Remote-control warfare briefing | #04

23 July 2014

Remote-control warfare is an emerging strategy that allows for conflict to be actioned at a distance. It incorporates technologies and light-footprint deployments that enable policymakers and military planners to approve actions that would unlikely be considered if using conventional means.

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

Special operations forces: US special forces trainers drawdown in Philippines as focus of bilateral military relationship shifts.

Private military and security companies: Audit finds that one employee of private background check provider reviewed over 15,000 security clearances in a single month.

Unmanned vehicles and autonomous weapon systems: Eminent task force delivers detailed report examining US drone policy.

Cyber warfare: Significant malware distribution and network monitoring on rise across Iraq.

Intelligence, surveillance and reconnaissance: British parliament passes 'emergency' data retention and surveillance legislation.

Special operations forces

US special forces trainers drawdown in Philippines as focus of bilateral military relationship shifts

In late June, Philippine defence secretary Voltaire Gazmin announced the drawdown of the US Joint Special Operations Task Force – Philippines (JSOTF-P) and the remaining presence of a small team of advisors in the form of the US Pacific Command (PACOM) Augmentation Team. JSOTF-P has been based on Mindanao for more than 12 years. Approximately 600 US special operations forces (SOF) personnel have been training and advising Philippine forces primarily fighting the Abu Sayyaf group but also those involved in episodic conflict with the Moro National Liberation Front (MNLF) and Moro Islamic Liberation Front (MILF).

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 reduction in the number of Abu Sayyaf fighters from 1,200 to 300 is in part attributed to SOF counterterrorism and counterinsurgency activities against Abu Sayyaf and MNLF. However, peace-brokering efforts by the Malaysian government and the Organisation of Islamic Cooperation (OIC) and persistent negotiations between the Philippine government and MILF also contributed significantly to a gradual reduction in insurgency violence.

The March 2014 signing of the Comprehensive Agreement on Bangsamoro, the final peace agreement signed between the government of the Philippines and MILF, is highly likely to have given the US administration the confidence to drawdown SOF in the country. Furthermore, the April signing of the Enhanced Defence Cooperation Agreement, a US executive to Philippine executive agreement as opposed to a formal treaty, provides rotational stationing of US troops and private contractors in the Philippines.

With the geopolitical context of Philippine-US military cooperation shifting from counterterrorism to maritime security and natural disaster response it is unclear whether the presence of SOF or conventional forces will be prioritised. It would be difficult from an operational and resource perspective for the US Special Operations Command (USSOCOM) and military planners to deploy SOF for natural disaster response and maritime security. SOF deployment for these operations would most likely be considered 'operational overkill'. Within the boundaries of US military spending priorities, it is more likely for conventional US forces to be assigned maritime security and natural disaster response roles.

Other developments

The initial deployment of 300 US special operation forces to Iraq for advisory and support roles will be bolstered by a second deployment of US armed forces to protect the US embassy and Baghdad International Airport. This will bring the total US deployment to 770 authorised troops. The Pentagon is increasingly fielding questions about 'mission creep' and the mission objectives for the SOF advisors. Members of the SOF community have suggested that the only effective role for the Joint Special Operations Command (JSOC) contingent would be to work as a targeting cell, though such a function would clearly cross over into a combat role. Even with improved signals intelligence and intelligence, surveillance and reconnaissance (ISR) from drones, JSOC are likely to be challenged by any requirement to only target the Islamic State of Iraq and the Levant (ISIS) and avoid other Sunni groups taking up arms against Baghdad. The tactical requirement to try to avoid Sunni groups and primarily focus targeting on ISIS is in order to not compromise political efforts to draw Sunni leaders into a more inclusive Iraqi government.

Special operations trainers from the Iranian Islamic Revolutionary Guard Corps' Quds Force and Hezbollah's Unit 3800 are thought to be providing advice and support to Iraq's armed forces and potentially Shiite militias to help halt any southward expansion by ISIS and Sunni militias. Some media outlets have reported that the Quds Force commander, Qassem Suleimani, arrived in Baghdad in late June and is playing a dominant role in shaping Iraq's security posture against ISIS. Prior to 2008, Quds Force trainers provided support to a number of Shiite militias, including the Mahdi Army, participating in ongoing sectarian violence in post–Saddam Iraq. It remains to be seen the degree to which Suleimani will draw upon the militias as opposed to the Iraqi armed forces, given the increased involvement of Shiite militias may trigger greater sectarian violence.

