Remote-control warfare briefing | #09

24 February 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

US special operations forces and British Army develop social media capabilities for information warfare and situational awareness

US Special Operations Command (USSOCOM) is reportedly seeking to develop social media data mining tools that will far exceed the capabilities of the NSA tools revealed by Edward Snowden. USSOCOM has previously acknowledged work on its Automated Visual Application For Tailored Analytical Reporting (AVATAR) data synthesis and collation tool. However, more recent discussion has focused on interoperability of data collection tools that access both institutional and open source information to deliver improved situational awareness to special operations forces (SOF).

The commander of USSOCOM, General Joseph Votel, told the National Defense Industrial Association's (NDIA) Special Operations / Low Intensity Conflict Symposium in January that US special operations forces are looking to significantly bolster manned and unmanned intelligence, surveillance and reconnaissance (ISR) capabilities and improve access to cutting edge technology. Todd Huntley, the head of the National Security Law Department of the Office of the Judge Advocate General, told the NDIA conference that the 'US should continue to build possibly illegal data mining tools rather than relinquish capabilities'.

Meanwhile, the British Army announced in late January that it is creating the 77th Brigade to undertake online psychological operations and engage in unconventional warfare on social media platforms. Made up of 1,500 to 2,000 soldiers (up to 42% reservists), the brigade will attempt to control the narrative of stories on social media relating to army operations. The formation of this new brigade is significant in light of the information warfare elements of Russia's annexation of Crimea and Islamic State's ongoing social media activities.

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

To date, there are limited examples of successful social engineering campaigns or targeted (nano-scale) propaganda operations for ISR purposes across social media platforms. It remains to be seen whether social media could provide the type of actionable intelligence required for highly-complex special operations forces campaigns. While the precise nature of SOF operations on social media platforms is unclear, their data reconnaissance and information campaigns activities could possible influence the use and legitimacy of such platforms. In much the same way Snowden recently characterised US cyber operations as placing the national economy on the frontline, information operations by special operation forces may increase the likelihood that social media platforms become militarised domains.

Other developments

In late January, the Philippine National Police Special Action Force (PNP SAF) lost 44 officers in a clash with the Moro Islamic Liberation Front (MILF) and the Bangsamoro Islamic Freedom Fighters (BIFF) in Maguindanao. The objective of the covert SAF operation – Oplan Wolverine – was to capture or kill the Jemaah Islamiah affiliated bomb-maker Zulkifli bin Hir (Marwan). Reports of a Mamasapano farmer seeing the body of a 'blue-eyed foreigner' and the fact that Marwan was one of the FBI's most wanted terrorists were seized upon by Philippine media commentators and the Philippine Communist Party as evidence that the United States had participated in or ordered the operation. Specifically, US Joint Special Operations Task Force Philippines members that have remained in the Philippines after the task force was disbanded in April 2014 allegedly provided intelligence identifying Marwan's location. Potential US involvement has become a sticking point because of the political tension around ongoing US military presence in Philippines and the risk the recent encounter poses to the peace agreement and ceasefire accord.

Canadian opposition parties have questioned the government's characterisation of Canadian special forces operations in Iraq. Canada is the first Western country to acknowledge that its special forces operators have engaged Islamic State in frontline exchanges. The questions come after Prime Minister Stephen Harper announced in late 2014 that Canada's contribution to a six-month mission in Iraq did not include a combat role and would be limited to 600 soldiers, including 69 special operations forces personnel providing training and support. While the mandate and mission authorisation is not for direct combat, Canadian special operations forces advising on the ground in combat zones rather than from forward operating bases increase the risk of direct engagement with Islamic State forces. More special operations forces engagement with Islamic State is therefore likely if the general consensus of US military commanders that more complex missions will involve combat zone advising and support is accepted.

The National Defense Industrial Association's Special Operations / Low Intensity Conflict Symposium was held in Washington DC in late January.[1] Michael J. Dumont, the US deputy assistant secretary of defence, outlined a range of challenges special operation forces face, including Boko Haram in Nigeria, Abu Sayyaf in the Philippines, al-Shabaab in Somalia and transnational crime syndicates in Central America. Comments by the head of USSOCOM, General Joseph Votel, that the United States may replace special operations forces in the Horn of Africa with conventional forces generated significant discussion, though US Africa Command (US AFRICOM) later clarified he was expressing an opinion only. Votel's comments come as US AFRICOM's General David Rodriguez publically called for a full-scale, multinational counterinsurgency campaign against Boko Haram, and the US Federal Business Opportunities register requested expressions of interest in fixed wing air transport for special operations forces in North Africa.

