Remote-control warfare briefing | #11

30 April 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 Operation Forces

US special operations forces withdraw from Yemen, severely limiting US counter-terrorism campaign

In late March, the US government withdrew an estimated 125 special forces operators from Yemen as the country descends into civil war. The sudden departure is causing significant political consternation for the Obama administration, which had held up US special operations in Yemen as a counter-terrorism success story amid a field of misadventures and operational failures. The Republican chair of the House Committee on Homeland Security, Michael McCaul, immediately expressed concern over the loss of the vital intelligence on al-Qaeda in the Arabian Peninsula (AQAP) and Islamic State (IS) being provided by US special operations forces (SOF) in Yemen, together with the inability to account for $500 million in physical assets, such as vehicles and weaponry likely abandoned and seized during the ongoing Houthi insurgency. Yemeni counter-terrorism units trained by US special operations forces are likely to be disbanded, and equipment provided to Yemeni forces is likely to have been seized by AQAP or Houthi rebels.

In his criticism, McCaul focused in on concerns that AQAP, as the al Qaeda franchise's strongest operational force, has effectively limited the US intelligence gathering capability. The US state department downplayed the significance of the withdrawal for regional counter-terrorism operations, highlighting continued US intelligence, surveillance and reconnaissance (ISR) activities, which are most likely drone flights from Saudi Arabia and Djibouti. However, the Obama administration is undoubtedly concerned by the rapid rate at which AQAP has been able to openly reassert its presence in Yemen.

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

Open Briefing Ltd is a non-profit company limited by guarantee.
Registered in England & Wales, No. 07649656.

This raises questions about the efficacy of US and Yemeni counter-terrorism operations. Specifically, it begs the question of whether collaborative training partnerships with indigenous forces, equipment provision for counter-terrorism operations and intelligence sharing are sufficient and sustainable over the long term. Counter-terrorism operations may be being less effective against groups such as AQAP and IS, in part because these groups' support networks are increasingly decentralised and they are developing greater resilience that enable them to re-generate once the focus of counter-terrorism campaigns moves on to different regions. The possibility that AQAP are adapting to the US counter-terrorism model of special operations forces and drones and reordering network and command structures to ensure rapid regeneration is likely a cause of concern for US military planners.

Following the withdrawal of US special operations forces, speculation has grown that Saudi Arabian special forces may be present on the ground in Yemen or are supporting fighters loyal to the ousted president, Abd Rabbuh Mansur Hadi. The Saudi ambassador to the United States, Adel al-Jubeir, denied Saudi special forces were in the southern city of Aden. However, CNN reported an unidentified Saudi source as claiming that Saudi special forces were 'on the ground in noncombat roles coordinating and guiding the battle'. Other reports are less clear about whether Saudi special forces have actually set foot in Yemen, and appear to suggest that support in the form of command coordination and intelligence, surveillance and reconnaissance is being delivered remotely.

The Arab League announcement of a proposed 40,000 strong regional force to confront the challenges of the region is likely to raise the stakes associated with Riyadh's potential involvement in Yemen. Iran may interpret the timing of the announcement of the regional force as a potential willingness to use it in the Yemen conflict. The force is anticipated to include an elite special operations command made up of forces from Egypt, Saudi Arabia, Jordon, Sudan and Morocco. Iran may perceive the force composition as a consolidation of sectarian divisions.

Any future regional or Saudi special forces involvement in Yemen is likely to stand in stark contrast to the US approach to counter-terrorism, and may selectively target particular networks based on sectarian affiliation. It is unclear whether US forces will be able to leverage intelligence from any regional special operations command, particularly considering the involvement of Sudan.

Other developments

On 18 March, General Joseph Votel, commander of US Special Operations Command told the House Armed Services Subcommittee on Emerging Threats and Capabilities that special operations forces must develop unconventional capabilities in social media platforms. In discussing the emerging use of social media platforms and networks to recruit individuals to causes, particularly in the case of Islamic State, Votel advocates that information campaigns and unconventional capabilities should become an area of routine operation and that special operations forces have an ability to cultivate networks that are not centrally controlled. Votel also used his testimony to impress upon the subcommittee that budget sequestration on the military as a whole does impact on special operations forces despite strong budget support for SOF activities and capabilities.[1]

[1] http://www.defense.gov/news/newsarticle.aspx?id=128461

US Army Special Operations Command is preparing for a training exercise across the southwest United States due to take place between July and September 2015. JADE HELM 15 will involve over eight SOF divisions, and focus capability testing on unconventional warfare exercises in challenging environmental conditions or domains.[2] A number of conspiracy theorists and conservative groups based in Texas allege the exercise is preparation to impose martial law or subdue right-leaning groups and individuals. These groups seized on the exercise's demarcation of Texas as hostile territory for the purposes of the exercise as evidence of their allegations.

