Remote-control warfare briefing | #02

27 May 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: United States renews lease of Djibouti base important for counterterrorism and drone strike operations.

Private military and security companies: Majority of US State Department funding for Afghanistan went to single private contractor with chequered record.

Unmanned vehicles and autonomous weapons systems: New reports spur debate over drone research, export and proliferation.

Cyber warfare: United States more cognizant of vulnerability to cyber counter-strikes.

Intelligence, surveillance and reconnaissance: NSA allegedly hardwired backdoor access tools into intercepted exported US routers.

Special operations forces

United States renews lease of Djibouti base important for counterterrorism and drone strike operations

The United States has renewed the lease of the only official US military base in Africa: Camp Lemonnier in Djibouti. Camp Lemonnier is a US Naval Expeditionary Base located at Djibouti's international airport. It is home to the Combined Joint Task Force – Horn of Africa (CJTF-HOA) of the US Africa Command (USAFRICOM). Elements of the US Special Operations Command (USSOCOM), including from the Joint Special Operations Command (JSOC), are also based there. The new lease agreement was announced by President Barack Obama and his Djibouti counterpart, Ismail Omar Guelleh, in early May. The lease fees have increased from $38 million to $63 million (plus $7 million in development aid) for a 10-year lease, with the option to extend the arrangement for another decade. The new lease agreement will also most likely include military technology transfer to the Djibouti armed forces.

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 base is an important staging ground for drone strikes and special operations forces (SOF) missions against al-Qaeda in the Arabian Peninsula (AQAP) militants in Yemen and al-Shabaab forces in Somalia. It is also essential for anti-piracy measures. It is the single most important military platform for the projection of US regional foreign policy across the Sahel, Horn of Africa and North Africa. The Pentagon has already invested over $500 million in construction projects in and around the base, and further spending programmes totalling $1 billion are planned for base upgrades.

The Pentagon have created a 150-member rapid response force at Camp Lemonnier, which has the capacity to respond to attacks on US interests in the region, such as the 2012 attack on the US diplomatic mission in Benghazi, Libya, or threats to the US embassy in Juba, South Sudan, in late 2013. These units tend to respond to high profile incidents that underscore a US presence. The new lease agreement gives certainty and support to US SOF counterterrorism activities and the development of regional SOF partnerships in Uganda, Ethiopia, Mali and Kenya. It is also an important base of operations for US interventions or support in conflicts in South Sudan or the Central African Republic. From a French perspective, the renewal would be positive news for any ongoing joint US-French activity, as France has an adjoining base and has been building up a SOF presence in Djibouti since 2006 to ensure capacity for a rapid response to conflict in Eritrea and Somalia. The renewed lease can also be interpreted as a snub to Russia, who has been making overtures to Djibouti seeking secure landing rights and a small parcel of land.

With increased US investment in the Djibouti base and growing demand for SOF training from Sub-Saharan governments, it is becoming harder for the US administration to downplay the US military footprint in Africa. For example, the international focus on the kidnapping activities of Boko Haram is making it more difficult to conceal the commitment of US National Guard personnel and SOF in training Nigerian Ranger battalions for counter-insurgency against the militant group. The need for deeper partnerships in Africa is not necessarily conducive to the US policy of downplaying SOF footprints across the continent. If the concept of building partner capacity and trust for US special force deployment is accepted, then the US administration may need to acclimatise to a more visible US footprint in Africa.

Other developments

The tenth Special Operations Forces Exhibition and Conference (SOFEX) was held in Jordan from 5 to 8 May. SOFEX is a biennial conference where SOF from around the globe discuss emerging security threats, training and technology. More than 600 figures from 52 countries and 371 defence companies from 41 countries took part in the conference. The Middle East Special Operations Commanders Conference was held alongside SOFEX 2014. A number of conference attendees were publically quoted highlighting the importance of greater SOF regional partnerships and the need for increased joint procurement of security infrastructure to protect national sovereignty.

The US House Armed Services Committee wants more information and greater oversight on the USSOCOM's Tactical Assault Light Operators Suit (TALOS) effort. USSOCOM is proposing to allocate $80 million to the TALOS programme, which is colloquially referred to as the new 'Iron Man' suit. The committee and defence industry specialists have concerns over potential cost blowouts inherent in delivering the technology. There are also concerns over whether the suit would have broad battle scenario applicability and utility or whether it would only be used on a limited set of operational scenarios, such as raids.