[1] https://www.youtube.com/watch?v=q_9AMItVJoI&feature=youtu.be&a=&utm_content=bufferc7286&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

Also of note

- **A UK House of Commons defence committee report has suggested that the British contribution to confronting Islamic State in Iraq and Syria has been modest.**[2] The committee advocated greater deployment and engagement of UK special forces 'provided they are able to operate within increasingly stringent legal constraints'.
- **Outgoing US defence secretary Chuck Hagel has ordered 100 US troops, predominately special operations forces personnel, to establish sites in Turkey, Qatar and Saudi Arabia to train vetted Syrian opposition fighters.** In the decision announced in late January, Hagel noted that further US deployments would be made once training sites are established. No Syrian fighters have signed up so far, but the United States anticipates training over 5,000 fighters each year over three years.
- **US senators John McCain and Dianne Feinstein have called for greater US special operations forces deployment in Iraq.** Feinstein, a Democrat member of the Senate intelligence committee, and McCain, the new Republican chair of the Senate armed services committee, argue that a greater US presence is required to counterbalance Iranian influence and improve US intelligence collection capability. The comments came ahead of the Obama administration proposing a new authorisation of military force (AUMF) to enable greater special forces deployment against IS.
- **Canadian special operation forces command (CANSOFCOM) has indicated that their near-term acquisition focus is on airborne ISR platforms.** Boeing is reportedly promoting their Reconfigurable Airborne Multi-Intelligence System (RAMIS) for consideration.
- **The Canadian Special Operations Regiment (CSOR) are training with Niger soldiers in Diffa, the site of a recent Boko Haram attack.** CSOR personnel are in Niger and Chad as part of the US-organised SOF training exercise Flintlock 2015, and are partnered with Niger for this year's exercise.
- **Commandant General Joseph F. Dunford, the new top general in the US Marine Corps, released a 16 force planning guidance that stresses the importance of interoperability of Marine Corps and special operations forces units.**[3] The emphasis on force interoperability is discussed in the context of the United States confronting an anti-access/area denial (A2/AD) environment in the Pacific region.
- **Pentagon officials were less than clear on whether US ground forces in Mogadishu, Somalia, supported a special operations forces drone strike on al-Shabaab on 31 January.** The strike reportedly claimed al-Shabaab's chief of external operations and planning for intelligence and security, Yusuf Dheeq. In a press release, the Pentagon press secretary, Rear Admiral John Kirby, refused to reveal the footprint of US special operations forces in Somalia.

[2] http://www.publications.parliament.uk/pa/cm201415/cmselect/cmdfence/690/690.pdf

[3] http://www.hqmc.marines.mil/Portals/142/Docs/2015CPG_Color.pdf

Private military and security companies

Deteriorating security situation sparks surge in private security spending in Yemen

Since September 2014, Yemen's security has seriously deteriorated, with the country further falling into a state of lawlessness and violence. Houthis rebels have gradually taken control of parts of the country, including the capital Sana'a. The Zaidi Shia group took control of the Yemeni government in a *coup d'état* on 21 September 2014, and took over the presidential palace on 22 January 2015, eventually leading to President Abd Rabbuh Mansur Hadi's house arrest and resignation. While the former Yemeni government accuses the Houthis of being backed by the Iranian government, the group claims the Hadi government was tied to anti-Shia external backers, such as al-Qaeda and Saudi Arabia. Since the coup, the country has experienced deep instability and volatility on the street, with several reports of robberies and attacks on businesses. Such insecurity has led businesses to turn to private security companies for protection.

The situation in Yemen further evidences the trend that private military and security companies (PMSCs) tend to proliferate and prosper within war-torn countries and areas experiencing severe security issues. Those areas are characterised by weak or destabilised state institutions commonly paired with a dysfunctioning formal security apparatus. Disappearing formal government structures and apparatus generate unchecked disorder on the streets, as is happening in the case of Yemen. In fact, the chair of Yemen's Chamber of Commerce's trade issues committee, Abdulellah Al-Khateed, reported that over 45 shops have experienced looting and armed robbery since September 2014, amounting to losses estimated at around $232,000. These incidents are further contributing to Yemen's financial difficulties, which are mainly due to the country's political instability and the resulting freezing of foreign aid, but are also linked to recurrent sabotage of the country's oil pipelines, gas transportation and electricity networks since 2012.

