Remote-control warfare briefing | #13

1 March 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: United Arab Emirates and Saudi Arabia pledge special forces to confront Islamic State and support Syrian armed opposition.

Private military and security companies: International anti-corruption organisation renews calls for better regulation of private military and security companies.

Unmanned vehicles and autonomous weapons systems: The dangers of fully-autonomous weapons discussed at World Economic Forum for first time.

Cyber conflict: US president announces Cybersecurity National Action Plan underpinned by $19 billion in proposed federal spending on cyber security.

Intelligence, surveillance and reconnaissance: UK government's draft surveillance legislation threatened by European Court of Human Rights ruling and parliamentary committee criticism.

Special operations forces

United Arab Emirates and Saudi Arabia pledge special forces to confront Islamic State and support Syrian armed opposition

Until now, most of the 27 countries participating in the US-led coalition against Islamic State (IS) have avoided SOF deployments in Syria, despite a number of teams operating in Iraq.[1] However, after a 12 February meeting in Brussels, the US defence secretary, Ash Carter, indicated that Saudi Arabia and the United Arab Emirates have committed to participating in airstrikes against Islamic State and sending special operations forces (SOF) to support and train Syrian opposition forces to retake key cities from the terrorist organisation. The Saudi foreign minister, Adel al Jubeir, confirmed the discussions, and Saudi military personnel have confirmed on state television the participation of Saudi ground forces.

[1] It is confirmed that the United States has SOF operating inside Syria and there is evidence of Russian and Iranian SOF in the country. There is speculation that French SOF are also operating within Syria. There is evidence that Canadian, Spanish, Italian, Australian and British SOF are operating very close to the Iraq-Syria border.

Open Briefing
27 Old Gloucester Street
Bloomsbury
London WC1N 3AX

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

The Turkish foreign affairs minister, Mevlut Cavusoglu, also indicated that Turkey might be willing to join Saudi Arabia in a ground operation against Islamic State. Special operations forces' missions are likely to range from training and advice to limited combat support and assistance.

The UAE and Saudi Arabia play an important regional role in countering the message of Islamic State. The US administration has long coveted the participation of Gulf state ground forces in the fight against Islamic State. The United States and coalition partners will use the participation of UAE and Saudi Arabia as a counter-narrative to Islamic State's 'clash of civilisations' rhetoric. From the coalition perspective, UAE and Saudi SOF involvement carries political, moral and military weight that can support the dismantling of IS ground forces and information-warfare capability.

The recapture of territory by Syrian government forces with the support of Russian airstrikes, has put the Syrian opposition forces on the back foot and inflicted only nominal losses on Islamic State. It is likely that Abu Dhabi and Riyadh perceive President Bashar al-Assad's resurgence in Syria as a longer-term security risk than Islamic State. While both Gulf States acknowledge the security threat posed by the terrorist organisation, it is not seen as an existential threat to the two kingdoms. The special operations forces of UAE and Saudi Arabia are therefore highly likely to use the deployments to bolster the ability of Syrian opposition groups to fight both Islamic State and al-Assad. In contrast, Kuwait and Egypt have reemphasised the need for a politically-negotiated outcome to Syria's civil war.

The SOF deployments in Syria are likely to be very different to those during the Iraq War and against the Taliban in Afghanistan. No single country in Syria has the numbers of SOF operatives and conventional force support to emulate the type of counterterrorism operations used in Afghanistan. SOF in Syria are unlikely to have the full spectrum of intelligence assets and air power support, and may need to rely on coalition partner forces for support. The deployment of reduced-footprint special operations forces by multiple coalition partners is a somewhat untested strategy.

Unconfirmed reports of Russian SOF operatives and intelligence agents being embedded with Syrian counterparts[2] and signals from Russia's political elite that ground operations in Damascus would be interpreted as a declaration of war highlights the dangers of misunderstanding and miscalculation in this conflict. There is also the potential for the actions of both the Syrian Army and the moderate opposition forces to be seen as operations endorsed, sponsored and enabled by the SOF teams of their allies, despite those team's limited control over local fighters and proxies.