French special forces freed a Dutch hostage from al-Qaeda in the Islamic Maghreb (AQIM) during raids in northern Mali in early April. According to the French president, François Hollande, freeing Sjaak Rijke was not the purpose of the raid, which was undertaken by French special forces after recent terrorist attacks in Mali and neighbouring countries. After Operation Serval in 2013-14, approximately 1,200 French soldiers have remained in Gao and another northern Mali base for counter-terrorism operations. French special forces normally stationed in Burkina Faso are possibly maintaining a greater presence in northern Mali to prevent or discourage the flow of foreign fighters and criminal networks with safe haven in southern Libya pushing down into Niger and Mali.

Also of note

- **The Philippines Senate Committee on Public Order inquiry into the Mamasapano raid in January 2015, which resulted in the deaths of 44 police commandos, suggests that six US nationals were involved in the planning and execution of the raid.**[3] The findings contradict statements by US officials that Americans played no role in the operation except to help evacuate wounded Filipino police officers.

- **Russian special operations forces participated in Arctic military drills in mid-March.** The drills focused on the rapid airlifting of special operations forces from central Russia to key Arctic outposts.

- **US Special Operations Command (USSOCOM) released a request for proposals (RFP) for mid-endurance unmanned aerial vehicle ISR services.**[4] The RFP released on 6 April requires the successful contractor to deliver over 300 to 1,200 hours per month of near real-time feed of ISR data using contractor owned and operated UAVs. USSOCOM are currently using mid-endurance Aerosonde Mk 4.7 from Textron Systems to obtain ISR for the Lebanese armed forces on Islamic State and Jabhat al-Nusra in northeast Lebanon.

- **India's Ministry of Home Affairs cannot find funding to establish a special forces regiment to counter Maoist insurgents in Chhattisgarh, Jharkhand, Bihar and Odisha provinces.** The proposed unit would most likely be modelled on the elite anti-Naxalite force Grey Hounds of Andhra Pradesh and specialise in guerrilla warfare.

[2] http://www.scribd.com/doc/258605525/Jade-Helm-Martial-Law-WW3-Prep-Document-1

[3] http://pnp.gov.ph/portal/images/boimamasapano/boi_final.pdf

[4] https://www.fbo.gov/index?s=opportunity&mode=form&id=d0101be5b3e3892f22f89f5927fc046c&tab=core&_cview=1

- **New designs for the Chinese PLA Navy's Shangclass nuclear attack submarine released in mid-March suggest a hangar for special operations force submersibles has been incorporated into the submarine designs.** The concept appears to be borrowed from the hangars used for US SEAL Delivery Vehicles (SDV).
- **The US Special Operations Command Syrian rebel training programme may face set backs with the programme head, Major General Michael Nagata, leaving his post as commander of Special Operations Command Central in May.** Republican senators have expressed concern over the future success of the programme due to Nagata's transfer.
- **The Movement of the Taliban in Pakistan released a video on 17 April showing the Mujahideen Special Group (MSG) training at a camp in northwestern Pakistan.** The Pakistani Taliban bill the MSG as their version of special forces, with advanced skills in assassination, assault drills and IED making.

Private Military and Security Companies

Sentencing in Blackwater Iraq shootings trial highlights need for better regulation of private military companies

On 13 April, four former Blackwater security contractors were sentenced to long prison terms for their roles in the killing of 17 Iraqi civilians in Baghdad's Nisour Square on 16 September 2007. In October 2014, a federal jury in the United States found the four former contractors guilty on charges ranging from weapons charges to manslaughter and murder. Ultimately, three of the former Blackwater employees, namely Paul Slough, Evan Liberty and Dustin Heard, were each sentenced to 30 years in prison and a fourth, former sniper Nicholas Slatten, received a life sentence.

The April sentences put an end to a long protracted judicial journey, and are hailed as a diplomatic victory for the United States, which has attempted to frame the trial's outcome as an example of the US criminal justice system's equity and trustworthiness. However, the convicted men remained largely defiant and unapologetic during the April sentencing. In addition, the judge, Royce C. Lamberth, was criticised for imposing sentences lower than those sought by the government for the guards convinced of manslaughter and weapons charges. Although Lamberth said that he agreed with the jury's October guilty verdict because unprovoked shootings 'just cannot ever be condoned by a court', he also described the defendants as 'good young men who've never been in trouble, who served their country'.

The UN working group on the use of mercenaries welcomed the sentencing. The chairperson, Elzbieta Karska, stated that 'The difficulty in bringing a prosecution in this case shows the need for an international treaty to address the increasingly significant role that private military companies play in transnational conflicts.'[5] In continuous public relations efforts to rebrand its image, the successor company to Blackwater, Academi, issued a press release welcoming the trial's completion and stating that the company was 'relieved that the justice system has completed its investigation into a tragedy that occurred at Nisour Square in 2007 and that any wrongdoing that was carried out has been addressed by our courts,' and took that opportunity to highlight that 'the security industry has evolved drastically since those events, and under the direction of new ownership and leadership, Academi has invested heavily in compliance and ethics programs, training for our employees, and preventive measures to strictly comply with all US and local government laws'.

