentially spread across the private military and security company sector (PMSC) is taking place under the guiding hand of Erik Prince, founder and previous owner of Blackwater (now called Academi). In recent months, Prince has commissioned Airborne Technologies, an Austrian company in which he holds a 25% stake, to convert two Thrush 510G crop-dusting aeroplanes into light ground-attack aircraft.[20] The planes are fitted with armoured cockpits and fuel tanks, and capable of carrying NATO or Russian guided weapons and reconnaissance payloads.[21] Prince has accomplished this without the knowledge of the board of his company, Frontier Services Group, from which the funds for the conversions were reportedly misappropriated. Converting these planes is also in contravention of US and European export laws. This is not Prince's first move into incorporating

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

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

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

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

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

[20] https://theintercept.com/2016/04/11/blackwater-founder-erik-prince-drive-to-build-private-air-force/

[21] https://warisboring.com/does-erik-prince-s-private-air-force-even-make-sense-f91cc2066a26?mc_cid=223780192b&mc_eid=76dba1fb5e&gi=72e3e6a75bc8#.sfe5s7pr8 and https://theintercept.com/2016/04/11/blackwater-founder-erik-prince-drive-to-build-private-air-force/

aircraft into his PMSCs, having used MH-6 Little Bird helicopters as transport for his Blackwater personnel in Iraq. He has reportedly long pursued a vision of offering a private air force option to his clients, from aircraft-only purchase to rental packages involving full crewed support. Prince reportedly considers African governments as his target customer base, and has considered converting up to 150 airframes; however, there have seemingly not been any firm orders with both of the initial two aircraft now gathering dust in storage.

Through research into financial transactions, the International Centre for Investigative Reporting (ICIR), a Nigerian government watchdog, claims to have uncovered evidence that the Nigerian government employed South African mercenaries in combat and training roles between December 2014 and April 2015 despite repeated denials by the Government.[22] Initially contracted to provide training to help locate the kidnapped Chibok schoolgirls, a deteriorating situation led to the former South African army members being merged with Nigerian forces in a unit called 72 Mobile Strike Group according to ICIR. This self-reliant unit, with its own air, intelligence, communications and logistics support, was led by a South African commander and carried out repeated strike raids against the insurgents in the Maiduguri region with considerable success. Three South Africa-based companies were linked to this operation: Conella Services Ltd, Pilgrims Africa and Specialised Tasks, Training, Equipment and Protection (STTEP), with Conella being the primary contractor. The defeat of the ruling People's Democratic Party, led by Goodluck Jonathan, ended the contract, and all personnel from the companies had been removed from the theatre by the second week of April 2015. The Nigerian government continues to deny the use of mercenaries and rejects the evidence provided by ICIR.[23]

Questions have been raised over whether the London-based private military and security company Aegis Defence Services, chaired by Conservative MP Sir Nicholas Soames, has been employing former child soldiers from Sierra Leone on its contracts in Iraq guarding US military bases.[24] According to a former director of operations at the company, James Ellery, no checks were carried out on the backgrounds of those recruited in Sierra Leone. It is therefore possible that former child soldiers were among the recruits. Contract documents state that soldiers from Sierra Leone were only paid $16 (£11) a day. Ellory, who previously served as chief of staff to the UN mission in Sierra Leone, which was involved in the demobilisation of thousands of child soldiers, said that the company had a 'duty' to recruit from countries with high unemployment and a decent labour pool in order to keep operating costs down. Aegis was not the only company to adopt this commercial strategy; an estimated 2,500 contractors were recruited from Sierra Leone by multiple PMSCs operating in the Middle East. Aegis was founded in 2002 by Tim Spicer, a former British Army officer previously employed by Sandline International and involved in the 1998 arms-to-Africa scandal during which Sandline imported 100 tonnes of weaponry to Sierra Leone in breach of international sanctions.