The secretary general of the Collective Security Treaty Organisation (CSTO) announced in late June that the organisation was creating joint special operation forces to thwart cyber-attacks. The purpose of the SOF collaboration is to counteract cyber-attacks and use special means to intercept signals and information messages, and may involve information and psychological operations subdivisions. CTSO preeminent member, Russia, is highly likely to be using this announcement as strategic counter-response to recent NATO cyber-preparedness activities reinvigorated by the Russian occupation of Crimea and Russian cyber campaigns against Ukraine.

Also of note

- **UK special forces are key recipients of increased and reassigned funding** announced by Prime Minister David Cameron in mid-July. Cameron stated 'it is not massed tanks on the European mainland we need, but the latest in cyber warfare, unmanned aircraft technology and Special Forces capability'.[1]
- **Army Lieutenant General Joseph Votel has been nominated by President Obama to replace Admiral William McRaven as Commander of US Special Operations Command**. In 2011 Votel took over the Joint Special Operations Command from McRaven who was promoted after Operation Neptune Spear killed Osama bin Laden.
- **Canadian Special Operations Forces Command (CANSOFCOM) plans to procure 17 armoured marginal terrain vehicles valued at $60 million were cancelled in July.** Military representatives suggested that the cancellation would not have an impact on CANSOFCOM capabilities despite the current fleet of BV-206s used for northern operations being over 30 years old.
- **USSOCOM entered into a $32.6 million agreement in early July with Airbus Defence and Space** for satellite communication services, including Inmarsat Broadband Global Area Network.
- **US state department has indicated that it may look for a new location for the 2015 Cobra Gold military drills** due to be held in Thailand. The drills involve multilateral SOF engagement and training. The announcement in late June is one of the many actions the United States has taken to express its objection to the military coup in Thailand.
- **Bulgarian special operations forces participated in landing drills with the US military codenamed Thracian Summer 2014 in July.** The drills were focused on low-altitude deployment of troops and cargo.
- **A War is Boring post on Somalia's counterterrorism force, the Gaashan, has revealed the likely nature of CIA and US SOF training of elite Somali soldiers to combat al-Shabaab on the streets of Mogadishu.**[2] The Gaashan, and its component unit Alpha Group (Danab), appear to have developed skills in SOF intelligence techniques and tradecraft, including Sensitive Site Exploitation. There are apparently 120 US personnel in Somalia in training roles.

[1] http://uk.reuters.com/article/2014/07/14/uk-britain-defence-idUKKBN0FI16I20140714

[2] https://medium.com/war-is-boring/american-commandos-secretly-training-the-new-somali-army-861e0f87cd86

Private military and security companies

Audit finds that one employee of private background check provider reviewed over 15,000 security clearances in a single month

A recent report by the inspector general of the US Office of Personnel Management (OPM) has found that an employee at US Investigations Services (USIS), which is contracted by the US government to review federal security clearances, had reviewed 15,152 cases in a single month during 2013.[3] As a result, the private background check provider has come under fire, as this number is considered highly abnormal: given a 40-hour week, it would mean that the employee had reviewed 1.5 cases per minute. The incident is gradually gaining attention because USIS also happens to be the company that processed and cleared Edward Snowden's application to work for the NSA.

Overall, USIS is mandated by the OPM to ensure that individuals applying for sensitive federal jobs have the required loyalty and integrity for such security-sensitive jobs. USIS personnel thus review material collected in previous investigations on applicants and determine whether they can be given security clearance. USIS is primarily contracted to ensure that the correct data was put together for a given applicant's file to be reviewed. The company's impressive yet hardly believable speed at which they processed security clearances is thought to be largely the result of the company trying (unsuccessfully) to meet tight official requirements and deadlines. In fact, the US Congress requires that 90% of clearance cases be processed within 60 days, mostly to ensure that applicants do not wait too long before obtaining their clearance and therefore being able to work effectively.

This latest development raises questions over the USIS' standards and work ethics, which further weakens the company's credibility and legitimacy following a January justice department filing that accused the company of defrauding the US government through fictitious quality data reviews during March 2008 to September 2012. While the justice department accused USIS of being motived by greed, the company stated that the incident was the work of a small group of individuals and that its new leadership would ensure that this sort of issue did not occur again.

