Remote-control warfare briefing | #01

24 April 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 special forces deployed to Uganda to assist in tracking down the LRA.

Private military and security companies: Kiev accused of hiring US private military company to supress pro-Russian dissent in Eastern Ukraine.

Unmanned vehicles and autonomous weapons systems: UK House of Commons defence committee concludes UAVs are a key military capability for the future.

Cyber warfare: US defence secretary highlights US cyber capabilities with PLA commanders during China visit.

Intelligence, surveillance and reconnaissance: New Israeli intelligence-gathering and surveillance system demonstrated during Brazilian carnival.

Special operations forces

US special forces deployed to Uganda to assist in tracking down the LRA

The US government has deployed an increased number of US special forces to Uganda to assist the African Union's (AU) Regional Task Force in tracking down the Lord's Resistance Army (LRA) and their leader, Joseph Kony. Announced in late March, the deployment includes four CV-22B Osprey tiltrotor aircraft, two MC-130P Hercules transport aircraft and a single KC-135R Stratotanker refuelling aircraft, together with 150 US Air Force special operations forces (SOF) personnel.

Although combat equipped, US forces are only authorised to engage the LRA in self-defence, in line with the rules of engagement for Operation Observant Compass, the US deployment to Uganda and other countries in Central Africa to counter the LRA. US Air Force SOFs will be providing information and assistance to enable quicker AU troop transport upon receipt of intelligence on Kony's position. The deployment builds upon the SOF and private contractor intelligence, surveillance and reconnaissance (ISR) support previous provided under Operation Tusker Sand.

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

Open Briefing Ltd is a non-profit company limited by guarantee.
Registered in England & Wales, No. 07649656.

The deployment is interesting for a number of reasons. The LRA's relative strength and frequency of armed operations have been generally diminishing, despite sporadic spikes in the Central Africa Republic (CAR) recently. Furthermore, the improved intelligence on Kony's position is a direct result of increased defections from the LRA, with an estimated 20% of core fighters leaving the group in 2013. It is therefore difficult to argue the US deployment is responding to a tangible, increased threat from the LRA, though it is possibly capitalising on an improved opportunity to capture Kony. The LRA has also never represented a direct threat to US national interests.

The US deployment could have been influenced by significant regional instability in CAR and South Sudan. LRA actions in these two countries would likely aggravate existing conflict and political turmoil, with CAR particularly vulnerable. The deployment is also a relatively inexpensive measure to demonstrate government commitment to a cause that is popular within the United States.

Alternatively, the Obama administration is using this operation to more effectively manage the public perceptions and diplomatic challenges of an alleged broadening of the US special operations footprint across Central, North and East Africa. Historically, less attention has been paid to the US SOF presence in Africa than operations in Iraq and Afghanistan. Assistance to AU forces detracts from the suggestion that US counterterrorism efforts are solely focused on confronting al-Qaeda on multiple fronts, across multiple continents. It could also serve to normalise the concept of expanded SOF deployment across conflict hotspots in North, Central and West Africa.

Other developments

Russian special operations Spetsnaz commandoes appear to have played an important role in Russia's occupation of Crimea. Unconfirmed reports suggest that several hundred members of the GRU 45th Guards Spetsnaz Regiment went into Crimea without insignia and helped garner enough support for a supposed civilian-led popular uprising though active measures and targeted provocations. Russia used similar tactics in the Republic of Georgia following the country's 2005 Rose Revolution. Military analysts have characterised Russian President Vladimir Putin's strategy in Crimea as something closer to paramilitary covert action than wholesale military attack.

US Department of Defence testimony before the House Armed Services Committee in early April has strongly endorsed the global SOF network plan of Admiral William McRaven, Commander, US Special Operations Command (USSOCOM). The evidence presented before the committee reinforced the strategic and tactical positioning of US SOF laid out in the 2014 Quadrennial Defence Review (QDR), which focused on the networked capabilities of SOF. The QDR highlights the role of SOF following the troop drawdown in Afghanistan and for counterterrorism in the Maghreb, Sahel and Horn of Africa.

US special forces seized a stolen commercial oil tanker, Morning Glory, that fled from a Libyan port controlled by anti-government rebels. The attempted theft of 234,000 barrels of crude oil valued at $35 million underscores the limited capacity of the Libyan government to manage a fragile political and security environment in which militias who ousted Muammar Gaddafi refuse to disarm. USSOCOM announced that they would begin training conventional Libyan forces shortly.

