Remote-control warfare briefing | #03

2 July 2014

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 commissioned by the Remote Control Project, a project of the Network for Social Change, hosted by Oxford Research Group.

Special operations forces: US president announces 300 special operations forces advisers will be sent to Iraq to assist the Iraqi military in non-combat roles.

Private military and security companies: Leaked defence company presentation reveals United States' Afghanistan exit strategy relies on private contractors.

Unmanned vehicles and autonomous weapons systems: Convention on Certain Conventional Weapons meeting of experts on lethal autonomous weapons systems prompts significant debate on 'killer robots'.

Cyber warfare: US justice department indicts five members of Chinese People's Liberation Army for hacking into US corporate networks.

Intelligence, surveillance and reconnaissance: United Kingdom's signals intelligence agency forced to reveal its policy on mass surveillance.

Special operations forces

US president announces 300 special operations forces advisers will be sent to Iraq to assist the Iraqi military in non-combat roles

After considerable domestic debate over the United States' response to the Islamic State in Iraq and the Levant's (ISIS) insurgency in Iraq, President Barack Obama has announced that 300 special operations forces (SOF) advisers will be sent to Iraq to assist the Iraqi military. The decision to send SOF into Iraq for non-combat roles, including training and advisory support, clearly seeks to balance a number of political and operational imperatives, while leaving the door open for a significant revision of US involvement if events demand it.

Politically, the light footprint and limited remit of the SOF is far short of air strikes and 'boots on the ground', but is not a total abstinence of US support for the current Iraq government. This position should temporary neutralise criticism from the hawks and the doves on either side of Obama.

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

Operationally, providing US SOF to the Iraqi military for training and advisory will also bolster the ability of the US military to assess on-the-ground intelligence, surveillance and reconnaissance (ISR) and identify any intelligence gaps that would render US air strikes less than effective or potentially counterproductive. The support mission may enable the United States to identify a target list for any future air strikes, though the SOF teams would not order strikes in their current role.

If required, the US administration can elevate support with greater confidence in the strategies required to push back ISIS in northern Iraq. Alternatively, if intelligence shows an overestimation of ISIS's presence and capability, the US SOF teams working with Iraqi counterterrorism teams may be sufficient to stop ISIS building any further momentum.

Obama has secured assurances of legal immunity from the Iraqi government for the 300 SOF members providing training and support. Baghdad's refusal to grant immunity to US troops beyond 2011 played a role in Washington pulling out all troops from Iraq by the end of that year. A more detailed agreement on legal immunity would be necessary if the US SOF teams or newly deployed regular troops were to undertake combat roles.

Other developments

The Nordic Defence Cooperation (NORDEFCO), which includes Denmark, Finland, Sweden and Norway, have been undertaking joint training and exercises with a number of Baltic States. The recent exercises of the Combined Joint Nordic and Baltic Exercise Plan were designed to improve interoperability between Nordic SOF units and those in partner Baltic states, such as Lithuania and Estonia. While tensions between Ukraine and Russia have reinvigorated NATO training and preparedness, the joint Nordic and Baltic rapid response and preparedness exercises may improve the regional capacity to respond to any small-scale regional insecurity.

A *New York Times* profile of the commander of US Special Operations Command Africa has provided a general overview of the US military's macro-level strategy across the African continent.[1] Brigadier General James B. Linder's remarks were very much on message with current US military strategy to build up local policing and security capacity through training by US special operation forces. Comments such as 'Africa is the battleground of the future' and 'The future of war is about winning people, not territory' are consistent with US Special Operations Command (USSOCOM) current operational and tactical philosophy. Despite Linder's support for balancing development and security in new SOF mandates, a number of civil society organisations question whether the professionalisation of security and police forces actually delivers sustained improvements and highlight the lack of congressional review of whether or not SOF counterterrorism programmes deliver long-term sustainable security.

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

Canadian Special Operation Forces Command (CANSOFCOM) is expanding their international training footprint. The Canadian government has allocated CAN $13 million (US $12.6 million) annually for its counterterrorism capacity-building programme. The government also has a non-recurrent funding envelope for SOF counterterrorism training in Africa, which has helped fund Canadian SOF presence in Kenya and Mali. More recently, Canadian SOF continue to conduct joint exercises with Jordanian SOF, including during the recent 2014 Eager Lion exercise in Jordan in late May, and are positioned to start the training exercises in Malaysia announced in April.

