This is a submission from the International Centre for Security Analysis (ICSA), King’s College London. ICSA is a multi-disciplinary research centre specialising in international security issues. The Inquiry on Cyber Security calls for evidence relating to, inter alia, the ‘development of offensive cyber capabilities and the norms governing their use’. In light of these terms of reference, this submission highlights the important role for Parliament to play in oversight of offensive cyber operations (OCOs), and makes a series of recommendations for improving the effectiveness of parliamentary oversight of OCOs.

Executive summary

- Covert action, including drone-strikes, the use of special operations forces and offensive cyber operations (OCOs), has been used more frequently as an instrument of government policy in recent years; OCOs give government the capability to conduct long-term, covert operations against foreign adversaries without parliamentary approval or oversight of on-going operations; the rising use of ‘remote control’ operations increases the need for democratic accountability; current arrangements for parliamentary oversight of covert action in general, and OCOs in particular, are less effective than they should be.
- There is an emerging convention that Parliament is consulted prior to major military operations, e.g. in Iraq (2003), Libya (2011), Syria (2013),
Iraq (2014), and Syria (2015). It is unlikely that covert action, including OCOs, will ever be subject to this new convention, because the point of ‘covert’ rather than ‘overt’ action is to maintain operational secrecy, which precludes open parliamentary debate. Given the significant impact that offensive cyber operations could have on an adversary, including the degradation or destruction of critical national infrastructure, potentially leading to severe disruption and even considerable loss of life, it is highly desirable that, in the absence of a requirement for parliamentary debate prior to such offensive cyber operations, other mechanisms should be identified to provide effective pre-operational, in-operation, and retrospective oversight of all but the most time-critical, emergency OCOs.

- Effective parliamentary oversight needs to be independent from Government. At present, responsibility to oversee OCOs conducted by the intelligence agencies and the Ministry of Defence is conferred on the Intelligence and Security Committee of Parliament (ISC). Regarding the independence of the ISC, we believe that there is a strong argument for the prime minister to relinquish her control over initial nomination of prospective members of the ISC. To preserve the role of the whole House (whether the Commons or the Lords) in approving candidates for ISC membership, we recommend that members of the ISC should be selected and approved on the following basis: each political party’s membership of the Committee should be proportionate to its membership of their respective House (Commons or Lords), and each party should select a slate of members to fill those places on the Committee. There should then be a vote of the whole House (Commons for MPs, Lords for peers) to accept or reject each party’s
proposed slate. It may be easier subsequently to ensure the proportionate representation of political parties on the Committee, especially in the case of members from the House of Lords, if the Committee’s membership were increased in size.

- The ISC’s responsibilities are enumerated in the Justice and Security Act (2013) and clarified in the ISC’s Memorandum of Understanding with the Government; there are, however, major shortcomings in the scope of the ISC’s remit to oversee OCOs, including prohibition from overseeing on-going operations and the broad discretion for the prime minister and relevant Secretary of State to refuse ISC access to ‘sensitive’ information ‘in the interests of national security.’ We recommend that the ISC’s Memorandum of Understanding with the Government should be revised to enhance ISC oversight of OCOs; we further recommend that the Memorandum should be published, more visibly than at present, on the ISC’s website.

- Existing legislation and the current Memorandum imply that rigorous parliamentary oversight might be an onerous burden, one that could potentially undermine operational effectiveness. In contrast, Government should welcome effective, well-informed parliamentary oversight as an important, independent and additional source of counsel: greater diversity of input can improve the quality of decision-making. Decisions made within homogenous groups are prone to shortcomings and flawed reasoning. For this reason, we recommend that the ISC’s Memorandum of Understanding with the Government be redrafted to confer the responsibility to oversee pre-operational and on-going operational phases of OCOs; Government should be required to arrange \textit{ad hoc}, closed sessions to advise the Committee on any
proposals for measures to escalate or intensify existing operations, to avoid ‘mission creep’ without the benefit of parliamentary oversight.