A US congressional research paper indicates that German defence contractor Rheinmetall built a $140 million military combat training centre in Russia to train SOF personnel.[1] Parts of Congress and the US intelligence community are suggesting that engagement and defence trade between NATO partners and Russia – particularly France, Italy and Germany – has provided Russian GRU Spetznaz with greatly modernised capabilities and tactical advantage over Ukrainian forces. Updated Russian military doctrines and the concurrent use of cyber warfare and special operation forces have been facilitated in part by NATO country defence contracts signed between 2003 and 2013. Having noted significant expansion in Russian special forces capabilities, the US administration has recently announced greater bilateral collaboration between US and Polish special forces and new training exercises with Estonia (Exercise Spring Storm), Latvia and Lithuania (Exercise Flaming Sword).

Also of note

- **Public Intelligence has released a restricted US Army guide to biometrics in Afghanistan.**[2] The guide outlines the use of biometric data collection by special operation forces and provides some insight into the US military's strategy of identity dominance.
- **US SOF are shifting their strategic posture to the Pacific** and regions where al-Qaeda affiliates are seeking safe haven after the Afghanistan war. This is in line with the broader US military pivot towards the Pacific and East Asia; however, US SOF representatives point out that US Pacific Command (USPACOM) has historically had a significant presence in the region.
- **The United States are providing active training and mission support to Iraqi SOF** in operations against fighters of the al-Qaeda-affiliated Islamic State of Iraq and the Levant.
- **Canadian Special Operations Forces Command is set to receive $60 million** to procure marginal terrain armoured vehicles for use in the Arctic.
- **The British government has agreed to keep 100 SAS troopers in Afghanistan** when British troops are withdrawn later this year, though they will not take part directly in counterterrorist operations.
- **French company Vaylon showcased work on a combination hang glider-dune buggy for French special forces at SOFEX 2014.** The light all-terrain vehicle prototype is designed to take off and fly in powered flight and paraglide modes. The development of the prototypes comes after French SOF indicated the need for a stealthier mode of air transport.
- **The US Defence Advanced Research Projects Agency (DARPA) are funding Logos Technologies to develop a hybrid powered motorbike** to assist special forces to penetrate remote areas and stealthily execute rapid raids in extreme terrain conditions and contested environments.
- **Australia's Special Operations Command (SOCOMD) capabilities and priorities post Afghanistan are under the microscope,** as the government has to make broader defence procurement decisions that may leave SOCOMD with a reduced budget.

[1] http://www.scribd.com/doc/219528494/CRS-AlliedMilSalesRussia-4-26-12-3

[2] https://publicintelligence.net/call-afghan-biometrics/

Private military and security companies

Majority of US State Department funding for Afghanistan went to single private contractor with chequered record

The US Department of State spent $4 billion on Afghan reconstruction projects from 2002 to March 2013. In April, a report by the Special Inspector General for Afghanistan (SIGAR), an auditing agency created by the US Congress to provide oversight on government spending in Afghanistan, revealed that $2.7 billion, or 69%, of that money went to a single private military contractor: DynCorp.[3] While the report does not criticise the Virginia-based contractor for any of its activities, DynCorp has a history of corruption scandals and a questionable performance record, particularly in Iraq and Afghanistan.

The main purpose for which DynCorp was awarded $2.7 billion in government contracts during that 11-year war period was 'police development'. According to the SIGAR report, that amount far exceeds that awarded to any State Department-contracted company. PAE Government Services Incorporated received $597.8 million from the State Department, placing it in second place, though this represents about a quarter of what DynCorp was awarded. The third company on the list received only one-tenth of the amount DynCorp received. This raises questions regarding the biding process through which the State Department awards its contracts, whether competing companies are seriously considered and how DynCorp's activities are monitored and evaluated.

The State Department's continued trust in DynCorp may come as a surprise considering the company's chequered record. A previous 2007 SIGAR report found that DynCorp seemed to have acted independently of its reporting officers at the State Department and had conducted unauthorised activities for which it billed the US government. In 2011, Wikileaks revealed through a diplomatic cable that DynCorp contractors had hired an underage Afghan boy to entertain them. More recently, in 2013 DynCorp was criticised for its substandard work on an Afghan National Army construction project in Kunduz province, which ended in a settlement with the US government. As the United States and international forces prepare to drawdown their military presence in Afghanistan, John Sopko, head of SIGAR has pledged to carefully examine how money has been spent in the country over the years. His reports have so far identified several cases of cost overruns, unquestioned subpar performance, and clear cases of corruption.

