RUSI

National Cyber Force

A Defence and Intelligence Partnership

UK Cyber Effects Network

# New Thinking on UK Cyber Effects

## An Edited Collection

Edited by Jamie MacColl, Emma De Angelis, Pia Hüsch and Tim Stevens

RUSI

National Cyber Force

A Defence and Intelligence Partnership

UK Cyber Effects Network

# New Thinking on UK Cyber Effects

## An Edited Collection

Edited by Jamie MacColl, Emma De Angelis, Pia Hüsch and Tim Stevens

**About RUSI**

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world.

RUSI is a research-led institute, producing independent, practical and nnovative analysis to address today's complex challenges. Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 194 years.

**About the UK Cyber Effects Network**

The UK Cyber Effects Network seeks to build and strengthen a community of interest focused on cyber effects issues. The Network aims to generate new thinking on the theory and practice of offensive cyber operations, and help develop the next generation of UK experts. The Network is administered by RUSI and funded by the National Cyber Force.

© 2026 The Royal United Services Institute for Defence and Security Studies

This work is licensed under a Creative Commons Attribution – Non Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

ISBN: 978-1-0667172-0-0 (print)
ISBN: 978-1-0667172-1-7 (e-book)

## Disclaimer

The content in this publication is provided for general information only. It is not intended to amount to advice on which you should rely. You must obtain professional or specialist advice before taking, or refraining from, any action based on the content in this publication.

The views expressed in this publication are those of the authors, and do not reflect the views of RUSI, the National Cyber Force or any other institution. Contributions to the publication by employees of His Majesty's Government do not represent official government policy.

To the fullest extent permitted by law, RUSI shall not be liable for any loss or damage of any nature whether foreseeable or unforeseeable (including, without limitation, in defamation) arising from or in connection with the reproduction, reliance on or use of the publication or any of the information contained in the publication by you or any third party. References to RUSI include its directors, trustees and employees..

# Contents

*Acknowledgements* ..... **vii**

*About the Editors* ..... **viii**

*Foreword*
Air Vice-Marshal Tim Neal-Hopes OBE ..... **ix**

**Introduction**
Jamie MacColl, Emma De Angelis, Pia Hüsch and Tim Stevens ..... **1**

**Chapter 1**

**The UK Approach to Cyber Conflict in Theory and Practice**
Neil Ashdown ..... **9**

**Chapter 2**

**From Compliance to Combat: Building a Cyber and Electromagnetic Warfighting Culture**
Carolyn Swinney ..... **25**

**Chapter 3**

**Friction and Initiative in Cyberspace Through the Doctrine of Cognitive Effect**
Monica Kello and Richard Harknett ..... **49**

**Chapter 4**

**The Illusion of Restraint: Precision, Accountability and Calibration in the Cognitive Contest**
Charl van der Walt, Zohra Hamila, Richard Derbyshire and Adam Ridley ..... **65**

**Chapter 5**

**Legal Mechanisms for Scaling UK Offensive Cyber Capabilities Through the Private Sector**
Pia Hüsch and Charles Coventry ..... **85**

**Chapter 6**
**Military Cyber Operations and the Art of Manoeuvre in War**
Stefan Soesanto and Wiktoria Gajos ..... **109**

**Chapter 7**

**Adapting the UK's Approach to Responsible Cyber Effects for the 2030s**

DW ..... **133**

**Conclusion: A British Way of Cyber Operations?**

Conrad Prince, Andrew C Dwyer and Emily O Goldman ..... **149**

**Acknowledgements**

The editors are grateful to all the contributors to this volume for their insights and efforts. We are also grateful to the National Cyber Force for providing funding for the volume and its support throughout the process.

A great deal of thanks must also go to various members of staff at RUSI that helped to guide and shape the volume, particularly the Publications Team and our colleagues in the RUSI Cyber and Tech Research Group.

We would also like to thank all the reviewers that provided formal and informal feedback on individual chapters.

## About The Editors

### Jamie MacColl

Jamie MacColl is a Senior Research Fellow at the Royal United Services Institute. Jamie leads RUSI's work on the UK Cyber Effects Network. His current research focuses on ransomware and other financially motivated cybercrimes, and the UK National Cyber Strategy. He is also currently a Senior Research Associate at Virtual Routes, a European think tank, and a member of the Technical Committee for the Cyber Monitoring Centre. Jamie holds an MPhil in International Relations and Politics from the University of Cambridge and BA in War Studies from King's College London.

### Emma De Angelis

Emma De Angelis is a Senior Associate Fellow of RUSI, and was Editor of the *RUSI Journal* between 2011 and 2025. She is the Executive Director of the Aurora Forum, which brings together the UK, the Nordic and Baltic countries to address collaboration on security and prosperity across the region.

### Pia Hüsch

Pia Hüsch is a Research Fellow in cyber, technology and national security at RUSI. Prior to joining RUSI, Pia conducted her doctoral research on offensive cyber operations in international law at the University of Glasgow. At RUSI, Pia conducts research on disruptive technologies, including on how national security and geopolitical considerations shape countries' science, tech and innovation policy. She researches tech policy issues (including AI policy), offensive cyber operations and cyber policy in the Indo-Pacific. Pia is a recognised expert in her field and has contributed to inquiries of the UK Foreign Affairs Committee and the UK Science and Technology Committee as well as a broad range of media outlets, including *The Economist* and the *BBC*.

### Tim Stevens

Tim Stevens is Reader in International Security at the Department of War Studies, King's College London, and co-director of its Cyber Security Research Group. He has published widely on cybersecurity and cyber conflict, including a *Research Handbook on Cyberwarfare* (Edward Elgar, 2024). Tim is an Associate Fellow of RUSI.

# Foreword

I am sure many of you, like me, are avid followers of emerging cyber strategy. In March 2026, the US released its latest cyber strategy and, in the UK, we eagerly await the National Cyber Action Plan. But I would like to start the journey of the UK Cyber Effects Network (UKCEN) by going back to our 2022 National Cyber Strategy and the challenge set to us all: ensuring that the UK is confident, capable and resilient in an ever-accelerating digital world, and that we can continue to adapt, innovate and invest to protect and promote our interests in cyberspace. I strongly believe that the fusion of operational insight, strategic foresight and healthy ethical debate is the foundation on which the UK can build to successfully meet this challenge.

More needs to be done to encourage open conversation about the strategy, concepts and doctrine that guide cyber effects operations. The UKCEN is an exciting new way by which we intend to help to inform and drive the national and international cyber effects conversation. It seeks to blend the operational insight of the National Cyber Force (NCF) with RUSI's breadth of perspective and hugely respected analytical rigour. It aims to be informed by cutting-edge research and place all these insights into the realities of modern statecraft.