[22] http://icirnigeria.org/how-nigeria-engaged-south-african-mercenaries-to-fight-boko-haram/ and http://www.economist.com/news/middle-east-and-africa/21646809-south-africa-struggles-vain-ban-soldiers-fortune-leash-dogs-war

[23] http://icirnigeria.org/how-nigeria-engaged-south-african-mercenaries-to-fight-boko-haram/

[24] http://www.theguardian.com/global-development/2016/apr/17/uk-firm-employed-former-child-soldiers-as-mercenaries-in-iraq?utm_source=Sailthru&utm_mediu%E2%80%A6

Also of note

- **The breakaway region of Nagorno-Karabakh, annexed by Armenia from Azerbaijan in 1992, has accused the Azerbaijani government of employing former fighters from Islamic State and the Turkish Grey Wolves ultra-nationalist organisation.**[25] These fighters have been linked to the execution of civilians and looting in Talish, located on the border with Azerbaijan.

[25] https://armenpress.am/eng/news/842113/nkr-has-grounds-to-believe-azerbaijan-uses-islamic-terrorists-on-the-frontline.html

Unmanned vehicles and autonomous weapons systems

US officials explore scenarios for Islamic State 'dirty bomb' attacks using drones

According to the US, British and French governments, it is increasingly likely that Islamic State (IS) will use a drone to attack a Western city with a radiological dispersal device (RDD) or 'dirty bomb'. Scenarios for how such an attack could be organised and executed have been released.[26] Islamic State has already used aerial drones in reconnaissance and observation roles in Syria and Iraq.[27] British officials report that Islamic State has shown interest in obtaining low-level crop-spraying drones and it is feared that they could use such drones to spray radioactive material in the heart of a major city.[28]

At the Nuclear Security Summit in Washington DC on 31 March 2016, US officials mapped out one scenario where toxic nuclear material could be stolen from a facility by corrupt insiders and sold to extremists on the dark web using the TOR anonymising network to hide the identities and locations of all parties involved.[29] The threat of this type of attack is now perceived to be so high that officials at the summit went so far as to carry out an exercise to rehearse an international response. It was also revealed that US special operations forces are being trained to seize and disable radioactive bombs.

Islamic State obtained 40 kg of uranium when they looted Mosul University in Iraq in 2014. While this is low-grade material that poses minimal real harm, the panic provoked by a dirty bomb attack using such material would be considerable. Separately, a batch of highly-dangerous IR-192 radioactive material went missing from a US-run storage facility in Basra, Iraq, in November 2015.[30] IR-192 is toxic enough that it would quickly be fatal to anyone within close proximity to the material. While it not believed to have been stolen by Islamic State or yet in their possession, as Basra is considerably to the south of their positions, such a possibility is a very serious concern and extensive efforts to recover the material continue. There are also reports of attempts to infiltrate European nuclear facilities, though few details have been released.[31]

Islamic State continue to improve the capabilities of their drone fleet. While still unsophisticated, especially when compared to Western military platforms, the equipment is cheap and easily obtainable and can be modified using aftermarket components to provide the desired capabilities.[32] Islamic State regularly use commercial and homemade drones for reconnaissance purposes. One drone was observed in flight by a Western military unit near Fallujah on 17 March 2015.[33] It was tracked back to its operator, who

[26] http://www.telegraph.co.uk/news/2016/04/01/isil-plotting-to-use-drones-for-nuclear-attack-on-west/

[27] http://www.openbriefing.org/thinktank/publications/hostile-drones-the-hostile-use-of-drones-by-non-state-actors-against-british-targets/

[28] http://www.telegraph.co.uk/news/2016/04/01/isil-plotting-to-use-drones-for-nuclear-attack-on-west/

[29] www.telegraph.co.uk/news/2016/04/01/isil-plotting-to-use-drones-for-nuclear-attack-on-west/

[30] http://www.independent.co.uk/news/world/middle-east/isis-nuclear-dirty-bomb-iraq-oil-field-a6879481.html

[31] http://www.telegraph.co.uk/news/2016/04/01/isil-plotting-to-use-drones-for-nuclear-attack-on-west/

[32] 3D printers are now capable of manufacturing drones in potentially unlimited numbers, provided the motors and electronic parts can be obtained.

