Remote-control warfare briefing | #08

23 January 2015

Remote-control warfare is an emerging strategy that allows for conflict to be actioned at a distance. It incorporates technologies and light-footprint deployments that enable policymakers and military planners to approve actions that would unlikely be considered if using conventional means.

These monthly briefings are produced by **Open Briefing** and commissioned by the **Remote Control** project, a project of the Network for Social Change, hosted by Oxford Research Group.

Special operations forces: Attacks in France, Australia and Canada highlight domestic deployment of special operations forces for counter-terrorism operations.

Private military and security companies: New trends in use of private military and security companies in conflict zones risks state of 'neomedievalism'.

Unmanned vehicles and autonomous weapons systems: Terrorist use of drones presents major potential threat to key sites and personnel in West.

Cyber warfare: Hack on Sony Pictures highlights key challenges in cyber security and conflict.

Intelligence, surveillance and reconnaissance: Paris shootings prompt widespread review of European surveillance and intelligence procedures.

Special operations forces

Attacks in France, Australia and Canada highlight domestic deployment of special operations forces for counter-terrorism operations

Recent attacks in France, Australia and Canada by individuals alleging inspiration from or direction by transnational extremist Islamist groups, such as Islamic State (IS) or al-Qaeda in the Arabian Peninsula (AQAP), have raised questions about the domestic use of special operations forces (SOF) to curtail political violence and respond to terrorist attacks.

The National Gendarmerie Intervention Group (GIGN), a special operations unit of the French armed forces, was deployed to track down Saïd and Chérif Kouachi, the suspects in the *Charlie Hebdo* attack on 7 January 2015. The French national police's Recherche Assistance Intervention Dissuasion (RAID) special operations unit was also deployed to resolve the hostage situation at the Paris kosher supermarket Hyper Cacher on 9 January.

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

British defence sources indicate that Prime Minister David Cameron has put UK special forces on high alert after the Paris attacks and intelligence reports of increased 'chatter' between surveillance targets. The SAS are reportedly re-enacting the Paris attacks in preparation for similar attacks in the United Kingdom. On 16 January, raids in Verviers, Belgium, which resulted in the death of two suspected terrorists, were lead by special operations units of the federal police.

In the aftermath of the Sydney Lindt café siege in December 2014, unidentified federal officers suggested that the New South Wales police should have called in the army's special operation forces rather than leaving it to the police force's special operations unit. Arguments were made that Special Air Service Regiment's counter-terrorism experience in Afghanistan made it a better candidate to handle the siege, despite the political challenges of characterising the Sydney siege as a terrorist act.

In contrast, the sergeant-at-arms of the House of Commons and the Royal Canadian Mounted Police ended the attack on Parliament Hill in the Canadian capital, Ottawa, in October 2014.

Political leaders can justify the involvement of special operations forces in domestic counter-terrorism as calling on the most experienced and capable forces available to successfully resolve terrorist incidents. The British prime minister's resolve to have SOF prepared for domestic terrorist attacks is likely being replicated across Western Europe and in other Five Eye jurisdictions, particularly where foreign fighters are returning from Syria and Iraq.

However, the increasing employment of military special forces to resolve terrorist actions in Western urban terrains does carry some risks. A military, as opposed to a law enforcement, response to domestic political violence is likely to support notions that the Iraqi and Syrian battlefields can be transposed to countries supporting US airstrikes and training Iraqi forces. The key advantage of military special operations forces – that they are likely to have fought combat operations in Afghanistan or Iraq – becomes a potential weakness when it heightens the sense of transposing a Middle Eastern battlefield into Western countries.

Furthermore, the use of special operations forces to address domestic political violence possibly reinforces higher public threat perceptions. It sends clear signals to the public that reinforce political discourses around the purported need for continued mass surveillance. Yet, in the attacks in France and Australia, questions have been raised about intelligence failures. The attackers in both cases were all previous under federal-level surveillance and well known to law enforcement and intelligence agencies.

The disposition of decision-makers to deploy or stand by special operations teams in response to terrorist attacks in Western cities is likely to continue in the face of the increased threat of 'blowback' from Western military actions in Syria, Iraq, Afghanistan and North Africa. That a militarised response risks moving the battlefield much closer to home and is at odds with the dominant 'control paradigm' and the preferred strategies of remote-control warfare (which action warfare at a distance and attempt to contain insecurity 'over there') reveals some of the inconsistencies at the heart of the current security approach.

Other developments

China's PLA Daily website published an article about the People's Liberation Army (PLA) and People's Armed Police (PAP) special operations units in December 2014.[1] Much of the information released by the PLA Daily and republished by regional newspapers[2] on China's 10 major special operations forces was already in the public domain, though not in a way that provided a broad overview of unit capabilities and force size. The formation of special operations units in China started in the 1980s, and operator numbers have increased from 12,000 in 1990 to over 30,000 today. Retired US Army Lieutenant Colonel Dennis Blasko produced a detailed analysis in response to the publication, outlining command structures, operational capabilities, training and doctrines.[3] China's SOF units have a high degree of variability in capabilities across military regions and organisational units. Based on available information, Chinese special operations forces have a predominantly anti-terrorist/anti-riot internal security mandate. Limited international operational experience coupled with limited intelligence networks that could support overseas operations means that Chinese special forces are unlikely to possess the unconventional warfare and counter-terrorism capabilities of their European and North American counterparts.