Our ultimate goal is to create a vibrant ecosystem of ideas and those who create them, engaging across both established scholars and practitioners, as well as eliciting the views of new talent entering the realm of cyber effects. The dynamic nature of cyberspace demands our thinking to be equally dynamic. This first volume has met that demand in full and stands as a testament to the fact that the UKCEN has got off to a running start. I want to thank the many friends, new and longstanding, who have contributed to this success. The 2025 Strategic Defence Review placed renewed emphasis on a 'whole of society' approach to national security – something we embody at the NCF through our unique partnership. Our strength against the increasing threat is integration, and the UKCEN is an excellent example of this.

The papers in this collection grapple with an era in which cyber effects are no longer peripheral to competition and conflict. In a digitally enabled world, it could be argued that cyber effects are at its core. Adversaries, whether nation states, terrorists or criminals, continue to scale their efforts and seek to exploit the ambiguities which are so often associated with cyberspace.

The authors, in response, have provided a fantastic intellectual tome that helps to frame our collective reply. Threads that span many of the chapters include: the doctrine of cognitive effect; the implications of responsible cyber power; technical frameworks by which to consider and articulate cyber effects; and 'what is the UK's national way of warfare in cyberspace?'

The UKCEN provides a rare opportunity to draw strategic coherence across these myriad topics and many more. It offers us the chance to blend experience and history with contemporary thinking to safely chart the next steps for a confident, capable and resilient UK. I hope you enjoy this volume and that it will be the first of many, as we collectively look to innovate and challenge today's thinking so we are ready to deliver strategic advantage in whatever tomorrow's national goals may require of this unique cyber effects community.

**Air Vice-Marshal Tim Neal-Hopes OBE**

# Introduction

**Jamie MacColl, Emma De Angelis, Pia Hüsch and Tim Stevens**

Cyber effects operations (or offensive cyber operations) have become a significant tool of statecraft in the 21st century. Recent conflicts in Iran, Venezuela, Ukraine and elsewhere have demonstrated the perceived utility of cyber operations for 'adding, deleting or manipulating data on systems or networks to deliver a physical, virtual or cognitive effect'.[1] Beyond the battlefield, cyber effects operations are increasingly used by states to sabotage, subvert or influence their adversaries while remaining below the threshold of armed conflict.

The UK has publicly avowed the use of cyber effects operations as an instrument of its national power. In 2020, the UK created an offensive cyber force, the National Cyber force (NCF), building primarily on the operational experience of GCHQ and the Ministry of Defence.[2] In 2023, the NCF published 'Responsible Cyber Power in Practice' (RCPiP), making it one of the few countries to set out how it will use cyber effects.[3] In RCPiP, the NCF outlined a number of different aspects to its approach to cyber effects operations, including: the ability of cyber operations to achieve cognitive as

1 The definition of offensive cyber operations used by the UK government in the 2022 National Cyber Strategy. See HM Government, 'National Cyber Strategy: Pioneering a Cyber Future with the Whole of the UK', December 2022, <https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022>, accessed 9 April 2026.

2 Joe Devanny et al., 'The National Cyber Force that Britain Needs?', Cyber Policy Institute, King's College London, April 2021, <https://www.kcl.ac.uk/policy-institute/assets/the-national-cyber-force-that-britain-needs.pdf>, accessed 9 April 2026.

3 National Cyber Force, 'The National Cyber Force: Responsible Cyber Power in Practice', April 2023, <https://www.gov.uk/government/publications/responsible-cyber-power-in-practice/>, accessed 9 April 2026.

well as technical effects; the importance of linking operations together as campaigns; and its commitment to ensuring that all its operations are precise, accountable and calibrated. The publication of RCPiP marked a significant step by the UK government in signalling greater transparency about its approach to cyber effects operations.

While this increased transparency has proved fertile territory for some researchers,[4] dedicated research on the UK context has been relatively limited. It is likely that there are several reasons for this. Scholarship on offensive cyber and cyber conflict has been dominated by US-focused scholars. Some are affiliated with or have access to public bodies responsible for conducting cyber effects operations, yet are able to publish (unclassified) research in a scholarly capacity. This established community of US scholars dominates much of the debate, leaving relatively little space for discussion on middle powers such as the UK. Researchers looking to work on the UK approach are also confronted by an almost complete lack of primary evidence on operations conducted by the NCF or other UK entities. Access to dedicated funding, particularly for sociotechnical research on cyber effects, further adds to this challenge.

Given this, there are several pressing questions about the UK approach to cyber effects operations that require interrogation. Does the UK's public commitment to responsible cyber power and 'precision, accountability and calibration' disadvantage it compared with its adversaries (and perhaps even its allies)? Can more resource-constrained states, such as the UK, campaign with the kind of persistence outlined in dominant US strategic thinking on cyber effects operations? How can the UK scale its cyber capabilities in conflict? While the NCF will have its own answers to these questions and others, it would surely also benefit from examination by researchers and practitioners outside the siloes of the UK government. Greater debate within the UK on these issues will also, in the long run, strengthen the contribution it can make to developing norms and international law, as well as the policy, doctrine and concepts of allies and partners.

4 Devanny et al., 'The National Cyber Force that Britain Needs?'; Marcus Willet, *Cyber Operations and their Responsible Use* (Abingdon: Routledge, 2024); Tim Stevens et al., 'Evaluating the National Cyber Force's 'Responsible Cyber Power in Practice', *RUSI Commentary*, 14 April 2023, <https://www.rusi.org/explore-our-research/publications/commentary/evaluating-national-cyber-forces-responsible-cyber-power-practice>, accessed 7 April 2026.

## The Development of the Edited Collection

To address some of these questions and concerns, the Cyber Effects Network launched an open call for abstracts in September 2025. We selected several papers for further development and also commissioned additional chapters directly. NCF staff were also offered the opportunity to contribute; one chapter by a serving NCF official has been included in this volume. Our aim in putting together this Edited Collection was to draw on a diverse range of contributors and, where possible, prioritise early- and mid-career researchers and practitioners. The academic authors of the chapters are multidisciplinary, drawing from International Relations, Strategic Studies, International Law and Cyber Security. Furthermore, the Edited Collection also includes contributions from practitioners in the private sector, the military and the UK government. The chapters have therefore been developed by a community of practice rather than one far removed from the reality of cyber operations. Although the volume has an explicit focus on the UK context, the authors work in or originate from a range of countries, including the US, Germany, South Africa and Switzerland.

## Structure of the Edited Collection

This Edited Collection has seven chapters and a roundtable-style conclusion that reflects on some of the themes that the authors raised. The first half of the Edited Collection focuses on the UK's broad approach to offensive cyber strategy, doctrine and policy, and the second half focuses on more specific issues such as adversaries' approaches, the role of the private sector and cyber operations during conflict.