[33] http://www.defensenews.com/story/defense/international/mideast-africa/2015/03/18/us-aircraft-bomb-islamic-state-drone-iraq/24979981/

recovered it and placed it in his vehicle, which was then destroyed by a coalition aircraft. In December 2015, Kurdish forces in Southern Kobanê in northern Syria reportedly downed two weaponised IS drones.[34] The aircraft appeared to be homemade, and both were laden with explosives. Another IS-operated drone was shot down by an Iraqi soldier in Al-Jirashi in Anbar province in April 2016. It was revealed to be a DJI Phantom 3 quadrotor,[35] readily available on the consumer market.[36]

Other developments

In a move that will further stretch already strained relations with Pakistan, the Indian military is in talks with the United States to purchase up to 40 surveillance versions of the Predator drone.[37] The Indian Air Force has also asked Washington about acquiring 100 armed Predator C Avenger drones, previously used by the US military against militants in Pakistan and Afghanistan. India is continuing to build up its capabilities to monitor its borders with Pakistan and China as well as improve its surveillance capability on the Indian Ocean. India is planning to acquire over 5,000 drones of various models over the next 10 years.[38] These will be added to existing surveillance drones purchased at the end of 2015 from Israel and being used to monitor the Kashmir region. The Indian Navy wants surveillance Predators to better match the greatly increased Chinese surveillance of the Indian Ocean. China's controversial moves to unilaterally annex large areas of the South China Sea have greatly increased tensions in the region, and increasing ship and submarine patrols of the Indian ocean are causing some concern in New Delhi. As part of ongoing negotiations over the drones, Washington is seeking agreements to allow the United States to operate out of Indian military bases or perhaps build their own.

The US Navy has christened a new ship developed by the Defense Advanced Research Projects Agency (DARPA) that will eventually run completely autonomously of human control. The USS Sea Hunter is a 132 ft (40.2 m) test vessel designed to seek out and track diesel-powered submarines on blue water patrols.[39] Diesel submarines have been identified as an immediate military threat due to a recent surge in launches of new quieter vessels by Iran and China. Diesel submarines have long managed to operate far more stealthily than nuclear submarines, which are hindered by noisy propulsion systems, though these are rapidly being improved. Officially designated Anti-Submarine Warfare Continuous Trial Unmanned Vessel (ACTUV), the development programme aims to produce an autonomous ship with sufficient range and endurance to operate anywhere in the world while obeying rules of navigation and avoiding collisions with other ships. The USS Sea Hunter can travel at speeds up to 27 knots and operate at sea for up to 70 days, depending on fuel burn. It will immediately operate unmanned, but will initially be remotely monitored by a human operator. Such vessels are widely seen as the future of naval operations within the Pentagon, paralleling similar developments of autonomous ground vehicles in the Army and ongoing improvements with the US Air Force's airborne vehicles.

[34] http://www.popularmechanics.com/military/weapons/a18577/isis-packing-drones-with-explosives/

[35] http://www.marinecorpstimes.com/story/military/tech/2016/04/17/islamic-state-drones-target-american-coalition-forces/83096864/

[36] http://www.dji.com/product/phantom-3-pro

[37] http://tribune.com.pk/story/1081218/india-in-talks-to-buy-us-predator-drones-has-eye-on-pakistan-china/

[38] http://www.ibtimes.co.in/india-plans-acquire-over-5000-uavs-10-years-report-672382

[39] https://www.defenseone.com/technology/2016/04/us-christens-first-ghost-ship-and-dawn-robotic-navy/127298/?oref=d_brief_nl