Also of note

- **US Special Operations Command have put a contract out for location intelligence and advanced human-geography geographic information system (GIS) data** for countries of interest for which there is no existing data. The countries include Jordan, Djibouti, Myanmar, Honduras, Iran, Morocco, Nigeria, Trinidad & Tobago, Burkina Faso, South Sudan, North Korea and China (Guangdong Province).
- **The *Washington Post* has reported on details of the FBI's involvement in SOF counterterrorism operations in Iraq.** Evidence has come to light that agents from the FBI's Hostage and Rescue Team were embedded with US Army Rangers during 2006 and that SOF have benefited from the FBI's digital surveillance capabilities.
- **NATO allied and partner SOF commanders met in Bucharest, Romania,** on 19 March to exchange of ideas and identify solutions to current geopolitical issues.
- **At the end of March, Iran's Islamic Revolutionary Guards Corps (IRGC) were gearing up to conduct a search and rescue operation in Pakistan** for five border guards abducted in February by the militant group Jaish ul-Adl.

Private military and security companies

Kiev accused of hiring US private military company to supress pro-Russian dissent in Eastern Ukraine

The Russian foreign ministry and the Information Telegraph Agency of Russia (ITAR-TASS) have accused Kiev of hiring US private military and security company (PMSC) Greystone, Ltd to suppress pro-Russian activists in Eastern Ukraine. The former Blackwater affiliate has had security contracts in Russia and Central Asia but has denied plans to deploy any personnel to Ukraine.

Although disputed by Kiev, the ensuing rumour and innuendo is a sign that the Kremlin is trying to take the moral high ground on security and military deployment. The rumour is likely to be marshalled by pro-Russian separatists as evidence that Ukrainian nationalism and Kiev's key domestic political supporters are pro-US, pro-NATO and pro-EU rather than patriots.

The rumour around PMSCs in Ukraine is mostly likely a counter to claims of Russian special operation forces coordinating pro-Russian militias and political groups to secure both Crimea and Eastern Ukraine. It is unlikely in the current environment that Kiev would secure 150 private military contractors disguised as members of an elite Ukrainian army unit to suppress pro-Russian protestors when the Ukrainian army is playing a clear overt role in Eastern Ukraine.

Other developments

PMSCs are likely to fill potential security gaps in Afghanistan if the US government and NATO cannot finalise bilateral security agreements (BSA) with a newly-elected Afghan president. If the planned drawdown of troops starts in early 2015, existing diplomatic missions, civil reconstruction efforts and aid initiatives will most likely need to rely upon PMSCs to support continued work in Afghanistan's fragile security environment. In this scenario, PMSCs are likely to operate under the auspices of Western agencies remaining in Afghanistan to deliver engineering projects, governance assistance and aid programmes.

A report by the Global Policy Forum and Rosa Luxemburg Stiftung published in February examined UN procurement and use of PMSCs in 2011-13. The report, *Contracting Insecurity: Private military and security companies and the future of the United Nations*, argues that UN is increasingly relying on private military and security companies for its peacekeeping and political missions, as well as for its humanitarian and development activities. The report states that in addition to armed and unarmed private security personnel, the UN uses PMSCs for logistical support, risk assessment and security training, among other services.

Also of note

- **The UN Working Group on the use of mercenaries concluded its 21st session in early March.** The working group is expected to submit a report on UN policy regarding the use of PMSCs to the General Assembly later this year.
- **Evidence likely to be offered in the upcoming trial of Blackwater private contractors shows deep hostility from several guards toward the Iraqi civilian population.** Blackwater contractors are alleged to have killed 14 Iraqis and wounded at least 18 others in Nisour Square, Baghdad, on 16 September 2007.
- **The April 2014 edition of *Vanity Fair* features an in-depth profile of British security services company G4S** and their ordnance-disposal work in South Sudan.

Unmanned vehicles and autonomous weapon systems

UK House of Commons defence committee concludes UAVs are a key military capability for the future

A report from the UK House of Commons Defence Committee, *Remote Control: Remotely Piloted Air Systems – current and future UK use*, has concluded that unmanned aerial vehicles (UAVs) are a key military capability for the future. However, the committee also recommended that the British Ministry of Defence (MoD) publish details about any incident involving civilian casualties and any lessons learned from review processes in order to address public concerns over the use of UAVs.

The committee acknowledged that the provision of intelligence, surveillance and reconnaissance from Remotely Piloted Air Systems (RPAS, the descriptor now used by the UK Royal Air Force and others) has been of strategic importance in improving the effectiveness of military operations in Iraq and Afghanistan. The committee suggests that British use of UAVs is consistent with rules of engagements and international law, and noted that the MoD has systems in place to review weapon discharge.