Other developments

Exercise Flintlock, a multilateral special operations forces training exercise, was held in Senegal and Mauritania from 8 February until the end of the month. The annual exercise is sponsored by US Africa Command and brings together special forces from members of the Trans-Sahara Counter-Terrorism Partnership, which includes 33 African and Western countries. The exercises reinforce existing bilateral training arrangements, which have recently been expanded by France and Spain, particularly in Cameroon, Chad and Mali, to ensure African forces have unconventional warfare capabilities. The focus on bridging the gaps between SOF and law enforcement possibly indicates anticipation of increased conflict and urban violence from Islamic State, al-Qaeda in the Islamic Maghreb (AQIM) and Boko Haram. On 8 February, the commander of US Special Operations Command Africa (SOCAFRICA), Brigadier General Donald Bolduc, used the Flintlock exercise as an opportunity to express concern that Islamic State and its affiliates were becoming more effective through nascent collaboration across hotspots in the Sahel and Sahara.

[2] https://inmoscowsshadows.wordpress.com/2015/09/26/russians-in-syria-zaslon-and-the-risks-of-going-native/

Eastern European NATO members are rapidly expanding SOF capabilities in response to hybrid warfare threats from Russia. The Czech Republic defence ministry is reportedly establishing a new special operations forces unit to complement the existing 601st Special Forces Group. Ukrainian armed forces representatives held bilateral discussions with the commander of US Special Operations Command Europe (SOCEUR) over further training and support for Ukraine's special operations forces.[3] Lithuania's defence ministry has increased its contribution to the Joint Multinational Training Group, which supports the development of SOF capabilities in the Ukrainian military. Eastern European NATO member's concerns over possible Russian hybrid warfare are shared by the US administration, which is proposing to expand SOCEUR's activity in Eastern Europe with $28.5 million to help fund more rapid force rotations in order to improve joint activities.

Europol, the European Union's law enforcement agency, released a report in late January advising that 'intelligence suggests IS has developed an external action command trained for special forces style attacks in the international environment.'[4] Europol notes that the November 2015 attacks in Paris may indicate that Islamic State is capable of transferring the military tactics employed on the urban battlefields of Iraq, Libya, Yemen and Pakistan to Europe. Europol also notes parallels between the Paris attacks and the 2008 attack in Mumbai in terms of terrorist tradecraft, command organisation and pre-attack reconnaissance activities. However, the report does not address the ability of Islamic State or other groups to access the technology that state special operations forces use to complete particular operations.

Also of note

- **The Canadian prime minister, Justin Trudeau, has announced that the number of Canadian special forces trainers in northern Iraq will almost triple to 230 over the next two years.** The Increased deployment is consistent with recent Canadian Department of National Defence (DND) performance reports that show that SOF funding increased 10% from $267.7 million to $295.2 million in 2014-15. This is significant considering the consistent defence budget cuts since 2012. The announcement comes as Trudeau follows through on an election promise to withdraw Canada from the air campaign against Islamic State.
- **US and South Korean special operations forces completed a 10-day winter training exercise in North Chungcheong Province, South Korea, in early February to improve joint readiness and capability.** The exercise took on greater importance, as North Korea launched a satellite into space in 7 February – a potential precursor to testing long-range ballistic missiles.
- **In mid-February, Cameroonian special operations forces killed over 160 Boko Haram militants in northeast Nigeria.** The force, which is part of a regional multinational counter-terrorism taskforce, also seized a large cache of IEDs and destroyed a training facility.
- **On 23-24 January, Indonesian special forces (Kopaska and Kopassas), in collaboration with over 2,000 soldiers and law enforcement agents, led the country's largest counterterrorism operation since 2009.** Operation Tinombala on Central Sulawesi unsuccessfully attempted to locate and capture the leader of the East Indonesia Mujahidin (MIT), Abu Wardah (aka Santoso), a key Islamic State supporter.

[3] https://usembassykyiv.wordpress.com/2016/01/25/helping-ukraine-defend-itself/

[4] https://www.europol.europa.eu/content/changes-modus-operandi-islamic-state-terrorist-attacks

- **The commander of the United States Forces Afghanistan has provided a 3,000-page report into the US airstrike on the Medecins Sans Frontieres hospital in Kunduz, Afghanistan, to US Central Command.** It is thought the investigation focuses on the US Army Green Beret team that called in the airstrike.
- **Over 200 members of the Indian Garud Commando Force** struggled to counter a limited attack on an Indian Air Force base in Punjab state in early January because of a lack of long-range night vision devices and handheld thermal imagers.
- **US Special Operations Command (SOCOM) has established a technology incubator, SofWerX, in Florida** to address concerns over acquisition red tape and technology lag for special operations.

