Remote-control warfare briefing | #17

2 August 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: Iraqi special forces play critical role retaking Fallujah from Islamic State.

Private military and security companies: Deaths of Nepalese security guards in Afghanistan highlights use of Asian contractors in conflict zones by private military and security companies.

Unmanned vehicles and autonomous weapons systems: Newly-released official estimates of casualties from US drone strikes step in right direction but too limited.

Cyber conflict: NATO designates cyberspace as an operational domain and includes cyber attacks in Article 5.

Intelligence, surveillance and reconnaissance: Proposal for greater communications surveillance powers for FBI voted down in US Senate, but Congress considering similar legislation.

Special operations forces

Iraqi special forces play critical role retaking Fallujah from Islamic State

In the second half of June, Iraqi special operations forces (SOF) retook Fallujah from Islamic State (IS) with support from predominately-Shia Popular Mobilisation Units (PMU) and US military advisors. Towards the end of June, the Iraqi defence ministry and the deputy commander of special forces, Brigadier Haider al-Obedi, claimed that Iraqi forces controlled 90% of the city, and the head of counterterrorism forces, Lieutenant General Abdul-Wahab al-Saadi, declared Fallujah 'fully liberated'. The campaign to retake Fallujah began in late May. Since then, over 2,500 IS fighters have been killed and over 1,000 people suspected of links to Islamic State have been arrested according to an Iraqi counterterrorism spokesperson.[1]

[1] http://www.businessinsider.com/ap-iraqi-commander-about-2500-is-militants-killed-in-fallujah-2016-6/?r=AU&IR=T

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

The expulsion of Islamic State from Fallujah, including IS fighters who had dug in in isolated pockets of the northern districts of the city, is an important development for Anbar province, the country's Sunni heartland. It also demonstrates the improving capability of Iraqi and US special operations forces to take back territory from Islamic State. However, the construction of a large trench to separate the northern parts of Fallujah from adjoining districts suggests an ongoing security risk and a potential lack of confidence that Islamic State has been completely removed from surrounding areas.

The close-quarter, urban fighting necessary to liberate the IS-controlled parts of the city posed significant risks to civilians. Post-liberation, sectarian tensions could be inflamed if the predominantly-Shia PMUs and Iraqi special forces are perceived to be taking insufficient care to avoid civilian casualties in majority-Sunni neighbourhoods while they maintain control of Fallujah and respond to any new attacks by Islamic State.

The involvement of US SOF advisers is likely restricted by their rules of engagement and limitations on the weapons that can be used in urban environments. In any case, much of the burden for combatting IS fighters is meant to fall to Iraqi special forces, such as the Golden Division. Iraqi Joint Special Operations Command initially indicated that the PMUs would not enter the centre of Fallujah; however, the units were called upon following fierce resistance from IS fighters. Human Rights Watch has documented reports that PMUs and Iraqi federal police have carried out torture and summary executions during the retaking of Fallujah.[2] On 4 June, the Iraqi prime minister, Haider al-Abadi, opened an investigation into allegations of abuse by PMUs, soldiers and police officers. Such incidents and the worsening humanitarian crisis in Fallujah will make holding the city problematic.

The success of the SOF-led model in recapturing territory from Islamic State in Fallujah is likely to influence preparations for the retaking of Mosul. On 11 July, the US defence secretary, Ash Carter, announced the deployment of an additional 560 US troops to Iraq during an unannounced visit to Baghdad. The new forces, likely to include SOF trainers and advisers, will primarily focus on building up Qayara air base, about 40 kilometres south of Mosul. The effort to retake Mosul presents substantial risks for both Iraqi and US special operations forces if the Shiite militias that make up most of the PMUs breach rules of engagement or unleash the sectarian persecution of civilians.

Other developments

The commander of the US military mission to Afghanistan, US Army General John Nicholson, indicated on 12 July that SOF and conventional forces deployed in the country will operate under new rules of engagement.[3] The new rules allow US forces to once more support offensive actions by Afghan troops. The change follows a Pentagon investigation into the confusion around the rules of engagement after NATO formally ended its combat role in 2014 and reflects the risks to remaining US forces from a resurgent Taliban. The investigation highlighted the Taliban takeover of Kunduz in 2015 as a situation where a lack of clarity on the rules of engagement left US special operations forces without clear direction over supporting Afghan troops coming under attack. The new rules suggest that the deteriorating security environment in Afghanistan is prompting mission creep in the training and advising role of US forces. The deteriorating situation has also led to the US president, Barack Obama, delaying scheduled troop drawdowns.