North Korea's military has been regularly sending surveillance drones into South Korean airspace, specifically the central and western regions of the heavily fortified Demilitarised Zone (DMZ).[40] An unnamed South Korean military official said that North Korean drones have been increasingly detected crossing the Military Demarcation Line that bisects the DMZ. In one incident in January, soldiers manning the border fired warning shots at a drone, which reportedly turned back. Seoul claims these drone missions are mapping out and probing South Korean troop positions. The drones themselves are believed to be based on Chinese Golden Way UV10 single-prop drones with a 36 km range.[41] However, in the past, Pyongyang has been sending versions of China's D-4, an older but larger surveillance aircraft acquired between 1988 and 1990.[42] Six North Korean drones have crashed in the South. One of these was in the vicinity of a nuclear power plant, raising concerns that this was a reconnaissance for a sabotage operation. Another flew over Seoul before crashing, taking pictures of the presidential residence, the Blue House.[43] North Korea has been expanding its drone force in recent years, though there are no indications anything sophisticated has entered service. Latest estimates are that the North has 300 aerial drones of at least seven types.

Also of note

- **Pakistan and Nigeria are among the reported customers of China's CH series military drones.**[44] Pakistan already uses CH-3 reconnaissance drones, but is reportedly interested in upgrading to the more powerful CH-4 combat drone.[45] Nigeria also uses CH-3 drones, and may too be upgrading to the CH-4.
- **An Armenian X-55 reconnaissance drone has been shot down by Azerbaijani armed forces as the UAV was flying along Azerbaijani frontline positions around the 19 April 2016.**[46] There has been conflict between the two South Caucasus countries since 1988 when Armenia made territorial claims against its neighbour.
- **An Israeli military document has reportedly confirmed the use of Hermes 450 Zik drones to conduct assassinations.**[47] Two incidents were mentioned in a *Ha'aretz*, article that was subsequently removed without explanation: four Palestinian fighters were killed on Zikim beach on 8 July 2015 and an attack by 13 fighters in a cross-border tunnel operation was foiled on 17 July 2015.

[40] http://www.upi.com/Top_News/World-News/2016/03/29/North-Korea-drones-keep-crossing-into-Souths-airspace/8491459270488/

[41] https://en.wikipedia.org/wiki/Golden_Way_UAV#UV10

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

[43] http://www.stripes.com/news/crashed-drones-were-north-korean-spy-effort-south-korean-officials-say-1.282077 and http://www.popularmechanics.com/military/weapons/a19090/inside-north-koreas-unmanned-aerial-vehicle-arsenal/

[44] http://www.thenews.com.pk/latest/114332-Pakistan-likely-to-buy-Chinas-drones

[45] http://quwa.org/2016/04/23/pakistan-talks-china-ch-4-armed-drone/

[46] http://en.trend.az/azerbaijan/karabakh/2521644.html

[47] https://www.middleeastmonitor.com/news/middle-east/24888-israeli-army-document-confirms-use-of-hermes-450-drones-in-assassinations

- **A US drone strike killed eight suspected members of al-Qaeda in southern Yemen on 26 March.** The attacks took place in the towns of al-Hudhn and Naqeel al-Hayala in the province of Abyan.[48]
- **A UK naval ice patrol ship, HMS Protector, has become the first ship to launch a drone manufactured on board the ship itself.**[49] The small reconnaissance platform was built using a 3D printer.

[48] http://www.theguardian.com/world/2016/mar/27/drone-strikes-yemen-kill-eight-militants

[49] http://theweek.com/articles/619455/future-americas-aircraft-carriers-floating-drone-factories

Cyber conflict

US Cyber Command operations against Islamic State becoming important force multiplier

The US administration has provided further details of the strategic focus of US Cyber Command (USCYBERCOM) operations against Islamic State after publicly acknowledging offensive operations in early March. On 12 April, the US deputy defence secretary, Robert Work, told media outlets that the United States is dropping 'cyber bombs' on Islamic State.[50] Work's comments forced a number of White House and Pentagon officials to clarify the scope and nature of USCYBERCOM operations against Islamic State.