Also of note

- **US SOF captured the alleged ringleader of the terrorist attacks in Benghazi, Libya, on 15 June.** The US Ambassador to the United Nations, Samantha Power, notified the UN Security Council of the capture under Article 51 of the UN Charter and indicated that the capture of Ahmed Abu Khatallah was necessary to prevent further attacks on US persons. Khatallah is now expected to face a US federal court.
- **The Pentagon has suspended military-to-military exercises with Thailand, including US SOF training exercises with Thai special forces, after the recent military coup in Thailand.** The suspension is likely to have tangible repercussions for US force projection in the region.
- **USSOCOM's Sensitive Site Exploitation (SSE) programme is looking to enhance in-the-field DNA and biometric analysis** rather than having to rely on labs to process site material collected by SOF teams. SSE indicates that it has already field tested three mobile rapid DNA devices and that its 2015 $15 million budget will include further project development.
- **US Ambassador to the Philippines Philip Goldberg indicated in June that the Joint Special Operations Task Force Philippines had provided intelligence and situational awareness support to Philippine forces** during the 23-day battle between government troops and a renegade offshoot of the Moro National Liberation Front in Zamboanga City in September 2013. While US SOF presence in the Philippines is well known, the nature of their engagement is not always clear.
- **In May, a report by three French senators proposed that Paris transfer cyber operations from the civilian intelligence agency the Direction Générale de Sécurité Exterieure (DGSE) to the command of French special forces.**[2] A number of the report's recommendations were based on lessons learnt from the Serval campaign in Mali.
- **Israeli defence company Elbit Systems is testing a 'pocket artillery' (120mm) heavy mortar system (Spear)** specifically designed for special forces. Spear will be easily mountable on light vehicles, providing compact but significant rapid firepower capability.
- **In May, the commander of US Special Operations Command Europe (SOCEUR), Major General Brad Webb, told a defence industry audience to focus on developing intelligence-gathering and communication systems** that can withstand the extreme climatic conditions of Africa and the Arctic.

[2] http://www.senat.fr/rap/r13-525/r13-525_mono.html

Private military and security companies

Leaked defence company presentation reveals United States' Afghanistan exit strategy relies on private contractors

Since President Barack Obama took office in 2009, the United States has attempted to design and implement an exit strategy in Afghanistan that would allow international forces to withdraw combat troops without endangering soldiers' lives or further aggravating Afghanistan's poor security situation. It first consisted of a 'winning strategy' through the 2009 troop surge and an emphasis on both counterinsurgency and counterterrorism. This aimed to consolidate strategic security gains that would provide breathing space, enabling a gradual political and security transition over to the Afghan people.

In late May of this year, Obama announced that the United States would keep up to 9,800 US troops in Afghanistan until 2016, mostly in an advisory role and to protect the US embassy. However, this announcement did not identify the high number of private contractors that will remain in Afghanistan, which largely outnumber US troops and special operations forces conducting ongoing counterterrorism operations against remaining al-Qaeda operatives.

A leaked PowerPoint presentation obtained by news website *Salon* from SAIC, a US defence company, lays out the range of roles contractors have played since Obama's 2009 strategy shift and troop surge.[3] The presentation describes how the company has been contracted to provide services related to 'Expeditionary Warfare; Irregular Warfare; Special Operations;' and also '…Stabilization and Reconstruction Operations'.

The active role private military and security companies (PMSCs) are playing in stabilisation and reconstruction operations suggests that such companies are increasingly being used in post-conflict development and peacebuilding, further reinforcing the privatisation of reconstruction and state building. This was echoed an April 2014 report by the Special Inspector General for Afghanistan (SIGAR) that revealed that 69% of the $4 billion the US state department spent on Afghan reconstruction projects from 2002 to March 2013 went to a single private military contractor, DynCorp, whose role was mainly to assist with police development and reconstruction projects.[4]

The leaked presentation was put together by SAIC to assist its subcontractors in better understanding the US Army's needs on the ground. According to the document, subcontractors are contracted to provide US forces with electronic and electro-optic technologies, as well as items as diverse as body armour and cold weather equipment. There are also plans for the contractors to help with intelligence analysis software as well as enhanced lethality, accuracy and 'destructive capabilities' when it comes to US Army operations on air, land and sea.