Foreign companies and international organisations operating in Yemen are increasingly likely to rely on private security companies to fill the current security vacuum. Official sources estimate the number of private security companies in Yemen to range between 40 and 50 licensed companies and 18 unlicensed ones. However, the situation is complicated further by the tribal nature of Yemeni society, and the reliance of local businesses on militia and tribal bodyguards for protection. Given that tribesmen are often behind kidnapping for ransom and other more organised crimes, the potential for different tribal militia to clash both with each other and local private security companies makes for a dangerous dynamic, which could further deteriorate Yemen's already poor security situation.

Other developments

Demand from schools, businesses and religious institutions in Europe for Israeli private security expertise is likely to continue following terrorist attacks in Brussels, Paris and most recently, Copenhagen. Concerned governments have stepped up their counter-terrorism efforts in the aftermath of the events, including French Prime Minister Manuel Valls heightening the country's Vigipirate security alert programme to its highest level and the Belgian government deploying hundreds of troops to guard possible targets, including Jewish sites and diplomatic missions. However, some stakeholders are increasingly looking to Israeli private security companies to hire trained and effectively-prepared security personnel. This includes companies such as Tactical Zone or Israel Special Forces, the latter having already deployed security staff to half a dozen countries worldwide. Demand for such companies is reported to have increased since the Paris attacks in January. It is likely to continue growing given their expertise in urban security provision, including risky sites security assessment and protection, early threat detection and security protocols in the event of an attack on a protected location.

Unease is growing over the Nigerian government's procurement of weapons and training in its fight against Boko Haram. Nuhu Ribadu, a prominent member of Nigeria's ruling party and the former head of the country's Economic and Financial Crimes Commission, has claimed that Western governments' unwillingness to send military aid has forced Nigeria to turn to the black market for weapons procurement. Moreover, in late January, the Nigerian government reportedly contracted around 100 South African private military contractors to train Nigerian soldiers to fight Boko Haram. South Africa's defence minister, Nosiviwe Mapisa-Nqakula, subsequently labelled these contractors 'mercenaries' that should be arrested on their return to South Africa (according to South Africa's Foreign Military Assistance Act, it is a crime for any South African citizen to be involved in foreign conflicts outside of official government efforts). These developments further highlight the Nigerian government's political and military weaknesses in the face of the Boko Haram threat. The region's inability to tackle Boko Haram also underscores the problem of coordination between African security institutions. Indeed, the African Union's plan to create a 7,500-strong West African task force to fight Boko Haram is likely to endure related coordination and leadership issues.

On 20 January, US President Barack Obama's declared in his State of the Union Address that the United States' 'combat mission in Afghanistan is over'; however, the number of US-contracted private military and security personnel still operating in Afghanistan suggests the reality may be more nuanced than that. Since 31 December 2014, combat duties have officially been transferred to Afghan security forces. However, the US defence department is currently employing 39,609 private contractors in Afghanistan according to the US Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.[4] Those contractors are reportedly carrying out duties including base support (9%), construction (12%) and transportation (10%), with the largest percentage being contracted for logistics and maintenance roles (42%). According to the Pentagon, three contractors who were recently killed by a Afghan army solider were overseeing maintenance work on Pilatus PC-12 aircraft (U-28s), which are regularly used by US Special Operations Command forces in Afghanistan. In other words, though the US contractors currently present in Afghanistan are not involved in combat duties *per se*, they are directly contributing to the US government's continuing remote-control warfare efforts in the country. As such, the Taliban still perceives the US government's advisory presence as *de facto* occupation. It is therefore highly likely that US contractors will continue to be priority targets for the Taliban.

Also of note

- **International mutual marine insurance company Skuld has advised ship owners against contracting private maritime security companies in Southeast Asian waters.** The company stressed that Southeast Asian littoral states have sole jurisdiction over maritime security in the region, and that currently no legal arrangements exist that would allow private security companies to provide security on board ships.
- **The City of London Police's overseas anti-corruption unit arrested two British businessmen over their suspected bribing of a Norwegian official as part of a deal with Nigerian private security company.** The two men reportedly made payments to a Norwegian civil servant in order to facilitate the sale of decommissioned Royal Norwegian Navy ships to an unnamed Nigerian security company.