It is clear that USIS will face difficulties improving its public image after this series of events, particularly that it is also held partly responsible for the Snowden case. Moreover, USIS' tarnished image inevitably risks casting doubt yet again over the US government's choices when it comes to hiring and overseeing private contractors for security-related jobs.

[3] http://www.opm.gov/our-inspector-general/reports/2014/audit-of-the-federal-investigative-services-case-review-process-over-background-investigations.pdf

Other developments

Former Blackwater employees have provided their accounts of the 2007 shootings in Nisour Square in Baghdad, which left 17 Iraqis dead. The contractors have been giving evidence in the trial of three of their former colleagues charged with manslaughter and a fourth charged with murder (a fifth guard has already pleaded guilty to manslaughter). Previous testimonies have included Iraqis accusing the Blackwater contractors of the killings and confronting them in court. Overall, the trial is providing insights into the atmosphere among Blackwater personnel in Iraq at the time. The Nisour Square killings are reported to have dramatically affected the atmosphere and trust among some of the contractors. The guards are accused of firing at unarmed civilians without provocation. The defence team has argued that the guards were shot at and returned fire fearing for their safety, while generally being on edge during what was one of the Iraq war's most violent periods.

Draken International is due to buy up to 28 Aero Vodochody L-159E multi-role combat aircraft from the Czech ministry of defence. Draken is a US provider of tactical fighter aircraft for contract air services, including military and contract customers. The aircraft have been in long-term storage, as they were unneeded surplus to the Czech air force. Draken also announced a strategic partnership with Aero Vodochody in which the Czech aircraft company will maintain aircraft at Draken's Florida facility and Draken will exclusively market the L-159 and future derivatives to customers in North and South America. Officially, spokespeople on both sides have stated that the deal, which was negotiated over a period of 18 months, represents effective cooperation between the Czech and American defence industries. Yet the deal may signify a wider commercial move by Draken to further penetrate European defence markets. The recently acquired L-159s are likely to be delivered soon to a Europe-based facility, in view of Draken's reported desire to expand its client base among NATO countries.

RT has reported that deputies from the Liberal Democratic Party of Russia have drafted a new law on the use of private military contractors for the Pskov regional legislature in northern Russia.[4] The lawmakers claim that capable and specialised companies are necessary to enforce national interests in cases when international politics or law prevent the government from using regular military forces. They point out that British and American PMSCs solve many foreign policy problems for Western governments, as well as bringing in additional taxes to their national economies. The current Russian criminal code directly bans the organising of or participation in non-state armed groups, and the federal law on weapons needs to be changes to allow military contractors to buy and use firearms and military hardware. However, the regional legislature is unable to pass the law by itself, and United Russia is thought to be preparing its own bill on private military companies together with the ministry of defence and the ministry of interior.

Also of note

- **The Civilian Extraterritorial Jurisdiction Act introduced by Representative David Price and Senator Patrick Leahy aims to increase accountability for contractors and government employees overseas.** If passed by the US Congress, it would address and close existing loopholes concerning prosecution for acts committed while working abroad. This would effectively result in contractors being held more accountable under US law.

[4] http://rt.com/politics/168904-russia-private-military-companies/

- **The US Department of Labor has released new data in line with the US Defence Base Act.** Under the US Defence Base Act, US defence contractors are compelled to be transparent regarding war zone deaths and injuries among their employees, which also include foreign workers and sub-contractors. The data is publicly available and accessible through the University of Denver's Private Security Monitor.[5]
- **Private security companies are in high demand in Kenya since last year's al-Shabaab attack on the Westgate shopping mall in Nairobi.** Many private security companies report a substantial increase in demand for their services from hotels, businesses and residential property management firms. Private security companies suggest their role will continue to be important even if the threat from al-Shabaab diminishes because of ongoing security concerns due to local criminal gangs and politicised violence.
- **G4S has confirmed that it will end its all its Israeli prison contracts within the next three years.** The move may have been triggered by increased activism, which saw G4S's annual general meeting disrupted by protests. However, it is highly likely that the company's decision was driven by fear of further reputational costs for the company, following important investors recently selling their stocks in the company.

Unmanned vehicles and autonomous weapon systems

Eminent task force delivers detailed report examining US drone policy

The Stimson Center's task force on unmanned aerial vehicle (UAV) policy released its report offering a holistic framework for US drone policy on 26 June.[6] The task force was made up of 10 senior-level participants from stakeholder constituencies, including the US military community, the intelligence community, the legal community, academia and the private sector. If adopted, its recommendations would represent a significant change in US drone policy.