Despite these safeguards, the committee has recommended that the MoD publish details of incidents involving civilian casualties and any lessons learned from reviews that would not compromise operations. The committee recommended that the MoD also publish an updated Joint Doctrine Note setting out its current approach UAVs no later than September 2014. The committee also recommended that the British government plays an active role in defining any future regulation or legal framework around the use of UAVs.

The committee also considered research and development partnerships, training and strategic procurement for UAVs, in particular the MQ-9 Reaper used by the RAF. There appears to be a number of strategic bilateral and multilateral partnership opportunities for the UK MoD, which include the existing partnership arrangements with the US Air Force or greater European collaborative efforts, such as an Anglo-French aerospace defence programme. The committee's comments on research and development partnerships come in the aftermath of Prime Minister David Cameron signing a £120 million, 24-month feasibility study into a Future Combat Air System in January. The agreement builds upon a study by BAE Systems and Dassault looking at the potential for a joint unmanned combat air vehicle (UCAV) programme. Increasing Anglo-French partnerships will mean greater interoperability for UAV operations between the two countries.

Other developments

Israel is increasingly concerned about Hezbollah's capacity and procurement of drone technology and the potential for the Arab-Israeli conflict to shift to a weaponised remote-control war, according to a 26 March article in *New Republic*. The article suggests that Tehran has provided Hezbollah with drone technology, which has been used to penetrate Israeli airspace on a number of occasions. Israel has the clear technical advantage as the world's largest UAV exporter – selling more than $4.6 billion worth of drones and support systems to foreign governments between 2005 and 2012. However, cruder UCAV technology employed by Hezbollah could still be devastating.

The UN Human Rights Committee criticised US drone strikes in a March report on compliance with the International Covenant on Civil and Political Rights. The committee commented that the US justifications for lethal drone strikes are too broad and that precautionary measures adopted to avoid civilian deaths are unclear. The committee recommended that drone strikes should be subject to independent oversight. A report released on 10 March by the UN Special Rapporteur on Human Rights on civilian deaths resulting from drone strikes also strongly criticised US UCAV 'targeted killing' campaigns in Pakistan, Yemen and Afghanistan. The report found that in 2013, drone attacks resulted in 45 civilian fatalities and 14 non-fatal injuries, a threefold increase from 2012 civilian fatalities. It is thought that Pakistan is trying to build on the special rapporteur's report and secure a resolution through the UN Human Rights Council triggering greater scrutiny of US drone strikes compliance with international human rights law.

Australia is planning to acquire Northrop Grumman MQ-4C Triton surveillance UAVs once the US Navy development programme has been completed. According to Prime Minister Tony Abbott, the acquisition should provide the country with unprecedented maritime surveillance capabilities. These capabilities are understood to be important to the Australian government's ability to monitor the movement of asylum seekers, energy infrastructure in the Indian Ocean and sea-lanes of communication. There is the option for the Triton to be weaponised.

Also of note

- **The British think tank Chatham House held a major conference on autonomous military technologies in London** in February. The Taranis demonstrator UAV manufactured by conference sponsor BAE Systems was discussed as an example of precursor technology to fully-autonomous weapons systems.
- **The South Korean military claim to have found two downed rudimentary drones allegedly used by North Korea for surveillance.** The drones only had still image capture capacity, which could not be remotely transmitted to the operator.
- **Russian forces may have intercepted a US surveillance UAV flying over Crimea** by hacking the connection between the UAV and its operator.
- **The International Committee of the Red Cross (ICRC) convened its first experts meeting on autonomous weapons systems** on 26-28 March.
- **The British Ministry of Defence and BAE Systems recently revealed that its stealth semi-autonomous demonstrator UCAV, Taranis, carried out a successful maiden test flight** at the Woomera test range in South Australia in August 2013.
- **Algeria has reportedly been in discussions with the Chinese military for the procurement of Xianglong (Soaring Dragon) UAVs** after successful tests in southern Algeria last year.

Cyber warfare

US defence secretary highlights US cyber capabilities with PLA commanders during China visit

US Defence Secretary Chuck Hagel used a visit to China in early April to broach the topic of cyber attacks and capabilities with People's Liberation Army senior commanders. The stated aim of this diplomatic candour on US cyber capabilities and emerging cyber doctrines is to ensure both powers have clear understandings of cyber 'red lines', similar to Cold-War era exchanges between Americans and Soviets over nuclear intentions. US concerns over China's state-controlled and state-condoned cyber activity are highly likely to be primarily focused on commercial espionage and intellectual-property theft as Hagel indicated. Numerous US energy, bio-technology and military companies have been victims of extensive cyber espionage.