[4] http://www.acq.osd.mil/log/PS/reports/CENTCOM%20Census%20Reports/5A_January2015.pdf

Unmanned vehicles and autonomous weapons systems

United States urges Europe to develop more advanced military technology

In light of the rapid technological advances being made by the likes of Russia and China in the field of unmanned vehicles and advanced weaponry, the US Department of Defense (DoD) has urged European countries to accelerate their own development programmes or face being left behind and technologically outgunned. The US deputy defence secretary, Robert Work, has said that bold and decisive action is needed to maintain Western military superiority in the near future. The DoD has recently commenced the Defense Innovation Initiative, which will strive to maintain the United States' global lead in this field.

At a January conference hosted by the Center for a New American Security, Work said 'We must coordinate and collaborate, avoid duplication, leverage niche capabilities, and push our establishments to innovate in technology, concepts, experimentation, and wargaming.' He also urged NATO member states to make good on the agreement to maintain defence spending at a minimum of 2% of national GDP. US defence spending is currently at 3.5-4% of GDP depending on the measuring formula. US defence spending has been in decline in recent years due to wider economic pressures, but there are indications that this will reverse in light of rising defence expenditure by potential foes, including an increasingly belligerent Russia, and the still-growing threat from Islamic State (IS). Russian and Chinese development of weaponry that would appear to be directly linked to US military assets, such as carrier-destroying and anti-satellite missiles, has been said to be a particular motivator.

Stated examples of upcoming US military technology included new/upgraded nuclear weaponry, a 'X-fighter' successor to the F-35 jet, space control capabilities, advanced sensors, missile and cyber defence, new unmanned air/surface/undersea vehicles, high-speed strike weapons, a new type of jet engine, high-energy lasers, rail gun technology, robotics and autonomous weaponry. While some of these are in partnership with fellow NATO members, most of these are solely US innovations, highlighting the reticence of European states to invest in defence at a time of continuing intense economic difficulties.

More details are available elsewhere on developments in unmanned aerial vehicle (UAV) technology. The United States' renowned Defense Advanced Research Projects Agency (DARPA) is starting to investigate 'drone packs', which would allow one pilot to single-handedly control a group of drones on a strike mission (today's platforms still require two crew each). Under the newly-announced Collaborative Operations in Denied Environment (CODE) project, each pack is envisaged to be able to work together to find, identify, track and engage multiple targets. Following recent debates about the legality of drone use and autonomous weaponry, DARPA have been keen to clarify that these would not be autonomous packs, and would not be firing on human targets without approval from a human operator.

However, such a stance may be short-lived as the advantages of operating autonomous packs of drones make them more and more necessary in light of financial restraints and the continuing shortages of drone crews. UAVs are still a fraction of the price of a conventional manned combat aircraft, and could potentially be much cheaper with miniaturisation. The arrival of autonomous air assets in the military inventory would enable the US military to deploy more aircraft, for longer periods, covering more territory and conduct more offensive operations, all for less money and with less exposure to danger for US military personnel. These advantages make it likely that autonomous drone technology will be developed, whatever the current reassurances to the contrary.

Other developments

White House security may include anti-drone technology after a rogue quadcopter crashed in the grounds of the executive mansion. On 26 January, a small drone flown over the White House was downed in the grounds by still-to-be-identified equipment. The drone in question was a basic four-rotor model, which was determined as 'non-threatening' by the US Secret Service. The government employee owner has pleaded it was all an innocent accident. It is widely suspected that the aircraft crashed when signal-jamming equipment severed the control frequency, though the White House has yet to comment on this. Such equipment is being developed by the military to defend ships, planes and key sites from future drone threats, including swarm raids by large numbers of drones. Other technologies can be used to target drones, such as missiles, other drones and lasers, but a signal jammer remains the simplest and cheapest approach yet, albeit still a short-range capability.

Almost 2,500 people have now been killed by drone strikes under the Obama administration. The Bureau of Investigative Journalism compiled the figure from continuing CIA and military operations in Syria, Pakistan, Somalia, Iraq and Yemen. Included in this were two strikes on Taliban-controlled areas of Pakistan. The first, on 15 January, was on a compound suspected of housing militants in the Tehsil Ladha area of South Waziristan, reportedly killing seven people. In the second, on 27 January, seven suspected militants were killed in a strike on a compound and a vehicle in the Shawal Valley in North Waziristan. The United States has launched 24 drone strikes in the Shawal Valley since September 2010. Elsewhere, on 31 January, a drone strike on a compound in Shabwah Province, southern Yemen, killed four members of al-Qaeda in the Arabian Peninsula (AQAP). One of them was reportedly Harith al-Nadhari, an ideologue and a member of AQAP's sharia committee, who had publicly praised the attack on the French satirical magazine *Charlie Hebdo*.