Private military and security companies

International anti-corruption organisation renews calls for better regulation of private military and security companies

The use of private military and security companies (PMSCs) in conflict zones has significantly increased in recent years. This upward trend has been led by their widespread deployment to Afghanistan and Iraq, where over 250,000 personnel are still employed on private sector contracts.[5] At the height of the international military operation in Iraq, there were around 80 companies from the United Kingdom alone operating in Iraq. Worldwide, the total value of the PMSC sector is currently estimated at around $200 billion.[6]

The increasing shift of military and security responsibilities away from the traditional providers of national governments and towards the independent and often multinational private sector has made it increasingly difficult to attribute responsibility for actions in the field. In a study published on 11 February, *Capacity Gained–Accountability Lost? Establishing a Better Political and Regulatory Framework*, Transparency International has renewed calls for the better regulation of PMSCs. The organisation is concerned about the lack of transparency of the procurement processes of contracts to PMSCs and the imposition of international quality standards. Transparency International is also concerned over the chances of corruption and the accompanying level of impunity that PMSCs could enjoy, especially in the corrupt environments that PMSCs are often deployed to.

Transparency International are particularly concerned over the ways in which the boundaries between state responsibilities and the roles private contractors are fulfilling are being redrawn. Most countries deny that they are outsourcing military responsibilities, often claiming that duties such as providing security for supplies or fixed assets are not traditional government responsibilities. However, while this may be true of some support duties, PMSCs are often involved in frontline combat operations, armed with heavy weaponry and exchanging fire with enemy combatants. In any case, the unconventional warfare being fought in the Middle East, with no clearly defined frontlines and with fighting erupting within supposedly government-controlled zones, has muddied the waters of what is defined as a traditional combat role. Transparency International has pointed towards German military operations in Afghanistan as an example. Here the Bundeswehr has abandoned a long-standing principal where roles like force protection, repairs and logistics were considered core military responsibilities, and has instead started delegating such duties to private companies.

[5] https://www.transparency.org/news/pressrelease/private_military_and_security_companies_a_call_for_better_regulation

[6] https://www.transparency.org/news/pressrelease/private_military_and_security_companies_a_call_for_better_regulation

Transparency International advocates heavily restricting, even banning, the future outsourcing of traditional government military and security responsibilities to the private sector. It argues that where PMSCs are employed, their responsibilities must be strictly stated, their liability to legal redress defined and their operations carried out within the international laws on conflict and human rights. It further argues that moves must also be made to ensure national governments do not 'outsource civil rights abuses' to PMSCs in an attempt to avoid prosecution. Finally, the organisation concludes that national registration and licensing systems are needed to provide clear and transparent standards with regard to the security screening and training of PMSC personnel.

Other developments

Three US civilians were seized from a private house in Baghdad by Iran-backed Shia militia forces over the weekend of 16-17 January. Details have since emerged that two of them may have been working for US giant General Dynamics on a multimillion-dollar deal to train Iraq's counterterrorism forces in the fight against Islamic State. A principal anti-IS force is the Iraqi Special Operations Force (ISOF), part of the country's National Counter Terrorism Service. Iraq's Special Operations Forces were created by the Americans in 2003 and were initially trained by the US military. Continuing this training became untenable after the agreement granting US forces in Iraq immunity from prosecution lapsed in 2011. This led to training being taken over by PMSCs under US coordination. The contract between Baghdad and the Pentagon to provide trainers for ISOF expired in November 2015. This gap in coverage led to a scramble within the Pentagon to provide temporary cover, which was why the pair from General Dynamics were in Baghdad.

Four former employees of Blackwater have filed appeals against their 2014 convictions for murder and manslaughter for shooting dead 14 civilians in Nisour Square, Baghdad, in 2007. At the time, Nicholas Slatten, Evan Liberty, Dustin Herd and Paul Slough were working for Blackwater on a US government contract to escort and protect US embassy officials. They claim that they believed their convoy was being targeted by a vehicle carrying a suicide bomber, and that they opened fire in self-defence, resulting in the deaths of the car driver and 13 others. In 2014, after a series of investigations and trials, Slatten was found guilty of murder and is currently serving a life sentence, while the other three were each given 30-year sentences for manslaughter. The appeal was motivated by a principal witness – a traffic officer operating from a kiosk in the square – apparently changing his testimony in a sentencing hearing in April 2015. Despite this revised testimony, US District Judge Royce Lamberth refused a new trial. The defence lawyers now contend that these changes made by the witness in his statement could acquit the four former contractors. Prosecutors will have a chance to respond to the filings before a federal appeals court hears arguments.

