# Remote-control warfare briefing | #14

7 April 2016

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:** Covert activities of French and Italian special operations forces in Libya revealed.

**Private military and security companies:** Mercenaries increasingly being used in Yemen conflict.

**Unmanned vehicles and autonomous weapons systems:** US Department of Defence developing robotics and autonomous systems strategy.

**Cyber conflict:** Developed economies of Asia-Pacific have highest cyber exposure in the region.

**Intelligence, surveillance and reconnaissance:** European Union and United States reach transatlantic data-transfer agreement.

## Special operations forces

### Covert activities of French and Italian special operations forces in Libya revealed

Italian and French media have revealed new covert activities in Libya by their countries' respective special operations forces (SOF). Media reports suggest that France's special forces and its external intelligence agency, the General Directorate for External Security (DGSE), have been involved in Libyan reconnaissance activities for a number of months. In Italy, *Corriere Della Sera* has reported that Comsubin and Col Moschin SOF units will be deployed to protect sensitive sites in Libya, including energy production infrastructure.[1] The Italian and French forces are likely to be loosely coordinating reconnaissance and occasional airstrikes in collaboration with US and British special operations forces.

[1] http://www.corriere.it/english/16_febbraio_26/intervention-libya-go-ahead-for-secret-missions-3ec41280-dc84a2d58f9c6b.shtml?refresh_ce-cp

**Open Briefing**
27 Old Gloucester Street
Bloomsbury
London WC1N 3AX

t 020 7193 9805
info@openbriefing.org
www.openbriefing.org

While these small footprint deployments have tried to keep their operations covert, the possibility of their involvement in a US bombing raid on an Islamic State (IS) training camp near Sabratha in northwestern Libya on 19 February refocused attention on their presence. The presence of these special operations forces is seen as a tactical halfway house.

NATO members have been reluctant to once again intervene in Libya for fear of further inflaming nationalist sentiment and increasing support for Islamic State and other militant Islamist organisations in Libya. Furthermore, partnerships with politically-divided local militias would likely result in Western countries being pulled into complex rivalries and undermining the push for Libyan unity. As such, many have argued for the formation of a national unity government before any Western military intervention in the conflict. However, due to their size, special operations forces must rely to some degree on local partners, which may include local militias. French special operations forces are allegedly stationed at the Benina air base near Benghazi, which is controlled by General Khalifa Hafter's forces. In the west of the country, the US and British SOF teams are alleged working with militias from Misrata. These alliances may represent significant risks for members of the international community trying to broker a political solution in Libya.

The willingness to accept these risks reflects concerns that Islamic State will shift key logistical support and infrastructure to Libya as attacks on its territory in Syria and Iraq intensify. Islamic State's current presence in Libya and the potential for the country to become a major rallying point for violent jihadist groups from the Sahara and Sahel is perceived by southern Europe as a significant security risk.

On the ground, SOF assets provide a pivot point for Italian, French, British and US policymakers and military planners to incrementally build up and expand their military presence if political solutions and diplomacy fail. In contrast, the commander of Special Operations Command, Africa (SOCAFRICA), Brig. Gen. Donald C. Bolduc, argues that Libya requires military intervention regardless of political negotiations because local militias lack the training and equipment necessary to effectively confront Islamic State. Indeed, it is likely that some European countries and the United States will expand their SOF presence in Libya in response to increasing numbers of IS fighters rather than wait for a political resolution or the formation of a national unity government. As in Iraq, Western intervention has let the 'genie out of the bottle' in Libya, and the United State and Europe are now considering further intervention in response.

**Other developments**

**South Korea's Yonhap news agency has described this year's South Korean and US Key Resolve (7-18 March) and Foal Eagle (7 March-30 April) exercises as training simulations of surgical strikes on nuclear and missile sites in conjunction with a precision strike against the North Korean leader, Kim Jong-un,** that would cause the North Korean central command to collapse. Precision strikes on the North Korean central command would considerably impede Pyongyang's ability to launch asymmetrical attacks against South Korea. The Korean People's Army threatened strikes on high value targets in Seoul in response to the reports of special operations forces training for beheading operations or high-density strikes. The commander of United States Special Operations Command (USSOCOM), General Joseph Votel, confirmed to the Senate Armed Services Committee on 8 March that the US special operations force presence in South Korea is at an all time high.[2]

[2] http://www.armed-services.senate.gov/imo/media/doc/16-23_03-08-16.pdf

**In late February, the United States' specialised expeditionary targeting force (ETF) in Iraq captured Islamic State operative Sleiman Daoud al-Afari, a chemical weapons expert who worked for Saddam Hussein's regime.** The capture possibly signals that US military planners in Iraq will employ a similar model to Joint Special Operations Command (JSOC) in Iraq and Afghanistan: incrementally building intelligence from captured militants in order to disrupt and destroy the leadership hierarchy. The increase in kill/capture missions has prompted questions about the detention of captured militants. Senate Armed Services Committee hearings in early March showed a clear disjuncture between military planners seeking opportunities for longer-term detention and the Pentagon's stated preference for shorter-term detention before handing prisoners over to local Iraqi or Kurdish authorities.[3] With no domestic detention facilities, such as Guantanamo Bay, available to detain captured combatants, the US administration is likely to selectively seek US indictment for high-value targets or high security-risk individuals and turn over lower-risk captives to local jurisdictions.

