Remote-control warfare briefing | #05

27 August 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: Amnesty International alleges failings in investigation of civilian deaths caused by US special forces in Afghanistan.

Private military and security companies: Increasing number of mercenaries in foreign conflicts from Balkans region.

Unmanned vehicles and autonomous weapons systems: United States initiates drone strikes against Islamic State in Iraq.

Cyber warfare: State and non-state hacker groups launch cyber attacks on Israel in response to Operation Protective Edge.

Intelligence, surveillance and reconnaissance: US officials grapple with political and economic costs of NSA's surveillance activities.

Special operations forces

Amnesty International alleges failings in investigation of civilian deaths caused by US special forces in Afghanistan

In a report published in August, Amnesty International alleged that the investigation and prosecution practices employed by US special operation forces (SOF) and the International Security Assistance Force (ISAF) in relation to Afghan civilian deaths are falling short of basic transparency requirements.[1] The report draws on over 125 interviews with Afghan witnesses, victims and family members, and focuses on 10 key case studies, which together resulted in more than 140 civilian deaths. Despite the high death toll, no criminal prosecutions have arisen from any of these cases.

[1] http://www.amnesty.org/en/library/asset/ASA11/006/2014/en/c628b1a4-821f-4168-a583-ac4a6159986e/asa110062014en.pdf

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

A disproportionate number of the case studies involve US special operations forces. The case study on US SOF killings in Nerkh and Maidan Shahr districts in Wardak province between November 2012 and February 2013 examines evidence that US special forces were involved in extrajudicial killings, torture and enforced disappearances. Two reported incidents of US special forces operations on family compounds in Nangarhar and Paktia provinces in 2010 resulted in a number civilian deaths, which may have been avoided with stricter rules of engagement and better intelligence. Nine civilians were killed In the Nangarhar incident. It is disputed as to whether US SOF announced their presence and identified themselves, leading to considerable confusion. Following the Paktia province incident, the then commander of the US Joint Special Operations Command, Vice Admiral William McRaven, visited the affected village to make a formal apology and provide the family with compensation.

Members of the Afghan government have expressed deep concern over the use of the US military justice system to examine incidents of civilian causalities. One of the key recommendations of the Amnesty report is for the Afghan government to leverage future bilateral security agreements signed with NATO and the United States to secure greater protection for civilians and mechanisms for the transparent investigation of and accountability for civilian casualties. While this is likely to be a concern for Afghan government officials, it will not be the number one priority while negotiating bilateral security agreements. Alternatively, NATO and the United States might focus on provisions relating to proactively avoiding civilian deaths and efforts to better communicate with the families of victims.

At present the ISAF status of force agreement provides international military forces with immunity from prosecution in Afghan courts for civilian deaths. This threatens the perceived legitimacy of the US and international forces, even in the eyes of those who have supported the military presence in Afghanistan. However, the US government is likely to resist or oppose wholesale reform of this arrangement because of the political fallout around US soldiers facing a military court in Afghanistan. The increasing number of private military contractors operating in Afghanistan may also exacerbate concerns around civilian deaths, including the investigation of and accountability for the actions of contractors.

Other developments

President Barack Obama's hallmark $5 billion Counterterrorism Partnerships Fund proposal announced during his West Point speech in May has received bipartisan criticism in the US Congress from the House budget committee and the Senate appropriations and armed services committees. The initial funding proposal, which was further detailed after the president's speech, will be primarily used for supporting SOF training of foreign partner forces and is part of the Overseas Contingency Operation budget. The hearings revealed that part of the spending will include intelligence, surveillance and reconnaissance (ISR) technology and equipment for partner forces training with US SOF and maritime and helicopter transport to enable alternative launch pads for foreign partner force operations. Senator Mark Pryor (D-Ark) proposed an unsuccessful amendment before the Senate Appropriations Committee to strip funding earmarked for the training and arming of vetted Syrian opposition rebels. Despite criticism from both parties, the funding is likely to pass Congress.