On 28 December 2014, *Der Spiegel* published documents from Edward Snowden's NSA collection that included a 2010 US special operations forces kill or capture list for Afghanistan.[4] The *Joint Prioritised Effects List* (JPEL)[5] appears to indicate that General Stanley McChrystal, then commander of US and NATO troops in Afghanistan, banned night raids in March and April 2010. The ban during this period was significant because of the political maelstrom caused by the night raids, in particular one in February 2010 in Gardez, Pakita province, by US SOF that resulted in civilian and government casualties. The documents also revealed that individuals were generally targeted based on their mobile phone number as opposed to names.

A number of failed or aborted rescue attempts in Yemen, Syria and Iraq may indicate that there is a heightened appreciation and understanding of US special forces tactics and capabilities. Former US Navy SEAL retired Rear Admiral George Worthington was quoted in a *Washington Post* article suggesting that Hollywood films and in-depth news accounts had revealed detailed special operations forces tactics to terrorist, criminal and insurgency organisations.[6] This raises the question of whether the tactical advantage special forces obtain through operational agility and harnessing the element of surprise can be eroded by counter-SOF tactics and decentralised communication networks, such as social media, that have the potential to feed live intelligence to all combatants.

[1] http://photo.81.cn/jrfc/2014-12/16/content_6270918.htm

[2] http://www.wantchinatimes.com/news-subclass-cnt.aspx?id=20141219000062&cid=1101

[3] http://warontherocks.com/2015/01/chinese-special-operations-forces-not-like-back-at-bragg/?singlepage=1

[4] http://www.spiegel.de/international/world/secret-docs-reveal-dubious-details-of-targeted-killings-in-afghanistan-a-1010358.html

[5] http://www.spiegel.de/media/media-35508.pdf

[6] http://www.washingtontimes.com/news/2014/dec/17/special-operations-forces-tactics-compromised-by-h/?page=all

Also of note

- **The Chadian military is to host Flintlock 2015 in February and March.** Flintlock is an annual multinational training exercise conducted by US Special Operations Command Forward – West Africa aimed at improving force interoperability and capacity building among counter-terrorism forces. This year's exercise is likely to take on a renewed importance after recent large-scale attacks by Boko Haram in northern Nigeria resulted in the killing of over 2,000 people.
- **Lithuania has recently formed a rapid reaction force to address hybrid, insurgent warfare similar to that seen in Ukraine in 2013 and 2014.** The force is made up of 2,500 personnel (representing a quarter of the country's active armed forces), and includes a special operations forces division for deployment within hours of reported offensives. The force is an interim self-defence measure until the NATO Very High Readiness Joint Task Force is operational in 2016.
- **Indian home minister Rajnath Singh met with a Mongolian Border Protection delegation in December to discuss security and defence issues, such as global terrorism and transnational organised crime.** Singh indicated that New Delhi would support Mongolia to increase its special operations forces and cyber security capabilities.
- **In late December, the *Ottawa Citizen* published detailed information on recent Canadian special operations forces training missions, which have included Belize, Kenya, Iraq, Jordan, Jamaica, Mali and Niger.**[7] A number of prominent Canadian MPs were unaware of many of the missions undertaken by the Canadian Special Operations Regiment (CSOR). Canadian Special Operations Forces Command (CANSOFCOM) missions have become more controversial after 69 SOF personnel were deployed to Iraq in October 2014 prior to parliament supporting the deployment.
- **An Islamic State sniper killed a key Iranian Quds Force unit commander, General Hamid Taqavi, on 27 December 2014.** The commander was advising Iraqi troops and Shia militia in Samarra, Iraq. The death of such a senior Quds Force figure highlights the extent of the unit's presence in Iraq.
- **Australian Prime Minister Tony Abbott has confirmed that a 200-strong Special Operations Task Group would train the Iraqi Counter-Terrorism Service (CTS),** despite concerns over human rights violations and the summary execution of prisoners in 2014.
- **The US defence department has announced a $498 million contract to build a fourth Mobile Landing Platform (MLP).** Also known as Afloat Forward Staging Bases, operational MLPs already provide staging grounds for special operations forces. The new MLP, which will come online in 2018, will provide additional mission support to special operations forces, particularly in the Middle East and North Africa theatre where base support may be more limited.
- **US Special Operations Command (USSOCOM) released details of the design requirements for its TALOS (Tactical Assault Light Operator Suit) combat suit on 18 December 2014.** Requirements for the powered armoured suit specified by USSOCOM include embedded technologies to reduce thermal and acoustic signatures, a robotic exoskeleton capable of lifting 100 kilograms and remotely-deployable advanced medical intervention devices.

