Remote-control warfare briefing | #07

12 December 2014

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 commissioned by the Remote Control Project, a project of the Network for Social Change, hosted by Oxford Research Group.

Special operations forces: Afghan policy reversal reinstates special forces night raids.

Private military and security companies: Historic verdict in Blackwater Iraq shootings trial could set precedent.

Unmanned vehicles and autonomous weapons systems: UN Convention on Certain Conventional Weapons discusses autonomous unmanned combat air vehicles.

Cyber warfare: United States facing multiple cyber offensives from state and non-state adversaries.

Intelligence, surveillance and reconnaissance: Bill designed to heavily restrict NSA domestic surveillance defeated in US Congress.

Special operations forces

Afghan policy reversal reinstates special forces night raids

In November, Afghan President Ashraf Ghani overturned the ban on special forces night raids instituted by former President Hamid Karzai in 2013. The policy reversal came on the heels of the recently concluded US-Afghanistan Bilateral Security Agreement (BSA), US President Barack Obama's recent force authorisation, and the NATO status of forces agreement. Collectively these agreements will result in a continued US and NATO presence in Afghanistan until 2017. These agreements also elevate the Afghan National Army Special Forces (ANA-SF) as operation leaders and relegate foreign special operations forces (SOF) to operational, advisory or 'combat enabling' support roles.

open briefing
the civil society intelligence agency

Open Briefing
27 Old Gloucester Street
Bloomsbury
London WC1N 3AX

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

US SOF operators are currently training approximately 200 ANA-SF in Kandahar and will provide air transport and support, night vision equipment and intelligence to those troops for night raid operations. While there is no clear data on the levels of civilian casualties during night raids compared to day time attacks, a former spokesperson for the International Security Assistance Force (ISAF) was cited by *The Diplomat* as stating that 85% of night raids were completed without the firing of live ammunition.[1]

Increasing Taliban movement and mobilisation during the cover of night is one driver influencing the policy reversal. Night raids significantly increase the tactical advantage of special forces and reinforce technical and equipment superiority. With continuing force drawdowns, it would appear that the Afghan National Army and remaining coalition forces are seeking to maximise any available tactical advantage. However, complex chain of command authorisations will limit the speed with which night operations can be planned and executed. The long-term tactical effectiveness of ANA-SF over the Taliban will also be dependent on continued access to advanced air transport and intelligence, surveillance and reconnaissance (ISR) equipment currently provided by the United States.

There is acute awareness of Afghan public opposition to night raids and the danger that the policy reversal may expose Ghani to some future political attacks despite the Afghan parliament supporting the signing of the BSA. The US administration has rebranded the practice as 'night operations' rather than 'night raids' in a bid to manage public perceptions. The fact that Ghani and the White House are willing to stir up negative public sentiment during a politically fragile period may give some indication of the seriousness with which the Afghan and US governments are taking the threat posed by a resurgence in Taliban activity. The delayed withdrawal of up to 1,000 US troops announced by US defence secretary Chuck Hagel on 6 December reinforces this assessment. The rise of the Islamic State and the limited effectiveness of conventional Iraqi Army forces after the US withdrawal from Iraq are also likely to be also influencing US foreign policy in relation to Afghanistan and the desire to avoid leaving a security vacuum for the Taliban.

Other developments

The release of the US Army's Special Operations Command (USASOC) white paper on counter-unconventional warfare (UW) has generated significant debate across the security and defence sector.[2] The white paper published in September highlights the relatively sophisticated development of unconventional warfare (hybrid or special warfare) capabilities by Russia, Iran and China. A number of prominent commentators and analysts have underscored the current institutional, political and operational barriers limiting the ability of the United States to develop counter-unconventional warfare doctrines. In particular, the lack of institutional coordination and operational integration between the CIA, US Special Operations Command (USSOCOM) and the state department limits the deployment of both hybrid warfare operations and counter-unconventional warfare. However, the announced formation of the US 1st Special Forces Command on 30 September appears to signal the administration's desire to improve hybrid warfare capability.

[1] http://thediplomat.com/2014/11/afghan-government-lifts-ban-on-night-raids/

[2] https://info.publicintelligence.net/USASOC-CounterUnconventionalWarfare.pdf

The Ukrainian military has alleged that Russian special operation forces are participating in attacks on Donetsk airport, though Russia denies it is supporting separatist rebels in eastern Ukraine. Kiev has also alleged that Moscow is providing separatist rebels with heavy ammunitions, smuggled under the guise of humanitarian aid. The increasing intensity of damage caused by the escalating conflict would suggest rebels have access to heavy ammunitions, though it is unclear how rebels have accessed this weaponry or guidance on effective use. Meanwhile, medical specialists from US Special Operations Command Europe (SOEUR) were in western Ukraine in late November training Ukrainian soldiers in basic battlefield medical procedures.