The OSCE has started using drones to monitor conflict areas in eastern Ukraine. Following an attack on a civilian bus in the Donetsk area on 13 January, which killed 12 and injured 16, a drone was used to take imagery of impact craters in order to identify the source. Such assets allow rapid deployment to incident sites, allowing evidence to be gathered while the sites are still fresh. Elsewhere in the region, the Russian Navy's Crimea-based Black Sea Fleet has reportedly taken delivery of a number of Orlan-10 drones. The Orlan-10 is a Russian-built light airframe used for reconnaissance and surveillance. One of these was shot down over eastern Ukraine in May 2014.

Also of note

- **China's Chengdu Aircraft Corporation has revealed a high-altitude long-endurance drone.** Tian Ye is claimed to have stealth capabilities through a shielded fan intake and a special fuselage shape, which suppresses the craft's infra-red signature. Its reported capabilities would put it alongside the United States' Global Hawk surveillance vehicle.
- **The United States and India are reported to be partnering on the development of small a surveillance drone based around the RQ-11 Raven surveillance platform.** However, current US export restrictions still threaten the programme, and may compel India to seek partners elsewhere.
- **Iran has deployed drones to skies of Iraq in the fight against Islamic State.** The Mohajer-4 surveillance drone is the latest incarnation of the Mohajer-1, which flew over Iraq during the 1980s Iran-Iraq conflicts. Meanwhile, Iran has revealed brief footage reportedly showing flight-testing of a complex twin-jet drone that could be used for combat missions.

- **Military historians have published details of a 1960s US drone that launched at supersonic speeds from the back of an A-12 Oxcart, a predecessor of the SR-71 Blackbird.** The D-21 Tagboard needed to be launched at Mach 3.3 for its ramjet to start. It would then fly along a pre-programmed route at 95,000 feet before ejecting its camera to be collected by a modified C-130, and itself then self-destructing. This programme was cancelled after a fatal accident, and transport was instead switched to B-52s. However, only four drone missions were conducted over China before the entire programme was terminated.

- **Drug traffickers across the US-Mexico border have been discovered using drones to ship supplies after one crash-landed in a Tijuana supermarket car park carrying 6 pounds (3 kilograms) of synthetic crystal meth.** It appears the traffickers got greedy, as the payload exceeded the capabilities of the drone.

Intelligence, surveillance and reconnaissance

European countries debate new counter-terrorism measures following terrorist attacks

In the wake of terrorist attacks in Paris and Copenhagen and the raid on a terrorist cell in Belgium, the debate over the extent of the counter-terrorism response continues to intensify as European governments examine their options. Conservatives, led by lawmaker Valérie Pécresse, have sparked outcry in France by holding up the USA Patriot Act as a template for legislative and security reform. Citing its success in implementing effective surveillance, especially of emails and social media, and in thwarting a great many terrorist attacks on US soil, Conservative politicians and party supporters are beginning to consider it a viable foundation on which to structure new French counter-terrorism legislation – arguing that its intrusion on civil liberties is justified.

Countering opposition voices who directly link the Patriot Act to torture, extraordinary rendition and Guantanamo Bay, US commentators have been appearing in the French news media arguing that the act did not authorise such actions and was actually a 'modest piece of legislation that made careful changes to surveillance law' to quote William Bendix, a US professor of political science appearing on the France 24 news channel. Bendix continues that it was how the legislation was subsequently interpreted by the courts and implemented by the intelligence services that led to the significant deviation from Congress's original intentions. Such intrusive legislation requires continual oversight, which was not apparent in this instance, and four-year 'sunset clauses' on each of its 17 provisions, inserted to safeguard against mission creep and overreach by the intelligence and security agencies and to maintain the Patriot Act as a temporary measure, were soon made permanent in all but two instances with little political opposition.

Another significant Europe-wide option involves a new data-retention law, which would replace one struck down by the European Court of Justice (ECJ). German Chancellor Angela Merkel has called on the EU to fast-track legislation that would permit the collection and storage of vast amounts of communications data. This mirrors the 2006 Data Retention Directive, which was struck down last year by the ECJ, who concluded that it constituted 'suspicionless mass surveillance' that was disproportionate to the threat and infringed fundamental civil rights. Although specific details of Merkel's proposal have yet to be released, the Data Retention Directive required all EU member-states to implement legislation requiring communications companies to store private data of EU citizens for at least six, but no more than 24, months. With court-issued warrants, security agencies could also request access to IP addresses and accompanying usage, as well as date, time, caller, recipient(s) and contents of emails, texts and phone calls.