Blackwater's legacy lives on in Afghanistan today, where Academi is still active on the ground. According to a US Special Investigator General for Afghanistan Reconstruction (SIGAR) report released in March 2015, Academi secured $569 million dollars from the US government to help with 'training, equipment, and logistical support' to Afghan forces in counternarcotic efforts,[6] which demonstrates the US government's continued trust in and reliance on private military contractors. The sentencing of the four former security contractors undoubtedly marks a watershed moment in the prosecution of private military and security company (PMSC) personnel, and will send a strong signal to the executives of PMSCs that such private armies do not operate outside the law. Ultimately, though, current trends and governments' continued reliance on PMSCs suggest that the Blackwater trial is unlikely to mark a long-term normative shift, and is highly likely to be limited to a short-term judicial precedent only.

[5] http://www.un.org/apps/news/story.asp?NewsID=50576#.VTT8aPmUd8E

[6] https://www.sigar.mil/pdf/special%20projects/SIGAR-15-40-SP.pdf

Other developments

The private military and security contracting industry has evolved and considerably adapted its services in the past decade. Private military contractors have played increasingly important roles in assisting states during their military campaigns, as evidenced by US reliance on private contractors in its military efforts in Iraq and Afghanistan. The advent of private maritime security companies has matched states' need for assistance in addressing the issue of piracy, as in the case of the Gulf of Eden off the coast of Somalia and in Southeast Asia. Lastly, the Snowden scandal also revealed the preponderance of private contractors within the intelligence community. Lately, the steadfast development of drone technology has meant that unmanned aerial vehicles (UAVs) have gradually become more complex, thus requiring additional human resources for drone-related logistics, weapons maintenance and ground station equipment. A single Combat Air Patrol (CAP) mission for a Predator or Reaper requires 160 to 180 personnel to complete a 24-hour mission. The Global Hawk system necessitate between 300 and 500 personnel. Therefore, it is likely that as technology continues to evolve, become more complex and require greater human resources, the private military and security contracting industry will continue to fill gaps in states' changing needs staffing levels. Given the lethality and expediency of drone warfare, reliance on private contractors is likely to pose issues of command and control, as well as oversight.

South Africa's shadow minister of police, Dianne Kohler Barnard, has criticised the alleged domestic implications the country's Private Security Industry Amendment (PSIRA) bill. Barnard issued a press release on 20 March criticising the support the South African government and the police minister, Nkosinathi Nhleko, have lent to the bill, which she deems xenophobic and potentially negative for the South African economy. The bill will require all security companies, as well as manufacturers, importers and distributors of security equipment, to be at least 51% owned by South Africans. It is likely that the shadow minister's comments are politically driven, but they take advantage of the window provided by the erratic progress of the bill and the South African government's unpersuasive approach to the controversy. Nhleko's allegations that the private security industry could threaten the country's national interests were never really substantiated and her response to concerns over South African job losses as a result of companies leaving consisted of proposing a discretionary clause offering a different ownership percentage to certain companies, which is perceived as arbitrary. Given the global and multinational nature of private military and security companies operating in South Africa and across the continent, it is unlikely that such domestic legislative efforts will produce the desired outcomes for South Africa's security and economy.

Continuity can be expected in the new Nigerian government's approach to Boko Haram, including the use of private military contractors. Nigerian forces recently claimed decisive gains in the country's fight against Boko Haram militants; however, it is likely that the extent of Nigeria's military successes has been exaggerated due to the recent presidential election. In the last days of the election campaign, the incumbent president, Goodluck Jonathan, made desperate attempts to effectively communicate to the electorate the strategic gains that had been made and allocate them solely to Nigerian forces, though it highly likely that foreign military assistance from neighbours such as Chad, Niger and Cameroon, as well as training and advisory support from private military and security companies proved decisive. Jonathan has been heavily criticised for his failure to end Boko Haram's six-year-long insurgency. However, the election of Mohammadu Buhari, a former military ruler from northern Nigeria who pledged to end the insurgency within months if elected, is unlikely to result in any drastic moves towards innovative approaches at a time when Nigerian forces appear to have seized momentum. Moreover, he is likely to continue relying on assistance from private military contractors, such as the Leon Lotz, the South African contractor and former Koevoet officer who was killed in Nigeria in March.

Also of note

- **Egypt's economic conference in Sharm el-Sheikh on March 13-16 has been praised as a success from a security viewpoint due to the government's use of Bedouin private security contractors.** The conference was a potential target for terrorist groups, as over 90 Arab and foreign countries were due to participate. However, the Egyptian government used nomadic Bedouin contractors to secure strategic routes in southern Sinai.
- **The Ukrainian president, Petro Poroshenko, promises that Ukraine's governors will not have their own private armies.** The president's declaration came as armed men close to Ukrainian billionaire and former governor of Dnipropetrovsk oblast Ihor Kolonoyskiy occupied the Kiev headquarters of state-owned energy company Ukrnafta. The president's statement is an attempt by the state to regain its monopoly over the use of force and re-establish clear-cut military vertical control and oversight.
- **US and British private military contractors might play a role in any ground invasion as part of the Saudi-led Operation Decisive Storm in Yemen.** If a ground invasion follows the air campaign in Yemen with the aim of reinstalling the disposed president, Abdu Rabu Mansour Hadi, it is possible that US and British private contractors could be involved.