[2] https://www.hrw.org/news/2016/06/09/iraq-fallujah-abuses-test-control-militias

[3] http://www.scout.com/military/warrior/story/1686300-new-afghan-rules-of-engagement-more-attacks

Al-Qaeda in the Arabian Peninsula (AQAP) released a video in mid-July showing a training camp most likely located in southern Yemen where it trains its 'special forces'.[4] The video provides footage of AQAP fighters undergoing weapons training and live-fire drills. Former Guantanamo Bay detainee Ibrahim al Qosi appears in the video and states that the facility trains fighters from different tribes and areas without requiring them to work with AQAP. While the training will not be on a par with nation-state special forces, the increasing sophistication of expeditionary militant forces may suggest training camps such as Hamza al Zinjibari in Yemen are imparting significant tactical tradecraft to trainees.[5] Members of the AQAP special forces battalion appear in the video calling on US forces to meet them on the battlefield – a likely acknowledgement that US special operations forces returned to Yemen in April 2016. The return of US special operations forces will most likely result in a higher tempo of airstrikes against AQAP targets.

The presence of special operations forces in Libya is becoming harder for European powers to downplay following the deaths of three French SOF soldiers in a helicopter crash in the country on 17 July.[6] The Benghazi Defence Brigades claims that it downed the helicopter, though the Libyan Army has stated that the crash was accidental. The French president, François Hollande, told media that the special forces operators died during 'dangerous intelligence operations'. The incident forced the French defence ministry spokesman, Stephane Le Foll, to confirm the deployment of French special forces to Libya. This disclosure stood in contrast to the French defence minister's acknowledgment in early June that French special forces were only deployed in northern Syria to advise and assist Syrian Democratic Forces fighting Islamic State.[7] The UK government has similarly tried to remain elusive on the deployment of special forces in Libya despite continuing reports from Libyan partners of combat and ISR support from British soldiers.[8] British special forces are also reported to have provided medical supplies to field hospitals and ballistic protection to Libyan soldiers.[9]

Also of note

- **The Norwegian government provided authorisation for the deployment of special forces to Syria during a parliamentary session on 22 June.** Norway already has 120 special forces soldiers in the Kurdistan Region on advise and assist missions. It is anticipated that upward of 60 special forces soldiers will be sent to Jordon to train anti-IS Syrian fighters.

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

[5] http://www.thedailybeast.com/articles/2016/06/29/istanbul-ataturk-airport-attack-shows-sophisticated-planning-by-terrorists.html

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

[7] http://www.theaustralian.com.au/news/world/middle-east-france-special-forces-advisers-to-syrian-frontline/news-story/c8eee618b7805debdbb23d212f38b71f

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

[9] Ibid.

- **NATO allies reinforced their commitment to confronting transnational security challenges associated with regional instability in Iraq, Syria, Libya and Afghanistan.** The NATO Warsaw Summit Communique issued on 9 July outlined the actions NATO members are taking, including enhancing the NATO Response Force (NRF), which includes special operations forces components, and reaffirming the Iraq Defence and Related Security Capacity Building (DCB) initiative, currently hosted at the King Abdullah II Special Operations Training Centre in Jordan.[10]
- **Comments from the Canadian defence minister, Harjit Sajjan, and senior military officials suggest that Canada is considering sending Canadian Special Operations Forces Command (CANSOFCOM) personnel to Mali** to provide additional support to French-led counterterrorism operations in the country.[11] Austria is also thought to be sending a small special forces contingent from its special operations group, Jagdkommando, to Mali.
- **Cameroonian special forces were deployed to the Lake Chad area on 24 June in what has been billed as one of the largest Cameroonian special forces campaigns against Boko Harem.** Concurrent with this campaign, the Chadian Army is leading a campaign to drive Boko Haram insurgents from the southern borders with Niger.

[10] http://www.nato.int/cps/en/natohq/official_texts_133169.htm

[11] http://www.huffingtonpost.ca/jonathan-wade/canadian-peacekeepers-mali_b_11050910.html

Private military and security companies

Deaths of Nepalese security guards in Afghanistan highlights use of Asian contractors in conflict zones by private military and security companies

Fourteen Nepalese security guards were killed and five injured in a suicide attack on a Canadian embassy bus in Kabul, Afghanistan, on 20 June.[12] Both the Taliban and Islamic State have claimed responsibility for the attack. The deaths have drawn attention to the use of Asian contractors in conflict zones by private military and security companies (PMSCs). Around 9,000 Nepalis officially work in Afghanistan, mostly as security guards at foreign military or diplomatic compounds, but some estimates place the total figure at over 20,000 when those who have entered the country illegally are included.

In an article for Canada's *Globe and Mail* newspaper, the political anthropologist Noah Coburn outlined his findings from interviewing over 200 security contractors in Nepal, India and Turkey who worked for various private security companies in Afghanistan that were funded by Canada, the United States and other Western donors.[13] While many of the contractors reported generally-positive experiences, he found that a large number were subject to a variety of abuses by their employers. Many reported being trafficked into the country and then forced to take lower wages than they had been promised. The contractors risk being sent to prison if they reported these abuses, as they are brought into the country illegally and do not have proper visas. The situation is compounded for some contractors, as Nepal, for example, does not have an embassy in Afghanistan. During his 12-month investigation, Coburn also found many instances of injured contractors being provided only a small amount of cash and immediately shipped back home then abandoned by their company.