The Edited Collection opens with 'The UK Approach to Cyber Conflict in Theory and Practice'. Neil Ashdown explores whether there is a distinct UK approach to cyber operations and how this approach may differ from the US experience. Ashdown suggests that the defining characteristic of this approach is pragmatism and compromise – in other words, a classic British 'fudge'. The chapter situates the UK's approach in its historical context and argues that there are continuities of the current use of cyber effects operations with the UK's previous experience of exploiting technology for strategic advantage.

In Chapter 2, Carolyn Swinney explores the development of the UK's institutions and strategy for cyber and electromagnetic warfare. 'From Compliance to Combat: Building a Cyber and Electromagnetic Warfighting Culture' examines the UK's attempt to integrate cyber and electromagnetic capabilities into a single CyberEM Command (now known as the Defence Cyber and EM Force). The chapter further argues that the central challenge is cultural rather than technical. Swinney, a serving RAF officer, contends that while the 2025 Strategic Defence Review recognises the growing importance of cyber and electronic warfare in modern conflict, the UK will only realise military advantage if it develops a 'warfighting culture' in this domain.

Chapter 3, 'Friction and Initiative in Cyberspace Through the Doctrine of Cognitive Effect', examines the NCF's Doctrine of Cognitive Effect. It argues that the doctrine's distinctive contribution lies in using cyber campaigns to impose 'friction' on adversaries at the technical, organisational and psychological levels. Monica Kello and Richard Harknett suggest that cyber operations are most effective not as isolated disruptive acts, but as linked campaigns designed to shape how adversaries perceive and navigate their environment. Using them in this way erodes trust within a targeted group or community over time. Using the UK National Crime Agency's Operation *Cronos* against the LockBit ransomware group as a case study, the authors show how technical disruption, organisational friction and carefully amplified cognitive effects can combine to produce strategic outcomes. They conclude that campaigns that aim to generate friction for adversaries offer an effective way for the UK to optimise its resources.

Chapter 4, 'The Illusion of Restraint: Precision, Accountability and Calibration in the Cognitive Contest', explores whether the UK's commitment to responsible cyber power places it at a disadvantage compared with adversaries, such as Russia and China. Similar to Chapter 3, it examines a key concept from the NCF's RCPiP – the UK's commitment to the principles of precision, accountability and calibration (PAC). Charl van der Walt, Zohra Hamila, Richard Derbyshire and Adam Ridley argue that the problem stems less from the principles themselves than from their being too often applied within a narrow, technical understanding of cyberspace. Instead, they should be applied in a broader cognitive and sociotechnical contest. By comparing the UK's approach with those of Russia and China, the chapter argues that adversaries are also constrained, but in ways designed to support narrative dominance, deniability and sustained political pressure. The authors contend

that – if embedded within a more realistic conception of cyber conflict and aligned with democratic strengths such as transparency – the commitment to PAC can operate not as a restraint on cyber effects operations, but as force multipliers.

One way to scale UK offensive cyber capabilities is by using the private sector. In Chapter 5, 'Legal Mechanisms for Scaling UK Offensive Cyber Capabilities through the Private Sector', Pia Hüsch and Charles Coventry look at the legal considerations involved in using the private sector to conduct cyber effects operations. They argue that, although a range of models exists for cooperation with industry, the most plausible mechanism in the current UK context is the use of carefully bounded warrants that allow private companies to undertake otherwise unlawful activities on the state's behalf. The chapter also stresses that such arrangements raise difficult questions under both domestic and international law. Hüsch and Coventry conclude that the UK debate remains underdeveloped and overly shaped by US policy proposals – such as the issuing of letters of marque – and suggest that scaling cyber effects operations by using the private sector will require much clearer public and legal thinking about which mechanisms are appropriate, lawful and politically acceptable in the UK.

Chapter 6 explores a theme of growing importance – the role of cyber operations in conflict. 'Military Cyber Operations and the Art of Manoeuvre in War' argues that cyber effects operations during conflict should be understood not simply as supporting tools for kinetic actions, but as a distinct form of manoeuvre warfare capable of shaping the trajectory of a conflict. To explore this concept, Stefan Soesanto and Wiktoria Gajos develop a set of six military cyber campaign archetypes, ranging from attacks on military assets to the degradation of civilian infrastructure. The chapter then maps these archetypes across eight phases of cyber warfare. Soesanto and Gajos contend that effective military cyber campaigns depend on the sustained accumulation of access, disruption and positional advantage over time, rather than on isolated technical effects, and suggest that cyber effects operations can be used to degrade an adversary's capacity to fight, recover and govern. The chapter provocatively concludes that the UK's commitment to 'responsibility' may impose constraints that limit its ability to conduct effective campaigns in wartime.

Finally, Chapter 7, 'Adapting the UK's Approach to Responsible Cyber Effects for the 2030s', looks to the future and imagines what the strategic and operating environment will be like for the UK in the 2030s. DW, an NCF official, suggests that while the principles set out in the National Cyber Force's RCPiP remain valuable, they will need to evolve if they are not to become irrelevant or overly constraining by the next decade. The chapter outlines three scenarios for 2035, ranging from deeper human–computer integration to AI-enabled Smart Cities and corporate-led technological governance. The implications of these scenarios, DW suggests, are that the UK should reconsider its commitment to some of its existing operating principles.

The Edited Collection ends with a roundtable-style Conclusion co-authored by a former senior UK intelligence official (Conrad Prince), a UK academic and the co-founder of the UK's Offensive Cyber Working Group (Andrew C Dwyer), and an experienced US cyber strategist (Emily O Goldman). It draws out several aspects of the themes of this volume, and in particular asks whether there is a distinct UK approach to cyber effects operations and examines the implications of this approach.

All three contributors to the Conclusion suggest that the defining characteristic of the UK's approach is pragmatism, a lesson learned through practice rather than derived through a 'grand theory'. Prince emphasises its roots in GCHQ's long experience of cyber operations and its heritage as a civilian intelligence agency. Dwyer describes the UK's emphasis on pragmatism as a characteristically British 'productive fudge' built on compromise and integration.

The UK's emphasis on integration across institutions and domains is a theme that all three authors explore. The 'British way' does not treat cyber effects operations as a standalone military tool or as limited to the cyber domain. Prince highlights the breadth of the NCF's remit across national security, defence, counterterrorism, and serious and organised crime. Goldman argues that the UK sees cyberspace as a more sociotechnical system, which encourages cyber campaign planners to think beyond immediate technical disruption and to shaping an adversary's perceptions and decision-making. Unsurprisingly, all three authors also converge on the NCF's 'doctrine of cognitive effect' as a key theme that runs through both the Edited Collection and as one of the most distinctive features of the UK's approach to cyber effects operations.