US special forces and Yemeni counterterrorism troops freed eight hostages held by al-Qaeda in the Arabian Peninsula in Hadhramaut province near the Saudi border on 25 November. The rescue operation left seven militants dead. The Pentagon played down the US role and emphasised the role of Yemeni troops. A second rescue mission involving US and Yemeni special forces was launched on 6 December to free US journalist Luke Somers and South African teacher Pierre Korkie; however, the hostages were both shot and killed by al-Qaeda militants during the rescue attempt.

Also of note

- **Belarusian President Alexander Lukashenko announced the formation of a new special operations force within the Belarusian Army and appointed a new defence minister.** Both announcements are likely a response to unconventional operations used by Russia in eastern Ukraine.
- **USSOCOM issued a 'request for information' (RFI)[3] in late October seeking electronic, mobile devices that can rapidly survey digital media, extract files, assess file structure properties on adversary devices.** Other requests for information include technology that reduces or cloaks soldiers' electronic signature, portable, near instantaneous language translation devices and digital trip wire.
- **USSOCOM are testing a new multi-role (anti-armour) shoulder-fired weapon, the Carl-Gustaf M4 by Saab Defense and Security USA.** The weapon is aimed at filling the gap left by other shoulder-fired weapons that are too lethal or destructive for urban environments and therefore contrary to rules of engagement in civilian population areas.
- **A new screening-tooling, layer-vetting process developed by US Central Command (CENTCOM) will be used to evaluate Syrian rebels seeking access to US training, support and weapons.** This includes biometric checks, psychological evaluations and stress tests. It is unclear how this vetting programme will differ to that currently used by the CIA, though it is clear that the normal Leahy laws for foreign force support will not apply.
- **The US administration appears to be reducing special forces training engagements with Burkina Faso and is possibly transferring the activities of the Special Operations Command Forward – West Africa and ISR operations to Niger.** The United States' training relationship with Nigeria is also weakening after Nigeria withdrew from training activities, most likely in response to the United States' refusal to sell helicopter gunships to Nigeria.

[3]https://www.fbo.gov/index?s=opportunity&mode=form&id=4e22e1318a9fe3856b346436d9610900&tab=core&_cview=0

- **Speculation continues over the future use of a temporary US Africa Command (AFRICOM) base in Chad near N'Djamena**. While information obtained by TomDispatch and the *Washington Post* suggests the United States is seeking to procure 'base camp facilities', AFRICOM has indicated that the camp will only serve as temporary lodgings for special operations forces training exercises next year.
- **A research paper by Australian Lieutenant-Colonel Ian Langford for the Directorate of Future Land Warfare has attempted to improve policymaker understanding of special operations forces capabilities.**[4] Importantly, Australia's SOF may be limited by the size of the 'operational enablers' who support SOF ground forces.

Private military and security companies

Historic verdict in Blackwater Iraq shootings trial could set precedent

In late October, four former Blackwater security guards were found guilty by a federal jury in the United States on charges ranging from weapons charges to manslaughter and murder in Iraq in 2007. The trial and verdict could set a precedent for future cases of prosecution involving private military and security companies (PMSCs). The former security guards were accused of having actively contributed to unleashing the violence that unfolded in Baghdad's Nisour Square on 16 September 2007 that led to the deaths of 17 Iraqis. Nicholas Slatten, a sniper, was the only defendant convicted of murder, for firing the first shots. The other three defendants, Paul Slough, Dusting Heard and Evan Liberty, were convicted of voluntary manslaughter and weapons charges. Most importantly, the federal jury found that the Nisour Square killings were not the result of unforeseeable battlefield events but were a criminal act on the part of the security guards.

Overall, these convictions represent an historic verdict with various medium- to long-term implications for different stakeholder. First, it is a victory for the families of the Nisour Square victims. It is also an important verdict for the families of the victims of other shootings involving PMSCs, whose fights for justice had been held up because of blurry legislation surrounding the prosecution of individuals contracted by PMSCs abroad. The Blackwater trial verdict is significant, as it shows private contractors can in fact be held accountable in the United States for their crimes abroad.

The verdict is also politically important for the US government, which has been criticised for the lack of accountability of its contractors employed on the battlefield in Iraq, Afghanistan and elsewhere. In a major bone of contention between Washington and Baghdad, the US government long insisted that the Blackwater guards be tried in the United States rather than Iraq. The issues has also been central to exit strategy discussions between the United States and Afghanistan, as one of the sticking points in the long drawn out negotiations over the Bilateral Security Agreement (BSA) was criminal immunity from prosecution for US servicemen. Ultimately, such a public trial and conviction represents a diplomatic victory for the US government, which perceives it as partly addressing the perception of US unaccountability that had gradually developed as a result of the actions of Blackwater and other PMSCs in Iraq and Afghanistan.