It is possible that the families of the Canadian embassy security guards will receive compensation, as the case has attracted considerable media attention. Injured contractors working for European and North American governments can also sue for compensation, if they can get a lawyer to take on their case. However, Western governments must do more to ensure that the PMSCs they award contracts to are adequately protecting their employees and looking after killed and injured contractors and their families, whatever country they come from.

There is also the wider question over whether it is ethical for Western governments to be using individuals from poorer regions of the world as proxy soldiers in place of conventional forces. As Coburn points out, European and North American governments are essentially exchanging Nepalese lives for Western lives by hiring contractors to undertake military tasks in conflict zones.

Nepal has stopped providing work permits for its citizens for Afghanistan, Iraq, Libya and Syria in the aftermath of the Canadian embassy bus attack.[14] The decision was taken after a parliamentary panel asked the government to clampdown on traffickers who send thousands of migrants every year to conflict zones, where they risked being exploited. Nepal is to also hold talks with the Afghan government regarding the security of Nepalis currently working in the country and to initiate steps to repatriate those who wish to return home.

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

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

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

Other developments

The man who killed 49 people at the Pulse nightclub in Orlando, Florida, on 12 June, worked for G4S Secure Solutions USA Inc, a subsidiary of the UK-based G4S.[15] The company refused to fire Omar Mateen despite his claims that he was connected to al-Qaeda, Hezbollah and the Boston Marathon bombers and wanted to be martyred. In 2013, while Mateen was working at St Lucie Courthouse, fellow G4S guards warned their supervisors that he had repeatedly made sexist, racist and anti-Semitic remarks. He had also voiced support for Nidal Hasan, the US Army major and self-proclaimed 'soldier of Allah' who killed 13 people and injured 30 more in a mass shooting at the Fort Hood in 2009. Mateen had also threatened a deputy sheriff, saying to him that he could have his al-Qaeda contacts kill him and his family. This last incident was reported to the FBI and to G4S, but the only action taken by by the company was to transfer him to another contract. The incident highlights the need for PMSCs to carry out better due diligence and screening of their employees, and to have proper procedures in place to deal appropriately with complaints against their staff.

The US Department of Justice has accused DynCorp of defrauding the US government during a contract to train Iraqi police. Papers filed by the justice department accuse the company of knowingly inflating costs during a four-year period.[16] The fraud allegation relates to a DynCorp subcontractor, called Corporate Bank, during the period between 2004 and 2008, when it held the Iraqi National Police training contract. According to the justice department, DynCorp was fully aware that the rates claimed by Corporate Bank for local security personnel, drivers and interpreters and hotel accommodation for US government officials were 'unreasonable', yet DynCorp nonetheless submitted them to the US state department for payment. The justice department charge states that 'DynCorp's invoices, which reflected these inflated subcontractor rates, and DynCorp's own fees and mark-ups, were false and fraudulent claims.' DynCorp also provides private security guards and aviation and logistics services, and is operating throughout the region; however, unlike previously, it was not among seven companies awarded state department contracts in February to protect US diplomats. DynCorp still holds contracts with the US Department of Defense, including a similar police training contract for the the Afghanistan Interior Ministry.

[15] http://www.newyorker.com/news/news-desk/the-security-firm-that-employed-the-orlando-shooter-protects-american-nuclear-facilities

[16] https://www.theguardian.com/us-news/2016/jul/19/dyncorp-iraq-military-contractor-fraud-pentagon

Unmanned vehicles and autonomous weapons systems

Newly-released official estimates of casualties from US drone strikes step in right direction but too limited

On 5 July, the White House took the unprecedented step of releasing statistics on the number of combatant and civilian casualties from the US military's drone operations.[17] However, there are considerable gaps in the data, which has angered and frustrated campaigners. The data only covers counterterrorism operations involving airstrikes from manned and unmanned aerial platforms and special operations forces raids in areas *outside* of Afghanistan, Iraq and Syria (which are categorised as 'areas of active hostilities') where the US military is directly engaged in fighting against terrorist groups, such as al-Qaeda, the Taliban and Islamic State. The countries where the raids took place are not specified, but likely include Pakistan, Yemen, Somalia and Libya. The data is also only from when Barack Obama first took office on 20 January 2009 until 31 December 2015, and so does not include figures from the preceding Bush administration. Furthermore, the figures are only broad estimates, rather than an accurate record of casualties.