[3] http://www.salon.com/2014/05/28/exclusive_new_document_details_americas_war_machine_and_secret_mass_of_contractors_in_afghanistan/

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

The use of private contractors for weapon enhancement and high-risk security tasks is hardly a new phenomenon. However, governments and state militaries have traditionally been the main actors involved in tasks related to stabilisation and reconstruction operations, as well as intelligence gathering. This had remained so because of concerns over effective monitoring and evaluation and because of secrecy and accountability issues. This is no longer the case.

Ultimately, Obama has made it clear that US forces will no longer be engaged in direct combat in Afghanistan past 2015, with the exception of targeted counterterrorism operations led by special forces. Yet, it is becoming increasingly clear that the US exit strategy in Afghanistan will also involve a high number of private security contractors – some fulfilling roles only state agencies would have previously undertaken.

Other developments

Questions are being raised over the possible role of US military contractors in Iraq. Iraq's security has deteriorated significantly following a series of attacks by Sunni militants and insurgent fighters gaining ground in several key Iraqi cities. In the north, Kurdish troops have taken over the city of Kirkuk following the departure of the Iraqi military. The United States withdrew its troops from in Iraq in 2011, but many US nationals remain on the ground, including embassy staff, private security contractors and private military advisers (plus 250 US military personnel, including Marine Corps security guards and advisers to the Iraqi government). The state department has reported that the US government has around 5,000 contractors in Iraq, 2,000 of which are civilians. It is unclear what role these contractors will play, and it is probable that the security situation will require some of them to be evacuated. However, given President Barack Obama's apparent unwillingness to send troops back to Iraq (with the exception of 300 special operations forces), it is highly likely that defence contractors – alongside CIA operatives – will continue to play an important role in the US government's remote-control warfare against Sunni insurgents.

A new US bill requires a review of the Pentagon's use of private contractors in Africa. In May, the US House of Representatives passed the 2015 National Defence Authorisation Act (NDAA), which includes a provision requiring a review of the US defence department's use, management and oversight of private contractors in Africa. The move was largely prompted by issues arising with regard to the use of contractors in Iraq and Afghanistan and US lawmakers' unwillingness to face similar issues in AFRICOM's contracts with private security companies. This comes as the US government has been increasing its resources in Africa, particularly in the Sahel and North Africa, which are perceived as strategic locations for counterterrorism. Of particular importance is the extent to which AFRICOM operations make use of private contractors and whether the state department enjoys enough control and oversight over activities in Africa. A report is to be submitted to the congressional defence panel by 15 April 2015.

Bill Gates' philanthropic foundation has sold its stake in British multinational security services company G4S. The Bill & Melinda Gates Foundation held as many as 49 million shares. The foundation recently attracted criticism for its G4S investment, as the company has contracts with Israeli prisons in occupied Palestine. G4S is still trying to rebuild its reputation following the problems it encountered adequately fulfilling the security contract for the 2012 Summer Olympics in London.

Also of note

- **The chief executive of the UK division of G4S, Eddie Aston, has left his position after less than six months in the job.** The is the third such departure in less than two years, and further adds to the company's instability.
- **G4S Australia Pty Ltd claims they warned the Australian immigration department before the deadly Manus Island detention centre riots in February 2014.** The security company tried to mobilise additional guards before violence broke at the regional processing centre in Papua New Guinea. A report for the Australian Department of Immigration and Border Protection found that G4S guards attacked transferees during the unrest. An Australian senate inquiry into the violence will provide its report by 16 July.
- **The first issue of *Private Military Contractor International* has been published.**[5] It is a digital magazine designed for PMSC operatives and companies. Each issue provides reviews of products, expert features as well as general news.
- **Police Scotland has announced that 17 private security companies will be working alongside police and military personnel to provide security and stewarding at the Glasgow 2014 Commonwealth Games.** This will be a crucial test for the companies involved, which includes G4S Secure Solutions (UK) Ltd, two years after the security problems of the 2012 Summer Olympics in London.
- **A two-day seminar on the Montreux Document was organised early June in Dakar, Senegal, with the support of Switzerland and the International Committee of the Red Cross.** The seminar aimed to give a new impetus to the agreement on the conduct of PMSCs in war zones by increasing the number of supporting states and providing stakeholders with a platform to exchange best practices in regulating PMSCs in sub-Saharan Africa.
- **Australia has increasingly been relying on external private security contractors to manage the security details of its government officials.** When then Australia's foreign minister Kevin Rudd travelled to Libya in December 2011, Control Risks was entrusted with securing his trip; checking routes, accommodation and potential threats; and designing potential evacuation plans. That particular contract amounted to just over AUS $55,000.