Prince, Dwyer and Goldman all end by raising questions about the future of the NCF and the UK's approach. Prince asks the most provocative question: given the multiple identities of the NCF, resource constraints and demands from a wide range of customers, 'what fundamentally is the role of the NCF?'. Prince concludes that: 'It is probably not possible for the NCF to try to be the sole UK government cyber effects organisation. A more realistic approach would be to act as a centre of excellence, supporting others as the spider in the centre of the web of UK cyber effects'. For Dwyer, one challenge for the NCF is to interrogate the limitations of cognitive effects, particularly during conflicts when there is a greater emphasis on technical disruption of military capabilities. Finally, all three contributors align on the role of the private sector as being a key question for the NCF. As Prince argues, the private sector is 'fundamental' to the challenge of scaling UK cyber effects capabilities. The wider the range of actors developing and delivering cyber effects, however, the greater the risks. Goldman is optimistic that the UK's approach is ultimately 'fit for purpose' for this challenge and others due to its pragmatism and its partnership with the US.

As editors, we share Prince's view that this Edited Collection is merely one stop on a long journey of thinking on the British way in cyber effects operations. We hope the volume moves this thinking forward, and that it encourages future contributions that challenge our understanding of cyber effects operations, cyber conflict and UK strategic culture. Maintaining the momentum of the research agenda in our own national context is critical as the UK attempts to gain advantage in a global political arena in a seemingly constant state of upheaval.

CHAPTER 1

# The UK Approach to Cyber Conflict in Theory and Practice

**Neil Ashdown**

Research on the UK approach to cyber operations and effects is challenging, because the language and key theories of the debate are strongly influenced by the US experience. Recognising this allows us to challenge underlying theoretical assumptions and reframe cyber operations as the latest development in a long history of technological exploitation for strategic advantage.

In this chapter, I first examine why so much of the literature on cyber conflict has downplayed historical continuities in favour of novelty and structural theoretical arguments. I locate the cause for this in the dominance of US academics and military practitioners.[1] This dynamic is explored through the example of Cyber Persistence Theory (CPT). I argue that the UK context renders unlikely the development of a single programme of cyber conflict research with a British 'flavour'.[2]

The chapter next examines the UK's approach to cyber operations, arguing that its defining characteristic is pragmatism and compromise. This is driven by limited resources and changing requirements. I identify key differences between the US and the UK approaches to cyber operations,

1 Joe Devanny and Tim Stevens, 'What Will Britain's New Cyber Force Actually Do?', *War on the Rocks*, 26 May 2021, <https://warontherocks.com/what-will-britains-new-cyber-force-actually-do/>, accessed 27 February 2026; Jordan Branch, 'What's in a Name? Metaphors and Cybersecurity', *International Organization* (Vol. 75, No. 1, 2020), pp. 1–32.

2 Conrad Prince, 'Encouraging New Thinking on Offensive Cyber Operations', *RUSI Commentary*, 10 September 2025, <https://www.rusi.org/explore-our-research/publications/commentary/encouraging-new-thinking-offensive-cyber-operations>, accessed 27 February 2026; Devanny and Stevens, 'What Will Britain's New Cyber Force Actually Do?'.

most notably the UK's willingness to blur boundaries between technical and cognitive effects.

The chapter then argues that modern cyber operations have clear continuities with the UK's approach to technological exploitation for strategic advantage that the country has practised since the late 19th century. CPT's claims appear less specific to cyber conflict than to a wider field of subthreshold competition. I argue that CPT's growing focus on integrated campaigning is suggestive of a recognition that cyber effects are best used and studied holistically with other aspects of statecraft, rather than in isolation.

Finally, I argue that the diversity of perspectives that a more holistic approach unlocks is a strength that the UK study of cyber effects should promote. The UK's approach to the theory and practice of conflict – based on compromise and innovation – is more appropriate in a rapidly deteriorating geopolitical environment. The UK government should encourage multidisciplinary, multivocal research on cyber effects as it postures to rapidly innovate and adapt in future conflict.

## A Persistent Question

How do states achieve strategic advantage through technology in conditions of competition, crisis and conflict? This question underlies much academic and policymaker debate on what has variously been termed 'cyber war', 'cybersecurity' and 'cyber conflict'. Asking what cyber war is,[3] whether it will ever occur,[4] or whether cyber conflict is an intelligence contest[5] is to touch on this underlying question.

One answer to the question of how states achieve strategic advantage through technology can be found in CPT. This is a body of theoretical work associated with three practitioner-scholars: Michael Fischerkeller; Emily Goldman; and Richard Harknett.[6] CPT answers the question from a distinctly US military and

3 John Arquilla and David Ronfeldt, 'Cyberwar is Coming!', *Comparative Strategy* (Vol. 12, No. 2, 1993), pp. 141–65.
4 Thomas Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013).
5 Robert Chesney and Max Smeets (eds), *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest* (Washington, DC: Georgetown University Press, 2023).
6 Michael P Fischerkeller, Emily O Goldman and Richard J Harknett, *Cyber Persistence Theory:*

International Relations-focused perspective. Fischerkeller and Harknett argue that technological change has created a novel 'cyber strategic environment'.[7] In this construct, states can accrue strategic advantage during periods of competition through campaigns of persistent activity in cyberspace, and during crises by pre-emptive campaigns to set favourable conditions for future contingencies.[8] Reflecting its disciplinary origins in realist International Relations theory, CPT's conclusions and precepts are based on what the authors assert are structural factors that apply equally to all states.[9]

The answer that CPT offers has been highly influential, shaping the academic debate and policy in the US, the UK and elsewhere.[10] It offers an analytical lens and a set of policy prescriptions that, in their derivation from claimed structural factors, downplay the importance of country-specific factors and comparisons with other aspects of contemporary and historical statecraft.

Rather than examining how cyber 'works' by deriving conclusions from deterministic structural claims, I argue for examining historical and contemporary examples of states seeking and achieving strategic advantage through the exploitation of technology. This approach is grounded in the examination of the contingent conditions of specific states and organisations throughout history.

This is a challenging task because the language of the debate reflects a strongly US and military perspective.[11] Yet, if we can loosen this terminology from some of its theoretical underpinnings, we can examine

*Redefining National Security in Cyberspace* (Oxford: Oxford University Press, 2022).

7 Michael Fischerkeller and Richard Harknett, 'The Strategic Nature of the Digital Age Propaganda, Surveillance, and Intelligence', *Brown Journal of World Affairs* (Vol. 30, No. 1, 2023), pp. 7–22.