A broader cross-section of US special operations forces commands are training in amphibious operations, ending the historical monopoly of this area by US Navy SEALs. US Army special forces (Delta Force) and Marine Corps Forces Special Operations Command (MARSOC) are increasingly undertaking sea-launched tactical training exercises. US Special Operations Command's (USSOCOM) requests for marine launch pads for special operations activities mirror the shift in personnel training. USSOCOM has been pushing for the conversion of commercial container ships into sea bases for SOF rather than them relying on US Navy aircraft carriers, which have substantial downsides from an operational perspective. In November 2013, the US Military Sealift Command awarded Maersk the contract to convert the maritime support vessel MV Cragside into a special operations base for up to 200 troops. The Pentagon finds this approach advantageous, as it is more economically efficient than terrestrial bases and the ships do not require the support of host states.

In late July, special forces and elite police units from 17 American countries participated in the annual Fuerzas Comando competition at Fort Tolemaida, Colombia. The US Southern Command-sponsored special operations skills competition is aimed at enhancing training and strengthening the bonds between SOF in the Western Hemisphere in order to increase cooperation on common issues, including counterterrorism and operations against organised crime and illicit drug trafficking. A team from Colombia won this year's event – the sixth time a Colombian team has won in the 10 years since the competition was established in 2004. The US team from the 7th Special Forces Group was second and El Salvador third. A number of notable absences from Fuerzas Comando included Mexico, Nicaragua, Venezuela, Bolivia and Ecuador.

Also of note

- **British SAS and US SOF have been deployed to northern Iraq to conduct ISR operations around Mount Sinjar.** The additional US deployment of 130 special operations forces 'assessors' was announced on the eve of US airstrikes against Islamic State (ISIS) targets in Iraq.
- **USSOCOM's Global Research Assessment Programme is proposing to evaluate the effectiveness of their information support operations (propaganda) in Colombia** against drug cartels and FARC rebels.
- **An ISIS fighter has revealed on twitter that the group has stolen Canadian-manufactured night vision goggles** initially provided to Iraq's special operations forces.
- **The US Navy is designing two new miniature submarines for their Navy SEALs, the Shallow Water Combat Submersible and the Dry Combat Submersible.** The new mini-subs are intended to have a longer range (60 nautical miles) and move at greater depths (190 feet below the surface) than existing models.
- **In June, Malaysian Royal Air Force and Army SOF and US Air Force Special Tactics Squadron** participated in Cope Taufan 2014, an air combat exercise focused on drills protecting the eastern Malaysia peninsular and South China Seas.

Private military and security companies

Increasing number of mercenaries in foreign conflicts from Balkans region

Rising numbers of mercenaries from the Balkan countries of the former Yugoslavia are fighting abroad, despite measures taken in Bosnia and Herzegovina, Kosovo and Serbia designed to stem the flow of foreign fighter into civil wars and insurgencies around the world. For example, Serbian officials have estimated that dozens of Serbian nationals have been fighting on both sides of the conflict in Ukraine. Serbian Prime Minister Aleksandar Vucic has stated that in most cases these Serbian fighters are mercenaries fighting for money rather than ideology. However, Bosnian militants fighting abroad are reported to be much more ideologically driven than their Serbian counterparts, with some reportedly influenced by Wahhabi extremism.

The increase in the export of Balkan fighters is affecting the region's stability, and has led some countries to take measures to criminalise mercenary activity; however, such laws are likely to prove difficult to implement. A significant issue is that organisations that recruit volunteers to fight abroad, such as the Serbian Chetnik Movement, usually operate with personnel located in Russia, which means that the mercenaries do not have to go through those Balkan countries with anti-mercenary laws.