**In late February, it was reported that the Pentagon has offered Nigeria a platoon-sized team of SOF operators for advise and assist missions to support its fight against Boko Haram.** The proposed deployment comes after the SOCAFRICA commander, Brig. Gen. Donald C. Bolduc, expressed concern during February's Exercise Flintlock in Senegal and Mauritania about Islamic State and its affiliates becoming more effective through networks in the Sahel and Sahara. If given executive approval, the US SOF deployment is expected to re-establish positive military-to-military relations between the United States and Nigeria after relations soured in late 2014 and 2015 when the United States blocked defence sales to Nigeria and refused to share intelligence over concerns Boko Haram had infiltrated the Nigerian Army. The proposed assistance will almost certainly improve the Nigerian army's ability to carry out night raids and ambushes against Boko Haram.

**Also of note**

- **A joint Somali-US SOF kill/capture raid in Awdhegle on 8 March resulted in 10 al-Shabaab casualties.** The raid, apparently aimed at capturing a high-value target, came days after US airstrikes on al-Shabaab's training camp north of Mogadishu killed 150 fighters.
- **Iranian Revolution Guard Corps (IRGC) commemorations for eight commandos killed in advise and assist missions in mid-February indicate that an elite Iranian special forces unit called Saberin is active in Syria.**[4]
- **On 2 March, Jordanian special forces killed seven suspected militants allegedly plotting an attack within Jordon.** The Jordanian security service suggested that intelligence on the group and their activities indicated a link to Islamic State. The night raid, which occurred close to the town of Irbid, near Jordon's northern border with Syria, will reinforce concerns over border security.
- **On 25 February, the Turkish Parliament's Foreign Affairs Commission debated a memorandum of understanding between Turkey and the United States to establish joint SOF exercises.** Detractors pointed out that joint exercises had already taken place without the agreement of the countries respective national legislatures, while supporters raised the implications for Turkey's standing as a NATO ally if the memorandum is not ratified.

[3] http://www.armed-services.senate.gov/imo/media/doc/16-23_03-08-16.pdf

[4] http://www.longwarjournal.org/archives/2016/02/irgc-saberin-special-forces-at-work-in-syria.php

- **The leader of the IS-linked Mujahidin Indonesia Timur (MIT), Abu Warda Santoso, has been identified by the US Department of State as a specially-designated global terrorist** for his incitement of violence and MIT's attacks against Indonesia's special counter-terrorism force, Special Detachment 88. Santoso alleges that Densus 88 has been infiltrated by US and Australian interests set on eradicating Islamic communities from Indonesia.
- **The head of US Central Command (USCENTCOM), General Lloyd Austin, has advocated the United States reboot its scrapped $500 million programme to train and equip moderate Syrian rebels.** In testimony before the Senate Armed Services Committee, Austin proposed a varied SOF-led training model focused on the shorter-term training of smaller units.[5] Despite consistent criticism of the programme, some US SOF voices are suggesting US trained rebels are performing very well and are critical to undermining Islamic State's territorial control.[6]
- **The interoperability of special operations forces was a key theme of the annual Global SOF Foundation Symposium held in Tampa, United States, in late February.** The proliferation of regional SOF operations and training programmes means that national militaries are increasingly participating in multiple partnerships with differing levels of priority.

[5] http://www.armed-services.senate.gov/imo/media/doc/Austin_03-08-16.pdf

[6] http://www.stripes.com/news/middle-east/us-backed-syrian-rebels-suffer-heavy-losses-1.398259

## Private military and security companies

**Mercenaries increasingly being used in Yemen conflict**

Houthi militias and other groups who support the ousted Yemeni president, Ali Abdullah Saleh, have reportedly extended their use of mercenaries in their fight against the Yemen Army. A new wave of fighters, sourced mostly from African countries, are being promised sizeable sums of money to help defend the Houthi-held capital, Sana'a, against an expected major offensive by Yemeni government forces. The Lebanese militia group Hezbollah has also increased its presence in the country in support of the Houthi.

