Remote-control warfare briefing | #10

23 March 2015

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 produced by **Open Briefing** and commissioned by the **Remote Control** project, a project of the Network for Social Change, hosted by Oxford Research Group.

Special operations forces

Key countries in Middle East and North Africa contemplating special operations forces deployments against Islamic State

On 25 February, the defence attaché at the Jordanian embassy in Washington DC, Princess Aisha bint Al Hussein, told the Global SOF Symposium in Florida, United States, that the responsibility for confronting terrorism in the name of Islam lies with Muslim countries, and not just those of the Arab world. Hussein stated that the recent immolation of Royal Jordanian Air Force pilot Muath al Kasasabeh has only served to unite the Hashemite kingdom in its fight against extremism. Hussein's speech comes as some key governments in the Middle East and North Africa are becoming more concerned about the regional threats posed by Islamic State (IS). Jordon faces the challenge of an estimated 1,500 nationals fighting with IS. Saudi Arabia has an estimated 2,000 to 2,500 nationals fighting with the group. Morocco and Tunisia have similar numbers.

Islamic State's identification of the House of Saud and the country's wealth and assets as a legitimate strategic target based on claims of apostasy has also encouraged the Gulf state and its neighbours to take a more defensive posture. In January, Saudi nationals fighting with Islamic State crossed the border from Iraq and killed a Saudi general and a border guard. The event resulted in Saudi Arabian special operations forces (SOF) undertaking large-scale border protection exercises and sustained border surveillance. Special forces have also increased training drills to prepare to respond to returning fighters initiating domestic attacks.

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

In mid February, an IS-affiliated group in Libya released a video in which it executed 21 Egyptian Coptic Christians. Egypt's president, Abdel Fatah al-Sisi, made a national address arguing that the country had a right to respond to the murders, including through concentrated airstrikes on Islamic State and their weapons storage facilities in Libya. An unidentified Egyptian military official noted that serious consideration was also being given to sending Task Force 999, a special operations and reconnaissance unit, into Libya.

In March, Kuwait is hosting a multilateral military training exercise, Eagle Resolve. A range of special and conventional forces involved in airstrikes on Islamic State as part of the Combined Joint Task Force-Operation Inherent Resolve are participating in Eagle Resolve. The exercise is based on agreements signed in 2013 to improve the cooperative defence efforts of the Gulf Cooperation Council and US Central Command (CENTCOM), and according to US officials it is not related to current engagements in Iraq and Syria. However, it is likely that scenarios within the current exercise are based on counterterrorism strikes.

CENTCOM has signalled the importance of Muslim countries, like Qatar, Saudi Arabia and Jordan, contributing to efforts to confront Islamic State. The visible participation of MENA partners has become an important aspect of the Obama administration's rhetoric and political position on US engagement in Iraq and Syria. Significant special forces deployments from regional powers also have the potential to reduce the likelihood of conventional US ground forces being required. However, for a range of geopolitical and domestic political reasons, allies such as Jordon prefer an atmosphere of ambiguity and plausible deniability around the extent of their special forces deployments. This stands in contrast to the commander of Iran's elite Quds Force, General Qassem Soleimani, who takes a highly-visible role in the operations room for the battle of Tikrit in Iraq.

Other developments

In early March, Australian Prime Minister Tony Abbott announced he would send 300 troops to train and support Iraqi forces in Taji district, northwest of Baghdad. New Zealand is also sending 140 troops alongside the Australian contingent, though the forces will not be operating under an ANZAC badge. Australian special operations forces, who have been training Iraqi counterterrorism forces, are to be withdrawn in September. It appears the focus now will be on conventional forces supporting Iraq's regular forces to take and hold ground. Unlike for the United States and Canada, the deployment of conventional forces by Australia and New Zealand has not raised significant political dispute around mission creep. While the Australian Labor Party opposition has conditioned its support on ground forces not being actively deployed to combat zones, it is highly likely these conventional forces will become involved in combat engagements, as has been the case for Canadian special forces through January and February. In contrast, Canada's defence minister, Jason Kenney, told the House of Commons defence committee that the Canadian government has no intention of increasing the numbers of special operators in northern Iraq.

Chechnya's president, Ramzan Kadyrov, signalled plans for the republic to build an international special operations force training centre modelled on Jordan's Special Operations Training Centre by the end of 2015. Kadyrov indicated that the centre is being privately financed, and is expected to provide training services to Belarus and Kazakhstan, with the prospect of other ex-Soviet and Latin American countries also accessing the facility. Fellow United Russia party and defence committee member Timur Akulov underscored the Chechen Republic's experience with 'international terror' and knowledge of counter-terrorism tactics as a key drawcard for potential trainees.

