Offensive Cyber Working Group

Scoping Workshop Report

December 2020

Version 1.0

Foreword

The Offensive Cyber Working Group (OCWG) is a new endeavour to bring together individuals from across academia, government, and industry to discuss contemporary developments in 'offensive cyber' within the UK. This has been coordinated by an academic steering committee to encourage debate, research, and collaboration across diverse disciplines, perspectives, and practice.

Shortly before the scoping workshop on the 18th of November 2020, the UK Prime Minister, Boris Johnson, formally announced the new National Cyber Force, where the "UK has been a world-leader on offensive cyber operations, with GCHQ pioneering the use and development of these cyber techniques".[1] This dynamic landscape demonstrates the potency of the current moment for academia to be involved in conversations core to UK strategy, technologies, and ethical engagements in order to conduct timely and relevant research.

This short report offers the community's first collective discussions on research themes in offensive cyber. As part of a commitment to academic openness, we offer this report to initiate and continue research and thinking in the UK and beyond. We would like to thank Louise Marie Hurel, Lilly Pijnenburg Muller, Nick Robinson, and Clare Stevens who assisted in recording the discussions in the workshop that inform the edited contents of this report.

The OCWG Steering Committee

(Dr Andrew Dwyer, Amy Ertan, Dr Tim Stevens, and Dr Leonie Tanczer)

[1] https://www.gchq.gov.uk/news/national-cyber-force (19 November 2020).

Introduction

The inaugural scoping workshop of the Offensive Cyber Working Group brought together senior and early career academics in conversation with those in government and industry to discuss 'offensive cyber'. This report does not provide a definition of offensive cyber or its operations as this was not agreed upon by participants. The workshop was invite-only and held online due to COVID-19 restrictions. Twenty-two participants attended across a wide range of disciplinary and professional backgrounds from eleven universities, various areas of government, and from elsewhere. The positive response from stakeholders involved with, or researching, offensive cyber demonstrated both the interest and timeliness of the scoping workshop at an important juncture in the UK defence and security landscape.

In this report, we outline the discussions of the workshop and organise these into emergent themes. This report does not capture the viewpoints of the organisations the attendees are affiliated with nor of the steering committee. Instead, it seeks to summarise the contrasting and diverse research interests that support the need for further engagement in this area and the building of a trusted stakeholder community.

The workshop was held on the 18th of November 2020 and comprised of two sessions:

1) The Challenges in, and for, Offensive Cyber, and;
2) Identifying Research Challenges in Offensive Cyber.

Each session attended to pre-identified workstreams by the steering committee – Ethics & Law; Strategy & Policy; and Techniques & Implementation. Session 1 addressed *what* offensive cyber is and identified cross-thematic challenges. Session 2 split participants according to interest and specialism in each workstream to articulate specialised research responses to challenges within their area.

Although this scoping workshop was orientated towards offensive cyber *within the UK*, with various areas of UK governmental expertise represented, this was not its exclusive focus. International comparison was common in order to attend to the specificity of the UK context and to build a nascent academic community.

High-Level Summary

Below is a summary of the challenges facing offensive cyber across five themes:

1. **Blurred Lines**: Issues of working across diverse disciplines and expertise; developing effective typologies or taxonomies; as well as understanding the terrains of engagement.
2. **Responsibility and Risk**: The benefits of regulation; the applicability of international law; as well as the balance of harms and associated proportionality of actions.

3. **Societal Debate**: Concerns over the militarisation of the debate; transparent government communication; and an aspiration to foster an informed public.
4. **Strategy and International Cooperation**: The development of norms; the strategic aims of the UK and other states; the analysis of thresholds and trigger points; as well as international alliances and their impact on offensive cyber.
5. **Operational Details**: How to deal with the resources and the maintainance of technology and people who conduct offensive cyber operations; their organisational structures; and how to interact with (non-governmental) third parties.

These challenges were discussed in Session 2 to offer a set of research priorities, matched to the high-level challenges above, in Table 1 on page 11.