Houthi forces have suffered a string of defeats in recent months as the Yemeni military has regained lost ground across the country and moved on towards Sana'a. Yemeni forces have been greatly helped by Operation Decisive Storm, a coalition of nine Arab states – Saudi Arabia, the United Arab Emirates, Bahrain, Kuwait, Qatar, Egypt, Jordan, Morocco, Senegal and Sudan – supported by the United States, United Kingdom and France, who supply intelligence, weapons and logistical support. In response to the level of civilian casualties in the conflict, Amnesty International is calling for a suspension of weapons transfers to members of the Saudi-led coalition that have been linked with violations of international humanitarian law.[7]

Meanwhile, there have been uncorroborated reports from various Iranian and fringe media sources that the UAE had contracted the US-based private military and security company (PMSC) DynCorp to replace Academi (formerly known as Blackwater) in Yemen. However, DynCorp has denied that it has any contracts to work in Yemen, and the stories are potentially part of an Iranian disinformation campaign designed to discredit its Sunni rivals.[8] Academi was tasked with securing the territory of Yemeni tribes that have either refused to join the coalition or have announced allegiance to the Houthi rebels. However, the company has suffered significant losses in the few months they have been operating in the country. Academi has also reportedly been forced to withdraw completely from operations around Bab-el-Mandeb in the southwest of the country after heavy losses there.

In November 2015, the *New York Times* reported that the UAE has previously dispatched hundreds of Colombian mercenaries to Yemen.[9]

[7] https://www.amnesty.org/en/latest/news/2015/10/yemen-call-for-suspension-of-arms-transfers-to-coalition-and-accountability-for-war-crimes/

[8] http://www.dyn-intl.com/inside-di/dyncorp-international-in-yemen-reports-are-false/

[9] http://www.nytimes.com/2015/11/26/world/middleeast/emirates-secretly-sends-colombian-mercenaries-to-fight-in-yemen.html?_r=0

**Other developments**

**A January 2016 US Department of Defense (DoD) report stated that the number of private contractors working for the DoD in the US-led Operation Inherent Resolve in Iraq has grown eight-fold in the past 12 months,** up from 250 to 2,028.[10] The DoD component is only a fraction of the overall contingent of US contractors, with other US Government departments, such as the state department, employing around 5,800 more contractors. This sharp rise is indicative of the increasingly heavy reliance the US government has developed on civilian staff in Iraq. In the 1980s, the US military started using contractors for support roles on operations, in sectors such as catering, accommodation maintenance and utilities. Today, the civilian contractor sector has extended to cover translation, logistics and transport, base security, convoy security, construction, communications, training, base management, administration, operation room support and tactical intelligence analysis. There is also a demand for contractors beyond these conventional roles. The CIA and other US intelligence agencies are increasingly using civilian contractors for work far closer to the frontline, providing security for bases and for agents operating in the field, and also on other highly classified intelligence duties.

**Human rights experts Patricia Arias and Saeed Mokbil from the United Nations Working Group on the use of Mercenaries visited Ukraine on 14-18 March to establish the use of mercenaries and PMSCs by both sides in the conflict and the impact on human rights and the safety of civilians.** The delegation met with government officials, parliamentarians, representatives of NGOs, former fighters and representatives from the self-declared Donetsk Peoples Republic (DPR) and Luhansk People's Republic (LPR). The Ukrainian government informed the delegation that at least 176 identified foreigners were serving in the armed groups of the DPR and LPR, which reportedly include large numbers of fighters from from Russia, Serbia, Belarus, France and Italy among others. In a preliminary statement issued after the visit, the working group called on the Ukrainian government to ensure accountability for human rights violations committed by foreign fighters during the conflict.[11] The delegation also revealed that there had been repeated human rights violations committed by mercenaries and other foreign fighters, including volunteers, independent militia members and professional military from foreign armed forces. The working group delegation will eventually submit a report to the UN Human Rights Council in September 2016.

**In March, Dr Wesley Mutwara, a senior lecturer in war and strategic studies and the chair of the history department at the University of Zimbabwe, warned that the proliferation of PMSCs in Africa poses a serious threat to the survival of some states teetering on the brink of civil strife.** Mutwara said that there has been a proliferation of these companies across the continent since the end of the Cold War and the security vacuum caused by the departure of Western and Soviet support structures. These departures resulted in many failed democratic transitions and widespread anarchic situations, and consequently an urgent need for security solutions. It was then that a large number of private military companies found themselves in demand. Mutwara said some of the conflicts in Africa were actually fuelled by the PMSCs, unravelling the traditional paradigm that the state monopolised the exercise of legitimate violence.

[10] http://www.acq.osd.mil/log/PS/.CENTCOM_reports.html/5A_January_2016_Final.pdf

[11] http://www.un.org/apps/news/story.asp?NewsID=53518#.VvlKV0dqsrk

**Also of note**

- **The Russian Duma is continuing to discuss legalising and regulating its PMSC sector.** The FSB and the Russian defence ministry have both aired concerns that this sizeable industry might one day turn their weapons against the government.
- **The world's major state aid donors have agreed to expand the definition of development aid to include military and security training.**[12] This may result in significant aid funding being diverted to PMSCs to provide such services.
- **US Democratic Party presidential candidate hopeful Hillary Clinton has been accused of overlooking human rights abuses in Mexico** while heavily funding security assistance contracts on behalf of the Mexican government.