[5] https://www.joomag.com/en/newsstand/private-military-contractor-international-april-2014/0907143001394362770

Unmanned vehicles and autonomous weapon systems

Convention on Certain Conventional Weapons meeting of experts on lethal autonomous weapons systems prompts significant debate on 'killer robots'

The Convention on Certain Conventional Weapons (CCW) meeting of experts on lethal autonomous weapons systems (LAWS) on 13-16 May led to significant public debate between NGOs, governments, legal academics, the defence industry and military analysts.[6] The meeting was the first multilateral discussion on LAWS, and most participants agreed that the CCW was an appropriate forum for continued and urgent discussions on autonomous weapons.

Ahead of the CCW meeting, Human Rights Watch and the International Human Rights Clinic (IHRC) at Harvard Law School released a report on the human rights implications of fully-autonomous weapon systems and specifically the issues posed by these systems for international humanitarian law (IHL).[7] The report recommended the prohibition of LAWS in both law enforcement and armed conflict contexts.

It is clear from the minutes of the meeting that both the definition of fully-autonomous systems and the implications for IHL are contested and will be subject to further debate. Some participants suggested that moratoriums at this stage may undermine current technological development efforts in civilian fields. A number of the delegates emphasised particular non-lethal areas for autonomous technology development, such as intelligence collection, rescue tasks, logistics and transportation.

Cuba, Ecuador, Egypt, Pakistan and the Holy See called for a ban on fully-autonomous weapons. No member state argued in favour of autonomous weapons systems, though Israel spoke about the potential desirability of such systems in certain circumstances and the Czech Republic University of Defence – not necessarily representing the national position – spoke of unreasonable limitations on research creating 'security disbalance'. Israel's position is unsurprising considering their advanced military-technology industry and competitive edge in relation to unmanned systems.

On 12 June, the UN Special Rapporteur on extrajudicial, summary or arbitrary executions, Christof Heyns, reiterated his call for states to impose moratoria on the development and use of fully-autonomous weapons systems.[8] Heyns also advocated that the Human Rights Council remain strongly focused on addressing emerging issues related to the impact of LAWS on international humanitarian law. This might suggest that other UN institutions beyond CCW should be involved in considering LAWS and that an arms non-proliferation framework is not the only means to address the issue.

[6] http://www.unog.ch/80256EE600585943/(httpPages)/6CE049BE22EC75A2C1257C8D00513E26?OpenDocument

[7] http://www.hrw.org/sites/default/files/reports/arms0514_ForUpload_0.pdf

[8] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session26/Documents/A-HRC-26-36_en.doc

Other developments

After almost six months without a drone strike, two CIA-led strikes in June killed more than a dozen Pakistani militants from the Haqqani network. Some analysts had speculated in late May that US drone strikes in Pakistan were coming to an end, and that intelligence supporting drone strikes is likely to dry up with the drawdown of US troops in Afghanistan at the end of 2014. However, there are number of factors that encouraged the US administration to resume drone strikes after a six month hiatus, including the breakdown in Pakistani Prime Minister Nawaz Sharif's peace negotiations with the Tehreek-e-Taliban Pakistan and the release of US soldier Sergeant Bowe Bergdahl, who had been held hostage by the Haqqani network for five years. There are conflicting reports about whether or not the strikes were taken with the express approval of the Pakistani military and government.

Three European defence companies, including Air Bus, have proposed the German, Italian and French governments jointly develop a European drone by 2020-25. Both industry insiders and some politicians have consistently argued that there is a need for European countries to develop their own unmanned aerial vehicles (UAVs) to meet national requirements, provide EU interoperability and reduced reliance on US and Israeli suppliers. Industry proposals have been developed in response to France's 2013 announcement it would seek to purchase 12 US Reaper drones, following France's military intervention in Mali. France and Britain are set to sign a £120 million feasibility study on an unmanned combat air vehicle (UCAV) in mid-July. This contrasts with Germany, which cancelled its contract with US aerospace company Northrop Grumman for a Euro Hawk UAV over cost concerns related to certificating the drone for flights in civil airspace.