The Challenges in, and for, Offensive Cyber

Offensive cyber is not yet settled with various interpretations discussed throughout the workshop, and the report does not attempt to outline a definitive position[2]. The challenges emphasised below offer some of the difficulties facing academia and research on offensive cyber more broadly. We provide a synthesis of the contributions under thematic headings that overlap across the three workstreams.

1) Blurred Lines

There was a persistent and common theme that spoke to the complexity of assessing what is, and is not, considered to be part of contemporary offensive cyber. This debate focused on issues of definition, working across domains and specialisms, as well as the boundaries between offensive and defensive cyber operations.

Interdisciplinarity was perceived as a means to establish common ground and bring together differing perspectives. However, this aspiration is frequently hindered by the prevalence of different sectoral siloes and difficulties in establishing effective modes of communication. This dynamic is complicated by a lack of a comprehensive **typology** or **taxonomy** to inform conceptual and operational distinctions between offensive and defensive cyber operations. Besides, the entanglement between assessments of campaigns or singular operations[3] and the line between offensive cyber and information operations remains contested.

Likewise, there is an underdevelopment in thinking about the **terrain of engagement**. This means that spaces of engagement, their interconnectivity, and their potential unintended consequences are not widely agreed upon nor understood.

2) Responsibility and Risk

Ethical behaviour and the assessment of responsibility in the practice of certain actions may introduce various technical and societal risks. The potential applicability and desirability of **regulation** needs to be further explored by the UK and other states as well as its compatibility with **international law**. An analysis of how these mechanisms may both constrain and enable certain forms of action is a current challenge to collective knowledge.

Interconnected with regulation and international law are various forms of potential **harm**. Due to the limited insights into current operations and their unintended consequences, assessments of harm are a challenge to map. This limits assessment of **proportionality** that is constricted by classification and whether offensive cyber operations can be understood as successful or not.

[2] For a perspective on what offensive cyber may be, see the section 'The Definitional Challenge' in Prince, C., 2020. On the Offensive: The UK's New Cyber Force. RUSI.

[3] Some participants referred to Harknett, R.J. and Smeets, M., 2020. Cyber campaigns and strategic outcomes. Journal of Strategic Studies, pp.1–34.

3) Societal Debate

As offensive cyber interacts with broader 'publics', the debate on how offensive cyber is presented, discussed, and acted upon is central to democratic governance.

Some participants were concerned with the **militarisation of debate** that has emerged as offensive cyber is primarily developed with or through the military and intelligence agencies. This was thought to limit potential alternative perspectives and readings on offensive cyber.

The militarisation debate was tied to the challenges inherent to **government communications** both in developing a strategy but also communicating and disseminating this understanding. While operational material is likely to be marked as classified, participants felt there may be opportunities to discuss strategic aspects of offensive cyber in non-classified environments.

Together, these limitations hinder public engagement and the creation of **an informed public**. As offensive cyber potentially develops and extends in reach, this will require greater openness and debate across society – from the media to Parliamentary scrutiny.

4) Strategy and International Cooperation

How the UK thinks through its strategy and its interaction on the international stage, especially in relation to more defined strategies currently in existence, such as by the USA,[4] is key.

In particular, and not uncommon to the UK, the formation of agreed **norms** around notions of non-war (thresholds below the level of armed conflict and 'grey zones'), the cyber security dilemma,[5] as well as notions of sovereignty and territorial integrity are still open.

These could be supported by further developed **strategic aims** in the UK, as there is little indication about the broader interaction of offensive cyber in the landscape and its value, especially with regards to practical **thresholds and trigger points**.

Yet the formation of norms and strategic aims does not happen in a vacuum but must be understood through the challenge of building and sustaining **international alliances**. It is unclear how the UK intends to interact with, and compete, in offensive cyber alongside allies such as the Five Eyes[6] and through NATO.

5) Operational Details

Challenges also exist with the use of certain emerging technologies and potential unintended consequences from them, such as with machine learning algorithms.

[4] Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command.

[5] Buchanan, B., 2016. The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations. Oxford: Oxford University Press.

[6] For a perspective on offensive cyber within the Five Eyes, see Gold, J., 2020. The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative.' CCDCOE, Tallinn, Estonia.