8 Michael Fischerkeller, Emily Goldman and Richard Harknett, 'NATO Must "Contingency Campaign" in Cyberspace', Book Binder, 16 December 2025, <https://bindinghook.com/nato-must-contingency-campaign-in-cyberspace/>, accessed 27 February 2026.

9 Fischerkeller, Goldman and Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace*.

10 Paul M Nakasone, 'A Cyber Force for Persistent Operations', *Joint Force Quarterly* (No. 92, 1st Quarter 2019), pp. 10–14; Richard J Harknett, Michael P Fischerkeller and Emily O Goldman, 'U.K. National Cyber Force, Responsible Cyber Power, and Cyber Persistence Theory', *Lawfare*, 5 April 2023, <https://www.lawfaremedia.org/article/uk-national-cyber-force-responsible-cyber-power-and-cyber-persistence-theory>, accessed 27 February 2026.

11 Branch, 'What's in a Name?'.

the continuities of modern cyber operations with earlier periods of technologically mediated competition, as well as those of cyber with other aspects of contemporary statecraft.

There are practical reasons for making this shift. The logic of security that CPT prescribes poses daunting requirements for a major cyber power, let alone a middle-tier country such as the UK – something recognised by proponents of CPT.[12] Exploring how states have derived advantage from their ability to operationalise technological exploitation in other places and times may reveal alternative logics of security that are more practical for middle powers.

## CPT and Other Theories

US International Relations theorists have played a key role in shaping the academic discourse on offensive cyber.[13] For CPT, the structure of the cyber strategic environment determines how states can achieve advantage and security; that structure applies equally to all states.[14]

This is a distinctly US approach to academic understanding of the world, rooted in the historical development of US International Relations as a discipline, and one unlikely to be uncritically accepted by many UK academics. Even the UK discipline of International Relations has long been characterised as largely a 'realist-free zone'.[15] Practitioners in government on both sides of the Atlantic may be an even harder sell. GCHQ , for example, perceives itself as 'intensely pragmatic' with little interest in 'establishing theoretical constructs around the way Sigint works'.[16]

There is also a practical issue. CPT purports to provide an objective description of the state of the world. Yet there is a compelling argument that

12 Monica Kello and Richard J Harknett, 'Towards a British Approach to Cyber Campaigning', *RUSI Commentary*, 24 February 2026, <https://www.rusi.org/explore-our-research/publications/commentary/towards-british-approach-cyber-campaigning>, accessed 27 February 2026.

13 Joe Burton and George Christou, 'Bridging the Gap Between Cyberwar and Cyberpeace', *International Affairs* (Vol. 97, No. 6, 2021), pp. 1727–47.

14 Fischerkeller, Goldman and Harknett, *Cyber Persistence Theory*.

15 John J Mearsheimer, 'E.H. Carr vs. Idealism: The Battle Rages On', *International Relations* (Vol. 19, No. 2, 2005), p. 144.

16 Daniel W B Lomas, 'Profiles in Intelligence: An Interview with Tony Comer', *Intelligence and National Security* (Vol. 38, No. 1, 2022), p. 6.

CPT is shaped by the perspectives and preoccupations of the US military, as shown by its emphasis on the distinction between cyber operations and intelligence activity.[17]

The academic and practical context in the UK is very different. The UK field is smaller than its US counterpart and the disciplinary composition is different, reflecting a mix of disciplines including history, war studies and security studies. Most of the literature available for academics and practitioners studying cyber operations emerges from the US, with some notable UK-focused exceptions.[18] Much of the UK-focused discussion comes from publications or commentary by former officials,[19] anonymous articles by serving practitioners,[20] or academic work by practitioners.[21]

In contrast to the prominent role played by the US agencies and military, the UK government has historically made little public engagement on offensive aspects of cyber. Prior to the creation of the Cyber Effects Network, the National Cyber Force's (NCF) most public intervention was the release, in April 2023, of 'Responsible Cyber Power in Practice' (RCPiP).[22] There is no UK equivalent of the 'scholar in residence' programmes that enabled the CPT authors to create their work. Nor has there been a similar public endorsement by the UK government or military of an academic theory on cyber conflict.[23]

17 Burton and Christou, 'Bridging the Gap Between Cyberwar and Cyberpeace'; Jon R Lindsay, 'Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-Scale Intelligence Problem', *Intelligence and National Security* (Vol. 36, No. 2, 2021), pp. 260–78.

18 Devanny and Stevens, 'What Will Britain's New Cyber Force Actually Do?'; Joe Devanny et al., 'The National Cyber Force That Britain Needs?', Cyber Security Research Group, Offensive Cyber Working Group and The Policy Institute, King's College London, April 2021 , <https://www.kcl.ac.uk/policy-institute/assets/the-national-cyber-force-that-britain-needs.pdf>, accessed 27 February 2026; Marcus Willett, *Cyber Operations and Their Responsible Use* (Abingdon: Routledge, 2024).

19 Willett, *Cyber Operations and Their Responsible Use*.

20 Lester Godefrey, 'Shape or Deter? Managing Cyber-Espionage Threats to National Security Interests', *Studies in Intelligence* (Vol. 66, No. 1, 2022), pp. 1–10.

21 Timothy Neal-Hopes, '"Preventing a Cyber Dresden": How the Evolution of Air Power Can Guide the Evolution of Cyber Power', Unpublished thesis, School of Advanced Air and Space Studies, Maxwell Air Force Base, Alabama, 2011.

22 National Cyber Force, 'National Cyber Force: Responsible Cyber Power in Practice', April 2023, <https://www.gov.uk/government/publications/responsible-cyber-power-in-practice>, accessed 27 February 2026.

23 Paul M Nakasone and Michael Sulmeyer, 'How to Compete in Cyberspace', *Foreign Affairs*, 25 August 2020.

The likely explanation for this is that until recently there was no requirement for a public 'theory of cyber operations'; the UK's approach to organising for offensive cyber has been determined largely in secret within government. The creation and shape of the NCF, for example, was not a matter of public debate, unlike the creation and development of US Cyber Command. The participants in that debate had little incentive to support the production of a British version of, or alternative to, CPT that could be appealed to in support of their position. The creation of the Cyber Effects Network represents a potential shift, but it remains unlikely that the UK will replicate the kind of policy advocacy debate on cyber operations seen in the US.

## The Organisation of the UK's Cyber Capabilities

This point becomes clear when we examine the nature of the development of the UK's cyber capabilities. This history is characterised by a series of hybrid organisations and compromises, notably described as bureaucratic 'fudge' – 'a solution to a problem that just about manages to keep everyone happy but that is no one's ideal first choice'.[24] The contrast between the idea of bureaucratic 'fudge' and the structurally determined precepts of CPT says something important about differences between the UK and the US.