UN peacekeeping forces in Mali are to get access to drones for surveillance of the volatile north of the country. The request comes after tensions in the north were reignited during Prime Minister Moussa Mara's visit to Kidal. Improved surveillance is particularly critical for the UN forces in light of the lower numbers of military personnel being deployed than were authorised by the Security Council. The French military intervention in Mali last year highlighted the lack of intelligence on northern Mali. France was forced to rely on US-operated UAV surveillance missions out of Niger. For UN peacekeeping forces, the objective is to trial UAVs for ISR to obtain better situational awareness of threats to civilians and options for the delivery of humanitarian aid. The United Nations are already using UAVs in the Democratic Republic of the Congo and are likely to increase requests for UAVs for use in the Central African Republic and South Sudan.

Also of note

- **In late May, Royal Canadian Air Force representatives indicated that they hoped to have an operational UAV fleet by 2023 for Arctic, coastline and international mission surveillance.** However, the $1 billion fleet and 650 member squadron is already experiencing project delays and lapses in political commitment.
- **Israel Defence Force (IDF) has plans for unmanned ground vehicles and other robotic systems for border patrols and inspection of Hamas's underground network of tunnels.** The IDF have also pulled Cobra attack helicopters out of service and replaced them with UCAVs as a cheaper option after treasury budget cuts.

- **US administration has admitted flying surveillance UAVs in small numbers over Iraq since 2013.** The UAV surveillance missions, known to the Iraqi government, apparently did not provide the US administration with foresight into the rapid capture of two Iraqi cities by ISIS. **US Office of Naval Research (ONR) is developing a ground-based air defence capability against UAVs through the use of lasers.** The laser system is expected to be ready for field testing in 2016.
- **Russian Deputy Defence Minister Yury Borisov has announced aims to test Sokol and Tranzas UCAVs in 2017.** The UCAVs are anticipated to carry 5-ton and 1-ton payloads respectively.
- **Defense Advanced Research Projects Agency (DAPRA) has unveiled new software for UAVs to prevent cyber attacks on US drone fleets.** After unconfirmed hacking of US UAVs by Iran and Russia, DAPRA have prioritised improving the security of UAV systems without compromising networking capacity and connection.
- **South African company Desert Wolf has sold a drone that fires pepper spray bullets to a mining company as a riot control device.** The non-lethal weapon has the capacity to carry up to 4,000 bullets and employ 'blinding lasers'.

Cyber warfare

US justice department indicts five members of Chinese People's Liberation Army for hacking into US corporate networks

Five members of a Chinese People's Liberation Army advanced persistent threat (APT) unit known as Unit 61398 were named in a US justice department indictment for hacking into the network of US companies, including Westinghouse Electric, Alcoa, Allegheny Technologies, the United Steelworkers Union, SolarWorld and the United States Steel Corporation. Unit 61398 are alleged to have accessed company business plans, emails and product research and development, and provided commercial information to Chinese state-owned corporations. This is the first criminal hacking charge that the United States has filed against specific foreign officials.

The indictment suggests state sponsorship of cyber espionage and there is no extradition treaty between China and the United States, which makes it highly unlikely that the Unit 61398 members will face a US court. To this end, commentators suggest that the indictment is symbolic only, though it does provide an opportunity for the United States to lay out the evidence in public and potentially shame China in international forums.

Others commentators suggest that the indictment is a US strategy to remove attention from Edward Snowden's leaks on US cyber spying and intelligence-gathering activities in China and elsewhere. However, this would require the US administration to craft a convincing and easily understandable distinction between cyber activity for national security purposes and cyber espionage for the purpose of intellectual property theft and commercial advantage. Otherwise, Beijing needs do no more than underline NSA activities and the complicity of US technology companies in NSA programmes. Beijing's rapid cancelation of participation in a US-China working group on cybersecurity raised very little public criticism.

It is questionable whether the justice department's selective indictment has done much to redress the lack of US legitimacy on anything cyber. The NSA's activities have greatly impeded the ability of the US administration to address cyber espionage and the theft of trade secrets. Questions have been raised as to why the justice department has not pursued the cyber espionage actor Putter Panda, linked to the PLA's 3rd Department 12th Bureau Unit 61486, over the cyber-espionage activity against US defence companies and European satellite and aerospace industries outlined in a recent report from the security technology and intelligence company CrowdStrike.[9] There is some suggestion that despite having sufficient evidence, US engagement in similar activity would become the focus if Putter Panda was indicted.