Opponents argue that police and security agencies do not require new powers, but need more effective intelligence-sharing facilities and additional funding. They also argue that France already has in place many of the anti-terror powers that Merkel is calling for EU countries to adopt. The Data Retention Directive was implemented and retained in France, alongside several other countries, while the courts in Germany struck it down in 2010.

Meanwhile, other legislation to restrict funding to jihadist groups, and restrict the movements of individuals suspected of traveling to train and/or fight with such groups is underway. Most European countries are favouring widespread travel bans, some are discussing the reinstatement of internal European border controls (terminating the very popular EU pillar that is open borders and passport-free travel) and the European Commission is assessing stiffer external border controls, better intelligence sharing networks, access to flight passenger records, and even the establishment of an EU security agency. This last measure is highly unlikely having few major government supporters. However, Europol, Europe's law enforcement agency/criminal intelligence hub, could be expanded to take on increased powers and duties, as could the fledgling European Union Intelligence Analysis Centre, a civil-military intelligence fusion facility, which currently has no collection network of its own, a comparatively small staff and few dedicated powers.

Other developments

The British government has threatened to end intelligence sharing with Germany if it pursues an investigation into UK-US intelligence operations. The government is becoming concerned that a German parliamentary inquiry, set up after the Edward Snowden revelations that the United Kingdom and United States had been spying on the German government, could result in highly-classified UK/US intelligence being published, including details of operations, code-breaking abilities and intelligence technology. This has already caused a stir within Germany's federal intelligence agency, the Bundesnachrichtendienst (BND). On 4 February, the agency's head, Gerhard Schindler, briefed German lawmakers on 'unusually tense relations with British partner agencies'. Germany relies heavily on UK-sourced intelligence, but links have been fractured by the Snowden leaks, last summer's arrest of a BND officer caught passing secrets to the CIA, and the discovery that the British Embassy in Berlin being used to eavesdrop on nearby German government buildings.

A Republican US presidential contender has called for key NSA powers to be permanently extended, including its highly controversial mass surveillance of domestic telephones. Florida Senator Marco Rubio penned an editorial for the Fox News website calling for the US Congress to perpetually extend key provisions of the Patriot Act when they come up for renewal on 1 June. Rubio has positioned himself as a defence and security hawk in the run-up to the 2016 presidential election, and is a vocal supporter of the NSA's intrusive surveillance programmes. This places him opposite nomination contenders such as Texas Senator Ted Cruz, who was one of just four Republicans who supported last November's Democrat-backed USA Freedom Act, which would have significantly reformed NSA operations, and Kentucky Senator Rand Paul, who voted down that bill alongside Rubio, but only because he did not believe it went far enough.

The United Kingdom's Investigatory Powers Tribunal has ruled that Britain's signals intelligence agency, GCHQ, contravened human rights legislation between 2007 and 2014 by failing to inform the British public of the safeguards that were in place. The tribunal made the ruling on 6 February in respect of a challenge from Liberty, Privacy International and other groups to GCHQ's warrantless mining of communications data collected by the United States' National Security Agency under the controversial PRISM and UPSTREAM programmes. The ruling will not affect the programmes, current GCHQ surveillance or the Five Eyes intelligence-sharing partnership, it simply establishes that British intelligence agencies are not permitted to conduct surveillance based on safeguards that are not in the public domain.

Also of note

- **The fight against Islamic State has prompted a dramatic increase in intelligence sharing between North American and European intelligence agencies.** Despite tensions caused by the Edward Snowden revelations about the US spying on European governments, counter-terrorism concerns have become the priority, with data on the international movements of thousands of suspects being widely shared.
- **Satellite imagery, increasingly eclipsed by the capabilities of signals intelligence, has undergone a minor rebirth monitoring areas where SIGINT coverage is sparse.** Satellites have been heavily used to gather data on Boko Harem's massacre of an estimated 2,000 villagers in the remote Baga-Doro Gowan area of Nigeria, and to track the group's movements around the region.
- **The UK Conservative Party has proposed legislation that would outlaw communications that the country's security agencies could not monitor.** Communications such as Snapchat, WhatsApp, iMessage and Facetime would be blocked if the party wins the May 2015 elections.
- **Denmark, the scene of two recent radical Islamist-linked shootings, is proposing new laws that will grant security agencies access to network data without warrants and order network operators to store comprehensive data on personal Internet traffic.** Bank transfers could also be delayed to give authorities the opportunity to review and approve them.
- **Chinese security agencies have clamped down on a popular mechanism to evade intensive internet censorship.** Virtual Private Networks, which allowed users unmonitored access to closed sites such as Facebook and Gmail, have now been prohibited.