A number of the recommendations, such as transferring responsibility for the drone programme from the CIA to the military, development of an independent commission to review lethal use of unmanned combat air vehicles (UCAVs) and greater after the fact public disclosure on UAV strikes, are reforms civil society groups have been pushing for over the last five years.

The report may represent the most significant questioning of US drone policy by former executive branch officials. The recommendation that US drone strikes for counterterrorism be subject to a strategic review and cost-benefit analysis, when read in the broader context of the report, indicates parts of the US military and security establishment have significant concerns about the potential ramifications of US drone policy.

The Stimson Center's report may provide the US administration with an important opportunity to review its drone policy and the impetus to advocate norms around the use of UAVs on an international stage. However, the Washington is also likely to be concerned that a review of drone policy may also generate pressure for reconsideration of the 2001 Authorization for the Use of Military Force (AUMF) passed by Congress after 9/11 attacks, which has been used to justify targeted killings in Pakistan and Yemen.

[5] http://psm.du.edu/articles_reports_statistics/data_and_statistics.html

[6] http://www.stimson.org/books-reports/recommendations-and-report-of-the-stimson-task-force-on-us-drone-policy/

The advantages the United States has enjoyed through the early adoption of UAV technology are diminishing as UAV technology rapidly proliferates. Furthermore, public concerns around UAV strikes as a counterterrorism strategy have significantly increased with mounting evidence of civilian deaths. As other countries develop or import UAV technology, the United States is turning to 'norms creation' around UAV use. US national security interests may be threatened by other state and non-state actors adopting the same legal, ethical and operational UAV policy as the United States has so far enacted.

Other developments

Al-Qassam Brigades, the military wing of Hamas, announced in mid-July that it has three UAV variants (armed, surveillance and attacking suicide mission) called Ababil-1. These were likely procured from Iran. Al-Qassam Brigades claimed that it had carried out three missions on 14 July, with one test mission being flown over the Israeli ministry of defence building in Tel Aviv, though the fact that on board weaponry was not used during this flight may suggest it does not have the full capability to carry an explosive payload. The Israeli Defence Force (IDF) reported on 14 July that they had shot down a UAV, possibly an Ababil-1, with a Patriot surface-to-air missile near the coastal city of Ashkelon. The IDF has previously intercepted Hezbollah UAVs from Lebanon with air force air-to-air missiles.

In addition to having Quds Force trainers on the ground, Iran are also flying UAV surveillance missions over Iraq based from Baghdad airfields. Deployment of Iran's fleet of surveillance drones in Iraq will provide an active demonstration of the technical advancement of Iran's fleet, though it is unclear if armed UAVs will be used. The vast majority of US UAVs in Iraq are thought to be unarmed, though some are armed with Hellfire missiles, particularly those near Baghdad airport and the US embassy. Coordination between the United States and Iran of UAV surveillance activities is highly unlikely.

A series of *Washington Post* articles in late June exposed the number of US drone crashes internationally and on United States' soil.[7] One article indicates that 47 Class A major crashes occurred in the United States between 2001 and 2013 according to data from the US armed forces. This figure likely underestimate the total number of crashes, as Class A incidents are crashes that inflicted at least $2 million in damage to the aircraft or other property. All major models of US drones, including the RQ-4 Global Hawk, Reaper and Predator, have reportedly crashed within the United States, though Predator flights over civilian areas are limited in the United States due to its reduced reliability. Internationally the United States has lost over 400 drones in major accidents since 2001. In the last 12 months alone, two Predator drones have crashed into the Mediterranean Sea after coolant failure issues.

Also of note

- **UN High Representative for Disarmament Affairs Angela Kane identified a number of emerging issues around autonomous weapons systems in a report to the Advisory Board on Disarmament Matters (UN Office of Disarmament Affairs)** and encouraged the board to make a contribution to the ongoing discussion around lethal autonomous weapons systems and the implications for international humanitarian law.[8]

[7] http://www.washingtonpost.com/sf/investigative/2014/06/20/when-drones-fall-from-the-sky/ and http://www.washingtonpost.com/sf/investigative/2014/06/22/crashes-mount-as-military-flies-more-drones-in-u-s/