The US Air Force (USAF) has announced that it is trialling using privately-owned fighter jets and pilots to train USAF pilots in the face of continued budget cuts that have seen the recent disbanding of one of its two Aggressor Squadrons, which were used to play the part of enemy fighters in aerial combat exercises. The company, Florida-based Draken International, will initially be participating in exercises run by the Nellis Weapon School within its Mission Employment Phase, a two-week course for experienced pilots from the US Air Force and the US Navy. However, after a trial period, its performance will be re-evaluated to see if it would be capable of participating in the larger 'Red Flag' and 'Green Flag' advanced aerial combat training exercises, which involve participants from NATO countries on live-firing manoeuvres.

Also of note

- **The South African president, Jacob Zuma, is expected to sign the Private Security Industry Regulation Amendment (PSIRA) Bill into law soon.** The act will force foreign-owned private security companies to sell at least 51% of shares to South African citizens.

Unmanned vehicles and autonomous weapons systems

The dangers of fully-autonomous weapons discussed at World Economic Forum for first time

Autonomous weapons – with varying degrees of autonomy – are currently being developed by the United States, United Kingdom, China, Israel, South Korea and Russia. Fully-autonomous weapons will be capable of identifying a target, adjusting behaviour in response to that target, and ultimately firing – all without human intervention. Possible scenarios for the development of this technology include swarms of highly-manoeuvrable airborne micro-drones that can approach a target en masse at high speed before detonating or submersible weapons silently patrolling oceans for submarines, all without any element of human control.

For the first time, fully-autonomous weapons have come under scrutiny at the World Economic Forum in Davos, Switzerland, prompting considerable interest in the subject. At the meeting on 20-23 January, there was considerable focus on the potential advantages and benefits to human progress of autonomous technologies, such as driverless cars; however, one panel changed the tone with a discussion on 'What if robots went to war?'. The panel chair, Sir Roger Carr, an artificial intelligence and robot ethics expert from the UK defence contractor BAE Systems, painted scenarios of rogue robots conducting war against each other and also humanity. While these scenarios have been given life by Hollywood for decades, recent technological developments have provoked groups to start taking this a little more seriously.

Opponents, such as the Campaign to Stop Killer Robots (a group of campaigners, academics and scientists), have emphasised that they have no desires to slow down the overall progress of autonomous capabilities or shut the entire industry down. However, they do hope to ring-fence and regulate the more dangerous sides of the developing technology and pre-emptively ban fully-autonomous weapons capable of selecting targets and using force without human intervention.

In Davos, Sir Roger said autonomous weapons would be 'devoid of responsibility' and would have 'no emotion or sense of mercy'. Despite coming from very different sectors, the panel's participants agreed on one thing during their hour-long discussion: autonomous weapons pose dangers to humans, and swift diplomatic action is needed to halt their development.

Other developments

The next generation of unmanned aerial vehicles (UAVs) and other drones could employ new stealth technologies to become 'invisible'. One military-funded scientist, Professor Boubacar Kanté from the electrical and computer engineering department of the University of California, says his team has developed a new cloaking system that could be used to create truly invisible drones in the near future.[7] His proposal employs the use of an ultrathin Teflon substrate studded with cylinders of ceramic, which can bend light waves around objects coated with it. The US defence department's Defence Advanced Research Projects Agency (DARPA) has also unveiled proposals for a drone that will carry critical supplies to troops and can then 'disappear' after being triggered by the operator or even external factors, such as environmental conditions.[8] The Inbound, Controlled, Air-Releasable, Unrecoverable Systems (ICARUS) project is a continuation of an earlier similar DARPA programme called VAnishing Programmable Resources (VAPR). VAPR proposed the use of vanishing polymers within airframes and on-board circuitry that would turn from solid to a gas when exposed to certain wavelengths of light.

According to ABI Research, a New York-based technology market intelligence company, sales of drones to the consumer market are expected to exceed 90 million units and generate $4.6 billion (£6 billion) in revenue within the next decade.[9] Previous estimates by the company have suggested an annual market growth of over 30%. The most popular models will be those with on-board cameras, though newer capabilities include motion-tracking, obstacle-avoidance and the ability to autonomously fly alongside the user. Future models are expected to move away from fixed manufactured designs to more open versions, allowing the user to design and add their own bespoke add-ons. Open platforms should allow a far greater array of uses for civilian drones. The private drone companies currently mostly offer aerial imagery for media and planning, but innovative add-ons could extend their range of services, opening up new markets.