Before his visit to China, the defence secretary had already talked up the United States' open approach to cyber warfare capabilities at the retirement ceremony of former NSA director General Keith Alexander. Hagel argued that the US had a restrained approach to cyber offensives, despite the Pentagon's increased spending on cyber operations and with efforts to have a 6,000 strong force by 2016 making US Cyber Command (USCYBERCOM) one of the largest cyber forces in the world. The Pentagon plans to spend $26 billion on cyber technology over the next five years, which together with drones and SOF makes it one of the only military programmes to receive funding increases during a period of relative austerity in military spending.

At a recent confirmation hearing, Vice Admiral Mike Rogers, Alexander's replacement as commander of USCYBERCOM and director of the NSA, stated that US military posture in cyberspace has been reactive, rather that proactive. However, leaks from Edward Snowden about NSA activities would suggest that US cyber activity is not solely defensive. This includes US spying on Brazil's Petrobras and the NSA's Operation Shotgiant, which infiltrated Huawei's servers and stole source code for specific Huawei products.

If cyber activity gives access, then it equally gives capacity to harm and control. From this perspective, and in the context of disclosures on NSA activities, some commentators indicate that it may be in US interests as a dominant cyber power to engage in norm setting around cyber-warfare activities. Others suggest that there is little strategic incentive for less-developed cyber powers, such as China, to disclose their capabilities at this point in time.

Other developments

Cyber confrontations over Russia's annexation of Crimea have led some commentators to highlight the cyber-warfare component of the current conflict between Russia and Ukraine. However, the extent of cyber offensives, their role in the broader conflict and which cyber actors are actually involved is subject to considerable debate. In mid-March, several NATO websites were targeted with distributed denial-of-service (DDoS) attacks by pro-Russian hacktivist group Cyber Berkut. In addition to the multitude of DDoS attacks, both sides and their various proxies are also using malware, including a program called Snake, to conduct cyber espionage. However, some commentators have questioned whether Russia will launch a full-scale cyberwar on Ukraine, suggesting it is unlikely that such action would be in Putin's interest and that subtlety is the order of the day in the cyber stakes.

A number of separate reports have raised concerns over Iranian cyber attacks and Iran's improving cyber capabilities. The Institute for National Security Studies points to Iran's modernised defensive capabilities applied to manage domestic unrest and high-quality cyber attacks against more militarily-advanced adversaries. Iranian and Russian collaboration on cyber-attack capacity is expected to amplify Iran as a cyber threat. Reports of consistent cyber attacks on US and Israeli banks in the period leading up to negotiations on Iran's nuclear programme indicate that cyber attacks are becoming an important ancillary mechanism to pressure and influence negotiations. Iran is also rumoured to be considering pursuing legal action against the United States for the US-Israel Stuxnet cyber attack. Legal action under a number of international instruments could force a more consistent dialogue on the boundaries of cyber operations.

The Australian Strategic Policy Institute (ASPI) released the *Cyber Maturity in the Asia-Pacific Region 2014* report on 14 April. Applying cyber-maturity benchmarks and indicators the report found that the United States is the most cyber-mature country. The cyber-maturity benchmarks are based on evaluation of whole-of-government policy and legislative structures, military organisation, business and digital economic strength and levels of cyber social awareness.

Also of note

- **Syrian Electronic Army (SEA) announced they accessed the network of US Central Command (CENTCOM)** and obtained hundreds of military documents. The attack was allegedly in retaliation for President Barack Obama's announcement that the United States targets Syria with electronic warfare. Sources suggest that the breach only appears to have obtained unclassified information.

- **China and the EU have agreed to work more closely on cybersecurity issues** by bolstering groups such as the China-EU Cyber Taskforce.
- **British Cabinet Office Minister Francis Maude launched the UK's Computer Emergency Response Team** (CERT-UK) to deal with cybersecurity incidents of national significance. Meanwhile, the Labour Party has called for a reporting regime for cyber attacks on private company that threaten critical national infrastructure.
- **The Intelligence and National Security Alliance published a white paper** in March suggesting that US agencies need to focus less on cyber-offensive tactics and examine broader goals and perspective on cyber attacks to properly allocate resources and counter assaults.
- **The FBI has put cyber crime and terrorism second only to counterterrorism and counter-intelligence** in its priority list.
- **North Korea's cyber-attack capabilities and activities against South Korea were outlined to US Congress in early March.** North Korea's primary cyber objectives have reportedly been to gather intelligence and seek disruption of networks in highly-wired South Korea.
- **On 21 March, the *Washington Examiner* interviewed Peter W. Singer,** a Brookings Institution scholar and co-author of *Cybersecurity and cyberwar: What everyone needs to know*, about key domestic cyber-warfare issues**.**
- **Israel experienced an increase in cyber attacks coinciding with the Anonymous operation #OpIsraelBirthday on 7 April,** led by members of AnonGhost.