[4] http://www.army.gov.au/~/media/Content/Our%20future/Publications/Papers/ARP%204/AustralianSpecialOperations_B5_web.pdf

Finally, the verdict has sparked discussions over the policing and prosecution of private security contractors in other countries. This includes Israel, where private security contractors have been used to provide security in West Bank Jewish settlements and have also been involved in controversial incidents. This might lead to increased calls for stronger international legislation and binding standards. The United States and Israel are likely to support such international efforts in principle, but are equally likely to decide not to adopt said binding standards for political reasons (as they did when deciding not to join the International Criminal Court).

The verdict is an important one given that PMSCs will continue to be employed in war zones, such as the Sahel region, Afghanistan and, yet again, Iraq. In fact, as a direct consequence of the Blackwater verdict, the UN working group on the use of mercenaries has called for stronger regulation of private security and highlighted the need for an international convention to better regulate and monitor those 'corporate actors whose operations pose potential threats to human rights'. Yet, it is highly likely that the rising dominance of PMSCs in those countries with weak and unstable structural conditions will increase their relative power and influence, thereby making it even more difficult to hold them accountable for their actions. Furthermore, the intense international attention on the Nisour Square shootings and subsequent trial ensured that those responsible eventually faced justice; there is no guarantee that all future crimes involving PMSCs will receive the same level of scrutiny.

Other developments

A Russian court has convicted two Russian citizens on charges of establishing an illegal mercenary group. It is the first time such charges have led to a conviction in Russia. The two men were found guilty of leading a squad composed of 250 mercenaries to fight in Syria. Conflicting reports have made the squad's loyalty difficult to attribute to either side of the conflict. On the one hand, several squad members admitted they were tasked with protecting Syrian power plants; whereas unconfirmed reports raised the possibility the mercenaries might be fighting against Syria's President Bashar al-Assad. Unlike the two men convicted for setting up the illegal mercenary squad, regular members of the group did not face charges in Russia, as there was a lack of evidence proving that they were remunerated for their work in Syria.

Iran has been using cash incentives (reported to range from $500 to $1000 a month) and promises of Iranian residency to recruit several thousand Afghan refugees to fight in Syria's civil war on the side of President Bashar al-Assad's regime. Afghan fighters were first identified on the ground in Syria in May-June. As of late October, following the release of videos on several media channels, it has become clear that Afghan individuals who have refugee status in Iran – some of whom used to be associated with the Taliban – are now fighting in Syria. The Afghan recruits' refugee status in Iran means that they are deprived of a supportive and vocal community, which makes them more discreet and expandable. The use of vulnerable and relatively poor Afghan refugees as mercenaries to be sent to Syria is certainly a controversial remote-control warfare strategy. It is likely that it grew from Iran's attempt to limit casualties among the Revolutionary Guard and Hezbollah fighters. Overall, the presence of these Afghan fighters introduces additional complexity to the Syrian conflict and adds to the array of actors who are active on the ground.

A bill was introduced in the Russian state duma in October proposing to legalise private military and security companies in Russia. The move had previously received political support from Russian President Vladimir Putin, and stems mainly from the fact that the worldwide PMSC market – estimated to be worth around $350 billion annually – is financial attractive. It is also likely that Russia's use of 'little green men' in Crimea and eastern Ukraine has made the legalisation of PMSCs more attractive to Putin. Moreover, military service is still mandatory in Russia, meaning that over 300,000 young men receive military training each year and the country is home to thousands of retired military professionals. It is likely that Russia could become an important player on the PMSC market given its well-established military tradition. The bill would allow Russian PMSCs to the same tasks as their Western counterparts as well the facilitation of 'alternative settlement of armed conflicts outside Russia'. Legalising PMSCs could allow Russia to more easily use such companies as proxies, while allowing for a degree of deniability and distancing the state from any extreme actions private contractors may undertake. On the other hand, it is unlikely that the Russian military establishment and security services will be willing to give away their long-standing monopoly on security provision and use of violence.

Also of note

- **A new book on PMSCs, *The Invisible Soldiers: How America Outsourced Our Security* by Ann Hagedorn, was published in September.** The author examines the trend towards diversification among PMSCS with respect to tasks, roles and responsibilities bestowed upon its contractors, as well as the diversity of locations in which they may be sent.
- **Russian lawmaker Roman Khudyakov has proposed the creation of a Russian Foreign Legion.** Comparing the idea to the French Foreign Legion (Légion étrangère), Khudyakov promotes the use of non-Russian citizens to fight terrorist threats in Russia's near abroad in Central Asia.
- **Human rights activist and journalist Rafael Marques de Morais is credited with releasing on Twitter a video allegedly showing private security employees committing torture in November.** The video allegedly shows mining company security contractors torturing diamond miners with a machete.
- **A cyber attack on the US government's leading security clearance contractor, USIS, went unnoticed for months.** The breach was first reported in August, but it is now confirmed that the private records of over 25,000 employees have been compromised. This raises questions over the contractor's vulnerability and exposure, which could prove costly for the US. government, both financially and politically.