On 9 March, over 1,000 special operations forces personnel from 29 countries finished training exercises as part of Exercise Flintlock 2015 in Mao, Chad. This year's US Africa Command-sponsored training exercise took on renewed relevance, as Boko Haram pledged allegiance to Islamic State on 7 March and is expanding its attacks across the Nigerian border into Chad, Niger and Cameroon. The exercise is just one element of ongoing efforts to build regional force cooperation and counter-terrorism expertise. While regional forces include the Chadian Army's Special Antiterrorism Group (SATG), with recent experience in Mali, and Cameroon's Israeli-trained Rapid Intervention Brigade (BIR), the *New York Times* reported on a leaked internal European Union assessment suggesting cooperation has so far been weak and may be limited in future.[1] Successful counter-terrorism efforts will require a degree of force interoperability in order to gain a tactical edge over Boko Haram; however, Western special force training partners, while providing a capability and skills boost, may not be able to facilitate interoperability from the outside. Major General James Linder of US Africa Command did announce in mid-February that the United States would be providing communications equipment to improve information exchange between regional partners. Limited confidence in the capability of regional forces to confront a Boko Haram insurgency seeking greater financial and weapons support from the other militant groups is likely to lead Western leaders, including US President Barack Obama, to increasingly characterise Boko Haram as an international threat.

Also of note

- **The US-based Global SOF Foundation released an advocacy and policy document, *Imperatives for 2015*, in March.**[2] Recommendations include sustaining or growing research and development on SOF-specific hardware and a broadening of the proposed Counterterrorism Partnership Fund's investment priorities for training partner counties beyond Iraq and Syria.
- **During an interview with the Combating Terrorism Center at West Point, Captain Robert Newson, a US Navy Seal who previously commanded Special Operations Command (Forward) in Yemen, delivered a strong critique of US counter-terrorism operations in Yemen.**[3] Newson stated that 'the "CT concept" – the solution that some people champion where the main or whole effort is drone strikes and special operations raids – is a fantasy. It may be cheaper and safer, but without broader efforts it is like mowing the grass in the jungle.'

[1] http://www.nytimes.com/2015/03/08/world/africa/african-training-exercise-turns-urgent-as-threats-grow.html

[2] http://globalsoffoundation.org/advocacy

[3] https://www.ctc.usma.edu/posts/a-view-from-the-ct-foxhole-an-interview-with-captain-robert-a-newson-military-fellow-council-on-foreign-relations

- **The United States Special Operations Command (USSOCOM) issued a request for information on urban warfare technology in early March.** The request is focused on technology required for unconventional warfare in Middle Eastern hotspots, and make reference to holographic field/area of interest visualisation and intelligence, surveillance and reconnaissance (ISR) tools feeding live social media analytics to anticipate group-level actions.
- **A member of the Canadian Special Operations Regiment was killed and three other soldiers injured in a friendly-fire incident on 7 March.** Iraqi Kurdish forces mistakenly fired on the Canadian forces as they were returning to an observation post.
- **Russian President Vladimir Putin issued a decree that Special Operation Forces Day will now be held on 27 February rather than in May.** The move is likely in honour of the date in 2014 that Russian special operations forces seized government buildings in Crimea and raised the Russian flag as part of Russia's military annexation of Crimea.
- **US special operations forces at RAF Mildenhall in the United Kingdom have increased personnel numbers and received delivery of CV-22 Osprey tiltrotor aircraft,** despite long-term US European Command plans to move US Air Force operations to Germany.
- **Japan's Technical Research and Development Institute has allocated $7.5 million of its 2015 budget to an exoskeleton research project,** Mobile Suit Gundam, which likely parallels US efforts on the TALOS suit.

Private military and security companies

Scandal over Sri Lankan 'floating armoury' highlights collusion between public and private sectors

The scandal over a former Sri Lankan defence secretary's 'floating armoury' has led a Sri Lankan court to ban him from foreign travel. Gotabaya Rajapaksa, who is also the brother of former President Mahinda Rajapaksa, is accused of maintaining his own private army with the floating armoury, stationed in the southern port of Galle. The police have seized more than 3,000 weapons from the armoury, which was operated by a Sri Lankan private security company, Avant Garde Maritime Services (Pvt) Ltd (AGMS).