Unmanned vehicles and autonomous weapons systems

Advocacy groups seek halt to autonomous military vehicles and weapons

In the build-up to the second round of the Convention on Certain Conventional Weapons – Meeting of Experts on Lethal Autonomous Weapons Systems, which took place in Geneva, Switzerland, on 13-17 April, there was a rush of reports from advocacy organisations expressing various degrees of concern over the ongoing and rapid development of unmanned vehicles and autonomous weapons systems.

In their report *Mind The Gap: The Lack of Accountability of Killer Robots*, Human Rights Watch (HRW) argued that the use of autonomous weaponry could provide considerable impunity for governments for the murder, deliberate or collateral, of civilians, and therefore the NGO seeks a UN-backed convention banning future development.[7] The human rights organisation's argument is grounded on the complexities of assigning effective blame for any illegal act carried out by autonomous platforms. Who is culpable: the software developer, the pilot/monitor (if there is one), the military commander who managed the mission, the politician who ordered the deployment of autonomous assets to begin with or all or none of the above? With multiple actors involved in any one military operation, it would be very difficult for courts to pinpoint the primary individual at fault in the absence of a person who 'pulled the trigger'. While many will point their finger at the military and/or political leadership, these individuals might claim that the software was at fault for not identifying civilians before launch, therefore directing the blame towards the software developer.

The HRW report states that an unmanned aerial vehicle's (UAV) independent capabilities will 'raise serious moral and legal concerns because they would possess the ability to select and engage their targets without meaningful human control…the lack of meaningful human control places fully autonomous weapons in an ambiguous and troubling position. On the one hand, while traditional weapons are tools in the hands of human beings, fully autonomous weapons, once deployed, would make their own determinations about the use of lethal force…They would thus challenge longstanding notions of the role of arms in armed conflict, and for some legal analyses, they would be more akin to a human soldier than to an inanimate weapon. On the other hand, fully autonomous weapons would fall far short of being human.' The organisation concludes by arguing for a ban 'on the development, production and use of fully autonomous weapons through an international legally binding agreement'.

The International Committee of the Red Cross (ICRC) is also opposed to such platforms, but does not call for an outright ban, at least not at this time. Instead, they call for greater consideration to legal and ethical issues prior to any further development of fully-autonomous hardware. In their own statement released prior to the CCW meeting, it said, 'The ICRC wishes to again emphasise the concerns raised by autonomous weapon systems under the principles of humanity and the dictates of public conscience…There is a sense of deep discomfort with the idea of any weapon system that places the use of force beyond human control…The ICRC encourages States that have not yet done so to establish weapons review mechanisms and stands ready to advise States in this regard.'[8]

[7] http://www.hrw.org/reports/2015/04/09/mind-gap

[8] https://www.icrc.org/en/document/lethal-autonomous-weapons-systems-LAWS

In a statement given at the conclusion of the CCW meeting, the International Committee for Robot Arms Control (ICRAC) mirrored HRW's stance, and called for an immediate UN-backed global ban on any further development and also a removal of all existing autonomous weapons from service. Examining the issue of the culpability of software developers, ICRAC said, 'Engineers operate in a policy and legal environment that is defined by states. As such, it is incumbent upon the States Parties to clearly communicate the requirement that all weapons must be kept under meaningful human control though a binding instrument.' It also expressed strong concern over the rapid proliferation of such technology, which could, in their opinion, fundamentally destabilise global security.

However, any campaign to bring about a ban is going to be extremely difficult. This is particularly because so many valued autonomous weapons are already in service (for example, Israel's Iron Dome and the US Patriot and Phalanx systems, all geared to automatically respond to threats) or are highly-expensive offensive weapons close to deployment (for example, the United Kingdom's Brimstone missile). These countries are unlikely to agree to a ban, and with the United States and United Kingdom holding UN Security Council vetoes, the prospects for such a ban are not looking good at all.

The United Kingdom has already stated its opposition to any outright ban. In a recent statement, the UK government explained, 'At present, we do not see the need for a prohibition on the use of Laws [lethal autonomous weapons systems], as international humanitarian law already provides sufficient regulation for this area…The United Kingdom is not developing lethal autonomous weapons systems, and the operation of weapons systems by the UK armed forces will always be under human oversight and control. As an indication of our commitment to this, we are focusing development efforts on remotely piloted systems rather than highly automated systems.'

With regards to the CCW meeting itself, the outcome was to continue discussions on identifying consensus-based policies on issues where progress was more probable. This suggests a ban is highly unlikely.