Despite these considerable limitations, the data still provides a groundbreaking insight to these controversial operations. According to the release, there have been a total of 473 strikes against terrorist targets outside the areas of active hostilities. These have resulted in an estimated 2,372 to 2,581 combatant deaths and 64 to 116 non-combatant deaths. The US Director of National Intelligence (DNI), who produced the report, explains that the numbers are based on all-source intelligence, including reports from the media and NGOs working in the regions.

The White House no doubt hopes that the relatively low civilian casualty figures will go some way to vindicating its strategy of directed strikes against terrorist targets as an effective and proportionate tool in counter-terrorist warfare in place of a full military ground deployment. However, despite the DNI and campaign groups seemingly sharing similar counting methods, the official statistics have already been dismissed as inaccurate by campaign groups.[18] For example, the American Civil Liberties Union (ACLU) argues that the DNI's numbers are dramatically lower than those documented by independent journalists and human rights groups. It claims that the true number of civilians killed in US strikes outside the areas of active hostilities is more likely to be in the 200 to 1,000 people range.

The US government accepts that there will be discrepancies, but claims to have access to additional sources that are not generally available to NGOs, including pre-strike intelligence and post-strike analysis processes, which it argues makes its tally more credible.[19] However, the government data does not specify the criteria it employs to define a viable target. It has previously published a 'fact sheet' described a risk assessment that is carried out prior to using lethal force.[20] This defines a target as anyone posing a continuing and imminent threat to US persons, that it is not feasible to capture alive and where there is a near certainty that non-combatants will not be injured or killed. However, there is no detailed definition of these criteria or any quantifiable measure that would allow these assessments to be reviewed and compared against US and international law.

[17] https://www.dni.gov/files/documents/Newsroom/Press%20Releases/DNIReleaseCTStrikesOutsideAreasofActiveHostilities.PDF

[18] https://www.aclu.org/blog/speak-freely/president-obamas-new-long-promised-drone-transparency-not-nearly-enough

[19] https://www.dni.gov/files/documents/Newsroom/Press%20Releases/DNIReleaseCTStrikesOutsideAreasofActiveHostilities.PDF

[20] https://www.whitehouse.gov/sites/default/files/uploads/2013.05.23_fact_sheet_on_ppg.pdf

The DNI's report is intended to be the first of an annual report on casualty figures, which stems from an Executive Order signed by Obama on 1 July 2016.[21] This has provoked frustration as, unlike Congressional legislation, a Presidential Executive Order can be cancelled by the president with no legislative interference. However, the White House probably deserves some credit, as it would have certainly struggled to garner sufficient support to pass a Bill on this issue from an extremely hostile and uncooperative Republican-controlled Senate. The annual nature of the report will of course come under doubt should Donald Trump win the presidential election in November, as he would be able to cancel Obama's Executive Order.

Other developments

Toy aerial drones, available in many stores across Iraq, are becoming increasingly popular among the country's Shiite militias, which have grown frustrated by the failures and shortcomings of the Iraqi state military. Inspired by the technologies deployed by the Western militaries operating in the region, militias have started purchasing the small and fragile aircraft to provide aerial reconnaissance capabilities.[22] Sadiq al-Husseini, commander of the Badr Organisation, the largest and oldest of the Shiite militias, says the drones have played a crucial role in the conflict with Islamic State, preventing casualties among his forces around Fallujah and helping them lock onto targets with their mortars and cut Islamic State's supply lines. The Badr Organisation and other Shiite militias continue to work closely with the Iraqi military, including providing fire support during the recent retaking of Fallujah. The militias' drones were used to identify IS positions deep in the city and help direct artillery fire onto them. According to one Iraqi policeman involved in the Fallujah offensive, such forward artillery observation operations helped bring the accuracy of artillery fire up from 70% to 95%.[23]

Two retired US Air Force generals have argued that there is still a place for manned combat aircraft in future air forces.[24] John Loh, a former US Air Force vice chief of staff and former commander of Air Combat Command, and Ronald Yates, a former commander of Air Force Systems Command and Air Force Materiel Command, contend that while unmanned aerial vehicles (UAVs) certainly offer some performance advantages over their manned equivalent, there are still going to be roles for manned aircraft for the foreseeable future. This will be particularly so in offensive roles in high-threat environments with heavy radar and anti-aircraft defences, which drones will still struggle to cope with. They argue that the next generation of drones should be geared more towards their strengths, with greater stealth capabilities, longer range, higher altitude, better sensors and better connection to communications networks to allow more-effective data-intensive connections to commanders and frontline units. While manned aircraft will continue to lead operations in intensive combat zones, Loh and Yates argue that UAVs can be used in counter-terrorist operations in places such as the Middle East and North Africa, plus peacekeeping work and treaty-enforcement operations.