AGMS describes itself as providing a 'comprehensive range of total risk mitigation solutions to the global maritime industry' and 'total logistical assistance to vessels transiting the Indian Ocean'.[4] The company has many senior Sri Lankan military commanders on its advisory board and management team. Controversially, it stores Sri Lankan government owned weapons and makes them available to maritime security guards working on ships operating around Sri Lanka. A standard issue from the company includes four AK-47 type assault rifles and 480 rounds of ammunition, together with ballistic helmets and body armour. AGMS also transfers and stores private military and security companies' own weapons. The practice of arming merchant ships has developed in the past decade due to the threat of piracy.

[4] http://www.avantmaritime.com/about_us

Although AGMS is a signatory of the International Code of Conduct for Private Security Service Providers (ICoC), floating armouries take advantage of weak international regulatory frameworks because they are only accountable to the state in which they are registered (also referred to as the flag state). Without better-established regulatory and legislative frameworks covering the use of private maritime security contractors, it is likely that such floating armouries will continue to flourish. Such armouries present a security risk in their own right, as they store large amounts of weaponry under varying degrees of security in close proximity to potentially fragile and conflict-ridden regions. Furthermore, these armouries risk increasing collusion between the private and public sectors, as seen in Sri Lanka. Indeed, Sri Lanka is particularly at risk because of its strategic location on one of the world's busiest sea routes.

Rajapaksa is accused of using the weapons to arm a private army, and local police say they have had complaints the firearms were used for intimidation. The Sri Lankan police are also investigating Rajapaksa over abductions, assaults and murders during his brother's time in office. The investigations are part of a wide probe of alleged corruption and repression by the former president and his relatives.

Other developments

The knife attack on the US ambassador to South Korea, Mark Lippert, has exposed the extent of the market for diplomatic security. The protection of diplomatic facilities and staff outside the embassy is the host state's responsibility, as countries are not supposed to deploy military forces into countries that host their diplomatic representation. However, the US Diplomatic Security Service shares diplomatic protection responsibilities with host states. Despite South Korea's strong record in protecting diplomatic assets on its soil, a militant Korean nationalist attacked Lippert with a knife, causing serious wounds to his face and arms. The Seoul attack occurred two years after the deadly siege in Benghazi, which resulted in the death of US ambassador J. Christopher Stevens. It is likely to cause questions to be raised over the Diplomatic Security Service's readiness, particularly in cases of unpredictable 'lone-wolf' attacks.

Such doubts over official diplomatic protection services are likely to provide increasing opportunities for private security contractors to fill a niche market. Indeed, the United States entrusted the life of the head of the Coalition Provisional Authority in Iraq, Paul Bremer, to the now notorious Blackwater. The Australian Department of Foreign Affairs and Trade has spent more than AUD $250 million on private military contractors in order to outsource the high risks associated with providing protection to diplomatic assets in volatile environments.

South African mercenaries are reportedly contributing to a series of successes in Nigerian security forces' efforts against Boko Haram. The presence of retired South African special forces operatives in Nigeria has been controversial, as mercenary activity is illegal under South African law. Moreover, South African defence minister, Nosiviwe Noluthando Mapisa-Nqakula, has pledged that South African citizens who participate in mercenary missions would be arrested upon their return, though the South African government does not officially acknowledge the military involvement of some of its citizens in Nigeria. Nigeria has been relatively isolated in its fight against Boko Haram, as the United States and the European Union have been reluctant to provide Nigeria with military assistance due to human rights concerns. On 12 March, it was reported that a former South African Defence Force soldier turned private security contractor, Leon Lotz, was killed in a friendly-fire incident in Nigeria's Borno State. Lotz was reportedly working for the Nigeria-based private security company Pilgrim Africa Ltd, which provides private armed protection against militant action. The company is owned by Cobus Claassens, a former member of the South African Army and the controversial private military company Executive Outcomes.

Recent developments in northern Iraq and Syria have generated a surge in volunteer military contractors and veteran soldiers going to offer their services in the fight against Islamic State (IS). While the US-led international coalition has mostly conducted airstrikes and reconnaissance missions, the Kurdish military forces, the Peshmerga, have been fighting Islamic State on the ground, expelling IS forces from key cities, such as Kobani, Mosul and Tikrit. The Peshmerga has attracted dozens of Western veterans, who state that they do not receive a salary but have joined the fight because they believe the radical group is a serious threat to international security. Many veterans from the wars in Afghanistan and Iraq, some of whom feel that they were misled by their own governments, particularly in Iraq, have been attracted to the fight against Islamic State, and perceive it as a clear case of good versus evil in which they can use their military training for the greater good.