Little is known of the detail of offensive cyber operations, and this is likely to remain at least partially so. However, the UK will need to procure and develop materials as well as specialists for offensive cyber and this will require extensive **resources and maintenance** depending on the form of strategy the UK wishes to undertake.

These different tools and technologies will interact with trigger points and **organisational structures** will be essential to respond to different threats and opportunities.

This is further complicated by the involvement of **third parties** that run much of today's internet infrastructure; and the role they may have in offensive operations and the relationships that may need to be built.

Identifying Research Challenges in Offensive Cyber

In Session 2, participants identified the varied research areas and questions to address challenges they had identified in Session 1. Below is an edited summary of the discussions and research priorities each workstream identified.

Ethics & Law

For some, 'cyber' and international law has been "done to death", yet there are some aspects that offensive cyber raises that are distinct. This includes the role of and **responsibilities of non-state actors**, especially in relation to **Human Rights Law**. Further questions were raised as to how this may apply to third parties such as social media companies. Human Rights Law applies not only to people but also to non-human and hybrid systems such as infrastructure – and thus this is one way in which the international community could agree to not target civilian infrastructure. However, **to ask if 'offensive cyber' is legal was judged to be the wrong question**. The latter requires further scoping and there is no generic overview of its permissibility. This issue was twinned with a concern that many sought 'international law' resolutions to what is more closely related to **norm-creation**; and we must be careful to distinguish between these forms.

If one turns to Article 51 of the UN Charter,[7] the notion of a retaliatory cyber-attack is a dark area that is arguably not permitted under international law[8]. There is also a distinction in **proportionality** between differing forms of attack that may at first appear similar. For example, an attack against the critical national infrastructure for domestic energy in Russia would not be equivalent to one in the UK; due to the former being more likely to result in greater mortality.

Questions were raised over the **ethical justification for a state *not* to develop offensive cyber capabilities or operations**. This may be more desirable than a kinetic attack that may not be reversible (such as a conventional missile strike). This may make offensive operations more ethical than other forms of (sub-)warfare activity – however this raised the question: when does an offensive operation lead to kinetic actions that are not reversible?

The UK was the first state to admit it would use offensive cyber operations if threatened by a foreign state or non-state actors.[9] The UK also emphasised that it does this in adherence to international law. Nonetheless, the Law on Armed Conflict does not explicitly permit offensive cyber operations. In particular, in 2018, the UK's then Attorney General said that the UK would not always go by the Law on Armed Conflict in this area[10]. This is part of a 'principled position' which does not recognise

[7] https://legal.un.org/repertory/art51.shtml

[8] Although the UK argues that it is permissible in some instances. See Cross, M., 2018. Cyber-warfare: retaliation would be lawful, says UK. Law Gazette.

[9] Blitz, J., 2013. UK becomes first state to admit to offensive cyber attack capability. Financial Times.

[10] See the speech from former UK Attorney General, Jeremy Wright, on "Cyber and International Law in the 21st Century" in 2018.

offensive cyber as solely based within the military but also within intelligence and a wider ecology of capabilities.

A Research Agenda for Ethics & Law

- The applicability of current law to offensive cyber, including Human Rights Law and the Law on Armed Conflict.
- Everyday harms that could emerge from offensive cyber.
- How military ethics could be applied to intelligence and non-state actors.
- Reinvestigate collateral damage and proportionality of offensive cyber beyond isolated cyber-weapons.
- Promotion of common legal understanding internationally, such as between NATO members.

Strategy & Policy

There is a heightened requirement for **international comparison**: one that overly focuses on differences between US and individual European states' policy was regarded as too narrow in scope. This could be further supported by **case studies** that are not focused on the conventional 'key' players in this field and include those from the Global South.

This is underpinned by current mismatches on **terminology** and **taxonomy.** Addressing this issue will require the bringing together of international academics. Linguistic comparisons between English, Russian and Chinese[11] policy could help establish greater consensus on the diffuse use of terms associated with the field. This may also be extended to analyse the movement in the use of terms like 'weapons', 'capabilities', and 'operations', at least within an Anglophone context.

