Securing change

Recommendations for the British government regarding remote-control warfare

Chris Abbott
Scott Hickie
Steve Hathorn
Raphaël Zaffran

June 2015

Published by Open Briefing, 4 June 2015

Open Briefing
27 Old Gloucester Street
London WC1N 3AX
United Kingdom

Tel +44 (0)20 7193 9805
info@openbriefing.org

www.openbriefing.org

Commissioned by the Remote Control project
remotecontrolproject.org

REMOTE CONTROL
Examining changes in military engagement

Chris Abbott is the founder and executive director of Open Briefing. He is also an honorary visiting research fellow in the School of Social and International Studies at the University of Bradford and was the deputy director of Oxford Research Group until 2009.

Scott Hickie is a senior analyst at Open Briefing. He is a lawyer and former political adviser in the New South Wales parliament. He has worked on climate change adaptation for the City of Toronto, and is currently a policy officer with the New South Wales government.

Steve Hathorn is a contributing analyst at Open Briefing. He is an intelligence analyst with nearly 20 years' experience in the British Army, Defence Intelligence Staff, National Criminal Intelligence Service, United Nations, International Criminal Court and the Competition and Markets Authority.

Raphaël Zaffran is an associate researcher at Open Briefing. He is an analyst and political scientist researching and teaching international security issues. He is currently pursuing a PhD at the Graduate Institute of International and Development Studies in Geneva.

Open Briefing is the world's first civil society intelligence agency. It is a unique not-for-profit social enterprise that provides intelligence and research services to civil society organisations and concerned citizens.

Open Briefing Ltd is a **not-for-profit social enterprise** run nearly entirely by volunteers.
Registered in England & Wales as a company limited by guarantee, No. 07649656.

Securing change

Recommendations for the British government regarding remote-control warfare

Chris Abbott, Scott Hickie, Steve Hathorn and Raphaël Zaffran

About this briefing

Since April 2014, Open Briefing has produced a series of monthly intelligence briefings on remote-control warfare. These briefings are commissioned by the Remote Control project, which was initiated by the Network for Social Change and is hosted by Oxford Research Group. Every six months, Open Briefing undertakes a more in-depth assessment of trends in remote-control warfare. This report presents the findings from the second such review, and focuses on the issues of most significance to the United Kingdom, though they affect many other states too. Previous briefings can be accessed at http://www.openbriefing.org/tag/remote-control-warfare-monthly-briefing/.

Contents

Introduction

The United States has led the way in developing a new way of conceptualising and executing war. The emphasis now is on effecting warfare at a distance by relying on smart technologies and light-footprint deployments rather than more traditional military approaches. With the rise of austerity in Europe, other Western states have adopted part or all of this 'remote-control warfare' approach.

Within this, policymakers and military planners are promoting the tactics and technologies judged to have worked during the war on terror and associated conflicts in Afghanistan and Iraq. As such, the five key aspects of remote-control warfare are: special-operations forces; private military and security companies; unmanned vehicles and autonomous weapons systems; intelligence, surveillance and reconnaissance; and cyber warfare.

In the United Kingdom, the election of a Conservative-majority government in the May 2015 general election is unlikely to result in any significant departure from this approach. In fact, increased reliance on the tactics of remote-control warfare is likely as budget savings are made across Whitehall and the government responds to multiple security threats and conflicts around the world.

However, the assessment of recent trends contained in this report makes it increasingly clear that remote-control warfare has its limits. The report outlines some of the key unforeseen consequences from the use of remote-control warfare, including the transposition of Middle Eastern battlefields to Western cities through the deployment of special forces to respond to terrorist incidents at home, the enabling of adversaries to develop sophisticated cyber offensive capabilities through reverse engineering the cyber weapons deployed against them, and the risks presented by the terrorist use of weaponised civilian drones to attack critical national infrastructure or VIPs.

From the deployment of larger and more autonomous armed drones, to the development of ever more sophisticated cyber defence and offensive capabilities, this report also outlines the ways in which states are pursuing various 'arms races' in an attempt to maintain the strategic edge over their adversaries.

In light of these and the other trends discussed in the following pages, this report makes 31 specific recommendations for the new British government. What is ultimately needed is a comprehensive rethink of defence and security strategy and a move away from remote-control warfare towards more enduring, accountable and effective responses to today's multiple security threats. While the planned Strategic Defence and Security Review and update of the National Security Strategy both present ideal opportunities for the United Kingdom to do this, previous strategy reviews have failed to live up to expectations in this regard.

The recommendations presented in this report will allow the British government to mitigate some of the pitfalls of the current strategy. The hope is that innovators within cabinet, parliament and the Ministry of Defence will take them up and leave their mark through the promotion of lasting stability and security in the United Kingdom and more globally.

Summary of recommendations for the British government regarding remote-control warfare

In relation to **special forces,** the British government should:

1. Clearly articulate the strategic objectives that are to be achieved by any increase in the deployment of special forces to Iraq.
2. Implement regular reporting to parliament on special forces deployments, budget allocation and the achievement of strategic goals.
3. Improve the training, equipment and arsenals of police firearms units rather than increasingly diverting special forces to counter-terrorism at home.
4. Encourage information-sharing protocols between military and law enforcement units.
5. Develop clear guidelines on the training and support of local military forces that take into account the human rights standards of partners.
6. Evaluate the geographic deployment of special forces, and ensure major conflicts are not drawing disproportionate special forces resources at the expense of partnerships and engagements in other regions.

In relation to **private military and security companies,** the British government should:

1. Develop national legislation specific to private military and security companies that better takes into account the peculiar nature of those companies, particularly those operating in conflict zones.
2. Ensure that the development of appropriate prosecution processes is put on the PMSC oversight agenda to the same extent as the strengthening of international regulatory frameworks.
3. Raise awareness of the provisions of the International Code of Conduct for Private Security Providers (ICoC) and place significant emphasis on the effective monitoring of companies' compliance with the ICoC.
4. Strengthen international collaboration through bodies such as the ICoC Association and support the association's efforts towards the standardised and international regulation of private military and security companies.
5. Systematically vet the floating armouries it authorises British private military and security companies to use and make inventories of their arsenals publicly available.
6. Lobby concerned states and private maritime security companies to bring the issue of floating armouries into regulatory tools, such as ICoC, making it central to certification processes and monitoring mechanisms.

In relation to **unmanned vehicles and autonomous weapons systems,** the British government should:

1. Actively support the creation of an effective international control regime for unmanned combat air vehicles and other armed drones.
2. Facilitate the creation of a treaty-based international body tasked with prohibiting the export of weapons-capable drones to countries subject to UN Security Council sanctions or with poor human rights records.
3. Make funding available for the purchase of counter-drone systems to provide protection for high-value target sites and critical national infrastructure.
4. Make funding for early warning and drone countermeasures available to police forces and specialist units for the purchase of radio detectors and frequency jammers.
5. Work with European partners to bring in EU-wide licencing and registration for all civilian drones.
6. Consider initiating a national moratorium on the development of lethal autonomous weapons systems in order to allow international experts to more fully consider the practical and ethical questions raised by such systems.
7. Promote international agreements of assured transparency under which countries provide data demonstrating that any lethal autonomous weapons systems in front line service possess a degree of accuracy that ensures a very high probability of correctly assessing the threat before responding.
8. Determine whether existing international law needs amending to clearly identify the level of command that would be liable should autonomous systems fail and innocent bystanders are injured or killed.

In relation to **intelligence, surveillance and reconnaissance,** the British government should:

1. Move away from the broad approach of attempting to counter *all* extremism and towards concentrating finite resources on tackling those at highest risk of adopting violent approaches.
2. Replace active intervention for lower-risk individuals and implement a broad campaign to undermine jihadist propaganda by promoting effective non-violent protest and campaign skills as alternatives to violence.
3. Consider adopting a full-time cyber capability that can utilise the data-rich environment from the thousands of malicious attacks against the government's secure internet and proactively disrupt the attackers' activities.
4. Hold a comprehensive debate over the costs and benefits of bulk surveillance and wholesale intelligence gathering and implement fundamental reforms to those operations.
5. Launch an honest campaign to improve transparency in surveillance operations, explaining to the public as much as is possible (while maintaining operational security) the true intelligence gathering process.