Not all the fighters coming from this region are mercenaries: Balkan citizens are also reported to be involved in jihadist activities in several conflict locations across the world. This month, 40 Islamist radicals were arrested in Kosovo on suspicion of being involved in extremist activities in Iraq and Syria. An April report from the International Centre for the Study of Radicalism at King's College London stated that 9.6% of their sample of 190 Western and European foreign fighters in Syria were from the Balkans.[2]

Overall, such a trend in what could be called 'war tourism' from Balkan countries undoubtedly has its roots in the region's violent past. Another factor is the younger generation's lack of prospects in their own countries, where the social climate may encourage the development of extremist views. Moreover, those mercenaries and jihadists who fight abroad are likely to represent a real threat on return to their respective countries, bringing violent experiences and extremist ideologies back home, and thus risking further destabilisation of already fragile societies.

Other developments

In August, the World Bank released research on the cost of crime and violence in Papua New Guinea's crime hotspots and the increasing presence of private security companies.[3] According to the survey, 84% of companies pay for private security, and private security accounts for an average of 5% of annual operating costs for a business in Papua New Guinea. Such a prevalence of private security is causing concerns that competition between private security companies may cause law and order issues in their own right or that those businesses without private security will be disproportionately targeted by criminals. The longer-term implications are that the national police force may become less reliable and operationally effective because of underutilisation and reduced community engagement.

[2] http://icsr.info/wp-content/uploads/2014/04/ICSR-Report-Greenbirds-Measuring-Importance-and-Infleunce-in-Syrian-Foreign-Fighter-Networks.pdf

[3] http://documents.worldbank.org/curated/en/2014/05/20030015/gates-hired-guns-mistrust-business-unusual-cost-crime-violence-businesses-papua-new-guinea

The European Parliament passed a resolution on 17 July praising a 15-point peace plan proposed by the Ukrainian president, which, among other others things, calls on Russia to respect an agreed ceasefire, accept the peace plan put forward by Ukraine and withdraw its mercenaries. The resolution was passed by 497 votes to 121, with 21 abstentions. The participation of mercenaries in the conflict in Ukraine has been a recurrent topic of debate in the media, with each side of the conflict accusing the other of using mercenaries and private security companies. However, the Ukrainian president plans to offer amnesty for those mercenaries who have not committed grave crimes. The emphasis of the European Parliament's resolution on the role played by pro-Russian mercenaries results from the rebel's recent breach of a ceasefire agreed in June.

The US Congress is waiting to see whether South African President Jacob Zuma will sign an amendment to his country's Private Security Industry Regulation Act (PSIRA). The proposed amendments will compel foreign security providers to hand over 51% of their businesses to South African citizens. This ownership clause is likely to have a negative impact on foreign investment in South Africa if it is implemented, as it also covers manufacturers and importers of security equipment, including electronics companies. It may also threaten the renewal of the United States' African Growth and Opportunities Act (AGOA), designed to assist the economies of sub-Saharan Africa and to improve economic relations between the United States and the region. The South African government requested a 15-year extension of the AGOA during the US-Africa Summit in August. Renewal of the AGOA could provide foreign investors with the necessary confidence for long-term investment in South Africa. However, the proposed amendments to PSIR are putting the renewal of the AGOA in jeopardy.

Also of note

- **The City of Montreal, Canada, wants its police department to increase the number of security contracts with private companies.** Private security companies regularly hire off-duty police officers through the police department when special events require heightened security. Renting out police services has been particularly lucrative for the Montreal police, amounting to around $3.9 million (CAD) each year.
- **After a series of scandals that have tarnished its public image, the British multinational security services company G4S has reported that it is back in profit,** with a pre-tax profit of £85 million for the six months up to the end of June, as opposed to its reported £94 million loss a year ago.
- **The UN open-ended intergovernmental working group to consider the possibility of elaborating an international regulatory framework on the regulation, monitoring and oversight of the activities of private military and security companies met from 21 to 25 July.** Several states, including South Africa, Pakistan and Senegal, argued that international regulation is urgently needed given the transnational dimension of PMSCs. However, the United States and EU countries opposed the idea, pointing to the complexity of implementing such a framework.
- **India's former ambassador to Syria, Rajendra Abhyankar, has claimed that four Indian youths suspected of having joined Islamic State (ISIS) may have done so as mercenaries.** In comments following a talk at the Observer Research Foundation in July, Abhyankar claimed the youths from Kalyan may not be ideologically driven as initially suspected.