Other developments

Senior US Congress representatives and military think tanks have called for a long-range armed 'superdrone' to form part of the next evolutionary step in the US military arsenal. They seek an airframe that can be launched from land or carrier, can fly for days at a time, can refuel, have a range of thousands of miles and is capable of carrying a weapons load similar to today's attack aircraft. Those in favour of this, including the chair of the Senate Armed Services Committee, Senator John McCain, believe current armed drone development programmes are taking too long and are failing to push technological boundaries, allowing adversaries to catch up. They also argue that the US Navy's plan to restrict drones to reconnaissance and surveillance roles is forcing naval carrier groups to operate long-distances from shore. This may move the ships out of reach of the latest long-range anti-ship missiles, but it also reduces the ability of carrier-based aircraft to operate against targets deep inland. Chinese anti-ship missiles have a potential range of 1,000 miles, which negates a large proportion of the flying range of the F/A-18 and the upcoming F-35 jets. In response, the Pentagon says it is close to buying a new long-range strike bomber to take on targets deep inland. It is also concerned that an airframe capable of meeting the lawmakers' requirements would be far too large to operate on aircraft carriers.

The United States, United Kingdom and France are developing multiple unmanned undersea vessels (UUV). The United Kingdom is to spend £17 million developing and implementing a fleet of underwater drones in partnership with the French military. Designed for mine-clearance duties, both surface and submersible vessels will be make up the Maritime Mine Counter Measures demonstrator, though an in-service date was not announced. UK-based BAE Systems and France-based Thales will be working on the project. Meanwhile, the US Navy is developing several models of its own. One, Proteus, is a large long-endurance underwater drone that will patrol littoral combat zones gathering surveillance data to be fed to nearby helicopters and warships. One further option being explored is for the drone to double as a submersible delivery system for special operations forces personnel. Another UUV, the Flimmer, is a submarine-launched drone that can operate in both the air and underwater.

Iran is developing 'suicide drones' in partnership with Hamas and Hezbollah. Different from conventional missiles in that they remain human-controlled, these aircraft are capable of carrying large explosive payloads over considerable distances and on defensive-evasive routes to target. These were tested in a live-fire exercise on target ships in the Straits of Hormuz in December 2014. The US Army reported that such technology is being shared with Hamas and Hezbollah for use against Israeli targets. If true, this could potentially escalate the conflict between Israel and militant Palestinian groups and destabilise the fractured peace that currently exists between the two. In related news, Google Earth has released updated imagery of the Iranian coast, which includes the highly-strategic Bandar-e-Jask military base on the Straits of Homuz. Visible for the first time on the base runway is a Mohajer-4 surveillance UAV and accompanying control station.[9]

Also of note

- **London's Metropolitan Police has drafted in drone technology to provide a rapid eye-in-the-sky for commanders.** These commercially-developed surveillance aircraft will be used to provide real-time coverage during incidents, such as armed sieges, terrorist attacks, major protests and monitoring crowds at sports events.
- **US drones have reportedly killed an al-Shabaab leader linked to the Nairobi Westgate shopping centre attack.** Adan Garar was killed on 12 March in Dinsoor in southern Somalia.
- **A US drone strike killed a senior Pakistan Taliban commander on 19 March.** Khawray Mehsud was killed with two other fighters in Kuraam, a border province in western Pakistan.
- **Syria claims to have shot down a US MQ-1 Predator drone that was on a surveillance mission near the Port of Latakia on 17 March.** However, there is confusion within US military circles why a drone from the US European Command was operating in a combat zone that is within US Central Command's area of responsibility.

[9] https://www.google.co.uk/maps/place/Bandar-e-Jask,+Hormozgan,+Iran/@25.653293,57.7991179,239m/data=!3m1!1e3!4m2!3m1!1s0x3ef2503858a76cf7:0x13cf339005067e5d (the UAV is to the south of the runway and the control vehicle to the north)

Intelligence, surveillance and reconnaissance

Governments continue to struggle balancing surveillance needs with privacy concerns

Strong public concerns over intrusive electronic surveillance continue to frustrate Western governments' attempts to increase monitoring in the wake of recent terrorist attacks in Europe. This is especially so in the United States, where consecutive polls show a strong majority (~60% in polls conducted in January and March 2015) preferring personal privacy over surveillance, as well as considerable opposition to current surveillance programmes.

This attitude has now been shown to exist in many other parts of the world with the publication of a poll of 15,000 people in 13 countries conducted on behalf of Amnesty International.[10] In every one of the 13 countries, there was no majority support for internal surveillance of their country's own citizens (only 26% support across the poll). At each end of the spectrum, only 17% of the entire sample favoured blanket surveillance of citizens, foreign nationals and foreign governments, but twice as many (34%) favoured no surveillance of any of these groups.

The degree of accepted surveillance also varied strongly. While France and the United Kingdom, countries at high risk of terrorist attacks, were found to be least opposed to state surveillance of citizens and foreign nationals and governments (both at 44%), Germany and Spain were the most opposed (69% and 67% respectively). This follows recent national outrage at revelations that the NSA has been conducting bulk interception of communications within those countries. Sixty three per cent of US citizens opposed state surveillance, at the higher end of the scale in the survey.