Also of note

- **A UN report has revealed collusion between Yemen's disposed president, Ali Abdullah Saleh, and the Shiite Houthi militia, which recently toppled the government of his successor, President Abd Rabbuh Mansour Hadi.**[5] The investigation found that Saleh directly funded the Houthi militia and ordered his supporters not to stop the rebels when they attempted to seize control of Yemen's capital, Sana'a. Since Saleh's removal from power, militias and private security companies organised along ethnic lines have gradually taken over the monopoly on violence and security provision in Yemen.
- **The number of private police officers is on the rise in the United States.** A private police force is one owned and controlled by a non-state organisation; however, the lines between public and private police have become increasingly blurred, given that security guards rights, responsibilities and uniforms are often akin to those of public police officers. Indeed, many private security companies hire moonlighting police officers as guards.

[5] http://www.un.org/ga/search/view_doc.asp?symbol=S/2015/125

Unmanned vehicles and autonomous weapons systems

Proliferation of drones leads to calls for international regulation

In a new report, the US think tank the Rand Corporation has urged the United States to use its position as the world's leading manufacturer and user of armed drones to lay the foundations for new international law on the use of drones by state military and security forces.[6] The United States already sets stringent operating agreements for allied countries who purchase US-made unmanned platforms, setting strict limits on their use against their own citizens and requiring strenuous efforts to minimise collateral damage in combat operations. All sales also have to be compatible with US national and foreign policy interests.

The variety of drones available provides a wide-ranging menu of capabilities to governments. While many of these capabilities are benign (for example, traffic surveillance, crop monitoring or emergency assistance), covert/high altitude surveillance and weaponised capabilities are open to abuse by less altruistic regimes. Just 10 or so years ago, the United States enjoyed a global monopoly in this technology. Today, unmanned aerial vehicles are now available from a sizeable number of international sources, many of which might be less inclined to require such conditional agreements. Israel has already sold surveillance-only drones to 38 countries including Thailand, Angola, Nigeria and Ivory Coast (the latter in spite of UN sanctions). Armed drones have only been used in combat by the United States, United Kingdom and Israel, but other countries, currently unable to access to US vehicles, will be joining this list in the very near future. China already has the technology, but is yet to use it; Russia expects to have armed drones in service within five years; Iran claims to have an armed drone capable of reaching Israel; and India has at least one model in development.

There is already an international treaty governing exports of payload-capable drones, the Missile Technology Control Regime, but this is purely informal and only involves 34 countries, lacking Israel, China, Iran, Pakistan and India among other drone manufacturers. Unanimously agreeing the content of any new international protocol on drone deployment will no doubt be a complex affair. Negotiating agreements blocking exports to authoritarian regimes, which may use such technology to suppress opposition, will be particularly difficult with some countries.

Any agreements will need to be future-ready for this fast-moving technology. While surveillance drones are trusted with operating all-but autonomously, flying programmed routes with minimal input from a human operator, it will be some time before weaponised drones are granted with such independence from human control. High-confidence targeting and minimal collateral harm will no doubt be necessary prerequisites to deploying weapons. Both of these will require human input for some years. However, the technology will eventually become sufficiently capable, and military chiefs may come to argue for autonomous systems to be deployed, so they can expand offensive capabilities beyond the limitations of available manpower. In between these two models is the 'swarm' concept of multiple drones attacking multiple targets, but being flown (or maybe just monitored) by one pilot.

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

Other developments

Drones continue to be seen flying over key sites in Paris as a journalist is fined for unauthorised flights on the edge of the city. Tristan Redman, a journalist for Al Jazeera, was fined €1,000 after being caught flying a drone as part of a report, ironically, into the mystery drone flights that continue to puzzle French authorities. Remote-controlled aircraft have recently been reported flying over the US embassy, the Eiffel Tower, the Invalides military museum, the submarine communications base at Sainte-Assise to the south of Paris, the Bastille and Place de la Concorde in recent weeks, in addition to earlier sightings over the Elysee Palace and multiple nuclear power stations across France. A drone seen flying over the temporary *Charlie Hebdo* offices and near the newly re-opened Hyper Cacher supermarket (scene of the second January shootings) was pursued by police but lost due to heavy traffic. The drone was later seen being collected by four men in a dark-coloured car who then fled along the city's busy ring road. The reasons for the flights continue to mystify authorities. Minimal details are known about the aircraft in question and no footage has been posted online from any onboard cameras. However, countermeasures are being developed. Last month, a French company demonstrated a 'drone-hunting drone'. Trailing a long mesh net, the hunter flew over a target drone, snared it in the low-slung net and brought it to the ground.