Dyncorp's questionable performance and accountability do not seem to have affected its ability to obtain new government contracts over the years. In July 2009, Forbes found that 53% of DynCorp's $3.1 billion of annual revenue was generated by the wars in Iraq and Afghanistan, making the company one of the big 'winners' of those military endeavours. Dyncorp's overwhelming presence in Afghanistan raises questions regarding the revolving door and the detrimental relationship existing between the US government and private military contractors. DynCorp's board of directors includes several retired generals and commanders from the US Marine Corps and the US Army.

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

Other developments

Rumours surrounding Kiev's hiring of foreign private military contractors in Ukraine continue. Unconfirmed media reports, primarily from Russian news outlets, have reported that foreign private military personnel had allegedly participated in Kiev-sponsored operations to maintain law and order in light of recent unrest in the eastern Ukraine town of Slavyansk. US private security firm Greystone, Ltd, formerly an affiliate of Blackwater/Xe Services (now Academi), was reported to have about 400 commandos on the ground. However, the presence of foreign mercenaries in Ukraine, their exact number, mandate and funders remain highly uncertain, and is possibly part of Russian information activities. Nonetheless, it is increasingly clear that Russian officials are using those reports to discard the Ukrainian leadership by fuelling a narrative according to which the Ukrainian authorities are hiring foreign mercenaries to suppress protest movements and making Ukrainian taxpayers pay for it. This inevitably risks adding to the secessionist discourse in Ukraine.

The Center for International Maritime Security (CIMSEC) has produced a two-part series on the history and prospects for private military and security companies (PMSCs) in South and Southeast Asia.[4] The feature evaluates the evolution of PMSCs in the region, and concludes that resource competition in the region, as well as the continued presence of piracy, indicates that PMSCs are likely to prosper in the South and Southeast Asian markets in the coming years. The report also speculates on the regional factors that have been conducive to the development of PMCSs, including particular government policies (or lack thereof) in addressing regional threats, as well as the evolution of PMSCs' legal status and protection. The report predicts that PMSCs are likely to continue to play a role in the region by filling gaps in state capacity, with smaller maritime Southeast Asian countries potentially calling upon PMSCs for port security, high-value transit and marine resource protection.

The UN Working Group on the use of Mercenaries carried out its first official visit to Comoros between 8 and 16 May 2014 in order to assess the impact of mercenaries on human rights. The history of Comoros has been tainted by repeated coups and attempted coups that involved mercenaries. Ongoing issues in Comoros, including weak government institutions and human rights violations, are deeply rooted in the country's mercenary past. The country has been relatively stable since 2001, but state and judicial institutions need to be further strengthened. Specifically, Comoros will need to establish safeguards against mercenaries. In the past, mercenarism has thrived on the problem of separatism in Comoros, partly because of scattered and inefficient state authority across the country's different islands. The UN working group has emphasised the need to continue strengthening state institutions though training and evaluation, while also looking at possible ways to regulate how PMSCs operate in the country.

[4] http://cimsec.org/whither-the-pmscs/

Also of note

- **The Brazilian press revealed that Academi is providing security training to Brazil's security forces** at the company's headquarters in North Carolina ahead of the 2014 World Cup. This is likely to cause further popular outrage given mounting negative opinion polls and protests regarding the sheer cost of the event.
- **Former Blackwater USA (now Academi) contractor Nicholas Slatten has been charged with murder by a grand jury** for his suspected role in a 2007 Baghdad shooting, which killed 17 Iraqi civilians. This indictment is the first of the kind, and is likely to further tarnish Academi's reputation, despite restructuring and rebranding efforts.
- **New Call of Duty video game focuses on private military and security companies.** A promotional video for the new game states that in this new edition, 'the world's most powerful military is not a country, it's a corporation'.

Unmanned vehicles and autonomous weapon systems

New reports spur debate over drone research, export and proliferation

A RAND report on unmanned aerial vehicle (UAV) capabilities, arms control and proliferation published in April has spurred significant and ongoing commentary within the military, defence and intelligence policy communities about UAV export, research and proliferation.[5] The report questions whether UAVs are transformative weapons delivering significant tactical advantage and highlights the strong US interest in guiding international norms around UAV use.