Unmanned vehicles and autonomous weapon systems

UN Convention on Certain Conventional Weapons discusses autonomous unmanned combat air vehicles

On 13-14 November, countries gathered at the United Nations in Geneva, Switzerland, to discuss the escalating use of unmanned aerial vehicles (UAVs) around the world. The UN Convention on Certain Conventional Weapons (CCW) meeting resulting in a joint call by several of the attending national representatives for the use of unmanned combat air vehicles (UCAVs) to be strictly monitored to prevent violations of international and humanitarian law. Spain, Ireland, the Netherlands and several other countries called for 'meaningful human control' of such weapons to be enshrined in international law. Spain also cited concerns that the world is on the brink of a new UAV arms race among both developed and developing countries.

While drones are still currently controlled by human pilots, technology is advancing so quickly that autonomous and intelligent unmanned combat vehicles are fast coming close to widespread deployment on combat operations. Developments in GPS, radar, laser and infrared sensors are allowing drones and missiles to more accurately identify their position, route and target. They can increasingly distinguish types of vehicle and locate human targets. Onboard technology is also continually improving to the point where vehicles are capable of high-speed in-flight data interpretation and analysis without human support. There are already weapons in use that can autonomously hunt, select, identify and hit targets. Some, such as the United Kingdom's Brimstone air-launched ground attack missile, even communicate with other weapons to autonomously coordinate and distribute strikes.

In 2012, the Pentagon issued a directive that defined the difference between *semi-autonomous* (where targets are chosen by human operators) and *autonomous* (where the weapons travel, identify and engage without human intervention). The directive also stated that all future weapons must 'allow commanders and operators to exercise appropriate levels of judgement over the use of force', suggesting that the use of fully autonomous weaponry will be heavily restricted. However, the integrity of this definition remains to be seen. A long-range anti-ship missile that is designed to choose its own radar-avoiding route and then engage a target of its own choice is only categorised as *semi-autonomous* by the Pentagon because operators are still involved in its targeting and killing decisions. Critics have challenged the directive as too vague and for creating loopholes that still allow for fully autonomous weapons to be developed and deployed.

The Convention on Certain Conventional Weapons is the section of the Geneva Conventions that relates to the impact of tools of war on civilian populations. Under this convention, weapons that indiscriminately target civilian populations or cause inhumane suffering to combatants can be banned or restricted. The 118 signatories to the CCW agreed to reconvene at the United Nations in Geneva from April 13-17 2015 to continue deliberations on unmanned aerial vehicles.

Other developments

US commanders in the fight against the Islamic State (IS) have complained about the lack of UAV assets being deployed to their theatre. The mission in Afghanistan is still considered the top priority by the Pentagon, and is therefore in possession of the lion's share of the inventory. This is leaving a significant gap in US capabilities in Syria and Iraq. Furthermore, IS tactics since the start of the Western air offensive have changed significantly. To avoid being targeted from the air, IS fighters have moved from operating in large numbers in the open countryside to moving in small groups within urban civilian populations. This has made it more difficult for conventional manned aircraft to operate and engage targets effectively. US President Barack Obama has now asked for funding for small surveillance UAVs for the region, possibly the Eagle or Blackjack vehicles in use by the US Marine Corps and Navy. In the meantime, the United Kingdom has redeployed some of its own Reapers from Afghanistan to the IS operation, though unconfirmed reports suggest only two platforms have so far been moved.

The United States reportedly now monitors half of its border with Mexico using drones, specifically in areas where there are few existing watchtowers, sensors or patrols. The Predator Bs make multiple sweeps of areas using HD cameras to identify man-made changes in the landscape, such as new rubbish, tyre tracks or footprints. Patrols are then deployed to areas of interest or, alternatively, sensors are planted to enable 24/7 monitoring. This is not intended to replace men on the ground but rather to reinforce – Border Patrol personnel levels have still doubled since 2000.

A two-year feasibility study has been launched by the British and French governments to initiate the development of a joint future unmanned combat air vehicle to replace current manned platforms. Six private industry partners (three from each country) have been identified to bring forward a system definition for a concept aircraft by the end of 2016. BAE Systems and Dassault will work on the vehicle design, Rolls Royce and Safran/Snecma will study engine development and Selex ES and Thales will cooperate on sensors and communications. The target date for a fully-developed test model is around 2030.