The American Civil Liberties Union has published a separate multinational poll of 18-34 year olds gauging support for Edward Snowden's whistleblowing.[11] This study asked around 1,000 individuals from the Five Eyes countries and several European countries: the United States, United Kingdom, Canada, Australia, New Zealand, Italy, Germany, Spain, France and the Netherlands. The most favourable views of Snowden were found in continental Europe, where between 78% and 86% who were familiar with Snowden expressed positive opinions of his whistleblowing of mass surveillance. In the United States, 56% had favourable opinions. There was also a strong belief among respondents that the leaks will lead to increased protections of personal privacy.

The opinions of this age group are highly significant, as over the coming years it is expected to surpass the baby boomers in many Western societies as the largest generation. Generation Y (also known as Millennials) will therefore become a strong political demographic, especially when you also consider this age group's enthusiasm for social media and political mobilisation.

[10] https://www.amnesty.org/en/articles/news/2015/03/global-opposition-to-usa-big-brother-mass-surveillance/

[11] https://www.aclu.org/news/international-poll-shows-millennials-have-positive-opinion-edward-snowden

The results from both polls clearly suggest that the terrorist threat is not perceived by the majority as severe enough to justify the widespread collection of communications data from the entire population. However, an arguably significant factor is an element of ignorance of how mass surveillance data is managed. Examination of public discourse strongly suggests a widespread belief that personal communications are closely monitored by intelligence officers whether the participating parties are involved in criminal/terrorist activity or not. The sheer number of individual communications in any one country's communications datasets – and there are many billions of phone calls, text messages, emails, etc. each year in the United Kingdom alone – makes such monitoring implausible, but repeated statements by government and law enforcement spokespeople to that effect do not yet appear to be making any headway in changing public perception. Also, it cannot be denied that electronic surveillance is vital in identifying and monitoring terrorist threats, possessing an inherent capability and capacity that far exceeds all other forms of intelligence gathering. Governments therefore have the not inconsiderable challenge of tackling this mindset and calming public unease if vital surveillance programmes are going to continue. Crucially, though, this is not just a question of good public relations, but a genuine exercise in rebuilding trust between citizens and the intelligence agencies.

Other developments

The French government is introducing new legislation this month that will both legitimise and extend the country's intelligence and security agencies' ability to monitor phone and internet use. This bill will replace legislation introduced in 1991, long before today's widespread use of mobile phones and internet existed, which has meant that French law enforcement have been conducting electronic surveillance outside any real legal framework. The new law sets into statute how intelligence officers can monitor phone lines, conduct cell-site analysis (tracking individuals movements through their mobile phones), intercept emails, take covert photographs, and conduct intrusive covert surveillance on private property. The legislation also creates a new oversight body, gives the French judiciary the power to end surveillance and provides a process by which individuals can seek redress for unjust surveillance. The French government has also announced that its intelligence services will hire an additional 2,680 people over the next three years. Human Rights Watch have already voiced their opposition, arguing the bill contains serious flaws, such as authorising surveillance methods that exceed international human rights law, provides insufficient public transparency and court oversight, and requires private communications companies to intrusively monitor their customers usage patterns.

US Republican presidential candidates are lining up on all sides of the NSA surveillance debate. So far, libertarian champion Kentucky Senator Rand Paul has argued about reining in the agency's spying capability, fellow Tea Party voice Texan Senator Ted Cruz is seeking fundamental reform, while both former Texas governor Jeb Bush and New Jersey Governor Chris Christie are campaigning for maintaining and strengthening the NSA. Two other possible Republican contenders, Scott Walker and Ben Carson, are yet to set out their respective stalls. And it seems that Paul and Cruz have aligned themselves with the voting majority, with a recent survey of Republican voters/potential voters showing 70% losing confidence in the NSA surveillance programme. With national security being a constant priority for the Republican base, this issue could push these two to the front of the race for the party nomination. It is expected that Bush and Christie will seek to counter this groundswell of opinion by labelling Paul and Cruz as both weak on national security. If such a strategy proves effective, Paul, with his fundamental opposition to the Patriot Act, will suffer most, with Cruz benefitting from any shifting Tea Party support.

The European Court of Human Rights is expected to soon decide whether the United Kingdom's mass surveillance is legal under European human rights legislation. This follows a joint appeal at Europe's highest court by civil liberties groups, including Privacy International, Amnesty International and Liberty, seeking to overturn a ruling last December by the United Kingdom's intelligence oversight body, the Investigatory Powers Tribunal (IPT), which declared lawful the mass surveillance of internet traffic in and out of the United Kingdom and an intelligence-sharing agreement between the United Kingdom and United States. The groups claim that, contrary to the IPT's finding, such mass surveillance breaches Articles 8 and 10 of the European Convention on Human Rights (ECHR), which enshrine the rights to privacy and freedom of expression. The campaigners are therefore seeking a ruling from ECHR that industrial-scale mass surveillance violates human rights law. The European Court has also been asked to consider whether British legislation that provides UK residents with better privacy protections breaches Article 14 of the ECHR, which outlaws unlawful discrimination. Due to the major repercussions of the court upholding the appeal, which would immediately apply to similar programmes underway across many other European countries, commentators are not expecting such a ruling. The United Kingdom has already reformed surveillance legislation, which is expected to be accepted as compatible with the ECHR.