The overarching message from US military and government officials is that USCYBERCOM is disrupting and sabotaging Islamic State's command and control (C2) capability by degrading and compromising telecommunications infrastructure and networks. An unidentified US official suggested that these types of operations significantly impeded IS C2 capability in the Syrian town of Shaddadi, which was recently recaptured by opposition forces.[51] It is highly likely USCYBERCOM are geo-identifying users of encrypted communication channels, blocking Islamic State's use of encrypted communications and forcing combatants on to less-secure communication channels or to use human couriers. In addition, USCYBERCOM is using spear phishing and watering hole attacks to implant malicious code on IS networks and computers, providing a continuous stream of intelligence and interrupting financial transactions used to pay fighters and receive income.

These cyber strategies are likely being used to redirect militants to battlefield spaces vulnerable to attacks by airstrikes or local ground forces, and are possibly contributing to US special operations forces kill or capture operations.

The White House's national security adviser, Susan Rice, hinted at robust debates behind closed doors between the NSA and USCYBERCOM about the extent to which cyber operations would reveal surveillance assets and implants.[52] While the scale of rhetoric on US cyber operations coming from the administration would suggest greater emphasis is placed on offensive operations rather than maintaining surveillance capacities, it is unlikely that substantial surveillance assets have been compromised by offensive cyber operations and that a balance between intelligence and offensive attacks remains contested across agencies. A proposal for USCYBERCOM to become a full combatant command, rather than a sub-unified command, is under consideration by the US defence secretary, Ashton Carter, and is likely to compound this tension.

In addition to balancing intelligence objectives with offensive cyber strikes, the NSA and USCYBERCOM are likely to have considered the ramifications of USCYBERCOM shifting its focus from the cyber activities of Russia, China, Iran and North Korea, some of the key originators of cyber attacks on the United States, to a non-state adversary. However, Islamic State's external operations in Paris, Turkey, Lebanon and Brussels and the desire of the US administration to capitalise on recent military gains are likely strong drivers underscoring US cyber escalation.

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

[51] http://www.thedailybeast.com/articles/2016/04/17/u-s-ratchets-up-cyber-attacks-on-isis.html

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

One apparently overlooked point is that the cyber proliferation risks associated with using cyber campaigns against non-state actors may be significant. Admiral Mike Rogers, commander of USCYBERCOM and director of the NSA, told the Senate Armed Services Committee on 5 April that he was concerned about Islamic State moving beyond using the cyber realm as a propaganda and recruitment tool and viewing 'cyber as a weapon'.[53] While unlikely in the short to medium term, extensive US cyber attacks may risk encouraging this shift without an acceptable corresponding US military advantage. With only limited understanding of cyber offensives, the proportionality the cyber campaign cannot be evaluated and the risks of proliferation cannot be weighed against military objectives.

Other developments

A January 2016 US Department of Homeland Security intelligence assessment of cyber attacks on the US energy sector was leaked in April.[54] The report finds that state-led Advanced Persistent Threats (APTs) targeting the energy sector are directed at maintaining persistent access as a contingency plan in the event of hostilities. However, the risk of disruptive or destructive attacks is considered low based on the fact that none of the 17 intrusions against the US energy sector reported in 2014 caused any damage or disruption. The assessment comes after the December 2015 cyber-enabled sabotage of Ukrainian power plants and recent reports on the cyber security of nuclear power-generation facilities. On 31 March, the US and British governments announced that mock cyber attack exercises against nuclear power plants would be carried out to improve emergency readiness and cyber security.[55]

The Australian prime minister, Malcolm Turnbull, announced the country's new $230 million (AUD) Cyber Security Strategy in mid-April.[56] This is the first time an Australian government has openly acknowledged an intention to develop and employ offensive cyber actions against adversaries compromising the country's security. Additional funding will be allocated to increasing cyber security capabilities across key law enforcement, intelligence and defence institutions as well as enhancing the cyber offensive capabilities of the Australian Signals Directorate (ASD). The strategy does not name any particular adversaries targeting Australian interests; however, the escalating scale of cyber attacks is noted by the ASD, with more than 1,200 cyber attacks on Australian interests in 2015, up from 940 the previous year. Some commentators suggest that the Australian government does not perceive the same risks associated with attacks in the cyber realm as allies who are spending more on cyber defensive and offensive capabilities and who – rhetorically at least – place significant emphasis on cyber threats.[57]