Unmanned vehicles and autonomous weapon systems

United States initiates drone strikes against Islamic State in Iraq

The United States has launched air strikes in Iraq in a bid to halt the territorial expansion of the Islamic State (ISIS). The first round of strikes hit ISIS mobile artillery and a mortar position near Erbil on 8 August. In the following week, 35 manned and unmanned air strikes were part of the campaign to recapture the strategic Mosul Dam from ISIS. US MQ-1 Predator unmanned combat air vehicles (UCAVs) armed with AGM-14 Hellfire missiles have been used in some of the strikes alongside F/A-18 carrier-based multirole fighter aircraft.

US forces have been reportedly flying up to 30-40 missions a day over northern Iraq since June. Iran has also been flying ISR missions over Iraq using unmanned aerial vehicles (UAVs), but on a much more limited scale. In terms of modes of attack, the force balance between manned and unmanned air strikes is an issue for the United States due to the overall strong demand for drones for US operations across the Middle East, Sahel and North Africa. The level of UCAV use in Iraq means that other US operations in the region currently have reduced access to drones. ISIS's likely cache of surface-to-air missiles may also be a factor in balancing air strikes from manned and unmanned weapons platforms.

Both manned and unmanned air strikes will require intensive ISR work by special forces on the ground. Those operatives already deployed, both British and US, will now most likely be assisting in targeting for air strikes.

The United States is unlikely to replicate the level and nature of the drone strike activities it has undertaken in Pakistan, Afghanistan and Yemen for a number of reasons. ISIS are now showing a strong ability to disperse fighters into existing populations, and without effective ISR collection and cataloguing, targeting drone strikes becomes difficult for US forces. Unconstrained air strikes risk further alienating Sunni communities who are already heavily targeted by ISIS recruitment activities. However, if ISIS concentrates its forces for an offensive to encircle Baghdad or significantly expanded territorial control, the United States may increase the level of air strikes, including by armed drones.

Other developments

The CIA undertook three separate drone strikes in northwest Pakistan during July. The strikes occurred near Datta Khel in North Waziristan, an area of significant jihadist activity. According to the Bureau of Investigative Journalism, the strikes resulted in between 32 and 46 fatalities, making July one of the most lethal months for drone strikes in two years in terms of casualties per strike.[4] Sanafi al Nasr, a senior al-Qaeda leader based in Syria, indicated that six al-Qaeda operatives were killed in the 10 July strike. A US official also reported that three suspected al-Qaeda in the Arabian Peninsula (AQAP) fighters were killed in a US drone strike in Yemen in early August, the first drone strike in the country for two months.

[4] http://www.thebureauinvestigates.com/2014/07/16/cia-drones-kill-at-least-13-in-pakistan-the-bloodiest-strike-for-more-than-a-year/

Major General Xu Hang, president of the PLA Academy of Armoured Forces Engineering, has indicated to Chinese media that the People's Liberation Army is investing significant time and resources in developing unmanned ground vehicles (UGVs). The comments come as the China North Industries Group Corp (NORINCO Group) inaugurated a recently created research centre for UGVs near Beijing in July. It is unclear whether the research centre will deliver significant ground combat capability in the short term, as there are critical technological challenges. PLA representatives have acknowledged that the focus is on refitting existing ground vehicle fleets for unmanned capability as opposed to developing new vehicles.

According to Japan's 2014 defence budget, currently nominal spending and investment on unmanned aerial vehicles is set to increase by 300%. Japan recently welcomed the deployment of two US RQ-4 Global Hawks to Misawa Air Base to assist Japanese forces in becoming more familiar with the vehicles. This deployment occurred ahead of Japan indicating its desire to acquire three Global Hawks and start developing its own indigenous UAV design and manufacturing capacity. The increase in UAV programme funding and capacity development is likely to be driven by concerns over North Korea's ballistic missile programmes and maritime boundary conflicts with China and South Korea. The developments come after Prime Minister Shinzō Abe oversaw a reinterpretation of Article 9 of Japan's constitution (the peace clause), which has opened up greater political and constitutional space for Japanese industry to try to keep up with China's UAV programme.