The US Federal Aviation Authority has published draft rules on the use of private drones. The new rules are not as strict as some had feared they would be and the prospect of widespread private and commercial use remains highly probable. Special pilot certification will be required for commercial use (but not private use), aircraft will be banned from flying near crowds and restricted to daytime use. A speed limit of 100mph and a maximum height of 500 feet were also introduced. However, a rule requiring line-of-sight control jeopardises Amazon's recent, and much heralded, proposal of drone parcel delivery. The rules will now go out for public debate and revision before coming official in early 2016. Such roles as aerial photography and mapping, crop monitoring and inspections of major structures are highly likely to be allowed. However, as with parcel delivery, the prospect of fast food delivery has dimmed. The impact on the potential use of drones by emergency services, such as the rapid deployment of medical kits to accidents or of surveillance drones to crime scenes is still to be determined.

Developments in long-endurance drones are providing improved surveillance capabilities to US and international customers. General Atomics Aeronautical Systems Inc has developed a long-endurance version of the MQ-1 Predator, the Predator XP, which enables long-range or long-loiter missions to be conducted. A prototype took off from the company's Castle Dome Flight Operations Facility at the Yuma Proving Ground, Arizona, on 6 February, and flew for 40 hours at a cruising altitude of 10,000 feet. The XP cannot be armed and is aimed at the foreign market. Meanwhile, the US Department of Defense has revealed that a long-range jet-powered Triton MQ-4C unmanned aerial vehicle (UAV), developed by Northrop Grumman and capable of 24-hour flights, is to be deployed to Guam as the United States beefs up its surveillance capabilities in the Western Pacific. The Triton is set for widespread deployment by the US Navy, which will purchase a total of 68 platforms over the next few years.

Also of note

- **The US Air Force's shortfall in drone pilots continues, with only 1,000 pilots available for a requirement of 1,700.** Overwork and the poor status of drone pilots within the flying classes of the US military are considered the primary reasons for the high turnover of personnel.
- **The United Nations' technology and innovation panel, which has been examining the future technological needs of peacekeeping missions, has recommended dramatically expanding the use of unmanned surveillance drones in UN military operations.** Aerial surveillance has long been a major shortfall of peacekeeping missions, and current technology should be exploited to fill the requirement.
- **Kalashnikov, Russia's world famous maker of combat automatic weapons, has acquired ZALA Aero, a Russian UAV manufacturer.** Plans have also been announced to develop and manufacture drones capable of air surveillance for crisis spots.
- **Weaponised drones are beginning to dominate the military UAV market, with a 34% share of UAV purchase deals predicted within ten years, according to market research firm Strategic Defense Intelligence.**[7] Medium Altitude/Long Endurance UAVs are currently the fastest growing sector of the overall UAV market. Europe is the fastest growing market but North America remains the largest by value.
- **Australia has started sending its pilots to the United States for training on the MQ-9 Reaper unmanned combat air vehicle.** Australia will be only the second country, after the United Kingdom, to fly US-manufactured combat drones.

[7] http://www.c4isrnet.com/story/militarytech/uas/2015/03/03/armeduavsdominatemarket/24328239/

Intelligence, surveillance and reconnaissance

UK surveillance laws need overhaul according to parliamentary committee

In a landmark report, the UK parliament's intelligence and security committee (ISC) concludes that the various pieces of legislation governing Britain's intelligence agencies and their mass surveillance operations requires a total overhaul to make them more transparent, comprehensible and appropriate to modern methods and requirements.

While the 18-month enquiry concluded that existing laws were not being broken by the intelligence agencies and that their bulk collection of data did not amount to unnecessary surveillance or a threat to individual privacy, it did say that the legal framework is unnecessarily complicated, to the point that it provided the agencies with a 'blank cheque to carry out whatever activities they deem necessary'. The combination of the over-complexity of the legislation, combined with the lack of transparency over how the legislation and surveillance powers are implemented, has led to public belief that there is widespread and indiscriminate surveillance.

The report go on to call for all current legislation governing the surveillance capabilities of the security and intelligence agencies to be replaced by a new, single act of parliament. This act should clearly set out surveillance capabilities, detailing the authorisation procedures, privacy constraints, transparency requirements, targeting criteria, sharing arrangements, oversight and other safeguards.