[7] http://ottawacitizen.com/news/national/canadas-secret-soldiers-special-forces-work-takes-place-under-the-radar and http://ottawacitizen.com/news/politics/jungle-warfare-one-reporters-glimpse-of-special-forces-training-in-jamaica

Private military and security companies

New trends in use of private military and security companies in conflict zones risks state of 'neomedievalism'

Nearly all the 1, 800 US government contractors currently working in Iraq work for the US state department. They are mainly tasked with advising the Iraqi government on counter-terrorism and providing security to US diplomatic facilities. US President Barack Obama recently authorised doubling US troop numbers, and though contractors remain in non-combat roles, the Pentagon recently issued a note that it would consult with private companies to possibly advise Iraq's ministry of defence on fighting the threat from Islamic State. Therefore, it is probable that PMSCs will become gradually engaged in direct combat roles in Iraq in the near future.

In light of this, a new book published by Oxford University Press highlights some increasingly important issues around the use of PMSCs. *The Modern Mercenary: Private Armies and What They Mean for World Order* by former DynCorp programme manager Sean McFate provides a rare insider's account of private military contractors' security provision in conflict zones, illustrated through case studies ranging from Liberia to Somalia to Afghanistan.[8]

McFate served as a paratrooper in the US Army's 82nd Airborne Division, and is now an adjunct professor at Georgetown University and the National Defense University. In *The Modern Mercenary*, he argues that the market for Private Military and Security Companies (PMSCs) is likely to evolve from a monopsony where the US government has been the main buyer, to an increasingly competitive market with additional actors. This prediction is likely to be proved correct given that the United States is scaling back its operations in Afghanistan and Russia, for example, is moving to amend its legal framework in order to better accommodate the use of PMSCs.

The use of PMSCs in conflict zones addresses both political and economic realities. On the one hand, decision-makers are increasingly loss-averse when it comes to putting the lives of soldiers at risk. On the other hand, the sheer cost of maintaining a standing army makes private military contractors contracted for specific tasks extremely attractive from a cost-efficiency viewpoint. In fact, the total cost to the United States of operating an infantry unit in Iraq was $110 million, while the same size unit from Blackwater only cost $99 million. In view of these trends, McFate suggests that a truly open market of private armies competing for contracts might result in turning warfare into a mere business. This could possibly create additional incentives among stakeholders to start new wars.

However, his prediction that modern mercenaries will eventually become more preponderant than the standing armies of NATO and China is highly unlikely to happen in the near future. McFate argues that 'international relations in the 21st century will have more in common with the 12th century than with the 20th'. He warns against the dangers of what he calls 'neomedievalism', which refers to the state gradually losing its monopoly over the legal use of forces, while wealthy groups and individuals become able to finance and mobilise private military endeavours abroad.

[8] http://ukcatalogue.oup.com/product/9780199360109.do

The author also attempts to challenge the widespread belief that mercenaries are always little more than 'murderous thugs'. He argues that a competitive marketplace, along with widely covered events such as the conviction of former Blackwater contractors in October 2014 for their roles in Baghdad's Nisour Square 2007 shootings, will rather tend to discipline or exclude 'bad mercenaries' from contracts. This claim is probably a little naive, as private military and security companies remain extremely opaque. Moreover, it took seven years for the Blackwater contractors to be prosecuted and eventually convicted for their roles in the Nisour Square shootings. The competitive marketplace of private armies will probably have little effect on constraining or changing them. Despite this, the author's subsequent claim that the United Nations could involve private military companies in its peacekeeping operations, though unlikely to occur in the near future, could possibly find supporters as member states become increasingly reluctant to contribute peacekeepers for UN operations.

Other developments

Following declassification revisions, the US Senate Select Committee on Intelligence's study of the CIA's detention and interrogation programme was released early December 2014.[9] In addition to releasing previously unknown details of various torture methods, the report revealed that 85% of interrogations that were part of the CIA's secret programme were outsourced to private contractors.[10] This includes psychologists hired and remunerated by the CIA for more than $80 million to design 'enhanced interrogation techniques'. Despite the fact that torture is a violation of US and international law, it is highly unlikely that the contractors will be prosecuted, which presents another instance of the unaccountability of private military and security contractors.

Two key international meetings aimed at further regulating private security provision took place in December 2014. The first annual general assembly meeting of the International Code of Conduct Association (ICoCA) took place on 4 December in London, United Kingdom. Its goal is to promote, govern and oversee the implementation of the International Code of Conduct for Private Security Service Providers. Then on 16 December, the constitutional meeting of the Montreux Document Forum (MDF) took place in Geneva Switzerland. The MDF provides a place for informal consultation among Montreux Document participants to discuss and exchange tools and best practices with regard to the implementation of Montreux document guidelines on PMSC regulation.