Also of note

- **Flight Tech, one of Brazil's first defence companies to produce UAVs, is exporting three Horus FT-100 mini-UAVs to an undisclosed African country** in the first UAV export deal from Brazil. The FT-100s were designed in collaboration with the Brazilian military, and have likely been acquired for domestic missions due to their comparatively limited flying range.
- **Integrated Instrument-making Corporation, a subsidiary of Russia's state-owned Rostec, displayed an amphibious unmanned aerial vehicle at the Innoprom-2014 industrial trade fair in Yekaterinburg, Russia.** The unique hybrid amphibious drone, called Chirok (Teal), has a hovercraft body, which enables it to take off from marine or uneven terrain surfaces.
- **Russian defence contractor Kamov has announced the proposed development of a vertical take-off and landing reconnaissance and strike rotary UAV, the Ka-175,** which may make its maiden flight within a year.
- **A July 2014 US Congressional Research Paper on navy shipboard lasers for surface, air and missile defence highlighted the potential benefits of shipboard lasers in countering unsophisticated UAVs.**[5] The paper points out the economic challenge for the US Navy if they rely on conventional missile defence systems to defend against multiple UAV threats, whereby the cost per defensive counter-strike may become unsustainable.
- **The Israeli Defense Forces (IDF) has openly praised Elbit Systems for the role that their Skylark mini-UAV and one-ton Hermes 900, debuted by the Israel Air Force, played in supporting ground forces during Operation Protective Edge.**

[5] http://fas.org/sgp/crs/weapons/R41526.pdf

- **The US Army's Rapid Equipping Force is testing a UAV system that can stay in the air as long as the drone remains remotely connected to ground power from the controller.** The Persistent Aerial Reconnaissance and Communications (PARC) system relies on a quadrotor receiving microfilament carrying electrical power and ethernet communications between ground control and the drone.
- **US Senate Appropriations Committee is concerned that Northrop Grumman MQ-4 Triton reconnaissance UAV is 25% (or $720 million) over budget and behind schedule.** The Triton is designed to fly up to 24-hour missions at a maximum of 60,000 feet, and provides 360 degree ocean and terrain surveillance with inbuilt radar, electro-optical and infrared sensors. The Triton is expected to be the next generation of maritime surveillance UAV, and has attracted interest from Japan, Korea and Australia.
- **The commercial UAV industry is anticipating an executive order from US President Barack Obama on privacy requirements for UAV operators.** It is expected that the order will make the National Telecommunications and Information Administration responsible for detailed guidelines.

Cyber warfare

State and non-state hacker groups launch cyber attacks on Israel in response to Operation Protective Edge

Cyber attacks and counter-attacks have spiked over the last two months as the conflict between Israel and Palestine has intensified. Information security firm ArborSERT has quantified the significant increase in distributed denial-of-service (DDoS) attacks against Israeli government agencies, financial services and military websites, including Mossad and the prime minister's office.[6] DDoS attacks have increased from an average of 30 per day in June to 150 per day in July, with the number of attack peaking on 21 July with a total of 429 attacks. Domain Name System (DNS) attacks have also increased. 70% of attacks appear to originate or have been routed through Qatar.

There are reports that the Qatari authorities are road testing cyber technologies by providing Hamas with new technology and untested capabilities. While these might not include advanced persistent threats (APTs), there is the suggestion that tunnels built by Hamas are closely monitored and that Hamas has the capability to track the movement of IDF troops through the tunnel network using cyber means. The IDF Computer Service Directorate also suggested that both the Iran Cyber Army and Turkey's cyber forces have participated in cyber attacks against Israel. In one case Iranian cyber forces are alleged to have coordinated a DDoS attack on IDF's Homefront Command website, which provides security information and rocket warnings.