In relation to **cyber warfare,** the British government should:

1. Actively support NATO to become a coherent cyber community that facilitates intelligence sharing, defence training and incident response.
2. Take steps to ensure that the intelligence and counter-terrorism agendas of the Five Eyes network do not disproportionately shape cyber security policy and detract from norm-building opportunities.
3. Participate in the agreement between the United States and Gulf Cooperation Council (GCC) to build GCC cyber security defences against external state and non-state threat actors by sharing UK institutional experience from the Cyber-Security Information Sharing Partnership (CISP) with GCC members.
4. Develop targeted bilateral initiatives through which to share cyber security expertise and threat intelligence with trusted partners in the Middle East, including Jordan and Israel.
5. Encourage the inclusion of cyber weapon proliferation in the terms of reference for the next House of Commons Defence Committee review into defence and cyber security.
6. Use the forthcoming National Security Strategy update to send clear signals to international partners on options to manage the proliferation of cyber weapons and flag the prioritisation of norm development.

Section I

Special operations forces

Military planners grapple with limitations of special forces in counter-terrorism operations; increasing deployment of special forces for domestic counter-terrorism brings new risks; ongoing conflicts prompt growth in regional special forces partnerships.

Military planners grapple with limitations of special forces in counter-terrorism operations

The counter-terrorism tactics used by special operations forces (SOF) are failing to deliver long-term security outcomes. As such, the political expectations placed on special forces are out of step with military realities. This is demonstrated by the difficulties experienced in ongoing US operations across Afghanistan, Iraq, Yemen, Somalia and Mali and emerging challenges in West Africa, which give cause for concern that the commitment of special forces may eventually translate into the deployment of conventional forces, despite significant political sensitivity.

In an interview in February 2015, Captain Robert Newson, a US Navy SEAL who previously commanded US Special Operations Command (Forward) in Yemen, delivered a strong critique of US counter-terrorism (CT) operations in Yemen. Newson argued that 'the "CT concept" – the solution that some people champion where the main or whole effort is drone strikes and special operations raids – is a fantasy. It may be cheaper and safer, but without broader efforts it is like mowing the grass in the jungle.'[1] Newson also noted that while these counter-terrorism operations do disrupt an adversary's operational planning and attack preparation, they do little more than buy time and space for broader strategic planning. He further suggested that the whole US military chain of command understands that special forces raids and drone strikes are only a stopgap measure to enable preparation for broader, more strategic intervention.

The withdrawal of US special forces from Yemen in March 2015 highlights the limitations of current counter-terrorism strategies. The withdrawal resulted in the loss of vital ongoing intelligence on al-Qaeda in the Arabian Peninsula (AQAP) and Islamic State (IS), together with an unaccounted for $500 million in physical assets, such as vehicles and weaponry, likely abandoned by the Yemeni army and seized by Houthi insurgents. Elsewhere, the overturning of the ban on night raids in Afghanistan in November 2014 suggests substantial Afghan and US concerns over the threat posed by a Taliban resurgence despite over 13 years of counter-terrorism operations. In many instances, special forces counter-terrorism operations are more 'treading water' than a long-term security and stabilisation strategy.

[1] https://www.ctc.usma.edu/posts/a-view-from-the-ct-foxhole-an-interview-with-captain-robert-a-newson-military-fellow-council-on-foreign-relations

This limitation is compounded by emerging evidence that counter-terrorism operations may be proving less effective against groups such as AQAP, the Taliban and Islamic State due to the increasing decentralisation of terrorist networks. Such groups are developing greater resilience and demonstrating an ability to regenerate their networks once Western counter-terrorism campaigns come to an end. Rear Admiral George Worthington (Ret.), a former commander of the US Naval Special Warfare Command, has suggested Hollywood films and in-depth news accounts have revealed detailed special forces tactics to terrorist, criminal and insurgency organisations, thereby reducing the tactical advantage usually enjoyed by special forces.[2] Operational agility and the ability of special forces to harness the element of surprise have been eroded by counter-SOF tactics and decentralised communication networks. The limitations of special forces is placing greater strain on multilateral- or US-trained local forces, who may not have the political, institutional or operational support to continue counter-terrorism campaigns after Western advisors leave.

The commitment of conventional forces to secure longer-term strategic objectives remains deeply contested in the United States and a number of its allies, including Canada, France, Australia and the United Kingdom. All have allocated a role for special forces in Iraq, for example, that emphasises advisory and training tasks but underscores the absence of combat troops, despite unconfirmed reports suggesting some special forces soldiers have been engaged in combat.

In January 2015, the UK parliament's Defence Committee report on the situation in Iraq and Syria and the response to Islamic State noted that the British contribution to Iraq had been modest compared to other alliance partners. The committee appears to suggest in Recommendation 12 that there is scope for the greater deployment of special forces in Iraq. However, policymakers and military planners will need to **clearly articulate the strategic objectives that are to be achieved by any increase in any such deployments.**

The risk facing Britain and her allies is that the current model of engagement, focused on special forces counter-terrorism advisory and training roles, will not achieve the desired military objectives. This may result in ever-increasing demands for further resources or, worse, ensnarement in a regional sectarian conflict. Incremental resource demands and mission creep may turn what started as a light footprint, limited engagement into a broader military commitment.

In order to counter this, the British government should **implement regular reporting to parliament on special forces deployments, budget allocation and the achievement of strategic goals.** Reporting should also identify other measures, such as institution building, development and aid support or diplomacy, that would better serve the United Kingdom's national interest.

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

Increasing deployment of special forces for domestic counter-terrorism brings new risks

Attacks in late 2014 and early 2015 in Canada, Australia and France raised questions about the possible use of Western special forces to curtail political violence and respond to terrorist incidents at home. The British, American, French and Australian governments all signalled a possible willingness to use special forces for domestic counter-terrorism operations in response to perceived threats from returning foreign fighters and 'lone wolf' attackers inspired by online recruitment campaigns. However, the increasing deployment of military special forces to resolve terrorist actions in Western cities involves considerable risk. Military, as opposed to law enforcement, responses to domestic political violence are likely to support notions that the Iraqi and Syrian battlefields can be transposed to countries supporting US airstrikes and training Iraqi forces. A key advantage of military special forces – that they are likely to have gained experience fighting combat operations in Afghanistan or Iraq – becomes a potential weakness when it heightens the sense of shifting a Middle Eastern battlefield into Western cities.

Trends in procurement for special forces may indicate a greater preparation for and focus on conflict in urban terrains. In March, US Special Operations Command (USSOCOM) issued a request for information on urban warfare technology. The request made reference to holographic field visualisation and intelligence, surveillance and reconnaissance (ISR) tools to deliver live social media analytics, helping ground forces anticipate group-level actions. USSOCOM are also reportedly testing a new multi-role (anti-armour) shoulder-fired weapon, as other weapons are too lethal or destructive for urban environments and therefore contrary to rules of engagement in civilian population areas. Similarly, reports on large-scale urban training events, such as the US Army Special Operations Command's JADE HELM 15, point to increased preparedness for urban theatres in current conflict zones. British special forces procurement trends are likely to substantially follow US trends, in part due to force interoperability needs, particularly in shared conflict theatres.