The NCF is the ultimate fudge in this respect. It is a hybrid organisation – a partnership bringing together personnel from across Defence and the UK intelligence services under the joint authority of the foreign and defence secretaries. That the NCF stems from a compromise is visible in some surprising absences – the organisation does not have its own email domain, for example.

The NCF, in turn, sits in a landscape of overlapping organisations involved in the 'cyber mission', with GCHQ at the centre of the Venn diagram. On the military side, this includes the Cyber & Specialist Operations Command (CSOC), stood up in 2025, which contains the Defence Cyber and Electromagnetic Force (DCEMF, initially referred to as the CyberEM Command).[25]

24 Devanny and Stevens, 'What Will Britain's New Cyber Force Actually Do?'.

25 Joyce Hakmeh, 'CyberEM Command: The UK's Strategic Leap in Integrated Modern Warfare', Expert Comment, Chatham House, 6 June 2025, <https://www.chathamhouse.org/2025/06/cyberem-command-uks-strategic-leap-integrated-modern-warfare>, accessed 27 February 2026; Ministry of Defence (MoD), '100 Days of Cyber & Specialist Operations

These overlapping arrangements emerged in the context of substantial budgetary shortfalls within Defence and delays to the release of the government's Defence Investment Plan, originally due in late 2025.[26] Yet even in this context, the creation of CSOC, DCEMF and the NCF did not prompt the kind of vociferous public debate seen in the US over the relationship between US Cyber Command and the National Security Agency.[27]

The ability to reshape organisations without encountering entrenched public debate is a key advantage of the UK system. Accounts of the development of the NCF emphasise that the creation of a hybrid organisation owed much to shared experience and working relationships among the people involved; trust among individuals overcame bureaucratic hurdles.[28] These relationships are possible because of the small scale of the UK's national security and defence apparatus; these make ad hoc compromises and partnership easier.

## The UK's Approach to Cyber Operations

There are clear similarities between the approaches to cyber operations of the US and the UK. These include the rejection of the analogy between cyber and nuclear weapons, and the belief that cyber capabilities need to be used regularly, not held in reserve. As the NCF's first commander, James Babbage, put it when launching RCPiP: 'Red buttons become rusty buttons'.[29]

These tenets align with the prescriptions of CPT, and US and UK practitioners agree on key aspects of the character of cyber conflict. Where differences emerge, it tends to be in the UK's ability to blur lines that, in the US, are more defined. One example is in their respective approaches to legal authorities. The NCF is emphatic that its operations are guided by legal frameworks and subject to robust accountability.[30] Nonetheless, the UK's approach is less

Command', Cyber & Specialist Operations Command blog, 10 December 2025, <https://cyberandspecialistoperationscommand.blog.gov.uk/2025/12/10/100-days-of-cyber-specialist-operations-command/>, accessed 27 February 2026.

26 Paul Seddon, 'UK Facing £28bn Defence Spending Gap Claims', *BBC News*, 9 January 2026.

27 Mark Pomerleau, 'Members of Congress Vow Not to Split Cyber Command, NSA', *DefenseScoop*, 16 May 2025 , <https://defensescoop.com/2025/05/16/members-of-congress-vow-not-to-split-cyber-command-nsa/>, accessed 27 February 2026.

28 Willett, *Cyber Operations and Their Responsible Use*, p. 140.

29 *The Economist*, 'Cyberwarfare is All in the Mind, Says Britain', 4 April 2023.

30 National Cyber Force, 'The National Cyber Force: Responsible Cyber Power in Practice'.

formally legalistic than the system of authorities that delimits the actions of US military and intelligence agencies. The UK system benefits from greater flexibility to align people, capabilities and requirements.[31]

Similarly, where the US draws a bright doctrinal line between cyber and information activities,[32] the UK's approach appears more ambiguous. RCPiP emphasises what the NCF terms the 'doctrine of cognitive effect', the idea that the UK can achieve 'advantage over adversaries by affecting their perception of the operating environment and weakening their ability to plan and conduct activities effectively'.[33] This description suggests that cyber-enabled information and psychological operations are a regular occurrence, rather than an outlier.[34] It also diverges from CPT's focus on persistent action to render an adversary's activities inconsequential, emphasising instead subtle methods that change an adversary's behaviour.[35]

## What is Old is New Again

Intelligence historian Rory Cormac has observed that the UK's approach to cyber effects as set out in RCPiP 'feels familiar to historians as the latest manifestation of the UK's long-standing approach to covert operations'.[36] The point can be generalised; the UK's approach to strategic competition via technology exploitation in the early 21st century (including through covert action, but also via other means) shows strong continuities with its approach in the late 19th and early 20th centuries. This section highlights some such

31 Willett, *Cyber Operations and Their Responsible Use*.
32 Skyler Onken and Margaret Webber, 'Reclaiming the Cyber Domain: Revising U.S. Doctrine to Treat Cyberspace as Battlespace and Not a Function', *Cyber Defense Review* (Vol. 10, No. 3, 2025), p. 147; Michael Warner, 'A Brief History of Cyber Conflict', in Jacquelyn G Schneider et al. (eds), *Ten Years In: Implementing Strategic Approaches to Cyberspace* (Newport, RI: Naval War College Press, 2020), pp. 13–29.
33 National Cyber Force, 'The National Cyber Force: Responsible Cyber Power in Practice', p. 15.
34 Willett, *Cyber Operations and Their Responsible Use*.
35 Godefrey, 'Shape or Deter?'.
36 Tim Stevens et al., 'Evaluating the National Cyber Force's "Responsible Cyber Power in Practice"', *RUSI Commentary*, 14 April 2023 , <https://www.rusi.org/explore-our-research/publications/commentary/evaluating-national-cyber-forces-responsible-cyber-power-practice>, accessed 27 February 2026.

continuities, including examples of 'initiative persistence' and technological 'contingency campaigning' *avant la lettre*.[37]

Prior to the First World War, Britain capitalised on its control over key technological enablers and leadership in research and development to cement its dominance over global telegraph networks. Doing so involved continual competition with rivals that fully recognised the strategic advantages that Britain accrued through this dominant position.[38]

Concurrently with this competition, Britain acted during peacetime to position itself for future crisis contingencies. These preparations meant that when war broke out in 1914, plans and capabilities were ready to be deployed. At the outbreak of conflict and thereafter, strategic pre-positioning, public–private collaboration, deception and technical operations enabled by physical access delivered effects ranging from herding adversaries on to less secure communications channels to creating uncertainty over the integrity of communications.[39]

However, Britain's dominant position in the peacetime competition over international telegraphy did not translate into similar pre-eminence in the integration of that technology into military campaigns on the Western Front. The fighting on land confronted Britain and other participants with a form of technology-mediated warfare, the outlines of which had only dimly been perceived in earlier conflicts.