- To undertake this reformed mandate, the ISC would require better support from a larger, more expert Secretariat. The ISC’s current core staff of four officials is arguably too small even to undertake its present duties. This raises serious questions about the Committee’s capacity to exercise effective oversight over OCOs. Government is investing more money in intelligence and cyber; it is therefore reasonable to expect a commensurately increased investment in parliamentary oversight of these activities. With enhanced responsibilities to oversee OCOs, we recommend that the ISC should be supported by a core Secretariat twice its current size (i.e. no smaller than eight, permanent full-time staff); such a Secretariat would facilitate more effective oversight of OCOs, but, to put this proposal in context, it would still be less than a quarter of the size of the staff supporting the U.S. Senate Select Committee on Intelligence.

- On the principle that parliamentary oversight must be independent from Government, we recommend that core Secretariat staff recruited to serve the ISC must be parliamentary staff, rather than secondees from Government Departments. Secondment from within Government may appear an expeditious route to recruiting staff with relevant skills and experience, but the notion of ‘poachers temporarily turning gamekeepers’ is incompatible with the exercise of effective, independent scrutiny of Government.

- In recent years, government investment in the capability to conduct OCOs has outstripped investment in the capacity to provide effective, expert parliamentary oversight of OCOs. Lack of capacity in the ISC
Secretariat is likely to undermine the effectiveness of OCO oversight; we recommend that the ISC increase cyber-relevant expertise in its Secretariat, recruiting specialist staff for technical and other relevant expertise.

- The ISC’s revised Memorandum of Understanding should require access to all relevant materials pertaining to OCO doctrine, official (including legal) guidance on how to assess the necessity, proportionality and legality of proposed OCOs, existing policies regarding the conduct of pre-operational OCO risk assessments, in-operation stock-takes to measure effectiveness, and post-operational 'lessons learned' exercises. The ISC’s access to these documents (and the right to question relevant officials and ministers) would enable effective parliamentary oversight of the totality of the OCO process, enabling judgements to be made about the vitality of existing arrangements and the quality of decision-making.

- The revised Memorandum of Understanding may need to exempt OCOs in support of time-sensitive, ‘threat-to-life’ operations from this enhanced convention of pre-operational scrutiny, but we recommend that government should commit to retrospective reporting of these operations to the Committee, as well as quarterly reporting to the Committee of all decisions about the approval of standard, non-urgent offensive cyber operations, and full briefing on planning and implementation of existing, strategic offensive cyber operations.
Details

Parliamentary oversight of covert action: the case of offensive cyber operations

1. In the absence of a War Powers Act, there is an emerging convention that the Government should consult Parliament before conducting a major military operation. There was no Parliamentary vote on a Government-tabled motion on the deployment of British forces in Afghanistan, but subsequent military operations have been subject to prior parliamentary votes.¹ This was the case immediately before the 2003 invasion of Iraq; the 2011 Libya intervention; the putative 2013 intervention in Syria (aborted after losing the parliamentary vote); the 2014 vote authorising airstrikes against Islamic State in Iraq; and before the 2015 vote authorising similar airstrikes in Syria.

2. In contrast, the UK government maintains a long-standing policy of refusing to comment publicly on covert operations, which includes refusal to subject such operations to effective parliamentary oversight. Covert operations are those operations that are conducted secretly, obscuring the UK Government’s role in the operation. Covert operations could include, but are not be limited to, drone-strikes, the use of special operations forces, secret intervention in the domestic politics of foreign states (encompassing a broad range of possible activities, from the funding of opposition political parties and civil society groups, to the execution of information operations or other activities to influence the outcome of elections or other political processes), and, most pertinently for this inquiry, the use of offensive cyber operations (OCOs).

3. There are important similarities between offensive cyber operations and the covert use of drone strikes and special operations forces. All three are conducted with operational secrecy, entail the execution of an effect against an adversary, degrading or destroying a targeted capability. OCOs may also be used as part of integrated military action, involving other strands such as special operations forces or airstrikes. Furthermore, it is entirely possible to envisage offensive cyber operations that lead to loss of life, e.g. by interfering with navigational equipment or critical national infrastructure.²

4. There is a long-standing debate about the need for greater democratic accountability and legislative oversight of covert operations.³ This debate has intensified in recent years, with the proliferating use of airstrikes,⁴ including drone strikes, and the parallel increased use of special operational forces. There is a strong historical precedent for controversial covert action leading to increased legislative scrutiny: the secret bombing of Cambodia during the Vietnam War, leading US Congress to pass the War Powers Resolution to constrain executive authority to commit US forces without congressional approval.