[21] https://www.whitehouse.gov/the-press-office/2016/07/01/executive-order-united-states-policy-pre-and-post-strike-measures

[22] http://www.wired.co.uk/article/iraq-isis-war-consumer-drones

[23] http://www.wired.co.uk/article/iraq-isis-war-consumer-drones

[24] http://www.defensenews.com/story/defense/commentary/2016/07/07/what-next-drone-warfare/86433910/

On 7 July, Dallas police used a police robot to deploy a C4 explosive device and kill Micah Xavier Johnson, who had shot 12 police officers, killing five. Dallas Police Chief David Brown gave the order to his SWAT team after a 45-minute gun battle and two hours of negotiating with the sniper. Using a tracked bomb disposal robot, a 1 lb (0.45 kg) C4 explosive device was placed against the wall Johnson was positioned behind.[25] While 1 lb is only a relatively small amount of C4, it can still be very destructive within a closed space due to air pressure forces rebounding of surrounding walls. Johnson was killed instantly in what is believed to be the first time US law enforcement has used a robot to kill a suspect.[26] The robot, a Northrop-Grumman Remotec Androx Mark V A-1, was still in position when the C4 was detonated, but only suffered minor damage to its extendable arm and tracks and remains operational.

Also of note

- **Between three and six suspected al-Qaeda militants were killed in a drone strike in south Yemen on 30 June.** The militants were in a vehicle travelling through Shabwa province when they were targeted by a US drone.[27]
- **Israel has unveiled a modular unmanned land combat vehicle that can be fitted out for various roles.**[28] The modules will allow it to carry out reconnaissance and combat roles.
- **Omar Mansoor, the leader of the Pakistani Taliban, was killed by a US drone strike on 9 July.**[29] The airstrike was in Afghanistan's Nangarhar province, which borders Pakistan. The attack also killed four other individuals described as members of Islamic State.
- **Hezbollah launched a drone from a site in Lebanon on 17 July and flew it over the northern Golan Heights.** Israeli forces launched two Patriot missiles in an attempt to down the drone, but the aircraft reportedly returned to base unscathed.[30]

[25] http://edition.cnn.com/2016/07/12/us/dallas-police-robot-c4-explosives/

[26] http://www.npr.org/sections/thetwo-way/2016/07/08/485262777/for-the-first-time-police-used-a-bomb-robot-to-kill

[27] http://english.alarabiya.net/en/News/middle-east/2016/07/02/A-drone-strike-kills-three-al-Qaeda-suspects-in-Yemen.html

[28] http://www.themanufacturer.com/articles/israel-unveils-new-modular-unmanned-combat-vehicle/

[29] http://www.wsj.com/articles/pakistani-taliban-leader-omar-mansoor-killed-in-drone-strike-1468440565

[30] http://www.israelnationalnews.com/News/Flash.aspx/364903

Cyber conflict

NATO designates cyberspace as an operational domain and includes cyber attacks in Article 5

At a press conference on 14 June, NATO's secretary general, Jens Stoltenberg, announced that NATO would recognise cyberspace as an operational domain as is the case for air, land and sea. The designation means that NATO members that are subject to major cyber attacks can invoke Article 5, the alliance's collective defence clause. If Article 5 is invoked, a severe cyber attack on one NATO member will be considered an attack on all NATO members. The development has its foundations in last year's NATO summit in Wales. The alliance officially adopted the policy on 8 July at the Warsaw Summit,[31] and bolstered its commitment with a Cyber Defence Pledge at the same time.[32]

The official designation of cyberspace as an operational domain happened at the same time as the websites of the NATO Allied Transformation Command and a NATO school in Oberammergau, Germany, went down. Unconfirmed reports speculated that the website interruptions were the result of cyber attacks linked with the Warsaw Summit.[33]

NATO representatives did not single out any one cyber threat actor as the driver of the enhanced policy; however, there are many indicators that NATO members are disproportionately concerned about Russian cyber attacks, espionage and intrusions. Stoltenberg's suggestion that it is hard to imagine conventional military attacks without blended cyber tactics could be interpreted as a reference to irregular warfare tactics used by Russia in Crimea. Additionally, the broader context of the largest military reinforcement in Europe since the end of the Cold War, interpreted as a bulwark against Russian military activities and mobilisation, would indicate that NATO is focused on Russia as a key threat.

The designation of cyberspace as an operational domain may also be part of a deterrence campaign. In the same way that the United States has attempted to employ deterrence against China and North Korea through indictments of cyber bad actors, diplomacy and sanctions, NATO may be using the policy and pledge to influence Russian cyber operations.