There are a number non-state actors and hacker groups alleged to be involved in the cyber conflict between Palestine and Israel. AnonGhost appears to be leading most DDoS attacks and cyber intrusions, and launched #OpSaveGaza on the eve of Operation Protective Edge. Others affiliated with the more widely-known Anonymous appear to be piggy-backing off AnonGhost attacks and thus increasing the magnitude of such attacks.

[6] http://www.arbornetworks.com/asert/2014/08/ddos-and-geopolitics-attack-analysis-in-the-context-of-the-israeli-hamas-conflict/

Cyber intelligence and security commentators argue that these attacks have not had any significant impact on Israeli infrastructure or internal communication channels. Despite the intensity and magnitude of cyber attacks, the actual level of intrusion, disruption and damage to Israeli operations appears limited. Israel's comparative cyber defence capabilities are at this point in time much more advanced than the capabilities of Hamas or non-state hacking collectives.

Other developments

In a recent interview with *Wired*, the whistleblower Edward Snowden revealed details of the NSA's automated cyber-attack programme codenamed MonsterMind.[7] Snowden describes the programme as being able to seek out internet traffic patterns indicating a malware source and automatically launch a counter attack. This means that in cases where initial attacks were routed through third parties (for example, an Eastern European cybercrime syndicate routing an attack through China), the third party infrastructure is attacked without human intervention. As such, MonsterMind has far broader implications than the covert ISR activities of the NSA, as it is a cyber weapon that could lead to significant miscalculation. Also, for the programme to work, the NSA needs access to almost all private communications entering the United States. Revealing MonsterMind at a time when the NSA and other Washington policy specialists are talking up the need for international norms for the cyber realm has further damaged the United States' standing in this area.

The threat intelligence firm Cyber Engineering Services Inc. (CyberESI) believe that Chinese hackers associated with the PLA compromised three Israeli defence contractors and suppliers between October 2011 and August 2012. The targets, Elisra Group, Israel Aerospace Industries and Rafael Advanced Defense Systems, have all been involved in Israel's Iron Dome defence system. It is believed that the hackers obtained schematics and specifications for Israel's Arrow 3 missile through the data compromise. A prominent Turkish hacker group Ayyildiz Tim (AYT) claimed to have hacked Iron Dome systems and the software of the Arrow 3 ballistic missile. However, it is unlikely that the group actually compromised any Iron Dome systems. CyberESI representatives suggest that the hackers behind the defence contractor data theft are likely to be from the PLA Unit 61398, which includes five Chinese nationals charged with espionage offences in the United States.

A US Inspector General cybercrime unit report and internal investigation has revealed that the US Nuclear Regulatory Commission (NRC) has been subject to approximately 17 data extraction and credential harvesting attempts over the last three years. The NRC is a high-value target, as it holds highly-confidential information about the US nuclear industry and the location and condition of all reactors. It is speculated that the campaign has been led by a state actor due to its sophistication and likely interest of foreign governments in US critical infrastructure vulnerabilities.