The British government should give consideration to the risks associated with the over-deployment of special forces in response to domestic terrorism incidents. Chief among these is the credence such deployments give to notions of taking the battlefield from the Middle East and North Africa into Western cities. Furthermore, although it can play well with a public and media demanding strong responses to terrorist attacks, the direct involvement of special forces in raids, arrests and hostage rescue involving terrorist suspects is largely unnecessary. In Britain, Specialist Firearms Officers are highly trained in order to respond to potential terrorist incidents, including building sieges and active shooters, and London's Specialist Firearms Command (SCO19) includes Counter Terrorist Specialist Firearms Officers.

Police firearms units are far more likely than special forces to be the first armed officers on the scene of any terrorist attack, and are therefore going to be the ones most likely to swiftly bring the incident to an end. Should a long standoff occur, special forces may then have time to deploy, but this is unlikely in a wide range of scenarios, even in central London. As such, the British government should **focus on improving the training, equipment and arsenals of police firearms units rather than increasingly diverting special forces to counter-terrorism at home.** In doing so, a balance needs to be struck to avoid the over-militarisation of the police that is occurring in the United States. Furthermore, special forces have a high level of collaboration with law enforcement and intelligence agencies, meaning their experience and advice can easily be drawn upon. **Information-sharing protocols between military and law enforcement units should therefore also be encouraged.**

Ongoing conflicts prompt growth in regional special forces partnerships

Insecurity and conflict in Eastern Europe, the Middle East and Sub-Saharan Africa are driving new regional special forces partnerships. Such partnerships range from advisory missions, which are focussed on training and knowledge transfer, to joint combat missions. They underscore broader strategic collaboration to address common threats. Multilateral special forces partnerships may, for a time, take the pressure off countries where conventional forces lack the skills and capacity to address critical security threats despite their significant size.

In February 2015, the defence attaché at the Jordanian embassy in Washington DC, Princess Aisha bint Al Hussein, told the Global SOF Symposium in Florida, United States, that the responsibility for confronting terrorism in the name of Islam lies with Muslim countries, and not just those of the Arab world. In March 2015, the Arab League announced a proposed 40,000 strong regional force to confront the challenges of the region, which is a likely acknowledgement of the need for regional collaboration. The force is expected to include an elite special operations command made up of forces from Egypt, Saudi Arabia, Jordon, Sudan and Morocco. In February and March 2015, over 1,000 special forces personnel from 29 Western and African countries participated in the US Africa Command-sponsored Exercise Flintlock in Chad. The exercise is just one element of ongoing efforts to build regional force cooperation and counter-terrorism expertise. However, Western special forces training partners may not be able to facilitate interoperability from the outside.

Russia's annexation of Crimea has also prompted new regional partnerships and training exercises between special forces in Europe. NATO's new spearhead division (Very High Readiness Joint Task Force) of its Response Force is expected to comprise 5,000 troops from member countries, including special forces personnel. In April 2015, 1,500 members of the spearhead division from Croatia, Denmark, Germany, Hungary, Lithuania, Norway, Slovenia, Poland and Portugal participated in the Noble Jump exercise. Chechnya has also proposed building a privately financed international special forces training centre modelled on Jordan's Special Operations Training Centre and aimed at servicing mostly ex-Soviet and Latin American countries.

The challenge with committing large numbers of special forces to multilateral forces is that it may limit the wider deployment of special forces teams to other regions. For example, the deployment of Western special forces in East and Southeast Asia is comparatively small compared to the Middle East, Sub-Saharan African and Eastern Europe, despite concerns over the emerging power shifts and maritime territorial disputes in the region. The limited presence of special forces from outside the region and the lack of knowledge about special forces partnerships and exchanges involving BRICS countries, in particular China and India, may have implications for Western allies.

Regional special forces collaborations and joint forces can provide a critical mass of personnel that start to emulate the size of small conventional force deployments. The risks, commitment and exposure for the participating countries are limited, but the collective capability of regional special forces is significant. British special forces have continued to participate in joint training exercises and will almost definitely continue involvement in multilateral force activities. However, just as arms export control regimes factor in human rights records, the same should be true for participation in regional special forces partnerships. Partnerships involve significant and specialised knowledge transfer, and the British government should **develop clear guidelines on the training and support of local forces that take into account the human rights standards of partners.** They should also **evaluate the geographic deployment of special forces, and ensure major conflicts are not drawing disproportionate special forces resources at the expense of partnerships and engagements in other regions.**

Section II

Private military and security companies

Blackwater trial highlights difficulties prosecuting private security contractors; governments seek to better regulate private military and security companies; floating armouries continue to be cause for concern.

Blackwater trial highlights difficulties prosecuting private security contractors

On 13 April 2015, US District Court Senior Judge Royce Lamberth sentenced four former Blackwater security contractors to long prison terms for their involvement in the killing of 17 Iraqi civilians in Baghdad's Nisour Square on 16 September 2007. In October 2014, a US federal jury had found the four contractors guilty on charges ranging from weapons charges to manslaughter and murder. Former US Army sniper Nicholas Slatten received a life sentence, while the three other former Blackwater employees, Paul Slough, Evan Liberty and Dustin Heard, were sentenced to 30 years each. The sentencing drew a long protracted judicial journey to a close. However, the overall trial process and its eventual conclusion has implications beyond this case, including for how states enforce the accountability of private military and security companies (PMSCs) and how they approach the process of prosecuting private contractors who commit crimes.

The trial and sentencing were hailed as diplomatic victories by the United States, which framed the trial's outcome as an example of the US criminal justice system's trustworthiness. However, the chairperson of UN Working Group on the use of mercenaries, Elżbieta Karska, argued after the April sentencing that 'The difficulty in bringing a prosecution in this case shows the need for an international treaty to address the increasingly significant role that private military companies play in transnational conflicts.'[3] The atmosphere surrounding the trial suggests that the prosecution of PMSC contractors remains a controversial endeavour due to the lack of both judicial precedent and a regulatory framework to act as guidelines for the judicial process. Indeed, Karska pointed out that 'such examples of accountability are the exception rather than the rule'. The convicted Blackwater contractors remained largely defiant during the April sentencing. Lamberth controversially described the defendants as 'good young men who've never been in trouble, who served their country'. The judge was also criticised for imposing sentences lower than those sought by the government for the guards convinced of manslaughter and weapons charges. This suggests a continued unease over the very idea of prosecuting PMSC contractors.

[3] http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15840&LangID=E

The Blackwater trial, verdict and sentencing received considerable attention in US and British media because of those states increasing reliance on PMSCs during the wars in Iraq and Afghanistan. Militaries on both sides of the Atlantic are now dependent on private contractors for the provision of protection services for supply convoys, key buildings and individuals, as well as intelligence gathering and training activities. This is undermining their capacity to operate autonomously. According to available data, the United States spends around 30% of its defence budget on private services and the United Kingdom around 25% (compared to only 5% in the case of Germany).[4] The British government has also become particularly dependent on private security companies at home, as evidenced by the privatisation of various aspects of the prison service (including prison escort) and the use of G4S to provide security for the London 2012 Olympics. G4S was also contracted by the UK Border Agency in 2012 to manage asylum-seeker housing. All of these instances led to controversies due to the lack of quality in service provision and the weak safeguards against human rights abuses. These aspects are part of the wider accountability concerns associated with the use of PMSCs.

Prosecuting PMSCs or individual contractors who commit crimes abroad is particularly difficult because conducting criminal investigations in foreign territories presents a range of diplomatic and jurisdiction issues that can make evidence gathering difficult and inhibit due process. Carrying out a proper investigation in a conflict zone can be even more difficult. Moreover, contractors operating in foreign conflict zones often end up with de facto immunity through anonymity. These factors lead to gaps in the evidence and make it very difficult for domestic law enforcement to investigate and arrest private contractors under suspicion.