[8] https://s3.amazonaws.com/unoda-web/wp-content/uploads/2014/07/FINAL_HR_Remarks_ABDM_62_2-July-2014.pdf

- **The French and British defence ministers signed a two-year agreement to work on the feasibility phase of a new jointly-developed unmanned combat air vehicle.** The UCAV study is part of a broader Future Air Combat System, which envisages deploying F-35 Joint Strike Fighters alongside UCAVs.
- **The US defence industry is seeking relaxation of export controls on UAVs** and arguing that the application of the Missile Technology Control Regime (MTCR) is leading to perverse outcomes for companies. The US state department has acknowledged that UAVs require deeper consideration, but for the moment export of UAVs is considered on a case-by-case basis taking into account Conventional Arms Transfer policy and international obligations such as the MTCR.
- **An updated version of the Predator UAV, the Predator XP, made its first flight at the US Army's Yuma Proving Ground Range Complex in Arizona on 27 June.** The upgrades include an automatic takeoff and landing system, improved video capture and imagery analysis software and an automatic identification system for maritime vessels.
- **UN use of UAVs for ISR in the Democratic Republic of the Congo and Mali continues to receive strong media coverage,** including the revelation that the South Sudanese government has refused the UN permission to fly UAV ISR missions over its country. Attention is now turning to how data collected from UAV ISR missions is shared with host governments, war crimes tribunals or the UN Security Council.
- **Taiwan's army is reportedly flying a new fleet of 32 commissioned UAVs** from of the country's east (Taitung), with the aim of monitoring the southeastern coastal areas of China.
- **Results from the Pew Research Center's Global Attitudes Project suggests that despite widespread opposition to US drone strikes and mass surveillance** only limited reputational harm has been inflicted on the United States in eyes of survey respondents.[9]
- **US European Command and NATO completed joint, long range ISR activities (United Vision 2014) with Global Hawk UAVs and alliance ground surveillance systems in early July.** The exercise was aimed at improving the interoperability of ground surveillance assets and UAVs.
- **BAE scientists claim that 3D printers could be so advanced by 2040 that they could produce small UAVs.** The scientists also suggested that technological advancement in UAV technology could involve dissolving circuit boards to prevent enemies from reverse engineering UAV technologies.
- **The University of Birmingham has built the world's first ever robot security guard.** Named Bob, the first robot security guard was built as part of a £7.2 million ($12.3 million) project called STRANDS, which works towards making robots act intelligently and independently in real-world environments. Bob the robot is able to independently scan and monitor rooms, as well as reporting any movement or abnormal changes back to its human superiors.

[9] http://www.pewglobal.org/2014/07/14/global-opposition-to-u-s-surveillance-and-drones-but-limited-harm-to-americas-image/

Cyber warfare

Significant malware distribution and network monitoring on rise across Iraq

Significant malware distribution and network monitoring is on the rise across Iraq according to a report by Intercrawler, a US cyber intelligence company. Specifically, the popular remote access tool njRAT, commonly used against Syrian opposition rebels, appears to being used widely across Iraqi internet service provider (ISP) networks. The trojans and malware are distributed via malicious web links, most likely embedded in political material on social media, and are likely being used to execute screen grabbing and key logging activities. In addition to the remote access tools, analysts have noted a surge in use of the TOR anonymity network in Iraq over the last few weeks, with internet users trying to hide their ISP addresses when undertaking malicious activities.

The increase in malware and the broad distribution of njRAT raises the question of whether state-sponsored actors are involved, using cyber tools to either disrupt Islamic State of Iraq and the Levant (ISIS) communications or gather intelligence of the militant group's movements. There is the possibility of Syrian Electronic Army involvement in cyber-attacks on ISIS for the purpose of gathering intelligence on behalf of the Syrian and Iranian governments. However, this raises the further question of how such intelligence, gathered through RATs, would be used by state actors, such as Iraq or Iran. For Iran, it is unclear whether the intelligence gathered through cyber operations is as actionable as ISR obtained via UAV flights over northern Iraq, with the implication that the allies cannot rely solely on cyber operations for ISR. Alternatively, the attacks could be directed at hampering ISIS communication and information operations, which have garnered significant global attention recently.