Also of note

- **The Israeli prime minister, Benjamin Netanyahu, has flatly denied that Israel spied on US negotiations with Iran and fed the intelligence to Republicans in the US Congress.** This contradicts recent US intelligence assessments that ranked Israel as the third most aggressive intelligence service against the United States after Russia and China.
- **An inquiry has been started into New Zealand's communications intercept agency, the Government Communications Security Bureau.** This follows revelations that the agency has conducted comprehensive surveillance on neighbouring states, including the personal communications of allied politicians.
- **Kenya is seeking assistance from the United States and Europe with intelligence and security measures after the recent attacks by Somali militants in Nairobi and on the Garissa University College campus.** Kenyan officials are conducting an intelligence gap analysis before requesting help with intelligence, surveillance, and reconnaissance capabilities.
- **Macedonia's government is under increasing domestic and international pressure following accusations that it orchestrated a major surveillance operation against 20,000 opposition politicians and activists.** The West is monitoring this closely, as it is jeopardising Macedonia's candidate status for joining the European Union and NATO. So far, the Macedonian prime minister, Nikola Gruevski, has rejected a snap general election.
- **The NSA is slowly moving towards a cloud-based database architecture in response to the Edward Snowden's leaks.** The new system is said to replace multiple relational databases plus also improve security and access.

Cyber Warfare

China’s cyber operations acknowledged in influential People’s Liberation Army publication

The Chinese People’s Liberation Army (PLA) acknowledged the existence of China’s cyber operations and capabilities in late 2013. The acknowledgement is contained in the most-recent edition of the highly-influential *Science of Military Strategy* report published by the PLA. The report was released in Mandarin in late 2013, but has only just been translated into English by Western researchers. The acknowledgement removes the limited plausible deniability that Beijing had sought to retain by obscuring the nature and scale of their cyber operations.

The various Chinese cyber actors operate under a doctrine of pre-emptive and active deployment of cyber units to establish ‘information dominance’. The concept as employed by the PLA emphasises seizing control of an adversaries access to their own information and disrupting information flow essential for centralised decision making and operations.

While detailed force structure and capability information is not disclosed, the report does provide insight into the three broad entities involved in cyber operations. These include a ‘specialized military network warfare force’ embedded in operational military units, specialists based in government departments, such as the Ministry of State Security (MSS) and Ministry of Public Security (MPS), and ‘external entities’ outside of government that participate in network warfare operations. The external entities may be reserved for offensive network attacks that would be politically or diplomatically problematic and risky for the Chinese government or PLA to be associated with.

This approach may allow the Chinese Communist Party (CCP) and PLA to dissociate themselves from particular offensives or argue that such activities are untaken by unsanctioned non-state actors. For example, North Korea denied responsibility for the Sony Pictures hack but endorsed the activities of the Guardians of Peace, who claimed responsibility for the attack. The use of external entities or informal networks of patriotic hackers may reduce the scope for deterrence action to be levelled at national governments, as they will argue that the action of non-state actors are beyond their control and direction.

The disclosures may be in response to pressure primarily from the United States on cyber transparency and mounting international momentum on the discussion of potential cyber norms. However, considering that the report was released in late 2013 and preceded the increased tension between the United States and China over cyber issues, a more likely explanation for the disclosures is rooted in domestic competition between the PLA and CCP. The PLA may be seeking to publicly establish its primacy as China’s top cyber authority.

The PLA publication does not provide details of force structure and size, offensive tradecraft and strategic targets. Analysts are left to speculate on capability based on reported cyber activities. Recent allegations of a 10-year cyber-espionage campaign in Southeast Asia and India allegedly carried out by a Chinese state-sponsored group would suggest long-term investment in cyber capabilities. In a report released on 12 April, cyber security company FireEye suggests that a group identified as APT30 targeted politically sensitive organisations in Malaysia, Vietnam, Thailand, Nepal, Singapore, Philippines and Indonesia, and increased its activity around the time of ASEAN meetings.[12] In contrast to other Chinese cyber-espionage campaigns focused on intellectual property theft, the APT30 campaign focused more on data relevant to Southeast Asian politics, particularly maritime disputes in the South China Sea and corruption issues.

[12] https://www2.fireeye.com/WEB-2015RPTAPT30.html

Despite the disclosure, an improvement in US-China cyber relations and diplomacy is unlikely. Both countries are taking assertive actions, with China keeping its options open with new banking technology regulations and anti-terrorism laws. US tech export companies have strongly objected to these laws, which would require telecommunication companies to hand over encryption keys and install back doors to their software to aid counter-terror investigations. What the disclosure does do, though, is underscore the importance of China in cyber norm building.