Ultimately, the Blackwater trial is unlikely to mark a long-term normative shift. It has reinforced the notion that prosecuting PMSCs is a complex, long and frustrating judicial process. Therefore, the UK government should learn from the trial experience and **develop national legislation specific to PMSCs that better takes into account the peculiar nature of those companies, particularly those operating in conflict zones.** The government should also work with its international partners to **ensure that the development of appropriate prosecution processes is put on the PMSC oversight agenda to the same extent as the strengthening of international regulatory frameworks.** Whereas the latter aims to establish important preventive measures and monitoring mechanisms, the former is central to effective implementation of regulation.

[4] https://www.opendemocracy.net/ourkingdom/harry-blain/confronting-britain's-militaryindustrial-complex and http://psm.du.edu/media/documents/reports_and_stats/journal_articles/reports_journal_author_k_kruck_theorising_the_use_of_private_military_and_security_companies.pdf

Governments seek to better regulate private military and security companies

A few countries have attempted to fill the gap in the international regulation of private military and security companies either through national legislation or through international efforts. National initiatives include the 2015 US House of Representatives' National Defense Authorization Act (NDAA) and South Africa's Private Security Industry Regulation Act (PSIRA), as well as the South African government's move to effectively outlaw South African PMSCs' foreign operations. On the other hand, the United Kingdom has tried to push the private security industry to engage in self-regulation and improve their standards and adherence to human rights principles. As a result, the British Association of Private Security Companies (BAPSC) now praises itself as having 'worked extensively with its members and humanitarian organisations such as the Red Cross to improve standards of training in international humanitarian law. It also acts as a channel between companies and international organisations such as the African Development Bank to ensure that consideration is given to human rights issues.'[5]

The lobbying of key actors in the private military and security industry is an important addition to the development of national and international legislation controlling private military and security companies. It should be continued, especially as means to increase awareness of the provisions of the International Code of Conduct for Private Security Providers (ICoC) and push companies to take enforcement and implementation seriously. The oversight mechanism for the code of conduct is the ICoC Association (ICoCA), which is a multi-stakeholder initiative made up of states, private security companies and civil society organisations. It handles the certification and monitoring of member companies' compliance with the code of conduct, and deals with complaints and alleged violations.

Such lobbying is also aligned with the Montreux Document of 17 September 2008, one of the first documents defining how international law applies to the activities conducted by PMSCs in conflict zones.[6] The Montreux Document specifies states' existing obligations and good practices under international law. Such soft law instruments help clarify obligations and enable states to transpose international rules into national law or policies. Since 2008, key stakeholders, such as Switzerland and the International Committee of the Red Cross, have been attempting to strengthen the document by pushing states to take measures so that their national practices comply with international law.

The 2000 Voluntary Principles on Security and Human Rights are also key in guiding the conduct of private security companies. They are non-binding guidelines designed specifically for oil, gas and mining companies, and address those companies' operational safety and security, which includes privately-contracted security services.

[5] http://www.bapsc.org.uk/

[6] http://www.eda.admin.ch/psc

The fourth session of the open-ended intergovernmental working group on the possibility of elaborating an international regulatory framework on the regulation, monitoring and oversight of the activities of private military and security companies took place from 27 April to 1 May 2015 at the United Nations in Geneva, Switzerland. It consisted of over 50 delegations from states and other stakeholders. The working group's agenda included items ranging from regulating sea-based private security activities to the use of private security companies by the United Nations, as well as updates regarding national legislations and measures for registering, licensing and contracting PMSCs.[7] Conclusions and suggestions included the need to elaborate a legally-binding instrument for the regulation, monitoring and oversight of PMSCs, possible contract templates based on the Montreux Document and mutual legal assistance programmes.

In order to strengthen such efforts, the British government should **raise awareness of the provisions of the ICoC and place significant emphasis on the effective monitoring of companies' compliance with the code of conduct,** as monitoring processes are central to accountability and essential for potential prosecutions. Ultimately, national laws are useful but difficult to enforce when private military companies operate abroad, which makes swift criminal investigation and prosecution unrealistic. Moreover, private contractors are likely to exploit gaps generated by unaligned or varying national legislation on PMSCs. Therefore, the British government should strive to **strengthen international collaboration through bodies such as the ICoC Association and support the association's efforts towards standardised and international PMSC regulation.** It is the only realistic route to ensure the prosecution of PMSCs is assured and does not lead to long protracted legal battles.

Floating armouries continue to be cause for concern

The scandal that erupted in March 2015 over former Sri Lankan defence secretary Gotabaya Rajapaksa's 'floating armoury' has again raised the issue of at-sea arsenals and the problems they pose not only for regulating private military and security companies but also for maritime security. A Sri Lankan court accused Rajapaksa of maintaining his own private army with a floating armoury stationed in the southern port of Galle. The police seized more than 3,000 weapons from the armoury, which was operated by a Sri Lankan private security company, Avant Garde Maritime Services (Pvt) Ltd (AGMS). Rajapaksa, who is the brother of former President Mahinda Rajapaksa, has challenged the investigations against him stating they are politically motivated. In May, he obtained an interim injunction from the country's supreme court against his arrest.

[7] http://www.ohchr.org/Documents/HRBodies/HRCouncil/WGMilitary/Session4/pow_4thsession.pdf

A December 2014 report by the Omega Research Foundation shed light on the curious phenomenon of floating armouries.[8] The report, commissioned by the Remote Control project, revealed that shipping companies have gradually moved to hiring private companies to provide armed guards and other protective measures against piracy. However, many states are now unwilling to host large private armouries on their soil. As such, companies have moved to storing weapons on vessels located in international waters, in particular around the edges of the Indian Ocean near the High Risk Area bounded by the Suez and the Strait of Hormuz. This also places these vessels and armouries outside of national jurisdiction. The practice shows clear gaps in private maritime security legislation and PMSC regulation in general. The report recommended coordinated international action to address the issue.

Floating armouries present a severe security risk, as they involve large and unregulated military arsenals off the coasts of fragile states and in areas at great risk of pirate attacks. In September 2014, the British government stated that it had authorised UK-registered security companies to make use of 31 floating armouries. However, little more is publicly known of the international picture. Mapping and inventory efforts are needed in order to determine the exact magnitude of the floating armoury phenomenon, clustering of vessel location, and crucially, the exact nature of the arsenals that are stationed off the coasts of potentially fragile states.

In the case of the floating armoury scandal in Sri Lanka, the concerned company, AGMS, describes itself as providing a 'comprehensive range of total risk mitigation solutions to the global maritime industry' and 'total logistical assistance to vessels transiting the Indian Ocean'. The company has many senior Sri Lankan military commanders on its advisory board and management team. Controversially, it stores Sri Lankan government owned weapons and makes them available to maritime security guards working on ships operating around Sri Lanka. Although AGMS is a signatory of the ICoC, floating armouries tend to exploit gaps in blurry international regulatory frameworks, especially the fact that they are only accountable to the state in which they are registered. Without better-established regulatory and legislative frameworks covering the use of private maritime security contractors, it is likely that such floating armouries will continue to flourish.

Given the economic interests it represents, the British government should more **systematically vet the floating armouries it authorises British PMSCs to use and make inventories publicly available** to allow more effective monitoring of their arsenals. The government should also lobby in international forums to put an end to the legal grey area that floating armouries have operated in. It should **lobby concerned states and private maritime security companies to bring the issue into regulatory tools, such as ICoC, making it central to certification processes and monitoring mechanisms.** Specifically, floating armouries should be made accountable to all members and observers of the ICoC and not only to the state in which they are registered.

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

Section III

Unmanned vehicles and autonomous weapons systems

Potential foes rapidly developing unmanned vehicles while United Kingdom lags behind; new risks from terrorist use of weaponised drones; speed of development of lethal autonomous weapons systems outpacing attempts at prohibition.

Potential foes rapidly developing unmanned vehicles while United Kingdom lags behind

The United States aside, NATO member states have been slow to develop and implement drone technology as the world's militaries move into the new era of unmanned and autonomous hardware. However, certain countries that could be categorised as potentially hostile to NATO states have been far more enthusiastic in adding such technology to their respective armouries.