² Professor Thomas Rid has rightly identified a signature feature of most historic offensive cyber operations as being their limited lethality. What is relevant here, however, is that offensive cyber operations can be used to effect significant deleterious consequences, up to and including lethality, and thereby merit parliamentary oversight on a similar basis to other forms of covert operations. See Thomas Rid, Cyber War Will Not Take Place, London: Hurst, 2013.


5. In today’s information environment, it would be exceedingly difficult to maintain operational secrecy surrounding a bombing campaign similar in scale to the Cambodia bombing. In contrast, given the digital, ‘under-the-radar’ nature of cyber-attacks, it likely that concerted, years-long offensive cyber operations are escaping public awareness and effective legislative scrutiny. By their nature, OCOs can be conducted in utmost secrecy for long periods of time. Even after their discovery, the attribution of these attacks to specific state or non-state actors can be extremely difficult. Covert operations clearly require operational secrecy, but it is reasonable to explore the potential for improving existing arrangements for parliamentary oversight of these significant and consequential exercises of executive power.

The US debate about legislative oversight of offensive cyber

6. To provide international context and comparison, it is worthwhile to note that there is a lively debate about the extent to which War Powers legislation in the US covers offensive cyber operations, or indeed presidential authorisation of US military action more broadly. For example, in 2011 President Obama authorised US intervention in Libya without Congressional approval. It has been reported that, prior to this intervention, the Obama administration debated using an offensive cyber operation against Libya as part of the US contribution to the coalition operation, specifically ‘to break through the firewalls of the Libyan government’s computer networks to sever military communications links and prevent the early-warning radars from

---

5 That is, when they are not leaked to New York Times reporters for books published during US presidential re-election years. See, for example, David Sanger’s revelations about ‘Operation OLYMIC GAMES’ in Confront and Conceal: Obama’s Secret Wars and Surprising Use of American Power, New York: Crown, 2012.
gathering information and relaying it to missile batteries aiming at NATO warplanes." Reportedly, the Obama administration was ‘unable to resolve whether the president had the power to proceed with such an attack without informing Congress.’

7. The legislation outlining congressional oversight of US covert action, the Intelligence Authorisation Act (1991), requires the president to notify Congress (through its two relevant committees, the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence) prior to, or exceptionally shortly after the use of covert action. The extent to which this legislation applies to presidential authorisation of OCOs is, however, open to interpretation.

8. This US political and constitutional debate highlights the fact that the problem of legislative oversight of offensive cyber operations is not uniquely British. The rising prevalence of state and non-state OCOs point to the need to think seriously about the structural factors shaping their use, not least striking the right balance between executive latitude in times of crisis (e.g. OCOs to disrupt or corrupt the communications of would-be participants in an imminent terrorist attack) and the broader role of legislative oversight. This inquiry is therefore a timely opportunity to sketch some possible lines of future reforms to improve the democratic accountability and legislative oversight of UK OCOs.

---


Offensive cyber operations

9. It is worthwhile to distinguish between passive and active cyber operations. The passive approach to cyber operations aims to compromise network security in order to gather information. This kind of cyber operation is essentially a form of intelligence collection, rather than an offensive action to change the operations of, degrade or destroy a targeted computer or computer network. However, the access necessary to collect information from a network could also be used as a starting point for an offensive cyber operation (access being a prerequisite for action), so there is in principle a relationship between the two forms of cyber operation. This makes it logical for the oversight of both passive and active operations to be the responsibility of the same parliamentary committee. There is also a direct connection between passive and offensive cyber operations in the case of information warfare, when information covertly extracted from a target network is disseminated publicly to damage that target (e.g. the leaking of material during the 2016 US presidential election campaign) – this is an offensive use of information generated by a passive – i.e., aimed at retrieving information – operation.

10. In contrast to passive, intelligence collection operations conducted with active cyber techniques, offensive cyber operations (OCOs) can be defined as: ‘activities that project force to create, deny, disrupt, degrade and destroy effects in and through cyberspace. These operations may transcend the virtual domain into effects in the physical and cognitive domains.’

---

of operations during armed conflict, as part of the integrated use of military capabilities including but not restricted to offensive cyber.