However, to study these phenomena and to develop appropriate **methods**, data is required in some form. Policymakers must be willing to share, but participants appreciated that this requires mutual respect and trust. Likewise, working with fields adjacent to those in strategy and policy, such as sociology, criminology, psychology, computer science, and geography, may offer new methods and concepts for researching offensive cyber.

Finally, there are the **long-term strategic implications** and the consequences of **emerging technology** for offensive cyber, such as the potential changes to cyber operations enabled by developments such as 'automated' cyber-attacks.[12]

A Research Agenda for Strategy & Policy

- The organisation of offensive cyber capabilities across different levels of conflict (including, but not limited to, thresholds below the level of armed

[11] See for example, K. Giles and W. Hagestad, 2013. Divided by a common language: Cyber definitions in Chinese, Russian and English. In: 2013 5th International Conference on Cyber Conflict (CYCON 2013). 2013 5th International Conference on Cyber Conflict (CYCON 2013). pp.1–17.

[12] See Buchanan, B., Bansemer, J., Cary, D., Lucas, J. and Musser, M., 2020. Automating Cyber Attacks: Hype and Reality. Center for Security and Emerging Technology.

conflict, ‘Grey Zones’, and those areas outside traditional military kinetic engagement), as well as the targets of this activity.

- The differences in understandings between ‘cyber-weapons’, ‘capabilities’, and ‘operations’ at an international level.
- Different perspectives on cyberspace as a military or public space.
- The role of public-private partnerships and industry in developing and deploying offensive cyber capabilities.
- The risks and unintended consequences involved in developing and deploying offensive cyber.
- The development of effective National Cyber Security Strategies.
- The strategic difference between offensive cyber from other capabilities.

Techniques & Implementation

The UK is experienced at conducting **full spectrum operations**,[13] but there is a need to categorise the effects specific to cyber capabilities – what are cyber means best suited for, to what ends, at campaign or tactical levels? Operational analysis of how that could work is useful but pragmatically difficult. Whilst integration of the tactical, operational, and strategic is preferable it may be difficult to implement in a stove-piped and compartmentalised operational setting.

Envisioning **research as a ‘force-multiplier’ for wider government discussions, debates, and policy considerations** would help improve understanding. Research likely needs to be at the conceptual level given restrictions on empirical accessibility and verifiability. This may be a useful way to overcome empirical restrictions, but case studies are also important, as would quantifying societal and national vulnerabilities as well as international cross-case comparisons.

Viewing offensive cyber through broader **sociotechnical conceptualisation** is essential. Timescales may operate differently where ‘effects’ may not be reducible down to immediate technical effects but to longer term social or strategic or political trends. Cyber capabilities are reliant on a whole ecosystem of human, organisational, cultural-specific practices and habits and norms, as well as the supply chain that necessarily precedes operations. **Developing cyber-specific chains of operation** from start to tactical deployment (e.g., difficult to separate the R&D of capabilities from their deployment, need for maintaining persistence and so on) could assist with developing concrete mechanisms for assessment.

The applicability of **historic cases** of military and intelligence experience could be developed, such as with previous cyber operations for learning lessons from similar contexts, learning how to deal with liminal spaces, shared spaces, and the novel challenges of joint military and intelligence activities. It is also essential to be aware of the emergent properties of offensive cyber, which cannot be wholly anticipated

[13] ”A full spectrum approach draws on a range of levers available to a state actor in a coordinated way to achieve (geo)political and strategic objectives. This can include overt and covert activities and the use of political, cultural, diplomatic, economic, military and other levers”. JCN 1/17, Future Force Concept (publishing.service.gov.uk)

in advance. We have historic experience of these kinds of grey areas, so research could help develop and evaluate conceptual frameworks.

A Research Agenda for Techniques and Implementation

- The development of methodologies to assess and standardise across assumptions of offensive cyber and 'technical speak'.
- The development of ways to communicate across classification levels.
- Measuring the effects of offensive cyber on political systems.
- Development of conceptual frameworks for chains of operation from start to tactical deployment (and the constricted space between R&D and use).
- Full analysis of the spectrum of capabilities. This includes a cross-government approach across various areas of the military as well as political and economic strengths.
- The application of previous experience in operations in other domains and their interconnection with cyber operations.
- How offensive cyber norms may be created and/or evolve in relation to precedents set by cyber operations.
- Understanding the sociotechnical effects of offensive cyber and their integration with capabilities.
- How to assess rapidly changing technologies, their development, and how their sometimes-short temporality restricts necessary research.