China, already heavily investing in conventional hardware, is planning 42,000 unmanned aerial and seaborne vehicles for both surveillance/reconnaissance and strike roles, according to the US Department of Defense's *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2015*.[9] This investment programme is reported to be costing $10.8 billion, and will be implemented over the next eight years. Washington is also becoming concerned that it might be losing its long-held military superiority in other areas, such as fighter jets, missile systems and cyber warfare. This should be ringing very loud alarm bells in other Western capitals in light of the highly-advanced equipment that the United States has been producing in recent years.

Russia is expected to unveil multiple new aerial drones in June 2015, including short- and medium-range variants, as well as large rotor-based models. These include the Eleron (short-range reconnaissance), Orlan-10 (medium-range reconnaissance), Forpost (medium-/long-range reconnaissance) and Gorizont (rotor-blade reconnaissance) platforms. Drones entering active military service are now at an all-time high in Russia, with 174 drones entering into service in 2014, almost as many as all previous years combined. The Russian government has now made drone development a military priority, and plans to spend $9.2 billion on new drones before 2020. This must be seen in light of the fact that the government of President Vladimir Putin has been increasingly belligerent in recent years as it seeks to recover from a post-Soviet era loss of global influence.

[9] http://i.cfr.org/content/publications/attachments/2015_China_Military_Power_Report.pdf

While not at the same technological level as Russia and China, Iran has been concentrating on mass deployment and has deployed drones throughout its substantial military. While some models have been created for the more usual short-/medium-range surveillance role, others have been designed to be fitted with explosives and launched on suicide missions against large ships as remotely-guided missiles. A recent exercise saw multiple such vehicles being launched towards barge modelled to resemble a US aircraft carrier. Such equipment will give Iran the means to launch a major swarm assault on Israel, which may overwhelm air defences. It has also been equipping Hamas and Hezbollah with drones to enable them to attack Israel.

In comparison, the United Kingdom has been markedly slow in the development and deployment of unmanned craft and autonomous weaponry. It has so far spent £2 billion (around $3 billion) on drones in the last eight years – an average of only £250 million per year. A lack of political will and funding has seen the once vaunted British military reduced to a second tier force. Investment is being made in drone technology but domestic designs are few and far between, with most purchases from US manufacturers. Only roughly half of the £2 billion invested over the last eight years has been spent on homegrown research and development of aircraft, such as the Watchkeeper long-range reconnaissance drone and the Taranis long-range stealth combat drone. While the United Kingdom is still funding major conventional projects, such as warships and fighter aircraft, these are being built in ever-fewer numbers, meaning the strategic capability of the combined forces is significantly weakened.

There is little doubt that the future lies in unmanned platforms. They are considerably cheaper than conventional manned platforms. They can also be deployed to theatre at greater speed, and pose less threat to human operators. Unmanned craft are also diverse in their capabilities, ranging from the well-known unmanned combat air vehicles, such as the Predator drone, to areas like naval fleet protection (for example, picket air defence, minesweepers and airborne radar), land forces support (for example, portable reconnaissance drones for frontline patrols, autonomous supply vehicles, IED detection and clearance, combat rescue vehicles and armed infantry-support drones) and next-stage air power (for example, loitering ground-attack weaponry, attack swarms and tiny close urban surveillance drones).

To counter the rapid development of unmanned vehicles by potentially hostile states, while at the same time mitigating its own relative lack of development in this area, the British government should **actively support the creation of an effective international control regime for unmanned combat air vehicles and other armed drones.** This should encourage countries with established and emerging drone capabilities to adopt a common code of practice that will regulate the capabilities and roles of weapons-capable unmanned platforms. The government should also **facilitate the creation of a treaty-based international body tasked with prohibiting the export of weapons-capable drones to countries subject to UN Security Council sanctions or with poor human rights records.**

New risks from terrorist use of weaponised drones

The wide availability of civilian drones and other remotely-controlled vehicles is offering terrorist groups new weapons platforms and a wide range of operational options. With models now available on the open market that are capable of carrying heavier payloads over longer distances from the control point, the threat of air-delivered remote control improvised explosive devices (RCIED) has become real. The capability to undertake surveillance via drones has already been evidenced by the unidentified flights over nuclear power stations and other sensitive locations in France and Belgium, but the risk is now moving to armed drones.

Conventional terrorist attacks usually require the attacker to approach the target, whether to plant an IED or to carry out a direct attack using personal weapons. This offers security agencies the opportunity to intercept the terrorists prior to an attack, foil an attack in progress or identify and catch the suspects after an attack through witnesses and surveillance imagery (as with the Tsarnaev brothers after the Boston Marathon bombings). Drones allow terrorists to deploy and detonate an IED from distance with far less chance of the bomb being discovered in advance or the attackers being identified.

Payload-capable drones have already been used by criminal groups, most notably drug trafficking gangs operating across the US-Mexico border, as well as those wishing to smuggle contraband into prisons in the United States. Hamas has been flying drones into Israel and Egypt for some time, though so far none have been identified as having been weaponised. Potential drone-based attacks have been thwarted in the United States, Germany, Spain and Egypt, with individuals and groups arrested during the planning stages of attacks.

A drone fitted with an IED could be launched from a discrete location up to two kilometres away and remotely flown towards a target, such as a VIP out in the open or in a moving car. For example, in September 2013, the German Pirate Party flew a camera-equipped drone over a crowd in Dresden listening to a speech by the German chancellor, Angela Merkel, and crash-landed it in front of the dais she was speaking from. Alternatively, a swarm of weaponised drones could be flown into a crowded area, such as an open-air concert or sports match, with devastating results. In January 2015, a drone crashed in the grounds of the White House. This was soon identified as an accidental overflight by a recreational craft, but it demonstrates the potential threat to even the most defended of facilities (in this particular case, there have been reports that jamming hardware disabled the drone causing it to crash, but these reports have not been confirmed by US authorities).

Payloads are not limited to explosives, with chemical and biological devices also possible. Furthermore, airborne drones are not the only option. Seaborne drones can be quite substantial in size (comparable to a small launch), and could be used to carry a sizeable payload towards another vessel, be it a ferry or warship. Submersible remotely-operated vehicles are also already available on the open market, though their payload capability is currently limited. Al-Qaeda operatives were able to cause a 40-by-60 foot hole in the USS Cole with a shaped charge deployed from a small craft in the port of Aden in Yemen in October 2000. Seventeen US sailors were killed in that attack, but terrorists could potentially cause even greater damage with a swarm attack using the remotely-operated platforms available today.

Defences against this emerging threat are currently relatively weak. Individuals can easily buy drones with cash, leaving very little in the way of a trail for investigators. The most complex part of planning such an attack is obtaining the explosive material and building the bomb, but long experience has shown what terrorists with the right resources and connections can achieve. Existing frequency jammers have a short-range effect, allowing a hostile drone to still get very close to the target before it can be disabled, plus they may well interfere with other vital communications in the vicinity. Jammers would also be less effective when defending mobile targets. However, after the January 2015 White House incident, it is thought that the Secret Service has accelerated testing of more-advanced jammers for use at key fixed sites. Some companies have developed other defensive measures, such as the Malou Tech Interceptor MP200, another drone designed to pursue hostile drones and entangle them in a low-hanging net. However, such a defence requires a high-speed response in order to be able to intercept a drone flying directly towards its target.

With such a significant threat level, it would be wise for the UK government to increase countermeasures at the earliest opportunity. The British government should **make funding available for the purchase of counter-drone systems,** such as the Anti-UAV Defence System (AUDS) by Blighter Surveillance Systems, Chess Dynamics and Enterprise Control Systems, to provide protection for high-value target sites and critical national infrastructure. The government should also **make funding for early warning and countermeasures available to police forces and specialist units,** such as the Diplomatic Protection Group (SO6), for the purchase of radio detectors, which alert security when a drone control frequency becomes active nearby, and frequency jammers. The government should also **work with European partners to bring in EU-wide licencing and registration for all civilian drones,** not just those conducting aerial surveillance work as is required under the current British law.