Shortly after the release of the RAND report, Forecast International published an article on future UAV markets and development.[6] According to an April report from the company, the global annual export market for UAVs is likely to grow from $942 million to $2.3 billion over the decade from 2013 to 2023. By 2017 worldwide UAV production could average about 960 unmanned aircraft annually, with the Aviation Industry Corporation of China (AVIC) expected to be the biggest UAV manufacturer. Half of the aircraft fleets of some militaries could be made of UAV systems by 2030.

These reports show a key point of divergence around UAV use and proliferation. On one hand, RAND's conclusion that the current fleet of medium-range, non-stealth UAVs only delivers tactical advantage in limited military contexts brings into question the idea of large UAV market growth and expansion over the next three to five years. On the other hand, market projections and government funding priorities suggest export markets and proliferation are growing exponentially, so much so that US UAV manufacturers are expressing increasing concern about losing market share and are becoming vocal about export restrictions imposed by the Missile Technology Control Regime (MTCR) and International Traffic in Arms Regulations (ITAR).

[5] http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR449/RAND_RR449.pdf

[6] http://www.forecastinternational.com/notable/DefenseNewsUAVMarketCouldDecline.pdf

One commentator extrapolated this a step further. In highlighting the limited effectiveness of drones against advanced enemies with air defence systems, Peter Dörrie suggested that the US 'pivot to Asia actually means drones to Africa'.[7] The operational context present in the Horn of Africa, the Sahel and parts of the Middle East enables drones to fulfil intelligence, surveillance and reconnaissance (ISR) and offensive needs. The same is not true of East Asia and the South China Sea; however, reports suggest that Asia will see the largest jump in UAV-related spending, reaching $7.7 billion. US military and advanced technology needs in an East Asian and Pacific theatre of modernised militaries are clearly different to US counterterrorism requirements in Africa and the Middle East. As such, it might be more accurate to speculate that manufacturing growth will occur in East Asia and the United States but that proliferation and deployment will most likely be across Africa.

Unsurprisingly, the US administration is now confronted with regional security partners that are demanding access to US UAV technology and the ability to develop national capabilities to run ISR activities. In the last month alone, the US administration and Pentagon faced vexing challenges around increasing requests from countries such as Algeria, Niger and Iraq for drone-technology transfer.

Other developments

On 19-20 April, the United States and Yemen conducted the largest series of drone attacks on al-Qaeda in the Arabian Peninsula (AQAP) militants this year. The drone strikes killed over 40 militants according to the Yemeni interior ministry, though it does not appear that key AQAP targets Nasser al Wuhayshi, head of AQAP, and Ibrahim al Asiri, AQAP's master bomb maker, were among the casualties. Three civilians were killed in the attack and five seriously injured. The strikes were followed up by Yemeni armed forces offensives to remove remaining AQAP elements from the targeted districts. US drone strikes in Yemen have greatly accelerated since 2011, to the point that in 2012 the number of strikes was comparable those in Pakistan. The US administration remains preoccupied with the threat posed by AQAP to US interests, though there is only limited evidence that the underlying security environment, which is resulting in endemic poverty and a general security vacuum, is being addressed.

The US national security community are openly questioning the US Navy's preference for a less advanced and capable drone fleet due to current budgetary pressures. The US Navy issued requirements for the Unmanned Carrier-Launched Airborne Surveillance and Strike (UNCLASS) program that will provide the navy with a carrier-version of non-stealthy surveillance drones as opposed to the navy's experimental X-47B aircraft, which over the longer term is likely to have stealth capability, longer range, and larger armament. Those criticising the navy's decision are likely to be concerned that non-stealthy, medium-range, small-payload Unmanned Combat Air Vehicles (UCAVs) will provide no strategic advantage for US sea power if confronted with China's Anti-Access/Area Denial (A2/AD) capabilities, specifically long-range ballistic and cruise missiles. The navy has defended against this criticism by arguing that carrier design will allow for capability growth and the ability to retrofit carriers, if necessary, in the future.