As a recent report from Open Briefing and the Remote Control project demonstrated, there is a very real security risk from terrorists and other hostile actors using civilian drones for attacks or intelligence gathering.[10] There is also an increasing number of near misses near airports between airliners and irresponsibly-piloted drones. Governments and manufacturers are now taking steps to tackle these risks. A variety of counter-drone systems are being developed, including net guns, signal jamming and even birds of prey, but with limited success. In April, at an as-yet unidentified location in the Untied Kingdom, Selex, a UK subsidiary of Italian conglomerate Finmeccanica, plans to demonstrate one of the most advanced countermeasures: the Falcon Shield system. Falcon Shield is designed to not only detect, identify, track and target hostile or suspicious mini-drones, then take control of them by manipulating electromagnetics so they can be landed safely. This electronic warfare system is scalable and can protect static or mobile targets. Likely customers will be law enforcement and civilian security companies, but the system will also be of interest to militaries.

[7] http://www.smh.com.au/technology/sci-tech/killer-robots-invisible-drones-not-science-fiction-any-more-welcome-to-war-20160118-gm8rwi.html 2/3

[8] http://www.nationaldefensemagazine.org/archive/2016/February/Pages/DARPAInvestinginVanishingAirVehicles.aspx

[9] http://uasmagazine.com/articles/1403/consumer-drone-sales-expected-to-skyrocket-in-coming-decade

[10] http://www.openbriefing.org/thinktank/publications/hostile-drones-the-hostile-use-of-drones-by-non-state-actors-against-british-targets/

Also of note

- **A Nigerian military unmanned combat aerial vehicle (UCAV) has been used to attack a group of Boko Haram fighters for the first time.** The armed drone was carrying out a surveillance mission over the Sambisa Forest in early February when it was used to drop a bomb on an encampment, possibly destroying an ammunition dump.
- **Yemeni forces fighting a Saudi-led coalition in the country claim to have shot down a coalition surveillance drone flying over the country's capital, Sana'a.** Saudi forces are in the country fighting to restore power to the fugitive Yemeni president, Saudi ally Abd Rabbuh Mansur Hadi.
- **Jalal Bala'idi, a senior commander of al-Qaeda in the Arabian Peninsula (AQAP) also known as Hamza al Zinjibari, is believed to have been killed in a US drone strike on 4 February.** Several fighters were reportedly killed in the strike, and jihadists on social media claim that one of them was Bala'idi, who was subject to a $5 million US reward for his location.
- **Turkey claims it has captured a US-supplied drone from Kurdish rebels during Turkish operations against Kurdish Workers Party (PKK) forces** in the Silopi district in southeastern Turkey close to the Turkey-Syria-Iraq border. The RQ20 Puma, a surveillance-only platform, is believed to have been delivered to Kurdish People's Protection Units (YPG) by the United States for use against Islamic State in Syria.
- **The United States has announced a plan to invest $600 million in maritime/submersible unmanned platforms over the next five years.** The US defence secretary, Ashton Carter, told sailors aboard the aircraft carrier USS Princeton that these platforms will be of variable size and payload and were 'a new capability you'll be seeing a lot more of'.[11]

Cyber conflict

US president announces Cybersecurity National Action Plan underpinned by $19 billion in proposed federal spending on cyber security

On 9 February, the US president, Barack Obama, announced a Cybersecurity National Action Plan (CNAP) underpinned by $19 billion in proposed federal spending on cyber security. The plan and the proposed 35% increase in the cyber security budget represent a major modernisation programme for improving the security of the United States' highest-risk networks. It comes at time when other key military and defence spending priorities are shrinking. CNAP includes establishing a federal Chief Information Security Officer (CISO), developing a Commission on Enhancing National Cybersecurity and assembling a Federal Privacy Council. It also includes enhanced funding for Department of Homeland Security advisers to audit and secure critical information communications technology networks (ICT) and supervisory control and data acquisition systems (SCADA) and support for developing human resources and talent.

[11] https://defensesystems.com/articles/2016/02/04/dod-navy-uuv-investments.aspx

CNAP is likely to spur advanced economies to more seriously discuss cyber risks with citizens and prepare institutions for cyber security activity. Some commentators suggest that CNAP reflects a president seeking a legacy at the end of his second term and an administration desperately seeking out reform opportunities in portfolios without obvious partisan divides.[12] While there may be some truth to that, CNAP is a genuine attempt to build a foundation for cyber security in a modern Western economy that is likely to be emulated by US allies and adversaries alike.