Speed of development of lethal autonomous weapons systems outpacing attempts at prohibition

Lethal autonomous weapons systems (LAWS) utilise artificial intelligence to select and fire upon targets without any human intervention. Although no such systems have been deployed yet, a number of robotic precursors with various degrees of autonomy and lethality are already in use. Ahead of a UN meeting of experts on lethal autonomous weapons systems in April 2015, the British government reiterated to the *Guardian* newspaper that it is not pursuing the manufacture of LAWS; however, nothing was said about whether or not they would purchase such systems from foreign manufacturers.[10] This is almost certainly the cause of London's current reluctance to pursue any new international agreement that will enforce limits on this burgeoning area of military technology. The United Kingdom claims that current international law already covers LAWS; however, this is highly debateable when there is no internationally agreed definition of what actually constitutes a lethal autonomous weapon. This may inevitably lead to heated debate as to whether a specific weapon is considered illegal or not.

Some countries already deploy systems that are able to respond automatically to incoming munitions, including the United States' Phalanx and C-Ram and Israel's Iron Dome. The United States currently has several LAWS under various stages of development. This includes the Special Weapons Observation Reconnaissance Detection System (SWORDS) vehicle from the Foster-Miller defence company, which is a tracked vehicle armed with various weapons options and designed to conduct programmed patrols of base perimeters, and the Autonomous Rotorcraft Sniper System (ARSS) being developed by the US Army, which is an airborne sniper vehicle designed to loiter over urban areas providing cover to ground patrols. There are also several non-lethal projects under development in the United States, covering casualty evacuation, supply transport and unarmed surveillance.

Supporters of the technology point to how a computer-controlled platform will remove a human from the front line, will be harder to defeat and will be able to respond quicker to sudden threats. These are certainly possible advantages in a conventional battlespace, where there are few civilians in the firing line. However, opponents counter with concerns that a computer will struggle to differentiate between armed fighters and unarmed civilians, a scenario that is highly likely in contemporary unconventional warzones. Indeed, assessing whether an individual is an armed threat is something that even human soldiers struggle with. There are also ethical questions over allowing a computer to decide between life and death.

[10] http://www.theguardian.com/politics/2015/apr/13/uk-opposes-international-ban-on-developing-killer-robots

Therefore, opponents call for the principle of meaningful human control, where a human operator retains the final say in whether lethal force can be used against a given target. They argue that this principle must be enshrined as soon as possible, as the rapid development of autonomous target recognition is already negating the need for human input and, once effective sensors are created, is only a short step away from autonomous weapons launch. The arguments in favour of pre-emptively banning the further development and use of fully-autonomous weapons are powerful, but there is likely to be much resistance to such calls, as many countries are keen to develop platforms that are capable of autonomous operation and will not agree to such restrictions. Even if limits are set on the capability of these weapons, the next obstacle will be how to enforce them. Such weaponry is clearly highly advanced and no country will be enthusiastic about international inspectors having access to such sensitive equipment. What is likely is that states will postpone the final deployment of LAWS until such time that a high degree of confidence in computer-only targeting is achieved.

These realities make it highly unlikely that the British government will support efforts to negotiate a treaty that would prohibit the development, production and deployment of fully-autonomous weapons. However, it should **consider initiating a national moratorium on the development of LAWS in order to allow international experts to more fully consider the practical and ethical questions raised by such systems.** Should LAWS come into front-line service, the British government should at a minimum **promote international agreements of assured transparency, with countries providing data demonstrating that these systems possess a degree of accuracy that ensures a very high probability of correctly assessing the threat before responding.** The government should also **determine whether existing international law needs amending to clearly identify the level of command that would be liable should autonomous systems fail and innocent bystanders are injured or killed.**

Section IV

Intelligence, surveillance and reconnaissance

West faces growing threat from Islamist extremism; cyber espionage threat from potential adversaries increasing; consequences of court rulings on GCHQ's mass collection programme.

West faces growing threat from Islamist extremism

The attacks in Ottawa, New York, Sydney, Dijon, Paris, Brussels, Copenhagen, Villejuif and Zvornik in the six months between October 2014 and April 2015 alone demonstrate that the extremist threat to Western countries remains high. In the United Kingdom, there has been a change in the frequency and severity of the terrorist plots the security services have foiled according to the Metropolitan Police Commissioner, Sir Bernard Hogan-Howe, who revealed the police had stopped four or five plots in 2014 alone.[11] The government's Joint Terrorism Analysis Centre (JTAC) assesses the current international terrorism threat level in the United Kingdom to be 'Severe', meaning an attack is highly likely. Be it deploying improvised explosive devices on civilian drones to target politicians and other VIPs or exploiting the surge in refugee boats coming from Libya to southern Europe to infiltrate extremists into Europe, the terrorist threat is continually evolving.

However, a direct attack by an established extremist group, such as al-Qaeda, Islamic State or one of their affiliates, remains unlikely. Western counter-terrorism strategies have become highly comprehensive, employing informants, undercover agents and the full spectrum of human, imagery, financial and communications surveillance. It has therefore become very difficult for such established groups to operate their command and control networks covertly.

An attack by a lone wolf or small independent group is substantially more probable. Of particular concern are cells that have reached an attack-ready stage – with plans, weapons and logistics in place – without being noticed by authorities, and are now merely waiting for the optimum opportunity. Such autonomous cells are extremely difficult to counter using conventional tactics, as they are not reliant on the command elements, financial support and communications necessary in the mastermind/sleeper cell-type network, and are therefore close to impossible to infiltrate.

[11] http://www.bbc.co.uk/news/uk-30166946

Instead, security agencies are relying heavily on comprehensive surveillance operations to identify potential attackers at an early stage, monitor their activities and contacts, and continually assess the level of threat they pose until they see the need to pre-emptively intervene. This has proven effective in the majority of cases, with large numbers of individuals becoming subject to such intervention, whether being mentored through the Channel programme of the UK government's Prevent strategy, subjected to a terrorism prevention and investigation measures notice or arrested and prosecuted. As of the end of 2014, there have been over 2,000 referrals, with over 500 categorised as requiring active intervention. However, events have shown that individuals and groups in other countries are managing to evade such efforts and execute their attacks. Counter-terrorist tactics are evolving fast to more effectively target this type of threat, but the risk remains very high. In these cases, good fortune and a rapid response that minimises casualties and damage are the best defence.

There have been some admirable approaches within the UK government's Prevent strategy, including, for example, providing funding and support to youth groups to help them attract at risk persons away from radical individuals and organisations. However, there has been growing criticism of its low success rate and concerns that it risks increasing suspicion and hostility between Muslims and the rest of British society. European countries have learnt many lessons from their own national programmes, and the United Kingdom would do well to consider some of their solutions. The British government should **move away from the broad approach of countering *all* extremism, which impacts thousands (with often negative consequences), and towards concentrating finite resources on tackling those at highest risk of adopting violent approaches.** The government should also **replace active intervention for lower-risk individuals and implement a broad campaign to undermine jihadist propaganda by promoting effective non-violent protest and campaign skills as alternatives to violence.** Extremism is often a simplistic solution for the isolated and disaffected, and this could be countered by offering lower-risk individuals real campaign and protest skills with which to express and work to resolve their social grievances.

Cyber espionage threat from potential adversaries increasing

With Russia rearming its military and reactivating its intelligence resources with considerable speed and NATO augmenting its Response Force with a spearhead Very High Readiness Joint Task Force, it is questionable whether the Cold War ever really ended or was just on hiatus. Whether that is the case or not, it is clear that the type of warfare has substantially evolved since the collapse of the Soviet Union. So too has the nature of intelligence operations. Before, the primary threat to national security was classic espionage, utilising agents, double agents (and the occasional triple agent), break-ins and blackmail among other tactics, to obtain the other side's secrets. Such operations were extremely high risk, with many of those involved being arrested or executed.