The United States Government Accountability Office (GAO) has published a report recommending increased guidance on pass-through contracts.[11] The use of so-called pass-through contracts is widespread, and consists of prime contractors using subcontractors to meet its contract requirements. The GAO reported that two-thirds of the $322 billion collectively spent in 2013 by the department of defence, the state department and USAID was awarded to private contractors who in turn used subcontractors. Such a practice is likely to generate waste and overpayment to private contractors. As a result, the GAO recommended that the concerned agencies issue guidelines to prime contractors while better documenting and monitoring the implementation of contract requirements.

[9] http://www.intelligence.senate.gov/study2014/sscistudy1.pdf

[10] http://www.huffingtonpost.com/2014/12/12/outsourcing-torture_n_6317236.html

[11] http://www.gao.gov/assets/670/667709.pdf

Also of note

- **There are around 100,000 private security contractors in Honduras, which amounts to three times the number of police officers.** Private security companies are legally required to be supervised by the national police, but this is seldom enforced. Such primacy reflects the dysfunctional state of Honduras' formal security apparatus.
- **China has unveiled an official website for military weapons procurement.**[12] The website falls under the General Armament Department of the People's Liberation Army (PLA), and lists China's weapon and armament needs as well as relevant procurement policies. The move is meant to increase transparency in procurement processes.
- **DynCorp International has been awarded two additional training contracts in Afghanistan.** The company was contracted by the US Army Contracting Command to provide 'advisory, training and mentoring services' to the Afghan National Police (ANP) and the Afghan National Army (ANA). Despite widely reported scandals and blunders, the contracts signal the US government's continued trust in DynCorp.
- **Russian President Vladimir Putin has signed a law allowing foreign mercenaries to contribute to the Russian military.** Provided they speak Russian and are not facing criminal charges, foreigners will be able to take part in situations of martial law and armed conflict. It is likely that the decree is mainly aimed at Russian-speaking mercenaries from the Caucasus or Central Asia, such as Tajiks or Kyrgyz citizens, who might face loyalty issues towards their own national armies.
- **A new report commissioned by the Remote Control project has shed light on PMSC 'floating armouries'.**[13] States are unwilling to host private armouries on their soil, which results in the deployment and storage of weapons on vessels located in international waters, outside of national jurisdiction. The practice shows clear loopholes in PMSC weapons legislation and regulation. The report recommends coordinated international action to address the issue.

[12] http://www.weain.mil.cn

[13] http://remotecontrolproject.org/wp-content/uploads/2014/12/FloatingArmouriesReport.pdf

Unmanned vehicles and autonomous weapon systems

Terrorist use of drones presents major potential threat to key sites and personnel in West

Since October 2014, approximately 20 unidentified drone flights have been reported over French nuclear power stations, mostly at night. On one night alone, five flights were conducted over separate stations many hundreds of miles apart, suggesting a coordinated action. Greenpeace has admitted flying paragliders over nuclear power stations in the past, but has denied any involvement in these new incursions. In December, another unmanned aerial vehicle (UAV) was seen flying over the large Doel nuclear power station in Belgium, which had only recently re-opened after being sabotaged by a suspected disgruntled worker. These incidents have raised concerns within security circles that these aircraft are being or could be used by terrorist or other hostile groups.

Platforms available today already offer a wide range of options for hostile groups. Such groups could take advantage of small helicopters capable of carrying HD cameras within close range of perimeter fences, building access points and critical infrastructure on surveillance and reconnaissance operations, or far larger models that could carry explosives weighing several kilogrammes to detonate precisely on target with minimal risk to the terrorists themselves. An attack by multiple drones on a nuclear power station could cause major destruction, which, while unlikely to cause a radioactive leak, could force the station to close for inspection and repairs, and would also raise considerable concern among nearby communities.

Terrorists could also use drones to target tourist sites and government/military infrastructure. In London, United Kingdom, police have reported an increased use of drones around locations such as Tower Bridge, the Tower of London, major shopping centres, sports stadiums and airports (including two near-misses with airliners), though none of these have been confirmed as terrorist-related. A recently-released batch of threat assessments by the Royal Canadian Mounted Police included a report entitled *Extremist Exploitation of Unmanned Aerial Vehicles*, which reported of plots by terrorist groups around the world to weaponise aircraft with improvised explosive devices and even chemical/biological devices. These plots targeted locations such as the US Capitol, the Pentagon, the UK Houses of Parliament and the principal military headquarters in Pakistan, though all were thwarted in the planning phase.

In 2012, a Massachusetts student was imprisoned for plotting to fly small drones into the Pentagon and the US Capitol. In April 2014, the FBI arrested Moroccan national El Mehdi Semlali Fahti in Connecticut, United States, for planning to arm drones with bombs and use them to attack a school and a federal building in the state. While no explosives were found in his possession at the time of his arrest, the suspect had admitted to undercover officers that he had previously successfully created a chemical weapon in Morocco and was confident that he could obtain everything in southern California that would be necessary to do it again. In July 2014, Hamas launched a small drone into Israeli territory. It was unarmed at the time, and was eventually destroyed by a Patriot missile, but Hamas have claimed to have other versions that will be used to conduct attacks. Hezbollah has been flying drones into Israeli airspace for several years. And Al-Qaeda has revealed plans to use drones for a range of brutal attacks.