Russia-based hackers have been linked to a number of cyber attacks, including against a French television network, a German steelmaker, the Polish stock market, the Ukrainian power grid and, more recently, the Dutch Safety Board. In contrast to alleged Chinese cyber intrusions in US cyber domains, which are primarily focused on commercial and defence industry espionage, Russian cyber operations appear more focused on intelligence-gathering and reconnaissance of critical infrastructure networks. In some instances, Russia may be using cyber operations as a response to the imposition of sanctions by the United States and its allies. The blurring of lines between cyber activists, criminals and state-sponsored hackers allows Russia to test the cyber boundaries of adversaries while maintaining plausible deniability.

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

[32] http://www.nato.int/cps/en/natohq/official_texts_133177.htm?utm_medium=email&utm_campaign=NATO%20Press%20Releases&utm_content=NATO%20Press%20Releases+CID_475fd59d4d97b8bf176eb559590f600d&utm_source=Email%20marketing%20software&utm_term=Eng

[33] http://www.wsj.com/articles/nato-linked-websites-go-down-cyberattack-suspected-1468001918

Russian state and non-state actors are alleged to be involved in a range of cyber operations that have not yet resulted in offensive responses or sanctions. NATO's enhanced cyber policy may be the start of a more organised and robust response to Russian cyber operations, particularly if supported by investment in improved collective cyber defences. The policy may also influence Russia to consider centralising more high-profile and invasive cyber operations within state apparatuses, particularly if NATO is seriously raising the stakes and potential costs of cyber operations.

Other developments

The second US-China Cybercrime and Related Issues High Level Joint Dialogue was held in Beijing on 14 June.[34] The dialogue is a part of continuing rapprochement between the Untied States and China after the major powers agreed in September 2015 that neither government would 'conduct or knowingly support cyber-enabled theft of intellectual property' for economic advantage.[35] On the eve of the second dialogue, cyber security researchers FireEye published a report that suggested a notable decline in China-based groups launching cyber intrusion campaigns since mid-2014.[36] However, while US indictments for Chinese nationals identified as participating in cyber espionage may have had some impact, this decline is likely the result of Chinese military restructuring and a centralisation of cyber operations, which has reduced the *number* but increased the *sophistication* of cyber incursions. Furthermore, China's proposed cybersecurity law reforms will impose stricter censorship and less privacy online, suggesting that despite dialogue and diplomacy the United States and China are still philosophically at odds over regulating the cyber realm.

The cyber division of South Korea's National Police Agency (NPA) released information on 13 June about a large-scale cyber operation allegedly carried out by North Korea. The operation had infected over 140,000 government and private sector computers across 160 institutions and companies with malware. It was likely part of a broader plan for a hybrid large-scale cyber attack and espionage campaign against Seoul. Defence companies were significant targets, and there are suspicions that sensitive military documents on the F-15 fighter jet were accessed. Days after the announcement, the South Korean president, Park Geun-hye, told the International Symposium on Cybercrime Response that the international community needs to cooperate to counter growing transnational threats and cybersecurity challenges. Cho Hyun-chun, chief of South Korea's Defence Security Command, told another conference that cyber attacks by North Korea's 6,000-strong cyber army are evolving and becoming bolder, pointing to the alleged involvement of Pyongyang in recent cyber heists of the SWIFT interbank payment system.

[34] https://www.dhs.gov/news/2016/06/15/second-us-china-cybercrime-and-related-issues-high-level-joint-dialogue

[35] https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

[36] https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf

A report by the US Institute for Critical Infrastructure Technology released on 29 June argues that Islamic State possess the capacity to acquire the means necessary to launch cyber attacks.[37] At present, Islamic State does not possess significant cyber capabilities on a par with more sophisticated state and non-state actors; however, there appears to be an ambition to procure external cyber capabilities from the dark web to support its information warfare strategies. The ongoing territorial losses Islamic State is experiencing in Iraq and Syria have raised questions about how the group may restructure in future, including building deeper and more sophisticated online communities for a truly disaggregated network. On a related matter, a Kosovar who stole information on US military personnel and provided the data to Islamic State was extradited to the United States earlier this year. The prosecution will act as a basic deterrence to the hacking community considering selling their skills to Islamic State.

Also of note

- **The United States and India are expected to sign a framework agreement for the US-India cyber relationship after the US president, Barack Obama, and the Indian prime minister, Narendra Modi, met in early June.** The framework commits the parties to real-time information sharing on malicious cyber security threats, attacks and activities, which has become critical after India has recently faced sophisticated advanced persistent threats (APTs) allegedly linked to Chinese and Pakistani groups.
- **Israel and the United States signed an agreement on 21 June to enable greater cyber defence and intelligence sharing.** The agreement comes as both Republican and Democrat representatives introduced bills aimed at strengthening joint cyber security research between the United States and Israel, the United States-Israel Cybersecurity Cooperation Enhancement Act and the Advanced Research Partnership Act of 2016.
- **Cyber security researchers SentinelOne has identified sophisticated malware for completing energy grid systems reconnaissance on a dark web hacking forum.**[38] While malware packages are commonly found on the dark web, 'Furtim' appears to have been developed by more sophisticated hackers, most likely state actors.
- **The EU Parliament approved its first set of community-wide cyber security rules on 6 July.**[39] The directive imposes reporting and security requirements on essential service operators and encourages resiliency measures rather than focusing on procedures for attack and threat management.