Also of Note

- **The US Defense Advanced Research Projects Agency (DARPA) has issued a request for ideas on the development of an airborne 'mothership' to transport UAVs to their target area and launch and recover them in-flight.** It is envisaged that this will be an existing large aircraft, such as the C-130 transport or the B-1 bomber. The initial timeline is to have a full flight demonstrator in operation within four years.
- **The United Kingdom launched its first drone strike against IS in Iraq over the weekend of 8-9 November.** The target was reported to be militants planting IEDs in the area of Bayji, north of Baghdad. Since the British parliament approved offensive air operations against IS in September, Tornado GR4 attack aircraft have conducted dozens of combat missions, but this is the first involving a UCAV.
- **China has unveiled an anti-drone laser capable of shooting down small aircraft at short ranges of up to two kilometres, altitudes up to 500 metres and flying at speeds below 50 metres per second.** It is considered that this limited capability will make it best suited for policing the skies over sensitive sites.

- **China is reportedly developing a holographic ground control system that permits UAV operators to directly interact with a holographic projection to monitor and fly the aircraft and engage targets.**
- **Iran claims to have produced a stealth UAV developed from captured US technology.** , The drone was reportedly reverse-engineered from a RQ-170 Sentinel that crashed in Iran in 2011, but the Iranian version is only 60% of the size. However, analysis of video footage of the aircraft taking off and flying has raised suspicions that such claims are unreliable and that the footage was doctored to make a much smaller aircraft look significantly larger and faster.
- **There are plans to use drones to deliver humanitarian aid to Syrian civilians trapped in combat areas.** Using airplanes cheap enough to allow for mass manufacture by Syrian refugees, and small enough to avoid being seen on radar, the US Air Force officer who privately developed this scheme hopes to transport sufficient food and medical supplies to relieve the besieged Syrians' plight. Initial funding has been provided, development of the aircraft continues and negotiations are planned with Turkish authorities to allow the country to be used as the base for trials next year and operational flights thereafter.
- **Pakistan has condemned a US drone strike that reportedly killed members of militant groups backed by the Pakistani government.** The strike by CIA Predators on the village of Garga in North Waziristan killed eight people and wounded several more. Local media reports that the dead were linked to the Haqqani Network and Gul Bahadar, the leader of a Pakistani Taliban faction, both of which do not support attacking the Pakistani state and are therefore considered 'good Taliban' by Islamabad.
- **The US Army has developed a pocket-sized drone for issue to platoon-sized groups to provide a local aerial surveillance asset.** The Cargo Pocket Intelligence Surveillance and Reconnaissance Program (CP-ISR) drone carries three tiny real-time cameras on a micro-helicopter platform, and can fly all-but silently for 25 minutes above and inside buildings or through dense woodland.

Cyber warfare

United States facing multiple cyber offensives from state and non-state adversaries

In November, Vice Admiral Michael Rogers, the commander of US Cyber Command, told the House Intelligence Committee that 'state-sponsored hackers are looking to get into the sorts of systems that control critical infrastructure and embedding the capabilities to attack them'. Rogers' comments on the ability of one or two countries to turn out the lights in the United States came after a number of US government services and industries revealed details of cyber incursions.

In November, the US National Oceanic and Atmospheric Administration (NOAA) and US Postal Service acknowledged they had been subject to hacking campaigns during September. The cyber attack on NOAA caused limited disruption, but could have had implications for the country's environmental intelligence. While no formal attribution has been made, Representative Frank Wolf (R-Va.) publically indicated that NOAA informed him privately that 'bad actors' based in China were responsible for the attack. The hack on the US Postal Service compromised data on 800,000 employees.

On 28 October, Security analysts Novetta produced a report on the Axiom Threat Actor, a group understood to be acting on behalf of the Chinese government.[5] The group is reported to have undertaken hacking attempts against various governments, NGOs, media organisations, pro-democracy groups and several Fortune 500 companies over the last six years. The focus on targets in North America, Europe and East and Southeast Asia and the intelligence value of information obtained for Chinese domestic and foreign policies points to Chinese intelligence agency support for Axiom's activities.