[12] http://news.trust.org/item/20160219182509-fbgt0/

## Unmanned vehicles and autonomous weapons systems

**US Department of Defence developing robotics and autonomous systems strategy**

The US Department of Defense (DoD) currently requires that a human operator/commander retains the final say on whether an armed remote-vehicle deploys its weaponry or whether an autonomous weapon strikes its target, something which campaign groups are very determined to see continue. However, it is widely believed that the Pentagon is considering using technology that will allow for these platforms to decide to deploy their lethal force independently of human oversight or control.

The Pentagon is currently working on the Third Offset Strategy, which is pursuing a military vision where every branch of the military – Army, Air Force, Navy and Marines – will have access to a wide range of unmanned vehicles providing logistics, communications, surveillance, reconnaissance and strike capabilities, combining as exponential force multipliers. Projects currently in early development include autonomous road vehicles for transporting supplies, submersibles for carrying out anti-submarine missions for naval task forces, portable drones for close-range reconnaissance by frontline ground forces, and micro-drones that can be launched from fighter aircraft flare dispensers and then operate as a coordinated swarm to provide electronic countermeasures, forward surveillance or a mass strike capability.

This programme is at an embryonic stage. There is still no 'book' being written on the development strategy, and there remain many considerations and concerns on how humans will work alongside such machines. One of the central discussions is on giving robotic systems the autonomy to deploy their weaponry without a human in the loop. A potential litmus test of the US military's intentions could be existing remotely-controlled weaponry, such as fixed machine gun emplacements situated on the perimeters of major bases, which were used in Afghanistan. Here, it was found that operators were often hesitant to use these in a counter-insurgency environment where there was a large civilian population in the battlespace because of the risk of collateral injuries. In the future, these could realistically be automated to react to targets occupying restricted security zones. If and when these become fully autonomous, it would signal the start of a new military paradigm.

Speaking at the National Defense Industrial Association's Ground Robotics Capabilities conference in Springfield, Virginia, Melissa Flagg, the US Deputy Assistant Secretary of Defense within the Office of the Undersecretary of Defense for Acquisition, Technology and Logistics' Research Directorate, said that the DoD currently believes that such weapons would primarily be used on deep strike operations, well inside enemy territory in highly-hostile environments where long-range communications and control would be extremely challenging. Under these circumstances, an open communications channel carrying constant control signals to unmanned air vehicles (UAVs) would compromise any chance of a surprise attack and create a risk of control of these vehicles being taken over by the enemy. However, if the vehicle is operating without human control, knows the route and the target (as cruise missiles do now) and can also react to air defence threats and alter its own flight path, proponents of this technology argue that it could be considered a viable requirement for it to then also engage its target independently, without waiting for human approval that might never be received through a wall of electronic countermeasures and defences.

A Pentagon team developing the DoD's robotics and autonomous systems policy, is currently putting together a strategic document that will set the medium- to long-term direction for defence investment in robotics and autonomous technology. This report, due in May 2016, adopts the concept where an all-arms force will utilise integrated units of humans and technology with proposed in-service dates from 2035 onwards. However, at the moment, campaigners will be relieved to know there is no sign of fully-autonomous weaponry being included.

**Other developments**

**A new report written by a former Pentagon staffer who helped establish the United States' policy on autonomous weapons has argued that such weapons could potentially be at risk from hacking, spoofing and other hostile manipulation** that could see the weapons turn on their controllers or detonate among civilian populations.[13] The report, *Autonomous Weapons and Operational Risk*, was published in February by the Center for a New American Security in Washington DC.[14] In the report, Scharre warns about extensive risks that would develop with weapons systems that are completely autonomous. Fundamentally, his concerns are with the difficulties that any programmed guidance and sensor systems would have trying to cope with the multiple threats and other issues that could arise in any mission in hostile environments. Even simple human coding errors have led to serious problems in the highly-technological platforms that are already in service today. The report provides the example of eight brand new F-22 Raptor aircraft flying across the Pacific and suffering total computer failure when they crossed the international date line, nearly resulting in the loss of all the aircraft. The report proposes an alternative to autonomous weapons: 'centaur warfighting'. In this, human operators and technology are closely integrated and the human acts in three simultaneous roles of *operator* (assisting the system with complex scenarios), *moral agent* (making value-based judgements on whether force is appropriate) and *fail safe* (intervening when systems fail or circumstances suddenly change).