The report also reveals some detail of how intelligence and security agencies have the capability to trawl through personal data, developing detailed 'bulk personal datasets' with minimal statutory or judicial oversight. The datasets of major targets could run to many millions of records, and there is currently no legal constraint on their storage, retention, sharing and destruction. Sources of personal data included UK and overseas government agencies, both within and outside the intelligence and security community, plus private sector corporations responding to statutory requests. A member of the ISC, Hazel Blears MP, said 'We have seen the datasets and concluded they are necessary and proportionate'. The British prime minister, David Cameron, has since announced that the intelligence services commissioner, the regulatory official tasked with reviewing intelligence agencies' warrants and activities, would be given statutory powers of oversight of the use of bulk personal datasets, extending the office's role into surveillance operations.

Of particular interest to privacy campaigners, the report concludes that intelligence agencies have neither the resources nor need to examine all the information they gather. Instead, it goes towards developing a resource from which they can quickly extract vital time-critical information, such as building rapid profiles and assessments of associates newly identified from surveillance. Therefore, they conclude such operations do not amount to literal 'mass surveillance'. In a move that will no doubt frustrate campaigners, the committee redacted the average percentage of daily internet traffic items that are selected to be read by GCHQ analysts, stating that such data 'will have gone through several stages of targeting filtering and searching so they are believed to be the ones of the very highest intelligence value' prior to being examined by intelligence officers.

Other conclusions were that measures should be taken to ensure UK nationals living abroad receive the same protection as citizens in the United Kingdom and that abuse of GCHQ's resources should become a criminal offence. The committee also argue that regulatory commissions, responsible for overseeing the activities of the intelligence agencies, should also be put on a statutory footing, as the existing non-statutory framework is unsatisfactory and inappropriate. There will also be additional privacy constraints on communications data that goes beyond the narrow definition of the 'what, when, where of communications', such as web domains visited or location tracking information on a smartphone. Such content has the potential to reveal considerable details of a person's movements and contacts and should therefore be granted appropriate protections according to the ISC.

Other developments

Terrorist groups have been employing new techniques involving leaving coded messages on major websites to communicate with their networks. In a new edition of *Gideon's Spies*, British investigative journalist Gordon Thomas reveals how al-Qaeda groups have been hiding messages within pages advertising goods on eBay. Intelligence agencies have also identified communications on social media networks such as Reddit, where codes based on hexadecimal formats and prime numbers hid planning and attack orders. Another identified method is hiding documents within messages on online porn sites. Intelligence agencies are also increasing surveillance of the deep web, a massive area of the internet that is not indexed or accessible by search engines such as Google and Bing. The deep web is said to be several thousand times larger than the visible internet. While the majority of content is innocuous, an element run on anonymous servers, known as the dark web, is used for criminal activities, such as child pornography image-sharing, human trafficking groups and online drug markets (for example, the infamous Silk Road).

Among the latest revelations from Edward Snowden is a 2010 report from the UK's Government Communication Headquarters (GCHQ) about a GCHQ/NSA joint operation to hack the internal computer networks of one of the world's largest SIM card manufacturers.[8] This operation led to the covert seizure of encryption keys used to protect the privacy of billions of worldwide mobile phone communications. The company targeted by the intelligence agencies, Gemalto, is a multinational firm incorporated in the Netherlands, which produces over two billion SIM chips a year, used in the mobile phones and next-generation credit cards of over 450 service providers around the world. Using these keys, intelligence agencies can monitor mobile communications without the need for warrants or approval from telecom companies and foreign governments. It also leaves no trace on the wireless provider's network that the communications were intercepted, and provides the means to unlock encrypted communications they had already intercepted, but did not yet have the ability to decrypt. Gemalto are urgently investigating the methods of the hack. Liberty groups have said this will send major shock waves through the security community.

At an American Bar Association breakfast conference in Washington DC on 24 February, former FBI director Robert Mueller argued that the current powers and practices of the US Foreign Intelligence Surveillance Act court are effective and do not need to be changed. Mueller states that the mass surveillance database is vital for US intelligence and law enforcement agencies. Using the Boston Marathon bombers as an example, the database allowed authorities to quickly discount many individuals as terrorist associates of the bombers, freeing resources to concentrate on other avenues of inquiry. Agencies and legislators are currently drafting the next reauthorisation bill, which will seek to address concerns of privacy, once current mass surveillance authority expires on 1 June 2015.