Intelligence, surveillance and reconnaissance

New Israeli intelligence-gathering and surveillance system demonstrated during Brazilian carnival

A new intelligence-gathering and surveillance system from Israel's Elbit Systems was recently demonstrated during the carnival in Sao Salvador da Bahia, Brazil. The system is comprised of the land-based GroundEye and the aerial SkEye, which generate simultaneous streams of high-resolution video, alerting users to the presence of pre-programmed targets of interest. While very little information is available, an Israeli military officer described the system as 'high-quality soda straws of surveillance imagery with "a type of cognitive capability…that significantly enhances the [capabilities of] young female observers we count on to monitor our borders.'

SkEye was first used by the Israeli Defence Force in the November 2012 Pillar of Defence operation in Gaza. SkEye has now been integrated into Israel's digital command-and-control network for surveillance and control of the country's northern borders. The surveillance system allows operators in command centres miles away from where the pod is deployed to monitor multiple events across very large areas.

SkEye had previously been demonstrated a Paris Air Show last year with a demonstration model of the system mounted to a Hermes 900 UAV. SkEye is capable of monitoring an area of up to 100 square kilometres and provides multiple camera apertures, which can be used to provide spherical coverage. SkEye differs from current video surveillance systems in that it enables several simultaneous users to independently probe any region of interest anywhere in the entire sector. GroundEye is based on technology developed for the airborne SkEye.

Advances in multi-channel and multi-operator surveillance technology are essentially starting to emulate techniques used to review footage in the aftermath of the 2013 Boston marathon bombings. It enables simultaneous scanning and surveillance of multiple points of interest. When used in the context of UAV operations, SkEye will provide greater vision to see incoming threats.

Other developments

Two Five Eyes countries are contending with debates about the collection and disclosure of personal telecommunications metadata in the aftermath of NSA leaks. An Australian Constitutional Affairs Committee inquiry on telecommunication data storage and interception has showed a number of agencies collecting personal telecommunications information without a warrant. Canada is also facing an emerging debate about collection, storage and access to personal telecommunications metadata.

The *Washington Post* revealed in late March that the NSA has created a surveillance system, MYSTIC and RETRO, that records 100% of foreign country phone calls and stores audio recordings on a monthly rolling basis. Alongside PRISM and increases in funding to US Cyber Command, the United States is maintaining a large intelligence, surveillance and reconnaissance budget, as pointed out by the Cato Institute in a 21 March 'federal spying budget' breakdown and by the chair of the US House Armed Services Committee.

Turkey's Prime Minister Recep Tayyip Erdoğan has set a clear agenda to empower the Turkish intelligence service, the National Intelligence Organisation (MIT), through a draft bill that would give the service full access to all private data and bank transactions. This comes after Erdoğan recently made moves to ban social media sites, such as Twitter, as part of a campaign to squash rumours of government corruption.

Also of note

- **On 8 April, the UK Interception of Communications Commissioner reported that British intelligence agencies do not engage in random mass surveillance.** However, authorisation and notices of communication data requests totalled 514,608 in 2013.
- **Google has adopted encrypted HTTPS connection as the default for its Gmail service.** Disclosures about the NSA's PRISM data-mining project indicated that email messages moving between Google's internal servers and data centres were potentially exposed to surveillance.
- **Psychological warfare officials from South Korea's cyber command are being investigated** for posting over 30,000 political postings attacking opposition politicians in the lead up to the 2012 presidential election.
- **BAE Systems are expected to receive a total of £30 million from the UK Ministry of Defence for projects to explore ways for the military to use social media** and psychological techniques to influence people's beliefs.
- **The search for missing Malaysia Airlines flight MH370 has highlighted the lack of co-ordination between ASEAN member states on sharing intelligence** and the lack of confidence and trust across the region in terms of sharing intelligence capabilities.

- **US reliance on and preference for high-resolution satellites and UAVs for imagining and reconnaissance is leading to a neglect in space-based radar satellites upgrades** and development according to an article in *Quartz* on the challenges in locating flight MH370.
- **Further information has come to light on the NSA's encouragement and support for tech-security company RSA to make a now-discredited cryptography system used by a wide range of companies and services.** Leaked NSA documents suggest that RSA adopted two encryption tools developed by the NSA, allowing the agency to eavesdrop on some internet communications.

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