The ability to operationalise technology, to defend one's own systems and exploit adversaries' systems was critical to the outcome of that conflict. All combatants learned about this form of technological competition on the job, with no side notably outperforming the others.[40] Highly varied levels

37 Neil Ashdown, 'CS Alert – Offensive Cyber in 1914', Offensive Cyber Working Group, 5 August 2021, <https://offensivecyber.org/2021/08/05/cs-alert-offensive-cyber-in-1914/>, accessed 27 February 2026.

38 P M Kennedy, 'Imperial Cable Communications and Strategy, 1870–1914', *English Historical Review* (Vol. 86, No. 341, 1971), pp. 728–52; Jonathan Reed Winkler, *Nexus: Strategic Communications and American Security in World War I* (Harvard, MA: Harvard University Press, 2008).

39 Jonathan Reed Winkler, 'Information Warfare in World War I', *Journal of Military History* (Vol. 73, No. 3, 2009), pp. 845–67.

40 John Ferris (ed.), *The British Army and Signals Intelligence During the First World War* (Wolfeboro

of intelligence collection and communications-security capability enabled persistent exploitation of vulnerabilities throughout the conflict. In isolation, this work was not decisive, but nor was it irrelevant. Strategic advantage accrued over time to the countries that could most effectively integrate technology use and exploitation into their military and diplomatic positioning, alongside other levers of national power.[41]

It was in this context that Britain developed and expanded organisations that specialised in the exploitation of technology. The historical development of British signals intelligence capability from 1918 to 1945 was characterised by organisational learning and agility – the ability to pivot, to work with partners, and to adopt new technologies in a resource-constrained environment. As historian John Ferris has argued, 'no other intelligence organisation on earth expanded and adapted like [GCHQ's predecessor] GC&CS between 1939 and 1945'.[42]

After the Second World War, as GCHQ again pivoted from a focus on the decryption of high-end German codes to the analysis at scale of Soviet traffic, the reorganisation involved judgements that 'sought to derive principles from the organisation of intelligence since 1918, *which no one fully understood*'.[43] Similarly, Cormac characterises the UK's approach to the use of covert action as adaptive, based on 'muddling through' in response to diminishing resources and rapidly changing circumstances.[44] The absence of grand theory was not a constraint and may, in fact, explain these organisations' successes.[45]

Falls, NH: Alan Sutton Publishing, 1992), p. 3.

41 Lindsay, 'Cyber Conflict vs. Cyber Command'.

42 John Ferris, *Behind the Enigma: The Authorised History of GCHQ, Britain's Secret Cyber-Intelligence Agency* (New York, NY: Bloomsbury, 2020), p. 213.

43 *Ibid.*, pp. 269, 273. Emphasis added.

44 Rory Cormac, *Disrupt and Deny: Spies, Special Forces, and the Secret Pursuit of British Foreign Policy* (Oxford: Oxford University Press, 2018).

45 Martin C Libicki, 'Why Cyber War Will Not and Should Not Have Its Grand Strategist', *Strategic Studies Quarterly* (Vol. 8, No. 1, 2014), pp. 23–39.

## Cyber: An Aspect of Broader Technologically Mediated Competition

The logic of action that CPT portrays as the consequence of a novel 'strategic environment' pre-dates the birth of digital computing (and nuclear weapons). It also extends beyond the 'cyber domain' to contemporary subthreshold competition.

Modern cyber operations – in their intent and effects, if not in their technical modalities – would have been familiar to earlier generations of military and intelligence practitioners. Forward-deployed Russian operators conducting rapid forensics on captured Ukrainian mobile devices in 2024 were doing the same thing in a different technological milieu as soldiers in the First World War conducting trench raids to capture codebooks.[46]

Modern digital technologies do differ from their precursors. Gaining access to a target's computer provides a greater set of affordances than intercepting a wireless transmission. The scale at which this activity can be conducted has also changed, as has the extent to which technology is now interwoven into people's lives.

Yet rather than supporting claims of a revolutionary new 'cyber strategic environment', the scale of the transformation is arguably grounds for rejecting a narrow focus on 'cyber' alone. The range of affordances and opportunities for exploitation created by complex sociotechnical systems greatly exceeds what can be achieved solely by manipulating data on adversary computers.

The key thread is not the specifics of the technology but of the operationalisation of exploitation for strategic advantage. The Israeli supply chain sabotage operation targeting Hezbollah in 2025 was not, by any current definition, a 'cyber operation', but it was an example of a state exploiting complex sociotechnical institutions for strategic advantage.[47]

46 Dan Black, 'Russia's Cyber Campaign Shifts to Ukraine's Frontlines', *RUSI Commentary*, 22 July 2024, <https://www.rusi.org/explore-our-research/publications/commentary/russias-cyber-campaign-shifts-ukraines-frontlines>, accessed 27 February 2026.

47 Raffi Berg, 'Ex-Israeli Agents Reveal How Pager Attacks Were Carried Out', *BBC News*, 23 December 2024.

This explains why many of the dynamics that the CPT ascribes to the 'cyber strategic environment' appear applicable to a broader range of conflictual activities short of open war. These include 'anti-submarine warfare, espionage-counterespionage, freedom-of-navigation operations, and intelligence, surveillance, and "exciter" flights'.[48]

It also explains the similarity between the core claims and prescriptions of CPT and analyses of other forms of subthreshold competition. The UK's 2021 Defence Command Paper, for instance, outlined a model of 'Persistent Engagement' that advocated integrated campaigning through the spectrum of constant competition, crisis and conflict.[49] A 2023 RAND report described 'a new concept for strategic disruption by special operations forces, involving proactive campaigns to delay, degrade, or deny an adversary's ability to achieve core interests through its preferred strategies'.[50] An analysis of the use of drones for long-range bombing observes that '[w]hen many actors can strike critical infrastructure cheaply, the distinction between limited war and strategic war begins to blur [… and] strategic effects [are] achieved through cumulative, low-signature attacks that fall below traditional thresholds of war'.[51]

These claims will be familiar to readers of CPT in a way that suggests that these analyses are all grappling with the same phenomenon. Viewed in a longer historical perspective, many of the claims made about the enduring characteristics of cyber conflict appear instead to reflect the US perception of subthreshold competition during a period of rapid technological change.[52]

## Towards a Focus on Campaigning

The idea that it is a mistake to study or practise cyber operations in isolation appears to be gaining currency. Proponents of CPT increasingly emphasise

48 Jason Healey, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace', *Journal of Cybersecurity* (Vol. 5, No. 1, 2019), p. 12.