11. Government Communications Headquarters (GCHQ) conducts offensive cyber operations. According to the 2015-16 annual report of the Intelligence and Security Committee, 18 per cent of GCHQ’s allocation of departmental effort comprises operational work including OCOs, but also covers cyber defence, counter-terrorism, protective security, economic security, weapons and serious crime. It is also likely that some of the 26 per cent of GCHQ’s work that is dedicated to capability exploitation makes some form of indirect, structural contribution to the development of GCHQ’s OCOs.9

12. The conduct of OCOs by the military is also envisaged as part of the 2015 Strategic Defence and Security Review/National Security Strategy, which committed to ‘provide the Armed Forces with advanced offensive cyber capabilities, drawing on the National Offensive Cyber Programme which is run in partnership between the MOD and GCHQ.’10

International law and offensive cyber

13. The September 2015 bilateral US-China agreement to mutually refrain from commercial cyber espionage points to emerging efforts by state

---

9 Annual Report 2015-2016 (HC444), Intelligence and Security Committee of Parliament, 2 July 2016, p. 15. Retrieved 1 February 2017: https://b1cbeb3-a-5e6631fd-sites.googlegroups.com/a/independent.gov.uk/isc/files/2015-2016_ISC_AR.pdf?attachauth=ANoY7cp33kt520d80UfYqXvwqncGtXAcKa104r5vE8CiyRr8mYVZJS9LmuWsX7HeTLRIHXjBupoqWSSdGh_MZYua-aFzz8lIf5uhqWaOzgZjFeD55OZbcQkG4JOY73aSc2SSegUMCXGmh92en_IVd9ejuTHuG44YoH68fMb5u2PNKIN6PaiudEPayzEoMV666mGAV_I5VDInG2P9SjaJnrP7q8IMUQ6eHWTV0_qMRyq1axgEE%3D&attredirects=0

actors to regulate state-conducted or state-sponsored cyber-attacks.\textsuperscript{11} There is, as yet, no formal framework of international treaties that specifically covers the use of offensive cyber operations, but existing international law is nonetheless applicable to the conduct of offensive cyber operations\textsuperscript{12}, as are the Laws of Armed Conflict, should OCOs be conducted as part of an armed conflict involving the UK.\textsuperscript{13} If an offensive cyber operation has substantially similar effects as a non-cyber, ‘kinetic’ attack, then it may meet the definition of an ‘armed attack’ or other ‘use of force’ under customary international law. Such acts are prohibited by the UN Charter (Article 2(4)). Even if an OCO failed to meet the definition of a ‘use of force’ it may yet contravene the customary principle of ‘non-intervention’ if it has the practical effect of interfering with affairs that should be the right of a state to decide freely without foreign intervention, \textit{e.g.} the conduct of a parliamentary or presidential election. International law recognises the legitimacy of necessary and proportionate usage of force in acts of self-defence and offensive cyber operations could fall within this remit.\textsuperscript{14}

14. Given the complexity of attributing the source of OCOs, rigorous enforcement of international agreements on their use would be seriously difficult. This submission addresses the logically prior issue of


the domestic governance of OCOs. There is an opportunity for the UK to set standards of best practice in the democratic accountability and legislative oversight of OCOs, offering an example for other states to emulate. In contrast, the example currently offered by the UK’s oversight practices is one of essentially unfettered executive autonomy.

**Domestic oversight: the Intelligence and Security Committee of Parliament**

15.Currently, the Intelligence and Security Committee of Parliament (ISC) has responsibility to oversee all UK offensive cyber operations. This responsibility is not referred to explicitly in the Justice and Security Act (2013), which is the most recent piece of legislation updating the terms of reference of the ISC.\textsuperscript{14} The ISC comprises nine members (seven MPs and two peers), who are respectively chosen by the Prime Minister in consultation with the Leader of the Opposition, and their appointments are subject to confirmation by a vote in their relevant House of Parliament.