Russian and US cyber security officials met in Geneva, Switzerland, in mid-April to review and discuss confidence-building agreements signed by the two countries in 2013. The agreements established confidence-building measures (CBMs) to create a Russian-US hotline to provide officials a direct line of communication during a cybersecurity crisis. Previous cyber security talks between the countries were suspended after Russia's annexation of Crimea, and US officials emphasised that the latest talks were not a resumption of the Bilateral Presidential Commission working group. The disruption of Ukrainian power distribution networks in December 2015 is likely to have created a level of concern in the military and intelligence community that cyber miscalculation is an increasing risk.

[53] http://www.armed-services.senate.gov/imo/media/doc/16-35_4-05-16.pdf

[54] https://publicintelligence.net/dhs-cyber-attacks-energy-sector/

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

[56] https://cybersecuritystrategy.dpmc.gov.au/assets/pdfs/dpmc-cyber-strategy.pdf

[57] https://theconversation.com/australia-still-doesnt-see-a-cyber-attack-as-the-menace-our-allies-fear-57719

Also of note

- **South Korea has alleged that North Korea is disrupting GPS signal reception.** South Korea advised the media that it had traced the signals disrupting GPS reception to four regions in North Korea near the Demilitarized Zone (DMZ).
- **On 19 April, Singapore's prime minister, Lee Hsien Loong, met with the Israeli prime minister, Benjamin Netanyahu, to discuss expanding cyber defence cooperation.** The bilateral talks represent an important dialogue between one of the world's largest cyber security exporters and a country rapidly developing institutional, legal and operational cyber security reforms to protect multinational corporation commerce.
- **Japan and Estonia pledged to strengthen cyber security cooperation after bilateral talks in April.** The emphasis on cyber security cooperation may suggest that Japan sees cyber security as a key vulnerability and is actively reaching out to countries with extensive cyber security experience. In 2008, the NATO Cooperative Cyber Defence Centre of Excellence was established in the Estonian capital, Tallinn.
- **On 22 March, Finland's Ministry of Defence was subject to its second sustained DDoS attack of 2016.** The attack occurred shortly before the Finnish president, Sauli Niinistö, met with his Russian counterpart, Vladimir Putin, and during a period when the Finnish and US governments are finalising plans for joint military exercises.
- **Bulgaria's president, Rosen Plevneliev, told reporters in April that Bulgaria will establish cyber security centre after a spate of cyber attacks in 2015 targeting state institution websites and critical infrastructure.** Plevneliev indicated that the new centre will monitor potential cyber security threats from international terrorist organisations and states with totalitarian regimes and weak democracies.
- **In April, the UK Ministry of Defence announced plans to establish a Cyber Security Operations Centre (CSOC) to lead defensive cyber operations and secure defence networks and systems against cyber threats.** The centre is estimated to cost £40 million and will likely be located at the MoD Corsham military base. CSOC will be primarily focused on military networks, whereas the civilian National Cyber Security Centre (NCSC) will support cyber security for both public and private UK institutions.

Intelligence, surveillance and reconnaissance

Studies find mass surveillance having negative impact on democracy and informed debate

A new study by Jon Penney, a legal academic and PhD candidate at the University of Oxford, has concluded that the creeping growth of mass surveillance is breeding fear and conformity, promoting meekness and fear, and stifling the free expression of opinion within the population it is supposedly intending to protect from harm.[58]

The report, *Chilling effects: Online surveillance and Wikipedia use*, sets out Penney's finding that people avoid visiting certain websites, such as those linked to terrorism or radicalism, out of fear of being targeted by law enforcement. In one intriguing piece of research, it was found that following Edward Snowden's widely-publicised 2013 revelations into the extent of state surveillance of the internet, there was a 20% decline in traffic to Wikipedia articles related to terrorism, particularly those mentioning explosive devices, al-Qaeda or the Taliban. Penney argues that this demonstrates that people are wary that any such online activity will be noticed by the authorities and bring them under suspicion of being linked to terrorism. An undesirable consequence of this, Penney argues, is that people are becoming less likely to learn about key issues, such as terrorism, international conflict and domestic security, and therefore informed political debate is diminished. People may also become increasingly reliant on traditional information sources, such as politicians and mainstream news outlets, which are often partisan, subjective and offer minimal detail.