Governments around the world are currently reviewing strategies for dealing with drones operating illegally, including developing rules of engagement for armed responses to UAVs fitted with weapons. For example, the New York Police Department are liaising with federal authorities and the military to design and implement a defence system for the city's open-air stadiums.

In a mirror of US drone use in Afghanistan, a drone fitted with a remote-controlled explosive device would be capable of targeting a VIP vehicle or to attack an individual out in the open – turning a key tactic of remote-control warfare back on the West. Last year in Germany, the German Pirate Party flew a drone over a crowd gathered to listen to a speech by German Chancellor Angela Merkel. While she was speaking, the drone was flown towards the podium, landing right in front of her. There was no real threat on this occasion; however, it certainly demonstrated the versatility and capability of such vehicles.

Other developments

There are growing concerns within the US military high command that strong demand for MQ-1 Predator and MQ-9 Reaper missions against Islamic State in Iraq and Syria is putting unsustainable pressure on the pilots, sensor operators, intelligence analysts and ground crew. Factors such as increased workloads, training truncated due to time-constraints and a narrow career structure are now driving crews to leave the UAV programme for the more conventional branches of the military. The US Air Force UAV wing is currently at 85% strength and decreasing, prompting defence chiefs to consider retention incentives, such as lucrative salary bonuses, to retain staff.

Between six and eight suspected militants were killed in a US drone strike in North Waziristan, Pakistan, on 20 December 2014. The target was a compound attributed to an Uzbek commander of the Taliban's Hafiz Gul Bahadar group. Hafiz Gul Bahadar is the top Taliban commander for North Waziristan, and administers the militant stronghold of Datta Khel. The strike reportedly killed an unnamed senior militant leader (possibly Punjabi Taliban commander Qari Imran). Meanwhile in Somalia, it is reported that the intelligence chief for al-Shabaab, Tahlil Abdishakur, was killed in a drone strike on an armed convoy at the end of December.

The Italian Air Force has signed an agreement with the country's police forces that will see its Reaper UAVs used to monitor major events, such as football matches and demonstrations. This means that these aircraft will soon be flying over Rome, Milan, Turin and elsewhere in one of the most comprehensive deployments of UAVs over a European government's own territory. In other developments, Taiwan recently displayed some of its increasing homegrown UAV inventory. This included the Cardinal, a hand-launched platform for short-range reconnaissance, and the Albatross, a larger platform with a 10-hour endurance and a range of approximately 100 miles. Officials did not reveal whether the latter would be armed. Australia has awarded a no-bid contract to a US firm to supply a hand-launched UAV for use by its special forces. Known as the Raven, the aircraft is designed to loiter overhead while providing real-time imagery to ground troops and commanders. And Russia has unveiled a domestic UAV design developed by United Instrument Corporation as part of a claimed $9.2 billion investment in UAV capabilities by the Russian military. With a range of 50 miles, the Corsair will be a surveillance-only asset with a due-delivery date of the end of 2016.

Also of note

- **The US Army is to build its first dedicated UAV air base, for its Gray Eagle and Shadow platforms.** Based near Fort Bliss in western Texas, it will be equipped with two runways and will be adjacent to the White Sands missile range to allow for comprehensive armed testing and training.
- **The US is spending $338 million on 20 more Reapers for the air force and 25 more Predators for the army.** The Air Force has also been blocked from retiring aging Predators in the latest congressional defence funding bill.
- **Al-Qaeda in the Arabian Peninsula has released a 16-minute training video on anti-drone surveillance techniques.** Entitled 'Combatting Spy Airplanes" and uploaded to a jihadist Twitter feed, it included designs for 'thermal insulation covers' made from material such as heavy canvas and aluminium foil to hide fighters from infrared cameras and advice on the deployment of anti-drone sniper teams.
- **Russia and the United States have each revealed plans for decoy naval vessels.** Russia is developing decoy drones that would be launched from submarines to help them evade detection. Meanwhile, a US consortium has published further details of testing of unmanned surface vessels that would be launched from littoral (coastal) combat ships for mine-hunting and anti-submarine roles.

Cyber warfare

Hack on Sony Pictures highlights key challenges in cyber security and conflict

The international relations fallout from the hacking of Sony Pictures Entertainment in November 2014 steadily increased through December and into January. The cyber attack that crippled Sony's networks ahead of the release of their film The Interview has raised three key issues in the consistent media commentary: characterisation, attribution and response.

The characterisation of the nature or relative seriousness of the Sony Pictures hack has ranged from cyber vandalism to cyber war. In much the same way as the US administration has sought to craft nuanced points of difference between state spying in the form of NSA activities and Chinese cyber espionage for commercial gain, President Barack Obama strategically labelled the Sony hack as cyber vandalism. The characterisation seeks to: highlight the fact that physical harm was not inflicted on humans or critical infrastructure, denigrate the attack as juvenile and unsophisticated and help shape expectations of a proportionate response. However, this underplayed characterisation is likely to pose challenges for managing and understanding cyber threats over the short term. Challenges can arise from treating damage to information systems and data as having less significance than physical asset damage.