[8] https://firstlook.org/theintercept/document/2015/02/19/cne-access-core-mobile-networks-2/

Also of note

- **The US Defense Advanced Research Projects Agency (DARPA) has revealed that Memex, their advanced search algorithm developed to index and map the networks within the hidden dark web has already played a key role in nearly 20 investigations** after only one year in use.
- **More releases from Edward Snowden detail how New Zealand's signals intelligence agency, the Communications Security Bureau, has been routinely spying on North Korea, China, Japan, Indonesia, Iran and Pacific island states, many of which are key trading partners.** These operations have been part of the country's contribution to the Five Eyes intelligence partnership with the United States, United Kingdom, Canada and Australia.
- **Indonesia is stepping up its communications security in light of the revelations that New Zealand has been routinely spying on the country.** Some of the security weakness has been attributed to part-private ownership of the country's telecoms industry, resulting in government calls for full nationalisation.
- **A devastating intelligence file known as 'The Bomb' has rocked Macedonia.** In a series of revelations, Zoran Zaev, leader of the centre-left opposition party Social Democratic Union of Macedonia, has been drip-feeding revelations of the Macedonian government arranging the imprisonment of a political rival and tapping the phones of over 20,000 citizens, including politicians, judges, activists, journalists, academics, religious leaders and even its own president. There are signs this has jeopardised accession talks with the European Union.
- **Ukraine is struggling to counter widespread intelligence leaks to Russia.** Much of Ukraine's intelligence apparatus was inherited from the former Soviet Union, and many of its members are believed to still be loyal to Moscow.

Cyber Warfare

CIA announces significant organisational changes to broaden cyber intelligence capacity

On 6 March, the director of the Central Intelligence Agency (CIA), John Brennan, announced significant organisational changes to the structure of the CIA. The changes include the establishment of a fifth wing, known as the directorate of digital innovation, which will in part collect and use digital intelligence in operations. The structure of the directorate will be modelled loosely on the CIA's Counterterrorism Center. It will be assigned missions ranging from cyber-espionage to ensuring the security of the CIA's internal email. It is expected to absorb existing entities, such as the Open Source Center, which monitors Twitter and other social media sites for intelligence on adversaries.

The organisational change is a significant move for an agency whose traditional role has been the collection of intelligence from human sources (HUMINT) and harnessing such intelligence for foreign operations and conflict. The change represents a tangible move into a sphere of signals collections from electronic sources (SIGINT), historically considered the responsibility of the NSA.

One interpretation is that the CIA perceives SIGINT and open source data as an increasingly important source of actionable intelligence, which can be collected more remotely than by intelligence agents working in the field. Alternatively, the organisational change could reflect an understanding that HUMINT has an equivalent digital signature that provides greater certainty to intelligence analysis.

On the surface there appears an increasing propensity for US institutions to characterise cyber security as having clear parallels with counter-terrorism. Both in rhetoric and organisational structure, the US appears to be casting cyber security and counter-cyber operations into the counter-terrorism paradigm. However, the type of cyber attacks experienced in recent years could not be characterised as terrorism, and invoking such labels is likely to result in disproportionate and expensive counter measures. Furthermore, a counter-terrorism paradigm may encourage a more short-term view of cyber operations, without sufficient consideration for long-term strategic goals. The highly-visible information warfare campaign conducted by Islamic State (IS) may have resulted in the perception that cyber operations fall within the counter-terrorism paradigm.

The potential difficulty with perceiving cyber security as counter-terrorism is that it may encourage aggressive intelligence and surveillance. This could include maintaining encryption vulnerabilities, device backdoors and mass surveillance, activities which the US administration are trying to play down for political and diplomatic reasons. There are implications for those countries seeking to dominate the cyber or information spectrum, and while the benefits are regularly touted, the costs are often insufficiently recognised or ignored altogether.

Other developments

The software security group Kaspersky Lab has identified a highly-advanced cyber threat group, which it has called the Equation Group. The group is characterised by Kaspersky as unprecedented in terms of the complexity and sophistication of its cyber espionage tradecraft. The group is alleged to have developed and inserted advance malware that reprograms hard drive firmware and maps air-gapped networks in the systems of thousands of high-profile victims across over 30 countries. In some instances, the delivery method employed was physical interdiction, whereby the group intercepted physical goods, such as hard drives, and installed trojans. While many commentators have implied that the NSA has a connection to or directly sponsors the Equation Group, Kaspersky Labs has made it clear that the only public evidence available is that there is a technical link between the malware the group used and the code of Stuxnet. The revelations are likely to have implications for current China-US discussions on Sino anti-terrorism laws that require IT companies to provide encryption keys and install backdoors granting law enforcement access for counterterrorism investigations. If linked more directly to the NSA, the actions of the Equation Group will undermine US efforts to challenge Chinese proposals.