A similar conclusion was reached in a 2015 study by researchers at MIT and Digital Fourth that examined Google search data from 11 countries, looking at keyword search terms from before and after the Snowden revelations. This study again found that mass surveillance was stifling free expression and thought and 'that there is a chilling effect on search behavior from government surveillance on the Internet'.[59]

Self-censorship has also been found beyond internet traffic. A survey of American writers in October 2013 found that while they were not concerned about counter-terrorism surveillance, they still tended to curb their content to avoid being labelled as sympathisers of terrorism.[60]

Increased conformity as a response to widespread surveillance has been a regular observation, dating back to Jeremy Bentham's 18th century Panopticon prison design. Bentham proffered a theory that the behaviour of large groups of people could be regulated by structures that easily allow a watchman to observe occupants at any time without them ever knowing if they are being watched or not.[61] This ever-present risk of observation would motivate the occupants to act as if they are always being watched. This self-censorship and self-regulation was a key tenet of Orwell's dystopian classic *Nineteen Eighty-Four*, in which the Thought Police could covertly monitor any citizen's activities, facial expressions and reactions to identify any challenge to the party's ideology and control.

[58] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645

[59] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564

[60] http://pen.org/chilling-effects

[61] https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham

It has long been argued by liberty and privacy groups that there is a hidden agenda to national governments pursuing ever-tighter mass surveillance programmes: they are exploiting the perceived terrorist threat to conduct intrusive monitoring of all aspects of citizens' lifestyles. With successive studies showing that the state's ability to carry out wide-ranging surveillance without the target's knowledge will lead to fundamental changes in social behaviour at both the individual and group level, it appears that such arguments have some weight, whether that was the original intention of governments or not.

A surprising supporter of reducing state surveillance recently surfaced in the guise of Alexander De Croo, deputy prime minister of Belgium, which has experienced several violent terrorist incidents in recent months.[62] De Croo believes that the civil liberties of citizens do not need to be sacrificed by mass warrantless surveillance in pursuit of terrorists. While his stance on state surveillance has softened since the Brussels airport bombings (he was previously in favour of allowing citizens to own unregistered phones and SIM cards, but now believes that all mobile phone numbers should be registered to the user), he still strongly believes that the privacy of innocent citizens and protection from unnecessary collateral surveillance must always be protected.

Other developments

An investigation by the news website Buzzfeed into the controversial use of spy planes over US air space by law enforcement and security agencies, including the FBI and the Department of Homeland Security (DHS), has led to an unprecedented and detailed insight into the drones' capabilities and their use.[63] As well as the expected high-resolution video cameras, the use of augmented reality and stingray devices used to track and monitor mobile devices has also been uncovered.[64] Analysing flights between August and December 2015 using flight tracking website Flightradar24, approximately 200 aircraft were found to be active across the United States targeting serious crime groups involved in drug and human trafficking, plus terrorists and responses to terror-related incidents. Some examples of counterterror operations were given, including two aircraft being deployed with hours of the San Bernardino shootings to the home of the attackers, Syed Rizwan Farook and Tashfeen Malik. The technology used on the aircraft is both advanced and wide-ranging, including exhaust mufflers to reduce the aircrafts' noise footprint; low-light and infrared cameras; augmented reality software, which adds data-heavy satellite imagery to live camera feeds to provide greater information to observers; and stingrays and cellmast simulators, which trick mobile phones into connecting to on-board receivers to enable detailed monitoring.