Other developments

US President Barack Obama signed a new executive order on 1 April establishing a sanctions programme for cyber attacks and cyber-enabled commercial espionage.[13] The sanctions apply to four cyber attack categories, including attacking critical infrastructure, disrupting major computer networks, stealing intellectual property and benefiting from the stolen secrets and property. Further escalation in cyber deterrence by the US administration has been met with criticism from China's foreign affairs spokesperson, Hua Chunying, and is likely to worsen US-China relations on cyber cooperation. The challenges of attribution have been flagged both internationally and within the United States as a limit on implementing the sanctions. A fortnight prior to the executive order being signed, the commander of US Cyber Command, Admiral Michael Rogers, told the US Senate Armed Service Committee on 19 March that a greater emphasis on increasing cyber offensive tradecraft as part of the United States' cyber deterrence strategy is required. Rogers indicated this approach is necessary to address increasing cyber attack threats and prevent US adversaries maintaining a persistent presence on US networks.

The Canadian Broadcasting Corporation (CBC) and The Intercept published sensitive details on the cyber warfare capabilities of the Communications Security Establishment Canada (CSEC) as public concern over draft anti-terrorism legislation (Bill C-51) continues.[14] The 2011 documents provided by NSA whistleblower Edward Snowden suggest that CSEC's cyber capabilities may go far beyond intelligence collection activities and include offensive activities, such as infrastructure destruction, use of false flags and internet traffic disruption. However, CSEC has advised the CBC that the 2011 documents do not necessarily reflect current CSEC practices and programmes. Many of the CSEC cyber capabilities are consistent with those developed by the NSA's elite cyber warfare unit, Tailored Access Operations. The documents also reveal details of the relationship and collaboration between the NSA and CSEC, which was suggested in previous documents released by Snowden.

[13] http://apps.washingtonpost.com/g/documents/world/executive-order-obama-establishes-sanctions-program-to-combat-cyberattacks-cyberspying/1502/

[14] http://www.cbc.ca/news/canada/communication-security-establishment-s-cyberwarfare-toolbox-revealed-1.3002978

The US international affairs think tank The Atlantic Council held a forum on 8 April on the future of the Iranian cyber threat. During and after the event a number of analysts and commentators argued that the staged lifting of sanctions as a result of the P5+1 negotiations on Iran's nuclear programme will increase the resources available to Iran to expand its cyber capabilities. In a recent study, the American Enterprise Institute (AEI) and cyber security company Norse drew similar conclusions based on significant increases in 'scans' (or attacks according to AEI) launched from Iranian IP addresses on Norse's 'honeypot' network emulations (sensors) throughout 2014 and early 2015.[15] The report's authors argue that Iranian state actors are actively mapping US critical infrastructure supervisory control and data acquisition (SCADA) systems in preparation for potential cyber attacks. The CEO of cyber security company Cylance, Stuart McClure, argues that Iran may tone down certain types of attacks that slightly more sophisticated cyber powers may tend to avoid, such as openly attacking financial institutions, and focus on cyber espionage.

Also of note

- **The increase in research by cyber security companies, such as Fire Eye, Symantec, Fox-IT and Kaspersky Labs, has led to allegations of geopolitically motivated research agendas** and close relationships with national intelligence agencies.[16]
- **Former US national intelligence director Dennis Blair told the Foreign Correspondents' Club of Japan in April that some cyber powers are reaching a point of capability and deterrence that resembles mutually assured destruction in nuclear weapons standoffs.[17]**
- **Reports suggest that Russia may have been involved in a cyber attack on unclassified White House and state department networks in October 2014.** While US officials have not confirmed the reports, some security experts are indicating that Russia is undertaking considerable reconnaissance missions against US network infrastructure as a precaution in the event of an escalation of hostilities between Russian and NATO.
- **The US defence secretary, Ash Carter, and the Japanese defence minister, Gen Nakatani, met in early April to make the first revisions to the 1997 US-Japan Defence Guidelines,** which now includes provisions on cyber security and warfare. The revisions and inclusion of cyber defence are the result of significant bilateral engagement.
- **The NATO secretary general, Jens Stoltenberg, engaged in a contentious debate with the chair of Russia's Federation Council Committee on International Affairs, Konstantin Kosachev, at the tenth annual Brussels Forum conference held on 20 March.** Kosachev asked if NATO would bomb countries it suspected of being involved in cyber attacks, an overt reference to the applicability of Article 5.[18]

[15] https://www.aei.org/wp-content/uploads/2015/04/Growing-Cyberthreat-From-Iran-final.pdf

[16] http://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies and http://blogs.wsj.com/digits/2015/03/23/when-cybersecurity-meets-geopolitics/

[17] http://www.pcworld.idg.com.au/article/572593/deterrence-will-keep-lid-cyberwar-former-spy-chief-says/

[18] http://www.defensenews.com/story/defense/policy-budget/warfare/2015/03/25/nato-cyber-russia-exercises/70427930/

Commissioned by the Remote Control Project

remotecontrolproject.org

REMOTE CONTROL

Examining changes in military engagement

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