**There has been an increasing number of near-misses caused by over-zealous or malicious amateur drone users flying their drones close to aircraft arriving and departing at major airports.** In some cases, drones have been reported within feet of airliners, prompting serious concerns that one will eventually be sucked into an engine, with potentially disastrous consequences. In the United States alone, the Federal Aviation Administration has seen reports of drone sightings near airports quadruple in the last 12 months, prompting urgent calls to aerospace and defence companies for a solution to this problem. Among the resulting proposals, two show significant potential. US defence and professional services company CACI has developed Skytracker, a new drone detection technology that identifies a rogue drone's control signal and tracks it back to the operator. CACI also claim that Skytracker allows law enforcement agents to deploy electronic countermeasures that could allow them to take over control of the drone and force it to land or return to its operator. Meanwhile, a UK company, OpenWorks Engineering, has developed Skywall 100, a man-portable, shoulder-mounted launcher that fires a projectile that then deploys a large net to snare a target drone. The advantages of this equipment is that it does not require the transmission of electronic signals and therefore would not interfere with airport radar and communications.

[13] http://www.cnas.org/autonomous-weapons-and-operational-risk#.VvrrfY-cGUl

[14] http://www.cnas.org/sites/default/files/publications-pdf/CNAS_Autonomous-weapons-operational-risk.pdf

**Afghanistan will shortly field up to 48 ScanEagle surveillance drones supplied by NATO.** Struggling all but alone against the Taliban and other violent Islamist groups, the Afghanistan National Army (ANA) will soon take delivery of the Boeing-manufactured drones. ScanEagle is a long-endurance UAV that can fly for over 24 hours, with a 15,000-foot ceiling and a range of 62 miles. It is catapult-launched from a small towed trailer, meaning no airfield or airstrip is needed – making it well-suited for Afghanistan's mountainous terrain. Afghan soldiers will be trained to operate the system. Initial cadres are already undergoing training in the United States, and the ANA will be assisted by international training and maintenance contractors for at least the first three years. Eight systems of six aircraft each are being provided for initial deployment in the north and south of Afghanistan where the fighting is at its heaviest. These are expected to become major force multipliers for the ANA, providing tactical surveillance and live video feed capabilities to ground troops and commanders – areas that the ANA has repeatedly appealed for international assistance with.

**Also of note**

- **The United Kingdom and France have confirmed a joint £1.5 billion stealth armed drone development programme.** With initial flights in 2020, the in-service target date is expected to be around 2030.
- **Drones flown by unidentified parties have been repeatedly spotted flying over the Kitsap-Bangor Naval base in Washington state.** The base is home to eight Trident ICBM submarines, and the US Navy has started a major investigation, including interviewing all residents in the area.
- **Iranian state footage from Syria has confirmed that Iran has deployed weaponised Shahed-129 drones to the area in support of Syrian government forces near Aleppo.** The S129 is a medium-altitude, long-endurance (MALE) UAV capable of being armed with four to eight glide bombs or missiles.
- **'Invisibility cloaks' that disguise a vehicle by altering its radar or infra-red signature could be illegal under the Geneva Convention** if the intent is to disguise a combat vehicle as a non-combatant, according to a UK report on emerging technologies and their impact on the laws of armed conflict.[15]
- **A Singaporean company has unveiled a short-range surveillance drone that can both fly and travel underwater.** ST Engineering's vehicle flies using a single rear propeller that then folds and feathers while two smaller propellers power the drone underwater.[16]

[15] https://www.theguardian.com/science/2016/mar/14/military-invisibility-cloaks-stealth-could-breach-geneva-conventions

[16] http://www.defensenews.com/story/defense/show-daily/singapore-air-show/2016/02/18/air-phibious-drone-flying-fish-uav-swims-and-flies/80563292/

## Cyber warfare

**Developed economies of Asia-Pacific have highest cyber exposure in the region**

In its *Asia-Pacific Defence Outlook 2016*, the multinational professional services company Deloitte Touche Tohmatsu has identified Japan, Australia, Singapore, South Korea and New Zealand as countries nine times more vulnerable to cyber attacks than other Asian economies.[17] The report identified the 'Cyber Five' based on the dependency of their domestic economies and productivity on internet-based interactions. China and India were considered to have less cyber vulnerability due to the lower connectivity of government and critical infrastructure and the lower contribution of knowledge industries to their GDPs.

Deloitte's cyber vulnerability index has limitations in that it does not incorporate cyber security countermeasures or other metrics used in the *Cyber Maturity in the Asia Pacific Region 2015* report by the International Cyber Policy Centre (ICPC) of the Australian Strategic Policy Institute.[18] The Cyber Five identified in the Deloitte vulnerability index are all included in the top six countries for cyber maturity in the ICPC report.