16.The ISC’s primary responsibility is to examine and oversee the ‘expenditure, administration, policy and operations’ of the security and intelligence agencies, \textit{i.e.} the Security Service, Secret Intelligence Service, and Government Communications Headquarters. In addition, the ISC ‘examines the intelligence-related work of the Cabinet Office including: the Joint Intelligence Committee (JIC); the Assessments Staff; and the National Security Secretariat. The Committee also provides oversight of Defence Intelligence in the Ministry of Defence and the Office for Security and Counter-Terrorism in the Home Office.’\textsuperscript{15}

\textsuperscript{14} For a summary of the ISC’s membership and activities, see Joanna Dawson, ‘The Intelligence and Security Committee,’ \textit{House of Commons Library Briefing Paper (02178)}, February 2016. Retrieved 7 February 2017:

17. Regarding the independence of the ISC from Government, we believe that there is a strong argument for a further stage in the evolution of the Committee, namely that the prime minister should relinquish her control over initial selection of prospective members of the ISC. To preserve the role of the whole House (whether the Commons or the Lords) in approving candidates for ISC membership, we recommend that members of the ISC should be selected and approved on the following basis: each political party’s membership of the Committee should be proportionate to its membership of the relevant House (Commons or Lords), and each party should select a slate of members to fill those places on the Committee. There should then be a vote of the whole House (Commons for MPs, Lords for peers) to accept or reject each party’s proposed slate. Following this reform, it may be easier to ensure the proportionate representation of political parties on the Committee – especially in the case of members from the House of Lords, who currently only comprise two members of the ISC – if the Committee’s membership were increased in size.

18. Implicit in the ISC’s oversight responsibilities is the assumption that, if the ISC can oversee the operations of the intelligence agencies, then offensive cyber operations conducted by the agencies would fall within its remit. The ISC’s role in overseeing OCOs is clarified more explicitly in a copy of the Memorandum of Understanding between the ISC and the Government, which was most recently published as an annex to the ISC’s annual report in 2014.\textsuperscript{16} We assume that the 2014 Memorandum

constitutes the most up-to-date terms of reference for the ISC. **We recommend, therefore, that as part of a general shift towards greater transparency and clarity about its activities, the ISC should find a more accessible place on its website to publish its Memorandum of Understanding, as it forms an important part of the corpus of documents identifying and clarifying its remit.**

19. As the ISC’s Memorandum of Understanding with the Government makes clear, the ISC may investigate the Ministry of Defence’s ‘offensive cyber’ activities, in addition to the strategic intelligence activities of Defence Intelligence. This is consistent with the fact that the ISC ‘is the only committee of Parliament that has regular access to protectively marked information that is sensitive for national security reasons: this means that only the ISC is in a position to scrutinise effectively the work of the Agencies and of those parts of Departments whose work is directly concerned with intelligence and security matters.’

20. There are, however, major shortcomings to the ISC’s remit in overseeing operations, including offensive cyber operations. The ISC’s Memorandum of Understanding identifies ‘overarching principles’ to govern its oversight of operational activities: ‘a. this work must not jeopardise the success of an operation or compromise the security and safety of those involved; and b. the ISC’s examination of an operational matter must not unduly impede the operational effectiveness of an Agency or Department.’ Moreover, the ISC’s ‘power to oversee operational activity is retrospective and on matters of significant national interest.’ The ISC cannot oversee on-going operational activity, and the prime minister ‘will nominate the National Security Adviser and his deputy for intelligence matters to consider, on his behalf, whether
the conditions for such oversight are met. The final decision will rest with the Prime Minister, in conjunction with the ISC.’

21. The ISC cannot, therefore, review an operational issue unless both it and the prime minister are ‘satisfied’ that the issue ‘is not part of any ongoing intelligence or security operation, and is of significant national interest.’ In practice, the prime minister exercises a veto over the operational oversight activities of the ISC, and no ISC investigation can be conducted into a live operation. Furthermore, according to Schedule 1 of the Justice and Security Act (2013), the ISC’s requests for information can be refused by a Secretary of State on the grounds of the sensitivity of the information or in the wider ‘interests of national security.’

22. This shortcoming in the ISC’s remit to oversee OCOs means that the Government can, without any parliamentary approval or operational oversight, degrade or destroy the critical national infrastructure of a foreign country, leading to severe disruption and potentially considerable loss of life. Given the covert nature of OCOs, it would not be immediately clear or discernible that this operation was conducted by the UK government. At the less lethal, but no less covert end of the spectrum, the Government can target foreign adversaries with hybrid, information warfare operations similar to that seen during the (presumably Russian) information operation conducted during the 2016 US presidential election. Again, under existing arrangements, the Government could execute these operations without any parliamentary oversight for the duration of the operation.