Cyber warfare

US president's State of the Union acknowledgement of cyber security challenges drives new policy debate

US President Barack Obama used his State of the Union address on 20 January to highlight cyber security challenges. He outlined the administration's legislative proposals requiring data breach notifications to victims and the National Cybersecurity and Communications Integration Center. The legislative proposals provide a domestic audience with tangible evidence of the White House responding to the high profile Sony Pictures hack. However, the combination of cyber espionage campaigns against the military and finance sectors, the potential loss of technological competitive edge, the low cost asymmetrical warfare capabilities of adversaries, and attacks on government institutions is likely to have provided the real impetus. The Defense Advanced Research Projects Agency (DARPA) has publicly acknowledged that cyber attacks against the US military are increasing both in frequency and magnitude, particularly over the last two years. A proportion of these attacks appear to target NSA data servers or associated IT infrastructure.

The legislative proposals are only one of the United States' cyber security initiatives rolled out during January and February. US Department of Defense officials are trying to expedite the filling of all 6,000 positions in the US Cyber Command by the end of 2015, a year earlier than originally scheduled. The House Intelligence Committee has also reorganised its subcommittee to enable a new focus on cyber security.

The existing cyber security cooperation and collaboration between the United States and United Kingdom achieved through the Computer Emergency Readiness Team programme will be enhanced by the proposed formation of a trans-Atlantic joint cyber cell. This will be made up of cyber defence experts from Britain's Government Communications Headquarters (GCHQ) and Security Service (MI5) and the United States' National Security Agency (NSA) and Federal Bureau of Investigation (FBI). It will be undertaking cyber war game training with the finance sector later this year.

Most significant though is the announced establishment of the US Cyber Threat Intelligence Integration Center (CTIIC), a federal agency that will coordinate collection and analysis of cyber threat intelligence across the government. The centre is in line with the parallels between the role of intelligence in addressing the threat of terrorism and cyber security drawn by Obama in his State of the Union. However, any perceived effectiveness of intelligence collection in the context of counter-terrorism may not apply equally to the cyber security realm. There are risks associated with cyber intelligence and counter-intelligence. It is reported that US confidence in attributing the Sony Pictures hack to threat actors aligned or working as proxies for North Korea is likely based on NSA techniques and intelligence collection processes that compromised or piggy backed off the intelligence assets of multiple allies and states including South Korea.

The implication is that the effective and accurate attribution of cyber attacks may be dependent on deep and persistent network penetration and surveillance. In this way, the implicit NSA advocacy for system vulnerabilities and its criticism of improved encryption technology may be part of a broader vision for an internet that enables the United States wide access and surveillance opportunities. However, the use of intelligence assets to search out cyber threats or risks may be invasive and penetrate deeply into the computer networks of both allies and adversaries alike. From a security perspective, the type of cyber surveillance that US policymakers believe they need to maintain for attribution and threat management may be unsustainable. Invading and compromising the private cyber domains of states could be characterised as an encroachment on sovereignty and a threat to national interests.

Other developments

Computer security company FireEye released a report in February detailing a social engineering and phishing campaign against Syrian opposition forces.[5] The operation included the use of female Skype avatars to build rapport with male opposition fighters. The user would then share a photo file embedded with a multi-staged malware installation tool resulting in the DarkComet remote access tool (RAT) installing on the target's computer. The threat actor, potentially based in Lebanon or possibly having some connection with Hezbollah, also used social media links seeded with malware on fake opposition websites and Facebook pages. The operation netted the threat actor over 7.7 GB of data, including annotated maps, battle plans, opposition positions and tactics and political strategy discussions. The operation demonstrates the capability of relatively simple social engineering and malware campaigns to obtain actionable military intelligence. This stands in stark contrast to the recent cyber vandalism campaigns by various groups over the recent months.