[7] http://www.wired.com/2014/08/edward-snowden/

Also of note

- **The Ukrainian prime minister's office and Ukrainian embassies have been targeted by an aggressive cyber campaign using a variation of the Snake malware** in what has all the hallmarks of a Russian operation.
- **In late July the Center for a New American Security (CNAS) published a report on the prioritisation of defending US cyber assets and systems critical to the US national interest**.[8] Some of the key recommendations for the US government include identifying prioritisation of cyber redundancy, implementing confidence building measures in the cyber field, seeking agreement on parties refraining from cyber intrusions into nuclear command and control systems and establishing a system of voluntary reporting of near-miss cyber incidents.
- **A number of reports have emerged alleging that the Kremlin is paying internet trolls to promote President Vladimir Putin and his policies in the US media** as part of a Russian disinformation programme. Some reports suggest the scheme has been operating over the last five years but has escalated with the conflict in Ukraine.
- **US Assistant Attorney General John Carlin told the Aspen Security Forum on 24 July that al-Qaeda has developed cyber capabilities, adopted cyber warfare as a strategy and tested the feasibility of such operations.** Deputy Director of the NSA Richard Ledgett advocated the need for international norms at the same forum, and suggested that China poses the greatest cyber threat to the US because state actors share intelligence and intellectual property with businesses.
- **The Canadian foreign ministry has claimed that a Chinese group hacked the National Research Council (NRC),** the Canadian government's research and technology organisation. The Canadian government has now segregated the NRC from other government networks.
- **Information security analysis company FireEye is researching whether there is a digital signature associated with malware signals that could be interpreted as the equivalent of a troop build-up at a border** and used as a potential precursor prediction tool for conflict.[9]
- **Taiwan's technology minister has accused China of undertaking cyber attacks against Taiwan as a means of testing Chinese cyber capabilities.** Taiwan's National Security Bureau claims that it is has witnessed over three million hacking attempts from China in the space of 12 months.
- **RAND Corporation published a detailed paper on cybercrime,** which highlights the emergence of online collaboration between diverse actors, including, for example, Vietnamese nationals partnering with Nigerian nationals on an e-commerce scam.[10]
- **NATO country defence forces have approved the creation of a military cyber base in Tallinn, Estonia.** The base will provide NATO with an advanced cyber laboratory.

[8] http://www.cnas.org/surviving-diet-poisoned-fruit

[9] http://www.telegraph.co.uk/news/worldnews/middleeast/israel/11034421/Gaza-and-Crimea-conflicts-could-have-been-predicted-by-monitoring-cyber-attacks.html

[10] http://www.rand.org/pubs/periodicals/rand-review/issues/2014/summer/wildweb.html

Intelligence, surveillance and reconnaissance

US officials grapple with political and economic costs of NSA's surveillance activities

On 18 July, former US state department official John Napier Tye had an article published in the *Washington Post* identifying the most relevant source of executive and administrative power for NSA interception and collection activities, Executive Order 12333, issued by then President Ronald Reagan in 1981.[11] Tye argues that the activities undertaken in line with the executive order are as significant as, if not more so, than those authorised by Section 215 of the Patriot Act or Section 702 of the Foreign Intelligence Surveillance Act. Executive Order 12333 permits the collection of communication content (not just metadata) and allows retention of incidentally collected communication in the course of a lawful overseas foreign intelligence investigation.

At the same time, Democrat senator and chair of the US Senate judiciary committee Patrick Leahy has introduced a new revised USA Freedom Act. The new version is hailed as strengthening privacy provision where the original House version of the bill was too weak. While Five Eye intelligence partners will respond to their own domestic dynamics, there will be pressure to achieve a degree of harmonisation and interoperability between the surveillance principles and regulations established under the USA Freedom Act and legislation implemented in the United Kingdom, Canada, New Zealand and Australia. There is a clear bipartisan acknowledgement of the need for NSA and broader surveillance reform, in part due to the growing realisation of the political and economic costs of the current approach, but congress has struggled to find a middle ground. There is a high level of dependence on signals intelligence in the programmes the NSA have rolled out since 9/11, which US lawmakers are struggling to balance against the economic costs.

A New America Foundation report published in late July is making a strong case through attempts to quantify and categorise some of the economic and political costs associated with NSA surveillance programmes.[12] The report highlights that US businesses have reported declining sales in cloud computing services, ISP services, data-management services and IT hardware as customer attempt to avoid US companies for fear of inbuilt vulnerabilities or broad surveillance and data retention. Some governments are now implementing data localisation strategies, which may substantially shift international internet traffic. If these trends continue, they may increasingly challenge US economic interests, particularly in developing countries considering new telecommunication infrastructure. The report also highlights the damages done to US multilateral and bilateral relations with countries such as Brazil and Germany and the general weakening of encryption standards and effectiveness.