23. As its Memorandum makes clear, part of the justification for restricting the ISC’s remit is to ensure that operational effectiveness is not impaired
by excessive or intrusive parliamentary oversight. According to a 2012 guidance note regarding the then Justice and Security Bill, the proposed Act would restrict the scope of the ISC’s oversight so that it did not ‘lessen the effectiveness of the intelligence services and other intelligence and security bodies or place any undue resource burden upon them.’ It is presumably on this basis that the ISC has been prohibited from overseeing on-going offensive cyber operations.

Recommendations for reforming parliamentary oversight of offensive cyber

24. It is unreasonable to expect that the Government should publicise operational details of covert action, given its long-standing principle of refusing to comment for operational reasons. There is every reason, however, to explore opportunities to improve existing mechanisms of parliamentary oversight to fill this salient gap in the democratic accountability of covert action. Parliamentary oversight should not be seen as an onerous burden, potentially prejudicial to operational effectiveness. It should be recognised that effective parliamentary scrutiny would not only enhance the legitimacy of offensive cyber (and other covert) operations, but also provide a useful source of challenging, independent advice that could improve the quality of the Government’s decision-making about its use of these operations, reducing the likelihood of unwise, counter-productive uses of UK power. Of course, some models of oversight are more cumbersome than others, but the point of departure in devising an appropriate model of oversight should

---

be mutual recognition that effective oversight can add value to the operational process.

25. **We recommend that Government should welcome the legislative branch’s contribution of independent, challenging scrutiny and advice at every stage of the offensive cyber operational cycle: pre-operational planning and its underlying doctrine and guidance framework, incorporating an appropriate parliamentary component in the process of reviewing the progress of on-going operations, and mandating rigorous retrospective review of completed operations.**

26. **As currently configured, the ISC lacks the capacity to undertake this proposed, enhanced set of responsibilities for overseeing offensive cyber operations. It would require new powers of operational oversight, which would be most expeditiously granted by revising its Memorandum of Understanding with the Government. It would further require a significant uplift in the size of the ISC Secretariat, and a concomitant effort to ensure that such recruitment focuses on bringing in technical and other relevant expertise to the Secretariat.**

27. There are major structural constraints on the ISC’s ability to undertake effective parliamentary oversight. First, it is tasked to oversee the operations of a relatively large intelligence community, comprising over 10,000 staff and a £2.6bn annual budget in 2014-15. According to the ISC’s 2015-16 annual report, it performs this task with the support of only four core Secretariat staff.\(^{18}\) Even when this core staff has been augmented, *e.g.* with the six temporary staff who supported the Detainee Inquiry, and the services of a part-time investigator, this

---

arguably represents a derisory investment in upholding the important constitutional duty of parliamentary oversight in the sphere of intelligence and security. A comparison with the ISC’s US congressional counterparts is instructive: the Senate Select Committee on Intelligence is supported by 43 staff\(^\text{19}\) and the House Permanent Select Committee on Intelligence is supported by 30 staff\(^\text{20}\). Whilst the US intelligence community is vastly bigger than its UK sister, it is nonetheless obvious that a proportionately larger core staff for the ISC would enable more effective execution of its oversight responsibilities. Implementation of such an uplift in Secretariat capacity would entail increased investment, but this would be a proportionate and worthwhile expenditure that would represent value for money in the enhanced rigour and granularity of oversight that it would enable the ISC to conduct. This is especially true given the very broad terms of reference that determine the scope of the ISC’s scrutiny. **We recommend that the ISC should substantial increase the size of its supporting Secretariat, in the first instance to a number no smaller than eight officials.** The ISC’s core staff should not be employees shared with other relevant Parliamentary Committees, should work full-time on ISC business, and should not be seconded from Government agencies or departments (on a temporary ‘poacher turned gamekeeper’ basis), in line with the guiding principle that the Committee should remain clearly independent of Government. The ISC should also consider following the example of the US Senate and

\(^{19}\) *Senate Select Committee on Intelligence Staff Directory*. Retrieved 14 February 2017: http://congressional-staff.insidegov.com/d/a/Senate/Senate-Select-Committee-on-Intelligence

House staff, as well as the example of other current UK parliamentary committees, of improving the accessibility and transparency of its operations by publicly naming its core staff.