[7] https://medium.com/war-is-boring/8367398d47f0

Iran unveiled its reverse-engineered version of the US UAV the RQ-170 Sentinel on 11 May. Iran was able to reverse engineer the Sentinel after the UAV was either compromised by Iranian cyber forces and safely landed or simply crashed in Iran. Lieutenant Commander of the Islamic Revolutionary Guard Corps General Hossein Salami suggested that Iran decoded all the Sentinel computer systems and added some specific optimisations, namely armed payload, to the Iranian version. At present there is no footage of the drone in flight and commentators have noted that it may be a detailed replica rather than a functional copy considering the use of the exact same landing gears and tyres as the Sentinel. Supreme Leader Ayatollah Ali Khamenei's attendance at the unveiling indicates that Tehran wanted to achieve maximum coverage of a potential expansion of Iranian military capability. Reports indicate that Iran's maturing drone development programme is benefiting from operational use in Syria. A number of Iranian drones – the Shahed, Azem, Mohajer, Hamaseh and Sarir – have been captured on satellite imagery of Damascus, Hama and Shayrat airbases.

Also of note

- **The Israel Air Force undertook training drills in late April to prepare pilots to shoot down potential Hezbollah and Hamas drones.** The drills are designed to prepare pilots for more advanced drones that are faster and can stay airborne longer.
- **A four-day meeting convened by states party to the Convention on Certain Conventional Weapons (CCW) was held in Geneva 13-16 May to discuss autonomous weapons systems.** The International Committee of the Red Cross (ICRC) gave an address to the opening of the informal expert meeting and called upon states to subject new weapons with autonomous features to a thorough legal review.
- **The US Air Force will be deploying two Global Hawk UAVs from Misawa Air Base in Japan.** The Global Hawks will be used for surveillance of North Korea and Chinese military activities. The Japanese Air Self-Defence Force is expected to procure three Global Hawks in 2015.
- **US Congress is mandating that Federal Aviation Administration experts develop safety standards to enable integration of UAVs into the national airspace by 2015.**
- **Ann Rogers and John Hill have released a new book *Unmanned: Drone Warfare and Global Security*,** which examines the concept of nano-war, whereby states bring military scale force to bear on specific individuals.
- **South Korean officials have confirmed drones found near the North Korean border in early April are most likely owned by North Korea.** The South Korean defence ministry announced that it is increasing airspace surveillance and that surface-to-air artillery have been alerted. North Korea has accused South Korea and the United States of fabricating the claims.

Cyber warfare

United States more cognizant of vulnerability to cyber counter-strikes

In Syria and Ukraine, the US administration has been forced to consider potential cyber counter-strikes in response to US foreign policy actions, such as sanctions or cyber warfare offensives.

At a Milken Institute Global Conference held in late April, former Defence Secretary Leon Panetta and US counterterrorism expert Richard Clarke indicated that the United States should expect a Russian coordinated cyber-attack on financial institutions in response to escalating sanctions. Russia is likely to possess the capacity to employ a tiered cyber-attack campaign involving both official cyber teams within military and intelligence agencies and Russian hacktivists. A cyber-attack would most likely leverage a broad network of US computers controlled through malware to create an army of botnets to attack US information networks.

Russia's proficient and versatile integration of cyber operations, with (dis)information campaigns, disciplined army movements and strategic use of special forces, has sent strong warning signals to the United States and NATO about Russia's modernised cyber capabilities. This elevated concern has occurred without Moscow even employing a third tier of cyber capability and attack, which involves the targeting of critical infrastructure, public and private, with the goal of disrupting or disabling essential services.

Russia's use of cyber measures in the annexation of Crimea and US Defence Secretary Chuck Hagel's attempted dialogue with Beijing over US cyber command both reveal that there is a lack of defined knowledge around 'cyber red-lines' and international norms. They represent two different pathways for countries to start defining the rules of cyber engagement: one through practical application, and the other through diplomacy and norm setting. The US administration's preferred approach is likely to be through dialogue, diplomacy and informal, bilateral norm setting. The implication is that the United States may want to avoid full-scale cyber confrontation in Ukraine, at least until there is greater consensus within NATO about cyber 'redlines' and defensive and offensive postures.

Other developments

The European Union Agency for Network and Information Security (ENISA) conducted its biannual cyber security stress test on 28 April. Over 200 organisations participated in the coordinated stress test, which employed a realistic pan-European cyber incident, including distributed denial-of-service attacks (DDoS), attacks on power grids and major cyber-security breaches. Some expert participants criticised the cyber war games as inadequate to prepare national governments for large-scale cyber attacks and claimed they were more about ensuring the necessary lines of communication are in place rather than technical and tactical proficiency in cyber defence.