Attributing the attack has also created significant challenges. The FBI has indicated that it possesses evidence that suggests the Guardians of Peace, supported by the North Korean government, were responsible for the attack. However, the issues has been clouded by claims North Korea may not have the capacity to sponsor a breach such as that of Sony's network. A separate investigation by cyber security company Norse found evidence that an insider attack was more likely, and suggested that North Korean involvement was a red herring. Norse's vice president indicated that the swiftness of the FBI's announcement identifying North Korea as the perpetrator or source of the cyber intrusion raised red flags for the information security industry.

While government agencies undoubtedly face pressure in an international case such as the Sony Pictures hack to rapidly identify the source of the attack, there are key investigative challenges in positively identifying threat sources that can in some instances mean attribution takes weeks or months. Agencies such as the FBI may also be reluctant to publicly talk about the methods used to identify attackers, particularly when evidence may reveal cyber surveillance capabilities, which in this case may have been NSA capabilities. Furthermore, the identification of non-state actors will often then create the further challenge of showing a relationship between non-state hackers and the state apparatus. The key issue is that justifiable cyber responses, both from a legal and diplomatic standpoint, needs to be grounded in reliable and accurate attribution.

Considerable media opinion and commentary has focused on how the United States should respond to the Sony Pictures hack in the short term and the reforms necessary over the longer term. The US treasury department announced economic sanctions against key North Korean entities – primarily companies involved in weapons sales – in a bid to further restrict North Korean access to US financial markets. It is questionable whether these sanctions will directly impede North Korean cyber capabilities, and are more likely to inflict general economic punishment. When North Korea's internet and 3G mobile networks were disabled or jammed on two occasion in late December, some analysts suggested that it was a US response to the Sony Pictures hack. Arbor Networks and Dyn Research indicated their analysis found that it was a significant denial of service attack targeting the approximately 1,000 North Korean internet addresses that caused the outage. US officials denied responsibility for the network outage, while Lizard Squad, a hacking collective responsible for recent attacks on Xbox Live, claimed responsibility for the concerted denial of service attack on North Korean addresses.

Outside of the question of proportionately of counter-cyber strikes, there is significant potential for interloping state and non-state bad actors to insert themselves into cyber battlefields and escalate conflicts. The potential for miscalculation in cyber conflict is significant due to the absence of international norms or consensus, lack of shared understanding of relative offensive capabilities and limitations in attribution. As such, the Sony Pictures hack has highlighted far-wider issues than initially apparent.

Other developments

An Islamic State (IS) affiliated hacker is suspected of taking over control of the US Central Command (CENTCOM) Twitter and YouTube accounts on 12 January. The hacker, identified as Junaid Hussain, allegedly used @CENTCOM to disseminate IS propaganda, make threats against US soldiers, allege access to secure CENTCOM networks and supposedly to release confidential information on US personnel (though this was already publicly available). The hacking of @CENTCOM occurred as President Barack Obama was addressing the Federal Trade Commission on efforts to help companies prevent cyber attacks. It is most likely that @CENTCOM was compromised through brute-force password cracking, and would suggest that CENTCOM did not have two-factor authentication set up on the account. Concerns over Islamic State's cyber capabilities and activities were also raised by a recent malware campaign that sought to track and identify Syrian opposition groups. Analysis by Citizen Lab, based at the University of Toronto's Munk School of Global Affairs, has revealed an email sent by IS to Syrian opposition group working in Raqqa on human rights abuses was embedded with malware. The malware appeared to have the potential to send infected computer IP addresses and allow geo-location. It is likely the malware, which shows a degree of sophistication, was developed and distributed by Islamic State.

The White House and key US Congress decision makers are pushing for US cyber security regulation. President Barack Obama has called for new legislation that will force US companies to publicly report incidents where cyber security breaches reveal consumer information or data and provide some liability exemptions for companies that share information. The measures would also include greater sharing of threat information between government agencies and private companies. While no longer in control of congress, the president may expect some Republican bipartisanship after the Republican chair of the House Select Committee on Intelligence made a case for cyber regulation in a *Wall Street Journal* op-ed[14] and the Republication chair of the House Committee on Homeland Security noted the critical need for 'rules of the game' for cyber security and warfare.

Details of a November 2014 cyber defence cooperation agreement between Nordic and Baltic states were published in mid-December.[15] Building upon an existing cross-border Nordic Defence Cooperation (NORDEFCO) agreement between Sweden, Norway, Finland and Denmark, the new cyber defence proposals aim to enable a common Nordic-Baltic response to cyber threats. This would be consistent with recent NATO discussions on the interpretation of Article 5 as applying to cyber offensives. Two of the reported drivers of the regional agreement are concern around returning Islamic State fighters launching domestic cyber attacks against European state IT assets and cyber espionage by foreign powers. Surprisingly, although identified as a potential cyber threat, Russia has not featured as prominently as other threats in Nordic security agencies' assessments, despite clear concern in the Baltic states after the annexation of Crimea. The concern around cyber espionage is a key driver behind the recent announcement by Denmark that it is establishing an offensive cyber warfare unit supported by $74 million in government funding between 2015 and 2017. Danish defence companies involved in supplying parts for the F-35 Joint Strike Fighter programme were subject to sustained mass cyber espionage campaigns between 2008 and 2012, and the Danish Government is likely seeking to improve cyber security and develop counter strike capability as a form of deterrence.