On 3 December, the Center for a New American Security released a report on China's cybersecurity strategy.[6] The report attempts to highlight opportunities for the United States and China to improve mutual understanding of motives, agenda and stakeholders in their respective cyber doctrines. The report suggests that China's cybersecurity strategy is 'driven primarily by the domestic political imperative to protect the longevity of the Chinese Communist Party (CCP).' This may include using cyber capabilities to express dissatisfaction with foreign powers over maritime territorial disputes, gaining an understanding of an adversary's military infrastructure and advancing alternative narratives of Chinese government activities. An November Australian Strategic Policy Institute paper on China's superpower also raised many of these points, but focused on the economic warfare component of China's cyber capabilities.[7]

The US Department of Homeland Security also revealed that it suspected Russian sponsored hackers had infiltrated critical energy utility systems in a malware campaign called Black Energy. The malware is said to be similar to that used by Russian cyber-espionage group Sandworm, who allegedly targeted NATO and European energy companies earlier in 2014. Concern over Russian cyber activities was highlighted in FireEye's October report on Russian cyber espionage operations and the APT28 threat group.[8] Unlike Chinese cyber groups, which target specific companies holding key intellectual property that would enable Chinese industries to rapidly modernise, the Russian APT28 team appears more focused on gathering information related to governments, militaries and security organisations that would be of geopolitical benefit to the Russian government.

Public disclosure of these high-profile cyber operations against US government agencies and corporate interests has likely influenced the White House in its response to the National Security Telecommunications Advisory Committee reports on the 'internet of things' (a proposed development of the internet whereby everyday objects have network connectivity) and cyber attacks on critical infrastructure. US President Barack Obama is likely to implement recommendations from the advisory panel that are aimed at improving planning for worst case cyber attacks and averting risks in the emerging internet of things.

[5] http://www.novetta.com/commercial/news/press-releases/pr-031814-2-22-2-2/

[6] http://www.cnas.org/sites/default/files/publications-pdf/CNAS_WarringState_Chang.pdf

[7] https://www.aspi.org.au/publications/chinas-cyberpower-international-and-domestic-priorities/SR74_China_cyberpower.pdf

[8] http://www.fireeye.com/resources/pdfs/apt28.pdf

Other developments

Malware recently uncovered by information security analysts may have been developed by Western intelligence agencies. The Regin advanced persistent threat (APT) has predominately targeted private individuals and small businesses in Russia and Saudi Arabia, with no infections reported in any of the Five Eyes jurisdictions. The complexity and sophistication of the code and the use of English words in the data validation commands further supports speculation that Regin is the product of a Western intelligence agency. Software analysis indicates that the malware is designed primarily for target surveillance and state espionage rather than intellectual property theft or system destruction. The focus on telecommunications targets as a key system choke or leverage point to access international communication flows further suggests that the back door-type Trojan is part of a state-backed surveillance campaign.

In late November, Sony Pictures confirmed that the FBI was investigating the comprising of the company's network. The hack resulted in the leaking of unreleased Sony films and forced the network to shut down. While neither Sony nor the FBI have sought to attribute the attack to a particular actor, speculation has emerged that North Korea or state-sponsored groups launched the attack in response to a film that Pyongyang had found offensive and which was to be released before the end of the year. The attack has raised questions about the cyber offensive capacities of North Korea. Some estimates suggest that North Korea has over 3,000 cyber specialists, and with potential access to technological transfer from key cyber powers such as China, Iran and Russia, North Korea may poses cyber capabilities beyond current estimates. However, there are questions over whether Pyongyang would potentially reveal elements of its cyber capacity simply to stop the dissemination of a film. Furthermore, Trustsec analyst David Kennedy has argued that North Korea is unlikely to possess the cyber capability necessary to undertake such a sophisticated attack. North Korean state media ran government denials of involvement and suggested that the hacking might have been the righteous actions of supporters of the DPRK.

Security company Cylance released a report detailing an advanced campaign of cyber attacks described as Operation Cleaver and attributed to 'bad actors' affiliated with the government of Iran, and particularly the Iranian Revolutionary Guard Corps (IRGC).[9] Observation of Operation Cleaver over the last two years revealed over 50 attacks on critical infrastructure, such as energy generation and distribution, airports and airlines. Historically Iranian cyber operations have predominately targeted Israeli and US interests; however, the report suggests that with targets across 16 countries, Iranian cyber capabilities are geared to extend beyond retaliating against regional adversaries or those involved in Stuxnet. In the same way Iranian nuclear power aspirations underscore a desire for regional influence and dominance, offensive cyber capacity to impact critical infrastructure and compromise supervisory control and data acquisition (SCADA) systems on a global scale may also reveal Iran's significant geopolitical aspirations. A spokesman for Iran's mission to the United Nations, Hamid Babaei, rejected the allegation made in Cylance's report, suggesting the allegations were aimed at hampering nuclear talks between Iran and the P5+1/EU3+3.