[11] http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html

[12] http://oti.newamerica.net/sites/newamerica.net/files/policydocs/Surveilance_Costs_Final.pdf

Other developments

Australia and Canada's political establishments are contending with contentious reforms to the surveillance and data-retention activities of key intelligence agencies. In Australia, the inability of the attorney general to clearly explain proposed surveillance reform led to the director general of the Australian Security and Intelligence Organisation, David Irvine, making a rare media appearance to explain proposed legislation. Irvine also told the Australian senate's legal and constitutional affairs references committee that it is appropriate that telecommunication companies retain metadata upwards of two years. In Canada, a *Globe and Mail* article revealed that reforms to Canada's electronic intelligence agency, the Communications Security Establishment Canada (CSEC), flagged as a critical legislative priority by then defence minister Peter MacKay, were derailed in 2009 when an unrelated police-surveillance bill was tabled and proved deeply unpopular.[13] The reforms would have provided greater oversight of CSEC's interpretation of its legislative and ministerial authorisations.

Recorded Future produced analysis in August of the encryption techniques employed by al-Qaeda and its affiliates after the Snowden NSA leaks.[14] The analysis reviews and reverse engineers encryption tools published by two media arms of al-Qaeda, Al Farj and the Global Islamic Media Front (GIMF). Recorded Future found that encryption tools published for mujahideen fighters and operatives are generally not tailored crypto tools developed by al-Qaeda. Instead, the available encryption tools are generally off-the-shelf open-source tools, some of which may have backdoors or in-built vulnerabilities that can be exploited by some intelligence agencies. This adds complexity to the issue of whether or not Snowden's leaks have actually provided jihadist organisations with improved abilities to avoid ISR.

The Office of the UN High Commissioner for Human Rights released a report in mid-July on the right to privacy in a digital age as requested by the UN General Assembly.[15] The report examines the protection of privacy in the context of mass data collection and surveillance and interception of digital communications. The report suggests civilian oversight bodies to combat the current lack of government transparency around surveillance policies, laws and practices, which may or may not cohere with international human rights law. Some governments may use the report at the next UN General Assembly session as a spring board for further discussion on the need for international norms on cyber security.

Also of note

- **Turkey became one of only 12 countries with an established satellite manufacture and testing centre when it opened the Satellite Assembly and Integration Test Centre (UMET**) at the Akinci air force base in Ankara. The centre will greatly expand Turkish ISR capabilities.
- **The Intercept ran an article in August on the high number of people on the FBI's Terrorist Screening Database** that have no identifiable or recognisable link with a listed terrorist organisation.[16]

[13] http://www.theglobeandmail.com/news/politics/wiretap-oversight-bill-derailed-in-2009/article20054907/

[14] https://www.recordedfuture.com/al-qaeda-encryption-technology-part-2/

[15] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

[16] https://firstlook.org/theintercept/article/2014/08/05/watch-commander/

- **In early August, NSA documents leaked by Edward Snowden underscored the significant signals intelligence support the United States provides Israel** and revealed that the NSA and Israel's SIGINT National Unit share extensive information on access, interception, analysis and reporting.[17]
- **The US state department has suggested that China's PLA anti-missile tests on 23 July 23 were a cover for anti-satellite tests.** China has completed similar tests in 2007 and 2010, and US defence experts suggest the PLA is trying to refine an anti-satellite capability to allow the option to attack navigation, surveillance and communication satellites.
- **Leaked intelligence indicates that German surveillance firm FinFisher helped the Bahrain government install spyware on target computers between 2010 and 2012** during pro-democracy protests in the country.
- **DigitalGlobe have launched their new WorldView 3 satellite that can move from pole to pole in 98 minutes and provide 30-centimetre resolution.** Earlier in the year, US government agencies were trying to force DigitalGlobe to degrade the resolution for public sales; however the National Oceanic and Atmospheric Administration has now given permission for the sale of higher-resolution images on open markets.

Commissioned by the Remote Control Project
remotecontrolproject.org

REMOTE CONTROL
Examining changes in military engagement

[17] https://firstlook.org/theintercept/2014/08/04/cash-weapons-surveillance/