28. A second, related problem is the question of expertise: a core staff of four is most unlikely to comprise all the expertise necessary to provide insightful assistance to committee members on all relevant issues across the ISC’s broad remit. This problem is, of course, broader than cyber, but cyber represents a clear case in which knowledge and understanding of the underlying issues, including both technical and legal aspects, is an prerequisite for effective oversight. We recommend that a substantial proportion of any uplift in ISC Secretariat staff should be recruited for cyber-relevant skills and expertise.

29. Third, it appears in the case of the Intelligence and Security Committee’s investigation into the lethal airstrikes in Syria that this was a reactive inquiry, called after the strikes had taken place. Parliamentary scrutiny of covert action would be more effective if the relevant Committee was kept abreast of operational plans and policy prior to the execution of such operations, which may perforce require a timetable that precludes prior notification of the Committee that an operation is imminent. In the case of OCOs, in which a significant number of operations are likely to be more strategic and long-running than the aforementioned lethal strikes, it would be both possible and appropriate for a parliamentary committee to be informed more thoroughly and at an earlier phase of the operational cycle. We recommend that a core requirement for effective scrutiny is that the Committee must be informed of developing doctrine, policy and operational planning regarding covert action, including OCOs.
30. Our recommendations for addressing the limitations in existing parliamentary oversight of covert action, including OCOs, point to a more robust and better-resourced mechanism to ensure democratic accountability and legislative oversight. Our recommendations draw on a comparison with legislative oversight practices in other states. For example, the model of US Congressional oversight of covert action provides for a structured approach in which the process of authorising covert action is clearly described in legislation, and involves the notification of relevant legislative authorities, including receipt of the executive finding authorising such activities.\textsuperscript{21}

31. We believe that a new, properly-constituted, appropriately-funded and sufficiently-staffed parliamentary committee would provide better, more robust oversight of offensive cyber operations. It would do so on the basis of routine access to the following official information:

- Mandatory receipt of all materials on the doctrine underpinning UK OCOs, including documents pertaining to proportionality and legality of responses, including relevant legal advice within agencies and departments, and oversight of the official policies regarding pre-operational OCO risk assessments, in-operational stock-taking to measure results, and post-operational 'lessons learned' exercises.

- Timely (within 48 hours) receipt of comprehensive documents pertaining to ministerial approval of offensive cyber operations. Ideally, this approval would precede the commencement of OCOs, although \textit{in extremis} notification could be retrospective.

Similarly, timely briefing of the Committee on the status of on-going OCOs, especially in light of escalation or other significant revision of lines of operation. This process would sensibly include full briefing of the Committee on post-operational ‘wash-up’ exercises and lessons learned reviews.
Conclusion

32. Our recommendations for addressing the limitations in existing parliamentary oversight of offensive cyber operations, and covert operations more broadly, point to the possibility of a more robust and better-resourced mechanism to ensure democratic accountability and legislative oversight. Our recommendations draw on a comparison with legislative oversight practices in the US. For example, the model of US Congressional oversight of covert action provides for a structured approach in which the process of authorising covert action is clearly described in legislation, and involves the notification of relevant legislative authorities, including receipt of the executive finding authorising such activities.22

33. The reforms we propose are incremental, focusing on improving the capacity of the ISC to execute its responsibilities to oversee offensive cyber operations, and enhancing its remit to undertake more granular, in-depth oversight of these operations. Given the clear reluctance of Government to enable effective parliamentary oversight of on-going operations, the prospects for successful implementation of even these incremental recommendations would depend on a concerted campaign to persuade Government of the substantial added value of enhanced parliamentary oversight, the flawed and unconvincing nature of arguments that improved oversight would undermine (rather than in fact improve) operational effectiveness, and the demonstrable

democratic imperative for improved accountability arrangements concerning offensive cyber operations.

34. Offensive cyber operations have become much more salient in recent years and will likely continue to be pressed on the public mind by high-profile reports of new cyber-attacks in coming years. This inquiry is a timely opportunity for the UK to take the lead in devising effective forms of parliamentary oversight for its offensive cyber operations. The UK can take a series of incremental steps to improve existing oversight and, in the process, create an effective model to be emulated by other states. This would undoubtedly require a shift in the Government’s mind-set about the value of substantial parliamentary oversight of offensive cyber operations. We believe that the rising use of such operations, and wider covert operations, makes such a change of view imperative.