[9] http://www.cylance.com/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf

Also of note

- **The Pew Research Center and the Imagining the Internet Center at Elon University surveyed 1,642 experts on cyber security and found that 61% believed that by 2025 a major cyber attack will have caused widespread harm to a country's security and capacity to defend itself and its people.**[10]
- **The Australian prime minister's office announced a review of the country's cyber security strategy in November.** The review comes as cyber attacks are estimated to have increased by 40% since 2010. The review evaluated the capacity and capability of government agencies to detect and respond to cyber threats.
- **In November, the South African Government established a Cyber Response Committee (CRC),** which will consider the creation of a cyber defence strategy, a national critical information infrastructure policy and potential legislation in the form of a cyber security bill.
- **The Syrian Electronic Army (SEA) redirected a number of media websites to SEA pages in late November,** including the United States' *Los Angeles Times*, *Forbes* and *Chicago Tribune*, Italy's *La Repubblica*, the Canadian Broadcasting Corporation and Britain's *Daily Telegraph* and *Independent*. SEA enacted the redirection by breaching a third party's domain registrar.
- **670 soldiers and civilians from 80 organisations in 28 countries participated in one of NATO's largest cyber warfare drills** in late November in the eastern Estonian city of Tartu. The drills were aimed at resolving vulnerabilities apparent in the aftermath of alleged Russia cyber operations in Ukraine. Jens Stoltenberg, the NATO chief also announced in early December that NATO had agreed to activate four trust funds to help pay for upgrading Ukraine's logistics and cyber warfare capacities.
- **US Cyber Command participated in a closed network cyber attack simulation called Cyber Flag in mid-November.** The drills held in Nellis Air Force Base, Nevada, were aimed at testing integration of cyber operations with air, land and naval forces.
- **According to a preliminary report prepared by Poland's Supreme Audit Office, Poland's government administrations have a poor level of preparedness for and capability to respond to cyber attacks.** While the report is not complete yet and has not been publically released, comments by the Supreme Audit Commission suggest substantial cyber vulnerabilities.
- **NATO and Jordanian officials announced a new cybercrime project in Amman that will improve Jordan's capacity to defend against cyber attacks on critical infrastructure.** The announcement for the project sponsored by NATO's Science for Peace and Security Programme made specific reference to the presence of the Islamic State and the potential for cyber attacks.
- **The US Navy has launched a 'task force cyber awakening'** to harden naval system hardware and software against cyber intrusion. The taskforce comes after a major navy computer system was hacked in 2013.

[10] http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/

- **In November, the Atlantic Council and the Swedish National Defence College published a major report on confidence-building measures in cyberspace**.[11] The report delivered a range of options to improve crisis management, restraint and engagement measures in the event of cyber conflict or attacks. The report is based upon a NATO Advanced Research Workshop held in March 2014.
- **Taiwan's National Security Bureau (NSB) reported to the legislature's foreign and national defence committee that China was escalating cyber attacks on government agencies and industries.** The NSB indicated that the attacks were extending beyond government agencies and also focusing on political parties and their affiliated organisations, academics and research institutes.
- **The Dutch government's National Cyber Security Centre recently completed their fourth annual assessment of cyber security.**[12] According to the report, cybercrime and digital espionage remain the biggest cyber security threats.

Intelligence, surveillance and reconnaissance

Bill designed to heavily restrict NSA domestic surveillance defeated in US Congress

The USA Freedom Act, a bipartisan bill that would have greatly reduced the NSA's domestic US operations, failed by just two votes to beat a filibuster in a late-night US Senate hearing on 18 November, ending its legislative journey. Introduced to the House of Representatives last year, it sought to terminate the agency's continuous mass collection of US phone data as revealed in the Edward Snowden disclosures. The bill had support from both sides of Congress, senior intelligence staff, technology and social media corporations and civil rights groups. There was also 'strong support' from the White House, but only after privacy protection and transparency requirements were significantly weakened by administration officials.

The opponents to the bill, mostly but not solely Republicans, argued that the removal of this communications dragnet would leave the country at an immediate and greatly increased risk of another domestic terrorist attack.

The bill would have required telephone companies – not government agencies – to retain huge metadata databases, which the later would only be able to access with the approval of the Foreign Intelligence Surveillance Court. Furthermore, this court would ensure the appointment of civil liberties advocates and a more limited definition of what can be legitimately described as a 'surveillance target' would be created.

However, many once-strong supporters of the bill among civil rights groups had been disappointed by the watering down of the legislation prior to its passage through Congress. While restricting widespread warrantless surveillance, it still permitted large-scale collection based solely on warrants citing 'reasonable articulable suspicion' of connections to terrorism. Also, there would have been no impact on operations to undermine encryption or related to overseas mass surveillance.