The cyber espionage charges and the deterioration in Sino-US relations over the last two months come at a time when the United States are more openly expressing concerns over Chinese activities in the South China Sea and Chinese military spending, which the Pentagon estimated at $145 billion in 2013.

Other developments

The US Department of Defence announced in June that the United States and specific allies are working to bolster the cyber offensive and defensive capabilities of vulnerable US allies. The announcement is likely to be a response to cyber attacks allegedly emanating from China and Russia. The recipients of cyber capacity-building support are likely to be geo-strategically important but developing Eastern European countries, for example Latvia and Lithuania, and Asia-Pacific states, such as the Philippines, Indonesia and Vietnam. These countries are most likely to be at risk from regional cyber attacks. The Pentagon also indicated that the United States and NATO are exploring the application of Article 5 of the NATO charter to cyber attacks – whereby an attack on any one NATO member would be considered an attack on the entire alliance.

Analysts are raising the possibility that the Chinese government is using information and communication technology (ICT) infrastructure support and aid to enable a broad-scale cyber-espionage campaign across the Caribbean, particularly in Guyana and Jamaica. It is alleged that Chinese ICT equipment, including government-issued laptops, has spyware installed across all networks, enabling significant interception of user communication. Chinese ICT aid has a strong presence in the Caribbean and if backdoors in Chinese hardware or firmware were used for covet intelligence collection, the Chinese government would not only have access to politically-sensitive material but also capture information of capital and offshore fund inflows from other states into tax havens and low tax jurisdictions in the region.

[9] http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf

The Islamic State in Iraq and the Levant (ISIS) have implemented a relatively organised information campaign and social media presence alongside their capture of key towns in northern Iraq. ISIS created an Arabic-language Twitter app called The Dawn of Glad Tidings that allows the insurgent group to automatically syndicate their tweets on app user's twitter accounts. There has also been clear coordination of ISIS inspired and created hashtags to ensure ISIS messages and retweets are identified as trending. The level of coordination and sophistication of the social media campaign has led some analysts to question whether the apparent international support and social media buy-in for ISIS is, in fact, over-inflated. At the same time, the campaign highlights that many militant groups have an advanced understanding of the information dimensions of insurgency and warfare. The Iraqi government has attempted to block internet access in the areas where ISIS have a physical foothold, and have requested that ISPs block access to social media sites. A complete cyber black-out is not possible as the government does not own the entire ICT infrastructure.

Also of note

- **A June report from McAfee and the Center for Strategic and International Studies estimated that cybercrime is costing the global economy $375-575 billion a year** and that costs are expected to rise.[10] The United States, Norway, the Netherlands, Germany and China have the highest GDP to cybercrime loss ratios.
- **Greater focus is being placed on the F-35's cyber capacities, such as attack capabilities against surface-to-air missiles,** as US security partners have robust debates over procurement of the F-35 Joint Strike Fighter.
- **Japan and the United States have provided $400,000 to the Association of Southeast Asian Nations (ASEAN) to develop capacity for cybercrime investigation.**
- **Demand for cyber security in the Gulf States and the wider Middle East is growing rapidly,** with current projections from Airbus Defence and Space estimating an 8-10% per year growth. The market is valued at $66 billion this year. The demand comes after numerous high-profile cyber attacks on Saudi Aramco and RAK Bank and the ongoing threat to large-scale oil and gas installations.
- **British and Israeli governments have signed a letter of intent to proceed with a joint £1.2 million cyber-research programme** across six thematic research areas: identity management, cyber-security governance, privacy assurance and perceptions, mobile and cloud security, usable security and cryptography.
- **NATO announced in late May that 17 countries participated in the Locked Shields cyber-warfare drill in March.** The aim of the drill was to allow NATO to test and boost its cyber-defence capabilities, particularly in smaller Eastern European states. NATO also approved the construction of NATO military cyber-training centre in Estonia.