Also of note

- **Germany's Federal Office for Information Security released a report in late December 2014 revealing that hackers compromised the systems of a steel mill and made it impossible to safely shut down a furnace.**[16] The attack, which started with a spear phishing campaign, enabled the hackers to gain access to sensitive networks and cause significant damage to the steel mill. The attack is only the second confirmed case in which a wholly digital attack caused physical equipment destruction.
- **The Indonesia government is considering the establishment of a National Cyber Agency to develop cyber security and counter-attack capabilities.** Data from the Indonesian Communications and Information Ministry showed that the country was the world's largest source of cyber crime attacks during part of 2013, and has consistently featured as one of the top five sources of cyber crime.

[14] http://www.wsj.com/articles/mike-rogers-stopping-the-next-cyberassault-1419543945

[15] http://www.defensenews.com/story/defense/international/europe/2014/12/10/common-threats-shape-nordic-baltic-cyber-cooperation-/20215605/

[16] http://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

- **Reports have emerged that the US Department of Homeland Security accidently released documents on the Aurora Project instead of Operation Aurora – a malware attack on Google – in response to a freedom of information request.**[17] The Aurora Project was a 2007 research effort to understand cyber security vulnerabilities common to electrical generators, and water pumps that could be used to shut down or damage critical infrastructure. Some of the documents identified specific infrastructure assets that were vulnerable to remote attacks.
- **Hacktivist group Anonymous announced it would launch a cyber retaliation against terrorist groups following the *Charlie Hebdo* and Hyper Cacher attacks in France.** Anonymous claimed on Twitter hashtag #OpCharleHebdo to have shut down ansar-alhaqq.net, though this would have only being a temporary shutdown resulting from a concerted distributed denial-of-service (DDoS) attack.
- **A new division with the Israeli Defence Force (IDF) C4I directorate, Matzpen ('Compass'), is building new big data networks and systems** in order to improve the IDF's ability to counter cyber attacks through predicting and detecting network behaviour. Matzpen's Operational Data Analysis Unit was deployed during recent conflict in mid-2014.
- **A Bloomberg report on 10 December 2014 suggests a 2008 fire on the Baku-Tbilisi-Ceyhan pipeline in eastern Turkey may have resulted from a cyber attack.**[18] US intelligence officials cited in the report suspect Russian hackers were behind the attack due to the relative sophistication and timing of the attack.
- **US Cyber Command is starting to develop operating capability, with at least 2,400 of the projected 6,000 personnel hired**. At the December 2014 TechNet Asia Pacific Conference, Lieutenant General James McLaughlin, deputy commander of US Cyber Command, noted that they are confronted by outdated equipment and systems and forthcoming military budget pressure imposed by the US Congress.
- **The Indian ministry of defence remains undecided about whether or not to go ahead with proposals to establish a cyber warfare command.** Proposals by the Indian army, navy and air force came after Chinese hackers allegedly broke into the Indian Defence Research and Development Organisation network.
- **IT security companies have released predictions of key cyber security issues for 2015.**[19] Korea's AhnLabs flagged an evolution in spear phishing attacks with more targeted attacks exhibiting much-higher levels of sophistication. McAfee identified the targeting of device vulnerability (webcams) as a way to gain greater access to control and information systems. RAND and many other companies all identified the Internet of Things leading to exploitation of device connectivity and Wi-Fi networks. Many companies identified the health sector as a likely target of cyber attacks in 2015.

[17] http://www.homelandsecuritynewswire.com/dr20150107-dhs-releases-the-wrong-foiarequested-documents-exposing-infrastructure-vulnerabilities

[18] http://www.bloomberg.com/news/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.html

[19] https://www2.fireeye.com/rs/fireye/images/wp-gazing-into%20the-cyber-security-future.pdf

Intelligence, surveillance and reconnaissance

Paris shootings prompt widespread review of European surveillance and intelligence procedures

In the wake of the twin terrorist attacks in Paris, the French authorities have been urgently reviewing their security capabilities to identify how three individuals, all well known to the security services, were able to obtain Kalashnikov assault rifles, considerable ammunition and a rocket-propelled grenade, and were able to plan and execute their operations without being detected. It has so far been revealed that the three gunmen, Saïd Kouachi, Chérif Kouachi and Amedy Coulibaly, had all had been on watchlists for many years. Having been identified as receiving training in Yemen from al-Qaeda in the Arabian Peninsula (AQAP) in 2011, the Kouachi brothers were placed under closer surveillance by the French security services. However, the absence of any suspicious activity during the surveillance operation led to the surveillance being dropped for greater priorities as authorities struggled to monitor hundreds of individuals returning to France having fought for extremist Islamist forces throughout the Middle East.