However, the focus on vulnerability as defined by economic dependency on e-commerce, highly-connected infrastructure and knowledge sectors does show which countries have the most to lose from cyber offensives and espionage in comparisons to those countries with lower levels of economic dependence. The Deloitte report highlights a vulnerability gap where countries with both lower exposure and high investment in cyber capabilities may have significant advantages in and incentives to conduct aggressive cyber operations. This leaves the Cyber Five with two broad strategic paths: improved cyber security or deterrence and countermeasures outside of the cyber realm, such as trade sanctions.

A report in late February suggests that some of the Cyber Five and other Southeast Asian middle powers have not reached an optimal level of cyber security or defence maturity. Cyber security company Cylance published a report on Operation Dust Storm identifying a long-term persistent threat using spear phishing and zero-day exploits against government and defence targets across Southeast Asia and the United States dating back to 2010.[19] The report noted that the bad actors employed increasingly sophisticated malware and zero-day exploits over the last five years and in 2015 exclusively focused attacks on Japanese critical infrastructure companies and Japanese subsidiaries of multinational companies.

Lack of international cooperation agreements on cyber threat information sharing and limitations on Japanese intelligence agencies may be isolating Japan as a prime target for cyber attacks and espionage. Professor Motohiro Tsuchiya of Keio University in Tokyo was quoted in news outlets citing constitutional limitations on domestic intelligence and surveillance activities as impeding cyber ISR and information sharing with regional partners.[20] This may pose a risk beyond Japan, as the country may become a testing ground for cyber operations.

[17] http://www2.deloitte.com/sg/en/pages/public-sector/articles/deloitte-2016-asia-pacific-defense-outlook.html

[18] https://www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2015/Cyber-Maturity-2015.pdf

[19] https://www.cylance.com/operation-dust-storm

[20] http://www.abc.net.au/news/2016-02-26/japan-vulnerable-to-cyber-attacks:-academics/7196450

While the Deloitte vulnerability index can be misinterpreted and only gives a small part of the full picture, it does highlight how varied economic structures across the Asia-Pacific may shape cyber operations in regional conflicts and reinforces the importance of cyber security for economies highly dependent on knowledge sectors and information technology.

### Other developments

**US-Iranian relations have been damaged by the revelation that the United States had developed a contingency plan for if the P5+1 Iranian nuclear deal failed involving a cyber attack operation named Nitro Zeus.** The operation was designed to disable and disrupt Iran's critical infrastructure sectors and military, including power grids, air defence systems and communications. It would most likely have been led by US Cyber Command and the NSA's Tailored Access Operations unit. The contingency plan reveals an important strategic trend in concurrently striking a target's civilian infrastructure and military capability. US intelligence agencies were also reportedly developing a cyber operation to sabotage Iran's underground Fordo Fuel Enrichment Plant. US Department of Justice indictments of seven Iranian hackers for unsophisticated cyber intrusions and reconnaissance on the Bowman Avenue Dam in New York State in 2013 have aggravated US-Iranian tensions further.

**The US defence secretary, Ash Carter, told the RSA Conference in San Francisco in early March that US Cyber Command (USCYBERCOM) had initiated offensive cyber attacks against Islamic State.**[21] While the defence secretary and USCYBERCOM have been tight lipped about what the offensive will involve, the objective appears to be disruption of key communication networks in Mosul and Raqqa or pushing Islamic State onto more interceptable communication platforms. Isolating Islamic State in Mosul and degrading internal trust in IS communication networks is most likely intended to lay the foundations for kinetic offensives to recapture Mosul from Islamic State. The announcement of USCYBERCOM attacks against IS assets is the first time a US administration has acknowledged it is engaging in an offensive cyber campaign. This signalling of cyber intentions rather than covert operations allows the administration to point to military operations degrading IS capabilities without further troop commitment as political pressure builds for greater participation by US special operations forces on the ground against Islamic State.

**Sweden-based cyber security company Unleash Research Labs has identified the Myanmar Army as the likely source of distributed denial of service (DDoS) attacks and website defacement after a three-year investigation.**[22] The investigation suggests that hacktivist activity could be linked back to a military network run by the Defense Services Computer Directorate, likely running controversial Blue Coat security technology. Independent media voices covering Myanmar such as Democratic Voice of Burma (DVB) and The Irrawaddy were the main targets of DDoS attacks, particularly during periods when the outlets ran extensive coverage of ethnic conflicts in Rakhine and Kachin states. The report also highlighted false flag hacktivist attacks whereby army cyber activities portrayed website defacements as actions of ethnic armies to justify conflict escalation.