[10] http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

- **Defense Advanced Research Projects Agency (DAPRA) has released information on developments in its Plan X foundational cyberwarfare programme,** including a new hacking visualisation tool making use of Oculus Rift virtual reality headsets to allow users to see a 3D visualisation of a cyber environment. DAPRA has also announced a competition seeking software that implements autonomous cyber-defence actions.
- **Institute for National Security Studies (INSS) published a report on Iran's Newscaster cyber-espionage campaign.**[11] The campaign used false social networking profiles to gather and intercept information from important Washington personalities. US network security company FireEye also produced a report on the Iranian hacking group Ajax Security Team.[12]
- **According to analysis from FireEye, Russia and Ukraine are still exchanging significant cyber attacks.**[13] Of note, CyberBerkut, a group of pro-Russia hackers, tried to derail Ukraine's presidential election vote count by infiltrating central election-centre computers, deleting key files and attempting to destroy the vote tallying system.
- **British government has signalled an intention to introduce life sentences for cyber attacks** that have a catastrophic effect, such loss of life, serious illness or injury or serious damage to national security.
- **A cybersecurity expert with the EastWest Institute has advocated that countries actively remove nuclear-powered facilities from the realm of potential cyber-attack targets on humanitarian grounds.** However, both the United States and Israel are unlikely to want international norms to develop in this direction at this point in time, particular in light of the use of Stuxnet in Iranian nuclear faculties.

[11] http://www.inss.org.il/index.aspx?id=4538&articleid=7091

[12] http://www.fireeye.com/resources/pdfs/fireeye-operation-saffron-rose.pdf

[13] http://www.fireeye.com/blog/technical/2014/05/strategic-analysis-as-russia-ukraine-conflict-continues-malware-activity-rises.html

Intelligence, surveillance and reconnaissance

United Kingdom's signals intelligence agency forced to reveal its policy on mass surveillance

The United Kingdom's Government Communications Headquarters (GCHQ) has been forced to reveal its policy on mass surveillance. A coalition of NGOs obtained details of GCHQ's policy on surveillance and communication interception.[14] Importantly and controversially, the policy defines all communications via social media networking sites and search engines outside of the United Kingdom as 'external communication' because the servers are based outside Britain, usually in the United States.

The distinction between internal and external communications in surveillance laws is that internal communications can only be intercepted with a specific warrant, which is not the case for external communications. The implication is that a surveillance standard for foreign communications can be applied in a domestic context, enabling a form of mass surveillance.

The public release of the policy comes at a time when it has just been revealed that GCHQ has three secret bases in northern Oman that covertly tap undersea cables passing through the Strait of Hormuz into the Persian/Arabian Gulf. The tapping is achieved with the assistance of British telecommunication companies BT and Vodafone Cable. While the GCHQ interception of overseas external communications can be authorised, it cannot be authorised to store all communication for examination under the Regulation of Investigatory Powers Act (RIPA). This means that the storage of communications coming from Oman may have been unauthorised because the full audio recordings were archived. Since 2009, a number of interception authorisations have been granted to allow GCHQ to collect information about the political intentions of foreign powers, terrorism, proliferation, mercenaries and private military companies, and serious financial fraud. It is likely that GCHQ argued to the relevant minister that the tapping of undersea cables was for these purposes.

Adding to the public concern over domestic surveillance by GCHQ and its replication of NSA interception activity was Washington's announcement in mid-May that it will spend £189 million on expanding RAF Croughton, a US Air Force (USAF) base near Milton Keynes. The base upgrade is highly likely linked to the current US focus on improving ISR capability in northern Africa. The USAF indicated that the base would have both US and UK personnel and be the principal intelligence centre for the US Africa Command (AFRICOM).

A number of prominent British politicians have expressed concern over GCHQ surveillance activities; however, any potential reforms are unlikely to go too far beyond the equivalent reform of the USA Freedom Act due to the high level of ISR interdependency and shared network infrastructure between Britain and the United States.

[14] https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/witness_st_of_charles_blandford_farr.pdf

Other developments

Seventeen NATO states, three partner countries and the US Army and Air Force participated in joint ISR field trials at Orland Air Station in Norway between 19 and 28 May. Unified Vision (UV14) is the largest ever ISR trial held by NATO, with more than 200 participants operating across aerial, ground and maritime environments. The trial focused on interoperability and fusion of all-source intelligence, including ground systems for collecting and exploiting ISR data (unattended ground sensors capable of collecting seismic or acoustic data), electronic warfare units, aerostats and signals intelligence systems. The trial's focus on interoperability and fusion is likely to be a result of gaps in NATO intelligence-sharing abilities highlighted in the Libyan theatre and Afghanistan missions and during the current Russia-Ukraine tensions and the potential for broader regional insecurity. Lessons learnt from the trial will be incorporated into NATO's Response Force 2016 concept.