Today, while conventional espionage efforts certainly continue, Russian efforts are geared towards more remote and low-risk approaches. Cyber espionage and warfare is now at the fore, with operators breaking into command, control and communications networks with the intention of accessing data and disrupting operations. China too has been steadily moving away from its long-held domestic focus, and is now adopting a more global political-military presence to match its global economic influence, with a commensurate expansion in its cyber espionage and warfare efforts. Iran has been developing the means to project power throughout the highly unstable Middle Eastern/Southern Asia regions, going head-to-head with Western powers still active in these areas. So far, primary tactics have been based on disruption, with major denial of service attacks on time-critical functions of the financial and communications industries among others. There have also been successive Iranian attacks on the networks of US defence companies, including phishing campaigns to access the personal data of company employees and install malicious key-tracking and activity-monitoring software. And North Korea, though significantly less capable in conventional military technology than the others, is highly active on the cyber front. In its latest cyber strategy released in April 2015, the US Department of Defense identified cyber warfare from these four countries as the greatest cyber security threats to the United States.[12]

The threat facing the United Kingdom is no less severe. The country's critical national infrastructure, primarily communications and energy networks and rail and air traffic control systems, are at significant risk, especially from multiple low-level attacks causing short-term disruption. However, these are probably the electronic equivalent of ageing Russian bombers flying close to national airspace – low-tech probing attacks to identify response strategies and weak spots in preparation for a possible major attack using advanced resources in the future.

The growing threat from increasingly belligerent potential adversaries requires the British government to implement measures, including legislation and regular stress tests, to ensure the country's critical infrastructure continues to be robust. In May 2013, the Ministry of Defence stood up the Joint Forces Cyber Group, which since September 2013 has included the Joint Cyber Reserve. This provides a reservist cyber warfare capability. With the cyber threat to the United Kingdom rapidly escalating, the government should **consider adopting a full-time cyber capability that can utilise the data-rich environment from the thousands of malicious attacks against the government's secure internet and proactively disrupt the attackers' activities,** in addition to the more defensive actions of identifying and repelling attacks.

[12] http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Consequences of court rulings on GCHQ's mass collection programme

The struggle between the security services and liberty groups across the Five Eyes intelligence-sharing network has continued as governments try to balance security and privacy in light of the revelations by the former NSA contractor Edward Snowden. In the United Kingdom, the latest developments include a change to legislation that came into effect on 3 May 2015 that effectively pulled the rug out from under campaign groups who are in the midst of pursuing their case of illegal surveillance through British and European courts. A discretely introduced clause within the Serious Crime Act 2015 amended the existing Computer Misuse Act 1990, and immediately exempted UK intelligence and law enforcement agencies from prosecution. This clause was so discrete that none of the United Kingdom's data regulators – let alone campaigners or the public – were consulted, with only national security agencies and government branches being aware of it.

The legislative change was formally announced on 14 May 2015, just before campaign groups were due to return to the Investigatory Powers Tribunal (the court which oversees UK intelligence operations) to argue that mass collection programmes were illegal. They claim this sudden change has significantly changed the legal landscape under which the lawsuit was being brought, and therefore forces a fundamental review of their argument. Privacy International, one of the groups bringing the lawsuit, claimed that not only was their case affected but the legislative amendment also gave British security agencies freedom to conduct more intrusive surveillance and data collection, such as cyber attacks on specified targets, though the Home Office denied this. While legislation amendments may head off judicial challenges within the United Kingdom, these will still be tested against European human rights law, as the civil liberties organisations, including Privacy International, Liberty and Amnesty International, are still pursuing GCHQ and the British government through the European Court of Human Rights with regards to its mass surveillance operations.

The controversy over the multinational Five Eyes intelligence alliance of the United Kingdom, United States, Canada, Australia and New Zealand is also still ongoing. There have been challenges from political and advocacy groups in all five countries and the European Union accusing intelligence agencies of using each other to circumvent domestic legislative restrictions. Gaps in the legislation in one country can be exploited by intelligence agencies in another of the Five Eyes partners where legislation restricts them. The suspicion is that the United Kingdom, United States, Canada, Australia and New Zealand are attempting to maintain the full range of mass surveillance capabilities but dispersed across the network, with national legislations coordinated to allow for this. However, at the end of May 2015, the US Senate ended many of the sweeping surveillance powers allowed in the United States under the Patriot Act and voted to advance the USA Freedom Act, which bans the NSA from bulk collecting telephone records and introduces new transparency rules for other surveillance activities.

With such strong opposition on multiple fronts showing little signs of easing, it is time for the UK government to **hold a comprehensive debate over the costs and benefits of bulk surveillance and wholesale intelligence gathering and implement fundamental reforms to those operations.** There is little doubt that there are limited resources with which to monitor the many thousands of extremists operating across national borders and throughout global financial, communications and social media networks. The British government and many of its allies have concluded that the scale of this threat warrants a high-level of surveillance. If the authorities want to win public support, they need to explain why. This should **include an *honest* campaign to improve transparency in surveillance operations, explaining to the public as much as is possible (while maintaining operational security) the true intelligence gathering process.**

Section V

Cyber warfare

International cyber norms remain out of reach despite developing cyber arms race; cyber becoming important dimension of conflict in Syria and Iraq; link between cyber offensives and proliferation of capabilities more apparent.

International cyber norms remain out of reach despite developing cyber arms race

Cyber attacks, espionage and surveillance have garnered unprecedented media coverage over 2015. The fallout from the Guardians of Peace's compromise of the Sony Pictures network, a US State of the Union speech referencing cyber security and the English translation of a previous People's Liberation Army disclosure of their cyber force structure have kept cyber issues at the front of diplomacy and political debate. At the same time, cyber security research companies have published multiple reports on state and non-state advanced persistent threat (APT) campaigns, including Regin,[13] Operation SMN (Axiom),[14] Equation Group,[15] APT28,[16] Black Energy,[17] Sandworm,[18] APT30[19] and Operation Clever.[20]

Within this threat environment, governments are increasingly establishing national institutions to manage cyber security. From late 2014 to mid-2015, Indonesia, Thailand, Singapore and South Korea all made announcements on establishing new cyber security and defence institutions and South Africa and Denmark reviewed their cyber security needs. However, the Sony Pictures 'cyber vandalism' incident revealed the geopolitical and operational difficulties associated with navigating cyber conflict. The challenges the United States experienced in whether to characterise the incident as a cyber attack, in providing evidence of attribution and in crafting a proportionate response underscore how problematic cyber conflict might be without a framework of international norms.

[13] http://www.kaspersky.com/about/news/virus/2014/Regin-a-malicious-platform-capable-of-spying-on-GSM-networks

[14] http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf

[15] http://www.kaspersky.com/about/news/virus/2015/equation-group-the-crown-creator-of-cyber-espionage

[16] https://www.fireeye.com/resources/pdfs/apt28.pdf

[17] http://www.ibtimes.co.uk/blackenergy-cyber-attacks-against-ukrainian-government-linked-russia-1467401

[18] http://www.isightpartners.com/2014/10/cve-2014-4114/

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

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

However, the dominant cyber powers, the United States and China, have failed to pursue multilateral opportunities on cyber security, and have instead focussed predominantly on unilateral measures to improve domestic cyber security. Even the bilateral measures that the United States has taken with allies are not related to norm formulation. For example, existing cyber security cooperation and collaboration between the United States and the United Kingdom achieved through the Computer Emergency Readiness Team programme is being enhanced by the proposed formation of a trans-Atlantic joint cyber cell. The cyber cell is made up of cyber defence experts from Britain's GCHQ and MI5 and the United States' NSA and FBI. The emergence of multilateral cyber norm building can be seen within NATO, which has invested greater political capital into clarifying the scope of Article 5 (the collective defence clause) to ensure that the provision has its intended deterrent effect on 'cyber aggression and offensives'. But even this is set in the context of an adversary – in this case, Russia.