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

[38] https://sentinelone.com/blogs/sfg-furtims-parent/ and http://motherboard.vice.com/read/researchers-found-a-hacking-tool-that-targets-energy-grids-on-dark-web-forum

[39] http://www.europarl.europa.eu/news/en/news-room/20160701IPR34481/Cybersecurity-MEPs-back-rules-to-help-vital-services-resist-online-threats

Intelligence, surveillance and reconnaissance

Proposal for greater communications surveillance powers for FBI voted down in US Senate, but Congress considering similar legislation

A Republican-backed proposal to expand the FBI's surveillance powers in the wake of the mass shooting at the Pulse nightclub in Orlando, Florida, was voted down in the US Senate on 22 June.[40] The proposal would have broadened the range of communications records that the FBI could have demanded from telecom companies without a warrant but under National Security Letters (NSLs) instead. The very existence of an NSL is usually kept a secret, and they are not processed through the public courts. National Security Letters issued through the Foreign Intelligence Surveillance Court (FISC) currently require a provider to hand over a user's full phone records. The proposal would have seen this extended to email records – requiring companies to hand over the metadata of timestamps and details of senders and recipients. Additionally, internet usage data would have been accessible, including the details of sites visited and social media log-in data. The legislation would not have given access to the actual content of emails. Opponents, which included major technology companies, strongly argued that these measures would have seriously undermined civil liberties while doing little to improve national security.

The amendment would also have made permanent a section of the USA Patriot Act that authorises intelligence agencies to conduct surveillance on 'lone wolf' suspects who do not have confirmed ties to a foreign terrorist group. That provision, which the justice department said last year had never been used, expires in December 2019. Lone wolf attacks are an increasing threat, with multiple attacks by individuals with no direct links to Islamic State or other violent groups having taken place across Europe and the United States in the past month. US intelligence agencies are keen to be granted the significant new tools included in the proposed amendment.

While it was voted down, this legislation is certainly not dead in the water. Two amendments are currently under consideration in the US Congress.[41] One is attached to the intelligence agencies 2017 budget bill, and has been the focus of considerable controversy in recent weeks. This particular amendment again seeks to allow the FBI to access email metadata and internet browsing histories through the National Security Letters obtained via the FISC. The second amendment is attached to the Commerce, Justice, Science and Related Agencies Appropriations Act.[42] Although this was voted down in the committee stage, its supporters are now trying to revive it.

[40] http://www.reuters.com/article/us-cyber-fbi-emails-idUSKCN0Z8160

[41] https://www.onthewire.io/expansion-of-fbi-surveillance-powers-still-on-the-horizon/

[42] https://www.onthewire.io/expansion-of-fbi-surveillance-powers-still-on-the-horizon/ and https://www.eff.org/deeplinks/2016/06/eff-urges-senate-not-expand-fbis-controversial-national-security-letter-authority

Civil rights groups and other opponents to the legislation are still fighting attempts to increase surveillance, especially within the unpopular NSL context. The Electronic Frontier Foundation (EFF) has focussed on the secrecy that surrounds National Security Letters.[43] EFF claims that hundreds of thousands of NSLs have been issued since 2001,[44] with only a handful having been made public (considering the large number of suspects currently under surveillance and the fact that their communications records are so vital in drawing up an accurate intelligence picture, such a figure is certainly not unrealistic). EFF also claims that the FBI has been abusing NSL requests, citing suspicion based on expansive and erroneous definitions of illegal activity. EFF also suggest that internet metadata could include details of geo-specific websites, which would allow the authorities to track a person's location just by the sites that they view.

Supporters of increasing surveillance powers counter that intelligence agencies need to be able to access communications records rapidly, especially for groups under active surveillance, in order to monitor their contact with other individuals and groups in the United States and abroad. Seeking such records through the courts could cause delays that would risk the authorities failing to prevent an attack as well as risk the disclosure of the request, which would jeopardise covert intelligence operations.[45]

Other developments

Details of secret warrants used for mass surveillance in the United Kingdom and abroad have been revealed for the first time in an official new report.[46] The Interception of Communications Commissioner's Office (IOCCO) has published an unprecedented overview of mass surveillance carried out via Section 94 of the Telecommunications Act 1984.[47] Under this legislation, unlimited power was granted to home secretaries to demand telecoms companies perform or cease any activity without any limit of time. The warrants are so secret that recipients within those companies are not allowed to mention their existence in any way. This legislation therefore authorised successive home secretaries to order mass surveillance for unlimited durations. The IOCCO report reveals that 94 orders (or 'directions') for mass surveillance were issued between 2001 and 2012, and all are still in force today. All of these are for bulk metadata containing senders/recipients and the dates and times of vast amounts of communications traffic. These orders were created by the MI5 and GCHQ on the grounds of 'national security'. In 2015 alone, MI5 made 20,042 applications to access communications data obtained via Section 94 orders.