NSA whistleblower Edward Snowden has released documents on the NSA's SOMALGET, a sub-programme of MYSTIC that is accessing and storing for 30 days audio from personal phone calls made in the Bahamas and Afghanistan. This extends far beyond the meta-data already known to have been captured from Mexico, Philippines and Kenya under the MYSTIC programme. The signals intelligence collection overreach by the NSA may restrict the US administration's long-term intelligence gathering capacity, as it is possible the Bahamas and other countries, particularly those in Central and South America, will reduce cooperation with Drug Enforcement Administration (DEA) requests for lawful intercepts. The use of DEA lawful intercept requests was the mechanism through which SOMALGET was implemented.

The US House Science and Technology Committee adopted an amendment from Florida Democrat Alan Grayson to remove the mandatory requirement for the National Institute of Standards and Technology (NIST) to consult with the NSA when developing security standards. The amendment comes after leaked NSA documents had revealed the NSA had a $250 million programme, SIGINT Enabling, with the purpose of covertly undermining encryption standards developed by NIST by using influence in the peer review process. NIST is currently reviewing all cryptographic standards and peer review procedures. While the committee's endorsement of the amendment indicates a level of bipartisan agreement, it is not clear how likely the amendment is to get through the House of Representatives and Senate. Concerns around cryptography and NSA capabilities to exploit vulnerabilities have been highlighted in the aftermath of the heart bleed bug, the recent developer withdrawal from maintaining freeware encryption tool TrueCrypt, and the decryption of new generation encryption tools within two hours by École polytechnique fédérale de Lausann (EPFL) researchers.

Also of note

- **Bundesnachrichtendienst (BND), the German foreign intelligence service, is planning real time monitoring of social media networks to bring the service up to speed with the United States' NSA and Britain's GCHQ.** The proposal, which will require parliamentary support and is part of a broader €300 million strategic technical initiative, also includes a biometric security-system evasion programme.

- **An increasing number of US ICT companies are urging the US administration to rein in NSA activities.** CISCO's CEO indicated serious concern over the NSA interception and tampering of CISCO exports for surveillance purposes. A coalition of US tech companies, including Google, Facebook, Microsoft, AOL, Apple, Twitter, LinkedIn, DropBox and Yahoo, have also criticised the USA Freedom Act and urged the senate to include stronger restrictions on NSA surveillance activities. House Intelligence Committee Chairman Mike Rogers accused the companies of putting business profits from European markets ahead of US national security.
- **Legislation to limit mass surveillance activities by the NSA, the USA Freedom Act, passed the House of Representatives by a margin of nearly three to one,** but is currently with a divided Senate Intelligence Committee. The committee is hearing conflicting concerns that the bill encumbers the NSA's ability to secure national security and that the compromise bill lacks sufficient teeth to meaningfully limit NSA activities.
- **Leaked NSA documents from 2011 shine light on the extent of NSA and state department harvesting and storage of facial images from the internet – up to 55,000 facial-recognition quality images per day.** The Department of Homeland Security is funding a pilot project to use the state department's database of photographs to match faces in a crowd.
- **US companies Total Military Management (TMM) and Raytheon announced a joint ISR research venture focused on video compression technology.** The research project is the result of strong demand from ISR communities for the next generation in video compression technology to store and archive large volumes of video footage.
- **Legal tensions between domestic and foreign Canadian intelligence collection agencies was recently revealed** after intelligence officials requested oversight institutions stop talking to each other about Canadian Security Intelligence Service (CSIS) and Communications Security Establishment Canada (CSEC) surveillance techniques. The collaboration between oversight committees underscores the increasing overlap between domestic and foreign surveillance.
- **The Supreme Court of Canada handed down a decision in June ruling that police must obtain search warrants to obtain basic subscriber information** such as a customer's name, address and phone number from telecommunication companies. The court's decision has immediate ramifications for two bills, C-13 on cyber bullying and S-4 on digital privacy, currently before the House of Commons.

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 produce actionable and predictive intelligence on defence, security and foreign policy matters. We tell you what has happened and what is likely to happen next. Most importantly, we tell you why.

We do this so that better informed citizens can more effectively engage in peace and security debates and civil society organisations can make the right advocacy choices. Together, we can influence positive policy decisions by our governments.

Open Briefing is a bold and ambitious not-for-profit social enterprise. We are a unique collaboration of intelligence, military, law enforcement and government professionals from around the world.

Challenge the status quo. Take intelligence into your own hands.

www.openbriefing.org