The repercussions of these attacks have been felt throughout Europe, and governments across the continent have started re-examining their counter-extremist strategies. The fact that just days after the Paris shootings a raid against a heavily-armed and well-trained Belgian cell, who were possibly hours from launching their operation to kill multiple police officers, only underlines the magnitude of the current threat. Counter-terrorist procedures have now been stepped-up throughout Europe. Troops have been deployed to cover probable targets in France and Belgium, while heavily armed police patrols are covering high-risk sites in many other countries.

A significant problem for European security services is the rise in these 'lone wolf' operations, carried out by individuals or very small and close-knit groups who plan and execute their attacks with minimal, if any, external contact or direction. Such individuals have attempted or successfully completed many attacks throughout Europe in recent years, including Bilal Abdulla and Kafeel Ahmed in London and Glasgow in 2007 and Anders Breivik in Norway in 2011. Traditional counter-terrorist methods rely heavily on monitoring communications, finance and supplies, together with information from informants and/or infiltration by undercover agents. Such methods have developed to become an effective tool against groups operating within conventional networks. However, 'lone wolf' extremists are all-but impossible to monitor and infiltrate, leaving authorities urgently trying to find new ways of identifying, monitoring and tackling such groups before they carry out their attacks.

The events in Paris have also further fuelled the liberty versus security debate. As was seen in the United States after 9/11 and the United Kingdom after 7/7, there are signs within French social and news media commentary that the widespread shock of the Paris attacks will see demands for more intense state surveillance overpower concerns of a pervasive state invasion of individual privacy.

Other developments

In December, after months of inter-party wrangling and despite a last-minute attempted block by Tea Party congressman Justin Amish, the US House of Representatives passed the Intelligence Authorisation Act by 325 votes to 100 to fund the country's intelligence agencies for another year. Fifty-five democrats and 45 republicans opposed the bill while the senate had already passed it unanimously. The act includes Clause 309, which puts into statute a 1981 presidential decree permitting widespread interception, retention and dissemination of communications, but now applies limits requiring communications that were not gathered through a court order or subpoena to not be held longer than five years, with some exceptions. Also last month, the Foreign Intelligence Surveillance Court approved the justice department's request for another 90-day extension of the National Security Agency's most controversial surveillance programme, allowing the government to continue its bulk collection of Americans' phone data. This renewed authority will expire on 27 February 2015.

The UK's Investigatory Powers Tribunal (IPT) has ruled that Britain's Government Communication Headquarters' (GCHQ) blanket monitoring of communications is not illegal under current legislation. The Tempora project involved tapping into fibre-optic networks to gain access to large amounts of internet users' personal data and usage. Privacy International, who bought the case to the IPT, have stated that they now intend to take their case to the European Court of Human Rights in the hope that Tempora will be found illegal under European human rights legislation. They also intend to argue that GCHQ operations in general breach citizens' privacy and freedom of expression rights as enshrined in Articles 8 and 10 of the European Convention on Human Rights.

For the first time, Japan and South Korea have agreed to share intelligence about North Korea's weapons programmes in a three-party pact with the United States. However, the agreement is narrowly defined, demonstrating that historical and territorial divisions still exist between the two countries. This is not a legally-binding treaty but a less-committed memorandum of understanding, and is restricted to North Korea's missile and nuclear development programmes. Furthermore, the intelligence will not be shared directly but via the United States. However, that this agreement exists in the first place is still a significant warming of relations between the two countries, and could start to break down the inherent mistrust that many South Koreans have towards Japan, their former colonial masters.

Also of note

- **A mysterious signals intelligence (SIGINT) operation has been discovered in Norway by a national newspaper.**[20] Fake mobile phone masts, of undetermined origin, capable of monitoring mobile communications have been found in the vicinity of the national parliament and the prime minister's office. Norwegian authorities are investigating.
- **Hong Kong police have inadvertently disrupted a Chinese intelligence operation to monitor democracy supporters in the city.** A Democratic Party lawmaker reported to police of being followed by the same two cars over several days, police then intercepted and arrested the vehicle occupants. However, they were soon discretely released without further details being given.

[20] http://mm.aftenposten.no/stortinget-og-statsministeren-overvakes/

- **Several European projects are underway to study Russian domestic and international propaganda strategies and identify methods on how to counter them in the global media.** The Netherlands, the Baltic states, Denmark and the United Kingdom are running schemes that include broadcasting Russian-language programmes from neighbouring countries.
- **Following several attacks by al-Shabaab from neighbouring Somalia, Kenya's parliament has backed powerful security legislation.** The bill will allow one-year's detention of suspects without trial, warrant-free communications intercept by state agencies and restrictions on press reports on security issues without state consent.

Commissioned by the Remote Control Project

remotecontrolproject.org

REMOTE CONTROL
Examining changes in military engagement