CNAP was announced on the same day that the Director of National Intelligence, James Clapper, released the *Worldwide Threat Assessment of the US Intelligence Community* to the Senate Armed Services Committee.[13] The report ranked cyber attacks as the highest threat to US security and identified Russia, Iran, China and North Korea as leading threat actors. The elevation of cyber attacks and espionage to high-risk threats is most likely the result of the recent series of low- to medium-level attacks, such as against the networks of Sony Pictures, the Department of Justice and the Office of Personnel Management, which have demonstrated the considerable cyber capabilities of US adversaries. The US administration and key cyber security agencies are likely to be concerned that the Untied States may face significant economic loss and damage to infrastructure if these emerging capabilities are combined with a stronger, more hostile intent.

The US Government Accountability Office's (GAO) review of the Department of Homeland Security's $1.2 billion National Cybersecurity Protection System (Einstein) expressed concern that the programme was failing to prevent attacks and network breaches.[14] Specifically, the GAO pointed out weaknesses in Einstein's ability to detect intrusions or patterns in malicious traffic, including advanced persistent threats (APTs) and capacity to block traffic identified as malicious by the programme. The GAO review, when considered in light of recent cyber intrusions on US government networks, has created sufficient political pressure for a government response.

Whatever becomes of CNAP at the national scale, the signal to both US allies and adversaries will not be overlooked: one of the world's dominant powers has acknowledged the need to harden and reinforce its cyber and ICT assets in the face of more-advanced cyber offensives. It is likely that Five Eye partners and some NATO members will subsequently develop policy proposals to improve domestic cyber security for key government agencies and critical infrastructure.

[12] http://www.wired.com/2016/02/obamas-cybersecurity-plan-is-meant-to-secure-his-legacy/

[13] http://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf

[14] http://gao.gov/assets/680/674829.pdf

Other developments

The Nuclear Threat Initiative (NTI), an NGO monitoring the security of nuclear facilities, has identified 20 countries with weapons-usable nuclear materials or certain types of nuclear facilities, such as power plants, have no laws or regulations to protect against cyber attacks at nuclear facilities.[15] The NTI report suggests that cyber attacks on nuclear power plants or storage facilities could compromise control and access systems, deliberately disable reactor cooling systems or corrupt accounting systems to hide theft of nuclear material. While the report only looked at legal and policy frameworks for managing cyber risk, as opposed to the actual vulnerability of nuclear facilities to benchmark countries, NTI's recommendations that governments should include identification of cyber risks within national threat assessments is likely to become a basic requirement for future assessment and benchmarking.

The Ukrainian government has alleged that the cyber attacks on Kiev's main airport, Boryspil, in January originated from a server in Russia. The malware that infected the airport's IT system was similar to that used in December 2015 on the western Ukrainian power grid, which helped take down the power supply to approximately 80,000 customers. Initial reports sought to link Russian government or state-sponsored hackers to the potential use of the malware toolkit BlackEnergy in the attacks; however, the precise tool used to attack Boryspil's IT system has not yet been identified. The Ukrainian government publicly attributed blame for the attack on Russia, and a US cyber intelligence company traced the attack back to a Moscow backed group known as Sandworm. The Ukrainian government has announced a review of cyber security measures for critical infrastructure in the aftermath of the attacks.

Israel is considering changing export controls for cyber related technology, which may have implications for importers who rely on one of the 300 Israeli cyber security companies. The Israeli prime minister, Benjamin Netanyahu, has outlined his vision for Israel to consolidate its position as a dominant cyber security exporter with combined annual exports exceeding $3.5 billion. Comments from Netanyahu suggest that in terms of new export controls anything that is not explicitly prohibited to protect national security will be allowed in order to let Israel's cyber industry grow. To placate concerns that export controls may be too lax to prevent certain countries accessing advance cyber capabilities, at the World Economic Forum in Davos Netanyahu substituted his pro-business narrative with a focus on the importance of cyber partners.

Also of note

- **South Korea has alleged that North Korea has launched up to five coordinated cyber attacks on government institutions and leading South Korean companies** following what Pyongyang claimed was successful hydrogen bomb and long-range ballistic missile tests. The deployment of malware targeted at people working in critical infrastructure areas appears to have been aimed at causing cascading ICT failure.