While ISIS have already demonstrated relatively sophisticated and coordinated use of social media for information campaigns, their capacity to defend and launch cyber-based attacks, distributed denial-of-service (DDoS) attacks and malware is not clear. Hackers associated with Anonymous issued an online warning that governments, such as Saudi Arabia and Qatar, who have or continue to support ISIS would find their government websites defaced by Anonymous hackers and subject to DDoS attacks. However, a few days after the announcement of Anonymous's Operation NO2ISIS, the twitter account @anonmessage was allegedly hacked by ISIS and used to spread militant propaganda and videos.

An Anonymous hacktivist told media outlets that the techniques used to gain control over the twitter account were similar to those used by the Syrian Electronic Army. Despite Anonymous inferring a link, it is unlikely SEA would provide any assistance or have any affiliation with ISIS. It is more likely that ISIS is adopting cyber tactics employed by SEA and leveraging publicly available tools.

Other developments

US officials have recently been openly discussing cyber warfare threats. The commander of US Cyber Command (USCYBERCOM), Admiral Michael Rogers, told an international cyber symposium hosted by the private Armed Forces Communications and Electronics Association on 24 June that 'this nation [the United States] will see either from another nation state or from a group or set of individuals, efforts designed to cause destructive cyber impacts against critical U.S. infrastructure.' Rogers, who is the director of the NSA, also discussed the offensive cyber capacity of Russia and China and the challenges of integrating cyber operations with kinetic military strikes, intelligence collection and domestic law enforcement. Days earlier at a Senate Appropriations Committee subcommittee on defence hearing, US defence secretary Chuck Hagel officially confirmed that the United States believed Russia had used offensive cyber operations during their annexation of Crimea. The level concern over hostile cyber capabilities is evident in the US state department's International Security Advisory Board draft report on international cooperation on cyber security, which reveals a US administration seeking the development of international norms and treaty obligations.[10]

NATO is updating its cyber defence policy to clarify that major cyber-attacks on member states could be covered by Article 5 of the North Atlantic Treaty, the collective defence clause. The policy change will be put to the Wales summit in September. The policy does not clarify the threshold that a cyber-attack would need to reach to be covered by Article 5 or what the NATO response would be, allowing NATO allies to determine the response on a case-by-case basis. The key principle to be established in the policy is that a certain intensity of cyber-attack and malicious intention could be treated as the equivalent of an armed attack. The policy update is guided in part by the work of 20 experts who examined the application of the laws of armed conflict to cyber warfare and produced a report titled the *Tallinn Manual*, published in April 2013.[11] The cyber dimensions of recent conflicts, including in Ukraine, and previous cyber operations in Estonia and Georgia have driven demand for the cyber defence policy.

New reports are emerging that cyber espionage campaigns against Western energy utilities are continuing and now provide attackers the ability to mount sabotage operations against their targets. Symantec have produced a report on the Energetic Bear (aka Dragonfly) cyber campaign against the industrial control systems of energy grid operators, major electricity generation installation operators and petroleum pipeline operators in the United States, Italy, Spain, France, Germany, Turkey and Poland.[12] At present, it appears that data collection was the primary objective; however it is clear Energetic Bear also allowed for sabotage operations. Due to the sophistication of the attacks, Symantec has speculated that there was state-sponsorship of these cyber activities. Based on the hours of operation, evidenced from malware timestamps, Symantec suggests that the attacks likely originated in Eastern Europe.

[10] http://insidecybersecurity.com/iwpfile.html?file=jul2014%2Fcs2014_0138.pdf

[11] http://www.knowledgecommons.in/wp-content/uploads/2014/03/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf

[12] http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

Also of note

- **The US administration has alleged Chinese hackers gained access to the Office of Personnel Management databases.** The databases include personal and security clearance information on US federal employees.
- **In early July, the US department of defence (DoD) launched a joint taskforce to investigate how the DoD information network (DoDIN) can be defended against cyber-attacks** and how information can still be shared across multiple agencies. The Pentagon's Missile Defence Agency is also examining cyber risk to missile guidance systems, such as radar satellites and sensors
- **Japan's government is evaluating options to address the increasing number of cyber-attacks on critical infrastructure.** According to Reuters, the country's first cyber security white paper released in early July indicated that there were 5.08 million cases of irregular access to central government information systems, including outright cyber-attacks, up from 1.08 million cases the previous year.[13] While the increase is in line with global trends, Prime Minister Shinzō Abe's intention to build a cyber security strategy headquarters shows an increasing concern in Tokyo over cyber threats, particularly from North Korea and China.
- **CrowdStrike have identified another Chinese hacking unit with alleged links to an unnamed Chinese government official.** Dubbed by CrowdStrike as 'Deep Panda', the group is alleged to have hacked US targets with specific Asian geopolitical expertise and subject matter knowledge for years and more recently started targeting US think tank specialists on Iraq. Deep Panda interest in documents on Iraq might stem from extensive Sino interests in Iraqi oil production, with China being the largest foreign investor in Iraq's oil sector.
- **The French ministry of defence is setting up their own cyber security training course to develop its own experts.** The ministry has been unable to compete with the private sector to secure cybersecurity specialists for the French military.
- **The Centre for International Governance Innovation (CIGI) released a paper on global cybercrime and the interplay of politics and law.**[14] The paper examines the application of domestic law to international cybercrime, drawing on the recent US indictment of five Chinese nationals for cyber espionage.
- **The North Korean military announced in early July that it has nearly doubled its number of cyber warfare personnel over the last two years,** with approximately 5,900 personnel working in the General Bureau of Reconnaissance. The North Korean military spokesperson also suggested that some elite cyber warfare personnel were based in other countries, including China.
- **The British government's Centre for Defence Enterprise and Defence Science and Technology Laboratory has announced a September networking conference for defence science and technology providers.** One of the competitions to be launched will be a fully-funded contract for automation of cyber defence responses.

[13] http://uk.reuters.com/article/2014/07/10/uk-japan-cybersecurity-idUKKBN0FF1PL20140710

[14] http://www.cigionline.org/sites/default/files/no8_1.pdf

Intelligence, surveillance and reconnaissance

British parliament passes 'emergency' data retention and surveillance legislation

The United Kingdom's three major political parties have supported legislation that requires telecommunication companies to retain customer metadata for 12 months and reasserts the application of data interception obligations on overseas communication services providers delivering services to British citizens. The UK government argue that the Data Retention and Investigatory Powers Bill is an emergency response to the European Court of Justice (ECJ) ruling in April that invalidated a 2006 EU directive allowing telecommunication companies to store customer metadata for up to two years. The ECJ held that the directive disproportionately interfered with the fundamental rights of privacy and protection of personal data.

The rapid passage of the Data Retention and Investigatory Powers Bill comes amid rising concerns over the capacity of the security services to monitor British fighters returning from Syria and Iraq and expectations of critical findings from the Intelligence and Security Committee's report into the murder of soldier Lee Rigby in London in May 2013. The British government argues that the establishment of a Privacy and Civil Liberties Oversight Board to scrutinise surveillance activity and a sunset clause of December 2016 on the legislation allows the government to respond to these issues while maintaining the necessary oversight and privacy safeguards. The application of the legislation to overseas telecommunication service providers is particularly contentious for ISP companies who have had their network assets compromised by GCHQ monitoring and data interception. Seven ISPs based in six countries have filed claims with the UK Investigatory Powers Tribunal (IPT) alleging GCHQ uses malware to intercept communications across their networks. GCHQ has previously argued that UK citizens accessing foreign servers is deemed external communications and can be monitored without the need for individual warrants.

The British legislation is the latest in a series of legislative reforms under consideration across the Five Eyes jurisdictions. Most of the jurisdictions are tying the review of existing arrangements that facilitate some form of bulk collection with rising concerns over returning fighters from Syria and Iraq. Worryingly for civil liberty campaigners, the safeguards offered as counterbalance to increasing intelligence collection in a particular jurisdiction may be overcome by the signals intelligence sharing arrangements between the Five Eye partners, which may enable other states to fill in the intelligence gaps of domestic jurisdictions.

More widely, the UK government's increasing focus on ISR and cyber capabilities is clearly evidence by Prime Minister David Cameron's announcement of £1.1 billion package 'to equip armed forces for the conflicts of this century, not the last', which includes an over £800 million boost to British intelligence, surveillance, and cyber capabilities.