Unsurprisingly, key cyber powers are more focused on research and development, capability acquisition and maintaining a technological edge than on building international consensus on the rules of the game for cyber security and conflict. This disproportionate focus on developing cyber defence and offensive capabilities beyond that of adversaries is triggering a cyber arms race.

At the other end of the spectrum, the predominance of counter-terrorism in the intelligence, surveillance and reconnaissance (ISR) activities of the Five Eyes network is also driving a focus on achieving technical and operational superiority over non-state adversaries rather than norm building. This pursuit of technological superiority is consistent with pre-election comments from the British prime minister, David Cameron, on banning end-to-end encryption technology. Paradoxically, Cameron's proposal aims to achieve greater security from terrorism through creating wholesale digital insecurity. In this context, cyber norms are considered neither necessary nor even possible when the adversaries are non-state actors.

Despite this, there are opportunities for the British government and military institutions to play a greater role in norm building. The government has opportunities to more effectively balance cyber diplomacy, confidence-building measures and norm development through regional partnerships while maintaining programmes driving cyber advantage and technological superiority. This means the British government should **actively support NATO to become a coherent cyber community that facilitates intelligence sharing, defence training and incident response.** Alongside this, the government must **take greater steps to ensure that the ISR and counter-terrorism agendas of the Five Eyes network do not disproportionately shape cyber security policy and detract from norm-building opportunities.**

Cyber becoming important dimension of conflict in Syria and Iraq

Considerable attention has been focused on Islamic State's (IS) attempted informational dominance of social media platforms to support their ongoing recruitment efforts. However, less attention has been paid to the cyber dimension of the conflict in Syria and Iraq.

In January 2015, an alleged IS-affiliated hacker took control of the US Central Command (USCENTCOM) Twitter and YouTube accounts. The hacker, identified as Junaid Hussain, allegedly used @CENTCOM to disseminate IS propaganda, make threats against US soldiers, claim access to secure CENTCOM networks and release supposedly confidential information on US personnel (though this was already publicly available).

In the aftermath of the *Charlie Hebdo* attack, the Middle East Cyber Army is alleged to have initiated a malware campaign using the #JeSuisCharlie hash tag to distribute a Darkcomet remote access tool alongside launching distributed denial-of-service (DDoS) attacks on over 19,000 French websites. The Anonymous hacktivist group said it launched cyber retaliations for the Paris attacks, claiming to have shut down the French jihadist website ansar-alhaqq.net with a DDoS attack.

In February 2015, computer security company FireEye and the University of Toronto's Munk School of Global Affairs Citizen Lab both highlighted a social engineering and phishing campaign against Syrian opposition forces. The campaign used a multi-staged malware tool resulting in the installation of the DarkComet remote access tool (RAT) and helped the threat actor net 7.7 GB of data, including annotated maps, opposition positions and tactics, battle plans and political strategy discussions.

The campaign against Syrian opposition fighters demonstrates the way in which relatively simple social engineering and malware campaigns can obtain actionable military intelligence. The potential for adapted off-the shelf malware to be deployed for intelligence collection is significant. Without a significant investment and increase in capability, it is unlikely that Islamic State can deploy APTs to sabotage supervisory control and data acquisition (SCADA) systems and critical national infrastructure. This does not mean that cyber campaigns are any less militarily damaging, more that the mode of attack is focused on intelligence collection than infrastructure sabotage. This contradicts the assessment of the NSA director, Admiral Michael Rogers, that Islamic State's digital potential is one of the most significant emerging cyber risks. Islamic State would need to use substantial financial resources to outsource or procure cyber capabilities that could pose a considerable threat beyond the Middle East and North Africa region.

The UK government has a number of policy options at its disposal to help improve cyber security in the Middle East and limit the impact of the cyber campaigns of Islamic State and other non-state actors. The British government should **participate in the May 2015 US and Gulf Cooperation Council (GCC) agreement to build GCC cyber security defences against external state and non-state threat actors by sharing UK institutional experience from the Cyber-Security Information Sharing Partnership (CISP) with GCC members.** In addition, the government should **develop targeted bilateral initiatives through which to share cyber security expertise and threat intelligence with trusted regional partners, including Jordan and Israel.**

Link between cyber offensives and proliferation of capabilities more apparent

Iran started developing cyber capacities in 2005 when the Iranian Revolutionary Guard Corps (IRGC) proposed the development of an Iranian Cyber Army. In 2009, cyber capabilities with a domestic focus were deployed with the Iranian Cyber Police unit (FETA) tasked with addressing internal political dissent. However, the discovery in 2010 of the Stuxnet computer worm that attacked the centrifuges at Iran's Natanz nuclear facility became a watershed moment for Iran that catalysed significant investment in cyber defensive and offensive capabilities. This led to the establishment of the Iranian Cyber Defence Command and Supreme Council of Cyberspace. Furthermore, a 2013 NSA document published by the Intercept in February 2015 shows the United States is concerned that Iran was able to bolster its offensive cyber operations by reverse engineering and analysing Stuxnet.[21]

A December 2014 report on Operation Cleaver by security company Cylance suggested that 'bad actors' affiliated with the IRGC have undertaken over 50 attacks on critical infrastructure, such as energy generation and distribution, in 16 countries since at least 2012.[22] These attacks, if directed by the IRGC, reveal a high level of modernisation in Iranian cyber capabilities and a strategic shift that moves beyond retaliating against regional adversaries or those involved in Stuxnet. Global offensive campaigns against critical infrastructure and supervisory control and data acquisition (SCADA) systems would indicate significantly emboldened geopolitical aspirations. An April 2015 forum held by the US international affairs think tank the Atlantic Council considered the likelihood that sanctions relief as a result of the P5+1 negotiations on Iran's nuclear programme will provide Iran with opportunities to expand its cyber capabilities.

In using offensive cyber measures in a bid to deny Iran nuclear weapon capabilities the United States has not only elicited a costly counter-response but has also provided adversaries opportunities to learn how to launch sophisticated cyber offensives themselves. Publically available information suggests that the United States and Israel did not give sufficient consideration to the concept of cyber weapons as intellectual property that can be reverse engineered, studied and redeveloped. This raises the question of whether existing cyber powers can exercise offensive cyber capabilities without altering the dispersion of cyber power itself.

The risk of reverse engineering may provide a perverse incentive for more destructive offensives. Attacks may more readily seek permanent destruction or inoperability of large network infrastructure. This approach may be even more likely when the targets are relatively closed economies (for example, North Korea) or countries subject to sanctions regimes with relatively limited spill over effects into global markets (for example, Iran).

[21] https://firstlook.org/theintercept/2015/02/10/nsa-iran-developing-sophisticated-cyber-attacks-learning-attacks/

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

While the United Kingdom has not been subject to the same magnitude of publicly documented cyber campaigns as the United States, internal debate over cyber doctrine within the machinery of government is likely. The UK Ministry of Defence's trilateral memorandum of understanding with the United States and Australia on cyber defence means a level of shared cyber policy and doctrine discussion. The UK government may be in a privileged position to undertake a sober assessment of whether certain cyber attacks technologies may exponentially increase cyber weapon proliferation, thereby creating a feedback loop of cyber security threats.

As a major cyber power, the United Kingdom is strongly positioned to influence both national and international discussions on cyber weapon proliferation. As a first step, the British government should **encourage the inclusion of cyber weapon proliferation in the terms of reference for the next House of Commons Defence Committee review into defence and cyber security.** The government should also **use the forthcoming National Security Strategy update to send clear signals to international partners on options to manage the proliferation of cyber weapons and flag the prioritisation of norm development.**

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