The CEO and chair of cyber security company Kaspersky Lab, Eugene Kaspersky, told World Economic Forum (WEF) attendees in Davos, Switzerland, that attacks on power plants, telecommunications and financial systems will become the face of modern cyber terrorism. Cyber security became a focal topic of the WEF 2015 meeting, with attendees hearing concerns from the UN Security Council Counter-Terrorism Committee that there is evidence transnational organised crime networks and extremist groups are colluding to launch sophisticated cyber attacks. Estonian President Toomas Hendrik Ilves argued that the cyber threat environment was becoming increasingly complex with hybrid criminal, terrorist and commercial networks forming partnerships and acting as proxies for state operations, what he dubbed the 'little green menization of cyberspace' (a reference to Russia's 'little green men' deployed in Crimea and eastern Ukraine). Business attendees were so concerned by the level and sophistication of increasing cyber attacks that discussion turned to establishing an international body to create cyber security standards similar to what the International Air Transport Association (IATA) provides for air transportation.

Iran's cyber capability potentially improved as a result of attacks by the United States' Stuxnet and Israeli Flame viruses. A 2013 NSA document recently published by The Intercept shows that the United States had become concerned that Iran had bolstered its offensive cyber operations from reverse engineering and analysing Stuxnet.[6] The NSA document appears to acknowledge that cyber attacks not only risk eliciting counter-responses but also help teach adversaries how to launch more sophisticated attacks. The document obtained by Edward Snowden is released at a time when a number of US policymakers and legislators are allegedly pushing for stronger US counter cyber strikes in closed door congressional briefings sessions. Some are advocating network destruction of threat actors as a viable form of retaliation. Recent US political debates on cyber security have missed the possibility that certain cyber attacks methodologies and technologies may exponentially increase cyber weapon proliferation, thereby creating a feedback loop of cyber security threats.

[5] https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-behind-the-syria-conflict.pdf

[6] https://firstlook.org/theintercept/2015/02/10/nsa-iran-developing-sophisticated-cyber-attacks-learning-attacks/

Also of note

- **A malware campaign used the #JeSuisCharlie hashtag to distribute a DarkComet remote access trojan.** According to Recorded Future, the Middle East Cyber Army may have been behind the campaign. Over 19,000 French websites were also hit with defacements and distributed denial-of-service (DDoS) attacks during the same period. The malware campaign is the most recent in a long line of campaigns that have leveraged real world crisis for online malware distribution.
- **Multiple Dutch government websites were subjected to a sustained DDoS attack on 10 February.** The attack brought down government websites for almost 12 hours, and prevented ministries from sending or receiving parliamentary papers.
- **Analysis by Kaspersky Labs on the Regin malware toolkit and QWERTY keylogger source codes has revealed that the same developer most likely designed both advanced persistent threat (APT) cyber-espionage tools.** The source code analysis also revealed references to what was then named the Australian Defence Signals Directorate. With previous links drawn between the NSA and QWERTY, the new source code comparison reinforces previous suspicions that Regin was developed by Five Eyes intelligence agencies.
- **Beijing has drawn the ire of US IT business interests after introducing new cyber security regulations.** The new regulations require technology companies to hand over secret source codes and adopt Chinese encryption algorithms before such technology is allowed to be used in key Chinese business sectors. Beijing has identified import of US internet hardware as a national security vulnerability after Edward Snowden revealed the NSA embedded surveillance tools in exported hardware and software products.
- **The Strategic Studies Institute and US Army War College published a monograph in late January on army support for military cyberspace operations.**[7] The report concludes that further work on defining cyber force roles in conflict escalation and deterrence is required in order to improve cyber integration into conventional and special forces.
- **The Singapore government announced in late January that they are setting up the Cyber Security Agency of Singapore.** Prime Minister Lee Hsien Loong's office advised that the agency would 'provide dedicated and centralised oversight of national cyber security functions' for a country whose international businesses have been subject to sustained cyber security challenges.
- **Finnish defence minister Carl Haglund has advocated for a national cyber attack capability and a legislative framework to appropriately recognise the potential benefits of cyber operations over kinetic military responses, particular in terms of disabling the weapons systems of adversaries without mass casualties.** The policy announcement comes as the Technical Research Centre of Finland established the country's first Cyber War Room laboratory in response to the growing magnitude of cyber attacks.
- **Taiwan's vice premier, Simon Chang, told the *Executive Yuan* in late January that China was using Taiwan as a cyber testing ground.** He claimed China heightened attacks during elections and negotiations on the Economic Cooperation Framework Agreement. Chang advocated Taipei adopt an information security defence programme.

[7] http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1246

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