Conclusions

The inaugural scoping workshop of the Offensive Cyber Working Group produced a diverse range of perspectives and research priorities from several disciplines, institutions, and practices. This scoping exercise has produced research agendas for the three workstreams that were identified in advance of the workshop: Ethics & Law, Strategy & Policy, and Techniques & Implementation.

In Table 1, we map the thematic challenges to the research priorities identified by each workstream in Session 2. Some challenges explicitly cut across the workstreams – such as *blurred lines* and *societal debate*. Interdisciplinarity figured highly in the discussion of challenges but are not directly addressed as a research priority. Likewise, societal debate emerges as part of this working group rather than a research priority. Thus, the research priorities are more focused than the broader challenges, but collectively open-up societal debate to help address the blurred lines currently present in offensive cyber.

Table 1: Mapping Challenges to Research Priorities.

Challenges of, and for, Offensive Cyber	**Research Priorities**
1) Blurred Lines	▪ The development of methodologies to assess and standardise across assumptions of offensive cyber and 'technical speak'.
2) Responsibility and Risk	▪ Everyday harms that could emerge from offensive cyber. ▪ How military ethics could be applied to intelligence and non-state actors. ▪ How to assess rapidly changing technologies, their development, and how their sometimes-short temporality restricts necessary research. ▪ The applicability of current law to offensive cyber, including Human Rights Law and the Law on Armed Conflict. ▪ The risks and unintended consequences involved in developing and deploying offensive cyber.
3) Societal Debate	▪ Different perspectives on cyberspace as a military or public space. ▪ The development of ways to communicate across classification levels.
4) Strategy and International Cooperation	▪ How offensive cyber norms may be created and/or evolve in relation to precedents set by cyber operations. ▪ Measuring the effects of offensive cyber on political systems. ▪ Promotion of common legal understanding internationally, such as between the UK and NATO.

	▪ The development of effective National Cyber Security Strategies. ▪ The differences in understandings between ‘cyber-weapons’, ‘capabilities’, and ‘operations’ at an international level. ▪ The strategic difference between offensive cyber from other capabilities.
5) Operational Details	▪ Development of conceptual frameworks for chains of operation from start to tactical deployment (and the constricted space between R&D and use). ▪ Full analysis of the spectrum of capabilities. This includes a cross-government approach across various areas of the military as well as political and economic strengths. ▪ Reinvestigate collateral damage and proportionality of offensive cyber beyond isolated cyber-weapons. ▪ The application of previous experience in operations and their interconnection with cyber operations. ▪ The organisation of offensive cyber capabilities across different levels of conflict (including, but not limited to, thresholds below the level of armed conflict, 'Grey Zones', and those areas outside traditional military kinetic engagement) as well as the targets of this activity. ▪ The role of public-private partnerships and industry in developing and deploying offensive cyber capabilities. ▪ Understanding the sociotechnical effects of offensive cyber and their integration with capabilities.

This scoping workshop does not claim a totality of the concerns within the broader research community involved in offensive cyber. However, the workshop marks the first attempt in the UK to structure, communicate, and articulate the priorities and challenges for academia. The event acts as a starting point to develop exciting, novel, and informed research that informs not only conceptual academic debates but also pragmatic and timely advice for government, industry, and the international community.

Next Steps

As a working group, we intend to explore opportunities to socialise and constructively contribute to the debate by critically considering the key issues surrounding offensive cyber. This will be done through:

- Working towards widely shared and agreeable definitions, terminologies, and taxonomies on offensive cyber.
- Studying the UK’s position and practices on offensive cyber across time.

- Running regular events on key themes to increase and raise awareness of research on offensive cyber underpinned by academic rigour and independent analyses.
- Securing suitable funding and enabling the advancement of academic research through improving collaboration.
- Ensuring appropriate measures are in place to encourage sharing between members according to the Chatham House Rule.
- Supporting early career researchers through providing a forum and community to develop.