[15] http://ntiindex.org/news-items/beyond-technology-addressing-nuclear-cyber-threat/ and http://www.ntiindex.org/wp-content/uploads/2013/12/NTI_2016-Index_FINAL.pdf

- **In late January, Singapore's communications and information minister announced that new cyber security legislation will be introduced into parliament** to give the county's Cyber Security Agency wider powers to manage cyber threats to critical infrastructure. The proposed legislation comes after Singapore, Malaysia, India and Japan finalised memorandums of understanding in late 2015 enabling greater cyber security knowledge sharing and attack detection across borders.
- **NATO and the European Union signed a technical cyber defence agreement in early February to improve cyber incident reporting and disclosure.** Commentators used the agreement as an opportunity to advocate for NATO and Asia Pacific allies to also create new cybersecurity partnerships, as the cyber insecurity of technologically-advanced allies in the region, such as South Korea, Japan, Taiwan, New Zealand and Australia, may provide opportunities to NATO's adversaries.[16]
- **The Australian Centre for Cyber Security (ACCS) released a series of reports in January and February arguing that Australia and other middle power countries are not sufficiently prepared to defend against coordinated state-sponsored cyber warfare.**[17] One of the reports suggested that the Australian Defence Force was about six years behind the US military in terms of cyber warfare preparedness.
- **Cyber attacks featured again in the World Economic Forum's annual *Global Risks Report*, with North America identifying cyber attacks as the most likely global risks for 2016.**[18] Germany, Japan, Estonia, the Netherlands, Malaysia, Singapore, Switzerland and the United States all identified cyber attacks as a likely threat in 2016.
- **In January, Denmark's Centre for Cyber Security reported that the Danish foreign ministry was subjected to a coordinated attack that breached the ministry's network security in late 2015**. Analysis of code used in the attack revealed references to Arabic names.
- **A Pentagon report by its Director, Operational Test & Evaluation (DOT&E) found that a number of US Army networks that support tactical and battle command platforms have cyber vulnerabilities** requiring significant cyber hardening in the near future.

[16] http://www.forbes.com/sites/anderscorr/2016/02/09/extend-nato-cyber-security-to-asian-pacific-allies/#c170622369c5

[17] https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/news/research-briefing-adf-cyber-war-readiness

[18] http://www3.weforum.org/docs/GRR/WEF_GRR16.pdf

Intelligence, surveillance and reconnaissance

UK government's draft surveillance legislation threatened by European Court of Human Rights ruling and parliamentary committee criticism.

On 12 January, in a case brought by two human rights activists, Máté Szabó and Beatrix Vissy, against the Hungarian government, the European Court of Human Rights (ECHR) ruled that mass surveillance was illegal, in a ruling that could have significant implications throughout Europe.

Current Hungarian legislation within the 2011 National Security Act only requires a government minister to authorise police requests to search the property and communications data of those being investigated for threats to national security. There is also no facility for judicial review or any requirement to show the targets actually had suspected or proven links to terrorism. Warrants were only required to relate to a premises, persons concerned or 'a range of persons', and were therefore potentially executable against any person. As a result, the judges concluded that the Hungarian government could 'intercept masses of data easily, concerning even persons outside the initial range of operation'. The court therefore concluded that Hungary does not have a sufficiently precise and effective legislation restricting surveillance to only those involved in serious crime and therefore did not protect the rights to privacy of people who were not. Therefore, the law violated Article 8 of the European Convention on Human Rights, which guarantees right to respect for privacy and family life, the home and correspondence.

This ruling came from the ECHR's Fourth Section and the ruling is not yet final, as Hungary has three months to apply to the court's full chamber to request the case be revisited. Whether this request is made or not, this finding still highlights the likelihood that the ECHR is moving to prohibit the unregulated mass surveillance of individuals not involved in serious crime or threats to national security.

The ruling is binding on all European countries, including the United Kingdom, where it will have a significant impact on the UK government's draft surveillance legislation, the Investigatory Powers Bill, which seeks to allow similar levels of surveillance to be conducted with the authority of a government minister. Under this ruling, many measures in the existing UK proposals would also be in breach of Article 8. The UK government could still introduce this legislation, but it will probably need a requirement for law enforcement and security agencies to provide detailed justifications that the targets are involved in serious crime or threats to national security before undertaking intrusive covert surveillance. There is little point in continuing to pass legislation that authorises mass surveillance, as the government would inevitably be challenged in British courts or the ECHR, and almost certainly lose. Ignoring the recent ECHR ruling would be extremely damaging to the government politically and diplomatically.

This Investigatory Powers Bill is currently being examined at the committee stage of the UK parliamentary legislative process. The Joint Committee on the Draft Investigatory Powers Bill has recently released a third report on the bill that criticises the right of security agencies to track the web browsing histories of UK citizens, increasing the pressure on the home secretary to substantially rewrite these sections.[19] The committee's report includes 86 recommendations it believes are needed to ensure the legislation is viable, can be understood by affected parties and includes adequate safeguards. MPs and peers are especially concerned about new powers that require all internet and phone companies to store everyone's internet browsing histories for 12 months, stating that while this particular proposal has potential as a viable security measure, the cost and other practical implications still need further work and detail.