[21] http://www.baltimoresun.com/news/maryland/bs-md-secret-cyber-campaign-20160306-story.html

[22] http://unleashed.blinkhackergroup.org/

**Also of note**

- **The December 2015 cyber attack on Ukraine's electricity distribution network has raised domestic concerns in the United States.** Two bills before Congress are garnering renewed attention, particularly the Energy Policy Modernization Act, which would vest emergency powers in the energy secretary to take control of the country's power grid in the event of a cyber attack.
- **The Israeli government is reportedly allocating $26 million to new cyber operations aimed at countering Boycott, Divestment, and Sanctions (BDS) campaigns and activists.**[23] Public comments from a Ministry of Foreign Affairs official suggest that the operations are likely to take the form of cyber sabotage and social network disruption measures.
- **North Korea has intensified a cyber offensive campaign against South Korea.** In early March, South Korea's National Intelligence Service told a parliamentary committee that North Korean intelligence agencies launched a cyber offensive against a railway company, financial institutions, such as major banks and insurers, and South Korean foreign affairs, security and military officials.[24] Data was successfully stolen from the smartphones of over 40 officials.
- **The US administration has requested the state department reopen negotiations on the Wassenaar Arrangement provisions on surveillance software exports.** The Wassenaar Agreement was intended to prevent the proliferation of commercial malware and hacking tools that are accessible by repressive regimes. The security sector and cyber security researchers alike have dismissed the US export regulations made pursuant to Wassenaar as unworkable.
- **Verizon reported a shipping company was the target of a network intrusion that compromised data on shipping cargo allowing the bad actor to secure detailed information on specific container cargo.** With this information, pirates can undertake 'hit and run' attacks taking the most valuable cargo rather than holding the crew and cargo for ransom.
- **The United Kingdom's shadow home secretary, Andy Burnham, speculated that crime rates would effectively double once cyber crime is officially added to Office for National Statistics crime data reports.** Preliminary field trials carried out in 2015 revealed that official crime rates increase by a 107% when cyber crime is included in reports.
- **A former Australian Defence Force (ADF) evaluation and testing specialist has raised concerns that the F-35 Joint Strike Fighter has not been subject to any cyber vulnerability testing yet.**[25] The former ADF member pointed out that as one of the most software driven aircrafts ever built, cyber security will be a critical component of the F-35's success.

[23] http://bigstory.ap.org/urn:publicid:ap.org:0601a79f13e041b9b5b312ec73063c98

[24] http://www.usnews.com/news/world/articles/2016-03-11/seoul-number-of-north-korean-cyberattacks-doubles

[25] http://warisboring.com/articles/aussie-who-led-weapons-tests-knocks-f-35/

## Intelligence, surveillance and reconnaissance

**European Union and United States reach transatlantic data-transfer agreement**

While the media has focussed on the FBI's pursuit of Apple to unlock the iPhone of San Bernardino attacker Syed Rizwan Farook, negotiations between the European Union and the US government on the transatlantic data-transfer agreement have continued unabated. In February, Brussels and Washington reached an agreement on the framework, aimed at helping companies from both blocs seamlessly shuffle data between each other. The previous proposal, going under the working name Safe Harbour, was struck down by an EU court last year following the political backlash to Edward Snowden's revelations of US spying operations on EU countries.

Companies and banks routinely transfer data across the Atlantic to conduct bank transfers, travel bookings and other transactions. Data transfers are also necessary for social media companies and internet advertisers. The new proposal, now under the name Privacy Shield, will be subject to an annual review by the EU to ensure that companies transferring data to the United States are abiding by European data protection standards and that the United States is not conducting indiscriminate mass surveillance on EU-based individuals and organisations. The EU has also called on US companies to work with EU data protection authorities and provide aggregate statistics of US government data access requests to establish whether such requests are targeted and not indicative of mass surveillance.

The changes include a new ombudsman that will act as a point of call for Europeans who feel that their data protection rights are being violated by US agencies. However, the main enforcers of the framework will be the US Department of Commerce and the US Federal Trade Commission after Washington resisted EU pressure for a greater role for European data protection authorities in enforcing the pact, a decision which has been heavily criticised by privacy advocates. Surveillance law experts, including Max Schrems who brought the original EU challenge against Safe Harbour, say that the EU-US agreement does not solve many key privacy problems and still facilitates mass surveillance. In short, the new agreement relies too heavily on assurances from the US authorities and still allows for the indiscriminate and mass gathering of data.

The announcement of Privacy Shield is linked to the Judicial Redress Act recently signed into law by the US president, Barack Obama. The Act incorporates provisions so that European citizens can use the US court system to seek legal protection of their privacy rights. However, the rights covered by this Act are extremely limited, and Europeans will only be able to use the US courts to sue US government agencies for infringement of the Privacy Act of 1974. The Privacy Act of 1974 established a set of principles that US government agencies need to follow related to collecting and maintaining personal data, such as providing individuals access to records about themselves, much as the United Kingdom's Data Protection Act (DPA) does. However, again, like the DPA, this Act includes so many exemptions as to make redress extremely complex for US, let alone EU, citizens. This will be even harder if cases are fenced off by agencies as a matter of national security as many EU claims will probably be.