[11] http://www.atlanticcouncil.org/images/publications/Confidence-Building_Measures_in_Cyberspace.pdf

[12] https://www.ncsc.nl/english/current-topics/news/cyber-securty-assessment-netherlands-4-cybercrime-and-digital-espionage-remain-the-biggest-threat.html

After the vote defeat, the bill's Senate sponsor, Senator Patrick Leahy (D-Vt.), blamed the loss on scare tactics. He vowed never to give up the fight, and declared he would take it to the next Congress for another attempt. So far, there has been no comment from the White House about whether the bill will be re-submitted. There are now concerns from those who support broader surveillance powers for the NSA and the FBI that the House will not reauthorize such powers in June next year.

Other developments

Newly-released internal documents have confirmed that the United Kingdom's intelligence agencies, GCHQ, MI5 and MI6, have for many years been given free rein to monitor privileged communications between lawyers and their clients, and conduct comprehensive surveillance on journalists. Such operations were signed off by a senior government minister, usually the home or foreign secretary. The documents were made public on behalf of two Libyans who claim they were subject to extraordinary rendition to Libya in joint UK-US operations conducted in 2004. The documents state that their communications with lawyers at the human rights group Reprieve were monitored by the government, thereby hindering their right to a fair hearing. Other documents released in recent weeks have revealed intelligence-sharing partnerships between the United Kingdom and foreign intelligence agencies, including the receipt of bulk communications intercept data without the need for a UK warrant.

Canada has announced that it is moving ahead with a C$92 million project that will install an electronic surveillance screen along the border with the United States between Quebec and Toronto. The screen will consist of CCTV, radar, ground sensors and thermal radiation detectors to improve counter-smuggling and counter-terrorist efforts. Expected to be operational by 2018, the sensor network will be connected to a collection centre that will develop the data to produce real-time intelligence analysis, issue alerts and provide instant imagery to mobile patrols.

Following a hatchet attack on police officers in New York, United States, in October, which saw four officers injured before the lone attacker was killed, the New York City Police Department (NYPD) is to broaden existing surveillance of social media sites, which seeks to identify young people who are at risk of being radicalised and drawn into extremist networks. In a parallel to the ongoing PREVENT strategy in the United Kingdom, NYPD's Operation Sentry began in 2006 and brought together law enforcement agencies from the United States and abroad to monitor and share intelligence on membership and activity of radical media forums. Critics of this operation say much of the talk is ultimately harmless and may see people unjustly prosecuted.

Also of note

- **A US federal judge has ordered that the FBI's new and cutting-edge facial recognition database should be made open to scrutiny by privacy activist groups.** Following a 2010 Freedom of Information request by the Electronic Privacy Information Center, a released government report revealed that the imagery analysis software used to collect data could fail up to 20% of the time. The Next Generation Identification Program has been ruled by a US District Judge as representing a 'significant public interest' due to its impact on privacy rights and should be subject to rigorous independent oversight.

- **Russia has launched a new batch of satellites to add to its orbiting fleet. One of these, Object 2014-24E, has attracted considerable interest as no-one has so far identified its use.** Russia has not declared the orbit of this object, and it is being closely monitored by the US military and the space community. Opinions on its role are currently mixed, ranging from it being an anti-satellite weapon to a more benign debris clearing satellite.
- **German legislators have identified a legal loophole that allows Germany's foreign intelligence agency, the BND, to spy on its own citizens.** While not usually allowed to spy on Germans or German companies, the loophole allows monitoring of citizens working abroad. Furthermore, all work-related communications are attributed to the employing company, and if that company is foreign, the BND is legally permitted to eavesdrop on them.
- **The US Air Force is disinvesting its highly successful MC-12W ISR fleet to the US Army and Air Force Special Operations Command.** The MC-12W is a highly-modified Hawker-Beechcraft airframe fitted with surveillance equipment to provide real-time imagery to ground troops. It is said that this aircraft has assisted in the kill or capture of 8,000 terrorists, the discovery of 650 weapons caches and helped divert convoys away from suspected IEDs and ambushes.
- **Germany and Brazil have jointly drafted a UN resolution on mass surveillance, interception of digital communications and personal data collection that could harm human rights to be considered by the General Assembly.** The proposed resolution calls for the UN. Human Rights Council to appoint a special rapporteur to identify and clarify standards protecting privacy rights. The proposal is scheduled to be voted on in December.

Commissioned by the Remote Control Project

remotecontrolproject.org

REMOTE CONTROL
Examining changes in military engagement

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

We produce actionable and predictive intelligence on defence, security and foreign policy matters. We tell you what has happened and what is likely to happen next. Most importantly, we tell you why.

We do this so that better informed citizens can more effectively engage in peace and security debates and civil society organisations can make the right advocacy choices. Together, we can influence positive policy decisions by our governments.

Open Briefing is a bold and ambitious not-for-profit social enterprise. We are a unique collaboration of intelligence, military, law enforcement and government professionals from around the world.

Challenge the status quo, and take intelligence into your own hands with Open Briefing.

www.openbriefing.org