[62] https://news.vice.com/article/belgiums-deputy-prime-minister-says-the-brussels-attacks-dont-justify-mass-surveillance

[63] https://www.buzzfeed.com/peteraldhous/spies-in-the-skies and http://www.ibtimes.co.uk/fbi-spy-planes-uncovered-report-reveals-how-us-intelligence-tracks-targets-sky-1553681

[64] https://theintercept.com/surveillance-catalogue/stingray-iii/

Germany's highest court has ruled that German anti-terrorism laws are partly unconstitutional. In a 6-2 vote in the Federal Constitutional Court, key sections of Germany's anti-terror legislation have been found to be unconstitutional and in need of fundamental redrafting. Sections covering covert surveillance, particularly in the bathrooms and bedrooms of private residences, were challenged on the grounds that the activities of innocent third parties may be recorded. There were additional concerns that privileged conversations, such as between targets and their doctors, lawyers or parliamentary representatives, could also be violated. The court found that the current wording was too vague and too broad and did not satisfy the principles of proportionality. It also called for the creation of an independent body that would examine surveillance data before it was passed to law enforcement and security agencies. The court gave the government until 30 June 2018 to pass replacement legislation, with the existing sections remaining in law until then. The findings were in response to lawsuits brought to the court by a former interior minister, Gerhart Baum, and the German Green Party, lawyers, journalists and doctors.

As part of its ongoing case challenging the UK government's mass surveillance programme, the human rights watchdog Privacy International has obtained confidential documents that give a detailed insight into the policies behind the programmes.[65] The documents reveal the extent to which the surveillance programmes have developed over the past decades. Termed Bulk Personal Datasets, the documents reveal that UK police and security agencies have been routinely 'summonsing' personal data from a vast array of public and private sector organisations beyond the more well-known financial and communication records. NHS records, tax records, registration for electronic petitions, supermarket loyalty card records, purchase histories, census data, travel records and commercial data (such as links to companies) have all been sought by agencies in relation to their targets as they build up their highly-detailed personality intelligence pictures. The documents also demonstrate the use of Section 94 of the Telecommunications Act 1984, which permits agencies to access data in bulk, including the metadata and contents of emails and SMS/MMS texts.

Also of note

- **The United States has agreed to provide intelligence support to the Nigerian government relating to locating to Boko Haram and the abducted Chibok schoolgirls.**[66] Communications intercept and drone-sourced aerial imagery will be among the data shared.
- **German intelligence agencies have been reportedly targeting a large number of allied countries and bodies.** According to *Der Spiegel*, these include the US State Department, the Israeli prime minister's office, the UK Ministry of Defence, the Austrian and Belgian interior ministries, EADS, Eurocopter, OPEC, the IMF, the UN International Drug Control Programme, NASA and US Air Force bases in Germany.[67]
- **China is developing a mass surveillance apparatus to tackle civil unrest.** The new setup will bring in big-data mining and analytic software to better handle the vast amount of information the state already gathers.[68]

[65] https://privacyinternational.org/node/853 and https://theintercept.com/2016/04/20/uk-surveillance-bulk-datasets-gchq/

[66] http://allafrica.com/stories/201604220048.html

[67] https://www.rt.com/news/338268-german-intelligence-israel-us/

[68] http://www.ibtimes.co.uk/how-china-uses-mass-surveillance-big-data-snooping-curb-social-unrest-1555880

Commissioned by the Remote Control Project

remotecontrolproject.org

Open Briefing is the world's first civil society intelligence agency. We are a unique international team of intelligence, military, law enforcement and government professionals working tirelessly behind the scenes to make a difference. We focus on doing three things:

- We provide **intelligence, security, training and equipment** to organisations striving to make the world a better place.
- We **scrutinise the actions of governments and militaries** and generate alternative policies.
- We deliver a **public intelligence service** so that *you* know what is really going on in the world.

Founded in 2011, Open Briefing is a groundbreaking non-profit social enterprise supported by volunteers and funded by charitable grants and public donations. We are *your* intelligence agency.

www.openbriefing.org