The US director of national intelligence, James Clapper, told the Senate armed services committee on 26 February that low- to medium-scale cyber attacks are more likely to have an impact on US national interests than a single large scale 'cyber Pearl Harbor'. Clapper stated that 'rather than a "cyber-Armageddon" scenario that debilitates the entire US infrastructure, we envision something different. We foresee an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security.' The testimony was not meant to play down the threat, but more suggest that death by a thousand 'cyber cuts' could have the same economic impact on the United States as a single devastating attack. In contrast, Admiral Mike Rogers, head of the NSA and US Cyber Command, was still invoking the notion of a cyber 'Pearl Harbor' at a National Defense Industry Association (NDIA) and New America Foundation sponsored forum on 26 February.

On 12 March, the US Senate intelligence committee approved the Cybersecurity Information Sharing Bill, which, if passed by both houses, will facilitate greater sharing of digital data and intelligence between the government and private sector. The bill is broadly supportive of an earlier executive order signed by President Barack Obama after his State of the Union address, and is likely to refocus institutional arrangements on information sharing. Lieutenant General Edward Cardon, commander of US Army Cyber Command (ARCYBER), noted in talks at Georgetown University on 12 February that cyber security is not solely a defence department problem, instead emphasising cooperation across federal government and the private sector. However, some private sector companies are likely to be sceptical about the ability of the Department of Homeland Security to share classified intelligence and leverage real-time input from the private sector, particularly after the lack of coordination between the government and Sony Pictures following the hack on the company in December 2014. Testimony provided by RAND Corporation to the House homeland security committee's subcommittee on cyber security, infrastructure protection and security technologies also challenged assumptions about how well information sharing can confront the changing signatures and tactics of attack groups.[9]

[9] http://www.rand.org/pubs/testimonies/CT425.html

Also of note

- **The UK Parliamentary Office of Science and Technology published a briefing on the dark net and ToR anonymous internet connection system** that notes that there is 'widespread agreement that banning online anonymity systems altogether is not seen as an acceptable policy option in the UK'.[10] The report is likely to have implications for Prime Minister David Cameron's proposal to crack down on use of encryption technology and services and criminalise some use of certain encryption technology.
- **Documents obtained by Edward Snowden and published on The Intercept show that the CIA has worked on strategies to exploit security flaws in Apple products since 2006.**[11] The CIA allegedly sponsored annual meetings of security researchers to discuss strategies to decrypt and ultimately penetrate Apple's encrypted firmware.
- **Japan's National Institute of Information and Communications Technology (NICT) reported in February that in 2014 Japanese computer networks received 25 billion attempted security breaches** or 12.8 billion excluding vulnerability testing. 40% of the attacks were traced back to Chinese networks.
- **In an interview with the BBC, the former head of the UK Secret Intelligence Service (MI6), John Sawers, has implied that the UK government does not have sufficient capability to counter hybrid and cyber warfare** from countries such as Russia.[12]
- **The Thai Army has announced the formation of a cyber warfare unit,** which is requiring officers to undertake penetration testing, forensic digital research and cyber security auditing, tasks more relevant to cyber security than cyber offensives.
- **Islamabad-based IT security firm Tranchulas allegedly targeted Indian government and defence establishments with a sustained malware campaign.** The campaign is believed to have provided the Pakistani government access to sensitive Indian government information. The report comes as a parliamentary panel in Islamabad is set to review prosecution exemptions for the Federal Intelligence Agency (FIA) contained in a cyber crime bill.
- **Israel announced the establishment of a new Cyber Defence Authority with an annual budget of $38-50 million.** The authority will include a Cyber Event Readiness Team (CERT) to respond to cyber attacks on private sector and civilians.
- **US federal investigators are treading carefully over the investigation into Marine General James E. Cartwright, who is alleged to have leaked information about Stuxnet to a *New York Times* reporter.** Federal investigators are likely to be concerned about the potential diplomatic fallout that could ensue if further details of Stuxnet are publically revealed.

[10] http://www.parliament.uk/business/publications/research/briefing-papers/POST-PN-488/the-darknet-and-online-anonymity

[11] https://firstlook.org/theintercept/2015/03/10/ispy-cia-campaign-steal-apples-secrets/

[12] http://www.bbc.com/news/uk-31669195

Commissioned by the Remote Control Project

remotecontrolproject.org

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, and take intelligence into your own hands with Open Briefing.

www.openbriefing.org