Declassified Australian Defence Force (ADF) papers reveal that the ADF is embracing both offensive and defensive cyber-warfare tactics, including deception and disinformation through the internet, for future military operations. Australia's cyber capacity is most likely being further developed by the Australian Signals Directorate and the Defence Science and Technology Organisation. The information activities' doctrine, which broadly outlines tactics and capabilities, was not disclosed in the 2013 defence white paper. It was released shortly after it was revealed Chinese intelligence agencies might have had access to the Australian parliamentary computer network for up to a year. The recent Australian Strategic Policy Institute report on cyber maturity in the Asia Pacific ranked Australia third after United States and China in terms of cyber-warfare capacity.[8] In 2014, the Australian cyber-warfare market within the military is forecast to be worth US$18.7 million. By 2024, expenditure is forecast to total US$336.5 million.

At the 2014 EU-Japan Summit on 5 May Japanese Prime Minister Shinzō Abe agreed with EU Council members that the EU and Japan will establish the EU-Japan Cyber Dialogue, which aims to collaboratively create an open, safe and secure cyberspace. On 12 May, Abe also secured new bilateral defence agreements with Israel with a focus on cyber-security arrangements. Common concerns shared by Abe and Israeli Prime Minister Benjamin Netanyahu include China's cyber war capabilities and the potential transfer of technology and capabilities to Iran and North Korea. There are, however, likely to be limitations on the relationship due to Japan's heavy dependence on Middle Eastern oil and need to preserve good relations with key suppliers. The raft of bilateral agreements and defence talks coincide with Abe's push for reform to Japan's constitution, which limits Japanese military activities to self-defence.

Also of note

- **Verizon's *2014 Data Breach Investigations Report* recorded 511 espionage incidents in 2013** with an increasing proportion of attacks originating from Eastern Europe**.** Of the attacks, 306 resulted in data disclosure. The report highlights China as the predominate source of cyber-espionage attacks.
- **The *New York Times* carried a story on LulzSec hacktivists** that raises the question of whether the FBI directed any cyber attacks or data breaches through hacktivist groups, including to gain access to Syrian government systems.[9]
- **The Indonesian Army have signed a memorandum of understanding with a local institution, the Institut Teknologi Del, to develop a cyber-defence and warfare centre.** The centre is to develop new offensive and defensive technologies for cyber-warfare operations.

[8] https://www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2014/ASPI_cyber_maturity_2014.pdf

[9] http://www.nytimes.com/2014/04/24/world/fbi-informant-is-tied-to-cyberattacks-abroad.html?_r=0

- **Researchers are building tools based on the principles of artificial intelligence and logic programming to help attribute cyber attacks.** The framework, InCA (Intelligent Cyber Attribution), enables decision makers to understand probabilistic assessments of cyber-attack attribution. Cyber response has been hampered by long investigation lead times. For example, experts took months to trace an eight-month series of DDoS, attacks on the largest US banks in 2012 and 2013 to Iranian hackers retaliating for US and international sanctions on Iran.
- **Pakistan has introduced legislation on cyber security, the first of its kind.** The legislation will establish the National Cyber Security Council to develop policy on emerging cyber-security threats.
- **A report by cloud provider Akamai showed that 43% of cyber-attack traffic in the fourth quarter of 2013 originated from Chinese IP addresses.**[10] The report noted that some hackers and cyber criminals might be launching attacks from compromised systems, thereby skewing the results. 19% of attacks originated in the United States.
- **The US National Institute of Standards and Technology is reviewing cryptographic standards** and guideline development processes after allegation were made that the NSA were intentionally undermining cryptographic standards as part of their surveillance programmes. After a two-month public comment period, the Visiting Committee on Advanced Technology (VCAT), the primary advisory committee, has now begun its review.

Intelligence, surveillance and reconnaissance

NSA allegedly hardwired backdoor access tools into intercepted exported US routers

The NSA is alleged to have intercepted US routers bound for export and hardwired backdoor access tools into them. The allegation is revealed in a new book by journalist Glenn Greenwald, and is based on a documents leaked by NSA contractor Edward Snowden.

The allegations are likely to have significant political and commercial implications for the United States who has consistently raised concerns and questions about Chinese companies, such as Huawei and Lenovo, hardwiring surveillance and vulnerability measures into telecommunications technology. Greenwald suggests that the concerns about Chinese companies amounted to a smear campaign to both protect the US market and boost US export credentials on a global scale, which in turn increased NSA surveillance capacity.