Other developments

British and US intelligence agencies are investing in new information operation capabilities, particularly across social media platforms, as a way to shape public opinion and sentiment. Documents leaked by former NSA contractor Edward Snowden show that the UK GCHQ's Joint Threat Research Intelligence Group (JTRIG) has developed a number of information operation applications. The applications provide GCHQ with the ability to manipulate and alter information presentation across social media platforms, block email and website access, covertly record real time Skype conversations and retrieve private Facebook photos. The US department of defence's military research arm, the Defense Advanced Research Projects Agency (DARPA), pre-emptively released information on its Social Media in Strategic Communication (SMISC) programme after revelations about Facebook's 'emotional contagion' news feed experiment and the JTRIG applications.[15]

The US Privacy and Civil Liberties Oversight Board (PCLOB) released its second report into NSA surveillance activities in early July focusing on electronic surveillance under Section 702 of the Foreign Intelligence Surveillance Act (FISA).[16] The first report focused on the domestic telephone metadata collection programme under Section 215 of the USA Patriot Act. The new report attempts to make a clear distinction between the bulk metadata collection programme and the 702 programme, which involves the collection of telephone calls and emails where the target is reasonably believed to be a non-US person located outside of the United States but can include US citizens communicating with non-US targets. The US government board identified a number of issues with NSA targeting policies and practices and accepted that information was incidentally collected on non-target individuals. Most importantly, the PCLOB recommended changes to the procedures and practices of the NSA in searching the 702 programme database for non-target names and phone numbers, which could constitute a form of 'backdoor wiretap'.

Revelations in July that US intelligence agents based in Germany were purchasing information on a parliamentary investigation into Snowden leaks from a low-level German intelligence agent have reignited diplomatic tensions between the United States and Germany. This is likely to lead to a reinforced German counter-espionage policy towards allies such as France, Britain and the United States. Berlin is likely to invest in greater monitoring of the allies' listening posts in Germany. More immediately, the German government has expelled the CIA station chief in Berlin. These developments have reignited diplomatic tensions between the two countries at a time when the fallout from the NSA's tapping of Chancellor Angela Merkel's mobile phone was gradually abating. Adding to the diplomatic tension, the German interior ministry announced the cancellation of a contract with US telecom company Verizon amid concerns over the security of signals, data and information moving through Verizon systems and hardware, and the German federal prosecutor announced an investigation into the NSA's hacking of Merkel's phone. While some commentators suggest the theatrics of the diplomatic row are in part a face saving activity for Germany, the cancellation of the Verizon contract may indicate that a deeper distrust has set in.

[15] http://www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2147488011

[16] http://www.pclob.gov/All%20Documents/Report%20on%20the%20Section%20702%20Program/PCLOB-Section-702-Report.pdf

Also of note

- **The most recent set of NSA documents leaked by Edward Snowden revealed the NSA RAMPART-A programme, a $170 million programme aimed at installing data interception equipment on strategic fibre optic cable choke points.** The programme involved the NSA entering into third party access agreements with 30 countries, including all Five Eyes partners, and multilaterals, such as NATO, to install the interception equipment. Under the arrangements, host nations agreed to not access the equipment to monitor US citizens and the NSA agreed to not monitor the host's domestic citizens. However, by securing broad international network coverage, these prohibitions became irrelevant.
- **US diplomats were in New Delhi, India, in early July to manage agitation over the NSA's surveillance of the Bharatiya Janata Party (BJP)** and to ensure historical surveillance activity will not hinder future bilateral relations. The BJP was one of six political organisations identified in a 2010 US Foreign Intelligence Surveillance Court (FISC) order as subject to NSA surveillance.
- **A German media outlet revealed allegations that the NSA monitors nine key servers running the anonymity network TOR** and have digital fingerprinting capabilities to monitor those visiting the TOR browser or Tails privacy-orientated operating system websites through their XKeyscore surveillance system. Those visiting these websites or using the TOR browser are placed on an NSA inspection list for targeted surveillance.
- **NSA director Admiral Michael Rogers suggested in an interview with the *New York Times* that while the Snowden leaks have meant some groups have enhanced their counter communication surveillance techniques, the 'sky is not falling'.**[17] Rogers' comments stand in stark contrast to his predecessor, General Keith Alexander, who said the Snowden leaks caused 'the greatest damage to our combined nations' intelligence systems that we have ever suffered'.
- **A report by Intercept revealed that the NSA and FBI monitored the emails of five prominent US activists and attorneys with Muslim backgrounds,** and that the NSA intelligence reports employed highly racist language.[18] The White House has requested that the intelligence agencies review training standards and policies.

Commissioned by the Remote Control Project
remotecontrolproject.org

[17] http://www.nytimes.com/2014/06/30/us/sky-isnt-falling-after-snowden-nsa-chief-says.html

[18] https://firstlook.org/theintercept/article/2014/07/09/under-surveillance/

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