[43] https://www.eff.org/deeplinks/2016/06/eff-urges-senate-not-expand-fbis-controversial-national-security-letter-authority

[44] https://www.eff.org/issues/national-security-letters/faq

[45] https://www.washingtonpost.com/news/monkey-cage/wp/2016/07/14/some-lawmakers-want-to-let-the-fbi-monitor-your-internet-and-email-activity-without-oversight/

[46] http://arstechnica.co.uk/tech-policy/2016/07/uk-secret-ongoing-mass-surveillance-iocco-report-section-94-telecommunications-act/

[47] http://www.iocco-uk.info/docs/56208%20HC33%20WEB.pdf

Details of communications between Islamic State militants has revealed a combination of direct command and control alongside innovation and improvisation.[48] The records were provided by European and US security agencies to a ProPublica TV production team putting together a documentary on terrorism in Europe for the US PBS programme Frontline. For example, Najim Laachroui, a 24-year-old explosives expert from Brussels who built the suicide vests used in the Paris attacks last November, communicated with a commander called Abu Ahmed in Syria through the encrypted Telegram app asking for Islamic State to test chemical mixtures for him. When Belgian police raided a property in Brussels linked to Laachroui's operations, Laachroui reported to Ahmed that the police had seized the ammunition for the AK-47 rifles that his cell needed for their upcoming attack on Brussels airport, where it is believed they planned to carry out mass shootings before detonating their suicide bombs. Ahmed advised Laachroui to instead attack just with bombs, which they did on 22 March. It was in the investigations after this attack that Laachroui's laptop was seized and his encrypted communications found and decoded.

A French parliamentary commission of inquiry into the series of attacks in Paris last year on the *Charlie Hebdo* offices, the Bataclan concert hall and elsewhere has argued for the creation of a single agency to better coordinate intelligence and counterterrorist operations. While concluding that most of the attacks could probably not have been avoided, the fact that all the attackers were known to security agencies pointed to a multi-layered intelligence structure that limited intelligence sharing. France has six intelligence units answering to the interior, defence and treasury ministries, and this cumbersome apparatus is akin to fighting while wearing lead boots according to the head of the inquiry, Georges Fenech. Fenech also said that without the multiple intelligence failings, the Bataclan attack, in which 90 people died, could have been prevented. The inquiry recommended that France needs to set up a national counterterrorism body modelled on the US National Counterterrorism Center and reporting directly to the prime minister. The inquiry made 40 proposals after its five-month investigation.

Also of note

- **NATO has pledged to provide increased military support, including surveillance aircraft, to Middle East and North African countries fighting Islamic State.** Alliance leaders also pledged to create a new naval counterterrorist mission in the Mediterranean and fund training programmes in Iraq and Afghanistan.[49]
- **Nigeria has inaugurated its Falcon Eye maritime surveillance system to help combat oil theft, piracy and smuggling.** Designed in Israel, the mass-surveillance system uses cameras and electro-optic equipment to monitor and track movements up to 35 miles offshore.[50]
- **Abu Dhabi has announced the installation of Falcon Eye across the UAE.** This will be used to link thousands of CCTV across the country on the road network and at vital facilities in order to control traffic and also 'human assemblies in non-dedicated areas'.[51]

[48] https://www.propublica.org/article/isis-via-whatsapp-blow-yourself-up-o-lion

[49] http://www.aljazeera.com/news/2016/07/nato-give-surveillance-planes-mena-countries-160709192055050.html

[50] http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=44090:nigerian-navys-falcon-eye-maritime-surveillance-system-fully-operation%E2%80%A6

[51] http://www.middleeasteye.net/news/abu-dhabi-announces-launch-israeli-installed-mass-surveillance-system-2107212621

- **An EU-US data-sharing agreement has been given the go-ahead for one year by EU member states.** The Privacy Shield allows companies to transfer personal data from the EU to the United States. A final obstacle was overcome when the United States gave assurances that access to data for law enforcement and national security will be subject to clear limitations, safeguards and oversight mechanisms and ruled out the mass surveillance of European citizens' data.
- **A sweeping anti-terrorism law has been signed by the Russian president, Vladimir Putin, that will greatly expand the Kremlin's ability to monitor and control digital communications.** This has sparked outcry from privacy and human rights advocates in this already surveillance-intensive country.

Commissioned by the Remote Control Project

remotecontrolproject.org

REMOTE CONTROL
Examining changes in military engagement

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