### Other developments

**While the FBI continues to have to fight Apple to gain access to one iPhone, proposed UK surveillance legislation could allow British security agencies to do much the same thing covertly.** The draft Investigatory Powers Bill, currently being redrafted after criticism from parliamentary committees that it uses deliberately broad and vague language, is set to introduce legislation that could be used to order technology and communications companies to sidestep subscribers' encryption and privacy protections by incorporating backdoors in their products and services. Another section of the Bill relates to a 'bulk equipment interference', the government's preferred term for hacking. The government states that this power will be reserved for the intelligence agencies and only directed towards foreign targets. However, critics argue this power could be used to authorise the spreading of technological back doors, for example GCHQ could exploit a manipulated operating system, installing it into any number of handsets to gain covert access and monitoring. Parliament's intelligence and security committee has recommended that the bulk equipment interference facility is removed from the draft Bill.[26]

**While many Republican and libertarian groups in the United States are calling for the repeal of Executive Order 12333, which gives the NSA broad authority to collect signals intelligence outside the country, the Obama administration is considering expanding it.** The Order was introduced by President Ronald Reagan, but it was revealed by NSA whistleblower Edward Snowden that the NSA had long since expanded its powers to include domestic surveillance too by accessing any US data that leaves US soil. US technology and communication companies often use servers based in other countries for their data, thereby bringing access within the remit of Executive Order 12333. The NSA has stated that it reduces 'collateral surveillance' and protects the privacy of innocent civilians through a broad minimalisation process that strips out irrelevant data when sharing intelligence with other government agencies. However, the White House proposal would remove this requirement and allow the freer exchanges of intelligence between agencies, potentially allowing access of personal phone and email records.[27]

**Admiral Michael Rogers, the director of the NSA and commander of US Cyber Command, has warned that increasingly complex encryption tools are making it much more difficult for security agencies to effectively monitor terrorist groups, such as Islamic State.**[28] He highlighted the attacks in Paris in November 2015 as an example of when security agencies were unaware of a major plot because the perpetrators used new technologies to encrypt and hide their communications. Rogers confirmed media analysis that speculated that the attackers' communications were encrypted and, as a result, there were very few indicators of an impending attack. Rogers' comments came as the FBI requested a court order requiring Apple to provide a backdoor into the data on the iPhone of Syed Rizwan Farook, one of the shooters in the San Bernardino terrorist attack in December 2015. The NSA director's remarks are the latest shot in a heated debate between the US intelligence and law enforcement communities and privacy advocates and communications companies. While the NSA has tried not to become embroiled in the debate on personal privacy, it has made no secret of how urgently it needs to find a way around encryption in order to continue its operations.

[26] http://motherboard.vice.com/read/while-apple-fights-fbi-uk-surveillance-law-could-demand-secret-backdoors

[27] http://www.nytimes.com/2016/02/26/us/politics/obama-administration-set-to-expand-sharing-of-data-that-nsa-intercepts.html?_r=1&mc_cid=bad57cfce4&mc_e%85

[28] https://www.yahoo.com/politics/nsa-chief-paris-would-not-have-happened-without-184040933.html?utm_source=Sailthru&utm_medium=email&utm_campaig…

**Also of note**

- **A new report from Privacy International has revealed that European companies have sold advanced surveillance equipment and software to the Technical Research Department within the Egyptian General Intelligence Service.**[29] Technology was reportedly supplied by Nokia Siemen Networks (Finland/Germany) and Advanced German Technology (Germany), together with software by the Hacking Team (Italy) and FinFisher (Germany).
- **The US Army has restarted training in countering electronic warfare and jamming by hostile forces.** Prompted by worsening relations with Russia, units are now practising responses to disruption of communications and navigations equipment – training that had ceased in the mid-1990s following the end of the Cold War.
- **Wikileaks has revealed that the NSA monitored communications between the German chancellor, Angela Merkel, and the UN secretary-general, Ban Ki-Moon, during the 2011 climate change negotiations.** It also released details of conversations between Merkel and the then French president, Nicolas Sarkozy, and then Italian prime minister, Silvio Berlusconi.
- **China is developing software intended to predict social instability before it arises** based on data-mining analysis of Chinese citizen's personal data, such as jobs, incomes, pastimes and habits.
- **The FBI is seeking help from high school students, asking them to report fellow students who are critical of Western governments and social values.** Based on the United Kingdom's controversial PREVENT strategy, it aims to identify potential extremists, but may result in targeting and harassment of Muslim Americans.

*Commissioned by the Remote Control Project*

**remotecontrolproject.org**

REMOTE CONTROL
Examining changes in military engagement



[29] https://www.privacyinternational.org/sites/default/files/egypt_reportEnglish.pdf