[19] http://www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/9302.htm

The committee is also seeking greater powers for surveillance commissioners, who need to be independent of government. Therefore, these commissioners need to be judicial appointments made by the Lord Chief Justice instead of political appointments made by the prime minister. They should also have the power to open their own investigations, independent of government. The overall conclusions of the committee's reports so far have repeatedly included a condemnation of the poor wording of the draft legislation, making it vague and confusing.

Other developments

In its continuing efforts to carry out operations beyond the Middle East, Islamic State has revealed plans to intensify its cyber campaign against the West by hacking the internet leviathan Google. This threat is the latest in a series of efforts to terrorise Western societies; however, the track record of Islamic State's cyber army suggests that the real risk is minimal. Previous threats have included a major operation against a variety of internet targets, including the White House, on the 2015 anniversary of the 9/11 attacks; however, there are no indications that an attempt was even made. It looks increasingly likely that Islamic State's cyber goals are still somewhat beyond its capabilities. This conclusion is corroborated by a number of guides on conducting covert activity over the internet posted online by Jihadist sympathisers, which suggest that Islamic State and its supporters do not yet have the sophisticated skills needed to effectively exploit anonymising tools available on the internet beyond those already widely known about, including by Western intelligence agencies.

In an appearance at a Washington think tank in January, the US director of national intelligence, James Clapper, revealed that the age of the internet of things (IoT) will provide security agencies with new means to track and monitor individuals.[20] Commentators have been intrigued by Clapper's frank openness regarding the potential exploitation of the IoT by law enforcement, when the official response to enquiries into state surveillance capabilities has previously been one of cagey discretion. Clapper's comments are in line with a new study by Harvard University's Barkman Centre, which concluded that a network of linked platforms and sensors in cars, radios, televisions, fridges, heating controls, bed sheets, light bulbs, cameras, door locks, toothbrushes and watches and other wearables will provide security agencies with extremely detailed access into a targeted individual's property and lifestyle.[21] Many of these, such as cameras, door locks, cars and heating controls, are already in the marketplace. As with communications data, IoT records will not be stored on government databases but instead by the manufacturers and service providers. Therefore, there significant protection standards will be required to enshrine the privacy of the innocent user.

[20] http://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper

[21] https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

A study by University College London (UCL) has concluded that the security protocols within the GCHQ-developed Secure Voice encryption standard include a 'back door' that allows the intelligence agency to intercept and monitor communications over the network. The protocol, named Mikey-Sakke, created by the Communications Electronics Security Group (CESG), GCHQ's information security wing, works by generating unique encryption keys, which are used to encrypt then decrypt voice conversations. However, the security researcher who conducted the study, Dr Steven Murdoch, has found the standard to be inherently and deliberately weak by design. The use of a key escrow within the encryption process allows the service provider to recover responder private keys and decrypt past calls without detection. Murdoch stated that 'Mikey-Sakke is designed to offer minimal security while allowing undetectable mass surveillance though key escrow, not to provide effective security.'[22] GCHQ has disputed the researcher's findings.

Also of note

- **The Singaporean government is conducting another of its periodic reviews into its human rights record later this year** and Privacy International has already released a report criticising its surveillance of social media and operations to control individual's private computers.
- **Multinational phone companies are fighting surveillance attempts by the government of the West African country of Guinea,** which is introducing legislation that will force the companies to hand over private phone data.
- **The Thai government has released a draft procurement document for a system that will allow it to conduct surveillance and monitoring of the social media accounts of law enforcement targets** through name, keywords and facial recognition.
- **The US Army has developed a robot based on the cockroach that can compress itself and squeeze into spaces a quarter of its normal size.** If deployed, it is expected to be used for close-range surveillance.

Commissioned by the Remote Control Project
remotecontrolproject.org

REMOTE CONTROL
Examining changes in military engagement

[22] http://www.v3.co.uk/v3-uk/news/2442829/gchq-developed-crypto-tools-have-built-in-backdoors-to-allow-snooping

Open Briefing is the world's first civil society intelligence agency.

We provide **intelligence, security and training** to organisations striving to make the world a better place.
We **scrutinise the actions of governments and militaries** and generate alternative policies.
We deliver a **public intelligence service** so that *you* know what is really going on in the world.

Founded in 2011, Open Briefing is a groundbreaking non-profit social enterprise. We are a unique international collaboration of intelligence, military, law enforcement and government professionals working tirelessly behind the scenes to make a difference. We are *your* intelligence agency.

www.openbriefing.org