Allegations have also been levelled at the NSA claiming that they were aware of vulnerabilities in the OpenSSL internet cryptographic protocol up to two years before the Heartbleed bug was identified. The claim has triggered broader questions about US government knowledge of cyber exploits, public disclosure of risks and the purchase of 'zero day exploits' (that is previously unknown vulnerabilities). In most cases, governments purchase zero day exploits from those who discover them in order to identify risk and create defensive patches; however, less than rigorous vetting of purchasers may mean some private company procurement is for 'offensive' use.

[10] http://www.akamai.com/dl/akamai/akamai-soti-q413.pdf?WT.mc_id=soti_Q413

Former Assistant Secretary of Defence for Homeland Defence and Americas' Security Affairs Paul Stockton noted in an essay earlier this year that government procurement of zero day exploits was creating a large grey market that poses a significant risk to US security interests. A representative of the White House cybersecurity coordinator refuted that there is a booming market for zero day exploits or that government participation in the market is fuelling the proliferation of exploits.

Other developments

On 30 April, the US Department of Justice released details of government applications to the Foreign Intelligence Surveillance Court for authority to conduct electronic surveillance activities. The US administration filed 1,655 applications with the court in 2013, down from 1,856 the previous year. The court did not reject any application, though it did modify 34 applications for surveillance.

In late April it was revealed that telecommunication company Verizon initiated a legal challenge to an NSA request for call-detail records before the Foreign Intelligence Surveillance Court. The court rejected Verizon's petition and upheld the NSA request citing the 1979 Supreme Court case of Smith v. Maryland, which legal scholars suggest is not a precedent for NSA surveillance activities. In early May, the US House Judiciary Committee unanimously passed the proposed USA Freedom Act, which if passed by Congress would prevent the NSA from collecting telecommunication metadata, but allow NSA to make applications on an individual, case-by-case basis.

Russia and the United States are not seeing eye-to-eye over permissions under the Treaty on Open Skies. The treaty allows the 34 signatories to fly aircraft through airspace of other signatories to collect intelligence using advanced cameras and sensors. Moscow cancelled a US flight scheduled for mid-April in what some have interpreted as a measure to reduce Western intelligence gathering on Russian troop movements near Ukraine and Crimea. However, US military and intelligence agencies, despite protest from the State Department, have urged the administration to deny Russian certification of its new surveillance aircraft, the Tu-214ON, and prevent Russian open-sky authorised surveillance.

Governments, the private sector and NGOs are developing complex research programmes that use 'big data' for conflict prediction and prevention. A number of recent media articles highlight how open-source data is being use by various institutions to predict conflict and anticipate crisis using big data. The articles highlighted big data analytic programmes, including the US Defence Department's Information Volume and Velocity programme, the CIA's Open Source Indicators and the UN's Global Pulse initiative.

Also of note

- **The United States is assisting Nigerian authorities to locate 250 school girls kidnapped by Boko Haram.** While the Pentagon initially indicated that drones would not be used, as any use of UAVs for ISR purposes would divert resources away from special forces using UAVs to track Joseph Kony's Lord's Resistance Army, US Defence Secretary Chuck Hagel later indicated that RQ-4 Global Hawk drones would be used. The British Royal Air Force has also deployed Raytheon Sentinel R1 Airborne Stand-off Radar (ASTOR) aircraft to support international search efforts.
- **Israel launched a synthetic aperture radar satellite, Ofeq 10 (Ofek/Horizon), into orbit at the beginning of April.** The satellite enhances Israel's intelligence capabilities and ability to monitor nuclear-programme developments in Iran.

- **A Houston based company Behavioral Recognition Systems (BRS Labs) have developed an artificial intelligence (AI) based CCTV video surveillance system.** The system, AISight, applies a reason-based rules system for video analytics that surpasses existing technology used in prison or nuclear facilities to identify changes in the observer environment. The system in use in Chicago and Washington DC is set up to 'autonomously build an ever-changing knowledge base of activity captured'.
- **A US Republican has proposed the US Missile Defence Agency (MDA) investigate the costs and security requirements of integrating Taiwan's early warning radar** with US missile defence and sensor systems. The system is one of the most advanced radars in the world, and US access would likely draw the ire of Beijing.
- **The Israeli Air Force revealed its F-15 Double Tail Knights Squadron undertakes aerial intelligence without leaving Israeli airspace** using long-range cameras, enabling ISR operations that have captured Hezbollah movements in southern Lebanon.

Commissioned by the Remote Control Project

remotecontrolproject.org

REMOTE CONTROL
Examining changes in military engagement