49 MoD, *Defence in a Competitive Age*, CP 411 (London: The Stationery Office, 2021), pp. 15–19.

50 Eric Robinson et al., *Strategic Disruption by Special Operations Forces: A Concept for Proactive Campaigning Short of Traditional War* (Santa Monica, CA: RAND, 2023).

51 History Does You, 'Strategic (Drone) Bombing: What Can It Do?', Substack newsletter, 19 November 2025, <https://secretaryrofdefenserock.substack.com/p/strategic-drone-bombing-what-can>, accessed 27 February 2026.

52 Jason Healey and Robert Jervis, 'The Escalation Inversion and Other Oddities of Situational Cyber Stability', *Texas National Security Review* (Vol. 3, No, 4, 2020), pp. 30–53.

the construct of contingency campaigning, described in one account as 'linked cyber operations and *activities conducted below the use-of-force* threshold'.[53] These other activities look very much like broader aspects of statecraft that are downplayed by a focus on cyber as a novel and distinct strategic environment.

Fischerkeller, Goldman and Harkett and others explore contingency campaigning using the case study of Ukraine's activities ahead of Russia's full-scale invasion in 2022.[54] Examples of contingency campaigning cited include Ukraine's efforts to build strong relationships with other states and with the private sector, as well as its efforts to build resilient telecommunications infrastructure. These are the same activities undertaken by Britain to secure and exploit its control of telegraph networks.

Where examples of contingency campaigning involve cyber operations, these blur the line separating them from cognitive effects. The authors offer the counterfactual hypothesis of Ukraine using 'cyber actions' to interfere with the 2021 *Zapad* exercises, thereby eroding Vladimir Putin's confidence in the Russian military, leading him not to pursue the invasion.[55] While the focus here is on cyber operations, in practice it is very likely that a decision-making change would involve the coordination of multiple non-cyber levers, as argued in this account by a GCHQ official: '[Peer competition in cyberspace] takes a lot more thinking, a lot more people, a lot more partnerships […] if you wanted to combine a démarche with a cyber operation to try and do a decision-making change that's bringing in quite a lot of UK government organisations'.[56]

The growing focus among proponents of CPT on campaigning suggests a recognition that cyber operations are not a novel arena of strategic competition, but rather continuous, with historical exploitation of technological systems and other aspects of contemporary statecraft. When we approach

53 Fischerkeller, Goldman and Harknett, 'NATO Must "Contingency Campaign" in Cyberspace'. Emphasis added.
54 *Ibid.*
55 *Ibid.*
56 Neil Ashdown, 'Advocates of Collaboration: Assembling Cyber Intelligence in the UK', PhD thesis, Royal Holloway University of London, 2024, p. 231.

the subject from this perspective, theories about the structure of the 'cyber strategic environment' appear less useful than specific questions about how actors with limited capabilities might realistically achieve certain desirable effects. The answers to these questions will be specific to countries, their capabilities, and their existing allies and partnerships.

## Dangerous Times Call for Pragmatism

The US alliance remains fundamental to the UK's defence and national security. Yet, at a time of jarring change in the world order, there is both an opportunity and a pressing need for the UK to chart its own course, even when travelling alongside allies and partners.

The UK's approach to cyber operations is a niche but important part of that wider debate. It is an area where academia, industry and civil society all have something to contribute. However, that contribution is unlikely to take the form of a well-funded research programme based on a structural theory of International Relations, and it is not clear what value another such theory would provide.

This does not mean that UK-focused research on cyber operations should shun CPT. Aspects of the theory resonate with the practitioners who engage in this work and with analyses of security in competition and crisis more broadly. Rather, a UK-focused approach should incorporate CPT and other work as part of a diverse, multidisciplinary engagement with the phenomenon of state exploitation of technology for strategic advantage.

Just as its small size and limited resources force the UK government and military offensive cyber community to adapt and act flexibly, so too the community of researchers working on the UK's approach may find advantages in its small size and haphazard blurring of disciplines. There will be benefits for the NCF in engaging with a messy academic field that seeks to explore multiple possibilities, through different methodologies, and guided by a range of lived experiences. The NCF is an organisation that 'derives strength from the diversity of its participants'.[57] At a time when the value of diversity is under attack, a commitment to a multiplicity of perspectives is important.

57 National Cyber Force, 'The National Cyber Force: Responsible Cyber Power in Practice'.

The UK has good reasons to be cautious of theories that proffer objective pronouncements based on structural claims about the 'cyber' environment. The last time the UK faced comparable upheaval, at the start of the 20th century, it was a great military and economic power that dominated critical information and communication technologies. But even in these favourable circumstances, Britain's military and intelligence services had to adapt rapidly as the country moved from competition and crisis into open conflict.

The UK in 2026 is facing a similarly worrying future from a far weaker position militarily, economically and technologically. These circumstances are likely to place an even greater premium on learning and adaptation. The NCF, born of counterterrorism operations against non-peer adversaries, will need to adapt to peer or more-than-peer warfare.[58] By 2035, the NCF may look as different from its current form as Bletchley Park looked in 1945 compared with 1939. Yet there are 'limits to pre-adaption'.[59] The goal now should be to posture the NCF so that it can innovate and adapt when crisis comes. That will require building an organisation that embraces conceptual and practical flexibility. There are lessons that can be drawn from history to help with that process. Equally, future historians will probably discover not the adoption of grand theories, but instead a familiar process of pragmatism, experimentation and fudge.

---

## About the Author


### Neil Ashdown

Neil Ashdown is the Head of Research for Tyburn St Raphael, a strategic advisory firm. He co-leads the UK Offensive Cyber Working Group. Neil completed his PhD at Royal Holloway University of London in 2024, where his thesis examined public–private collaboration on cyber intelligence in the UK. He was the deputy editor of *Jane's Intelligence Review* from 2014 to 2019.


58 Willett, *Cyber Operations and Their Responsible Use*.
59 Ferris, *Behind the Enigma*, p. 173.

CHAPTER 2

# From Compliance to Combat
## Building a Cyber and Electromagnetic Warfighting Culture

**Carolyn Swinney**

## The Strategic Defence Review Imperative

The Russo-Ukrainian War has offered important lessons for modern conventional warfare in Europe. The House of Lords referred to this as a 'wake-up call' in the title of its 2024 report,[1] challenging long-held UK assumptions. The report highlights significant findings for cyber and electronic warfare (EW). Russia's February 2022 full-scale invasion began with a cyberattack on Viasat, the satellite network providing Ukraine with internet connectivity. The UK National Cyber Security Centre (NCSC) assessed that the probable intent was to deny Ukrainian military communications, but the impact was much wider and included civilian and commercial users.[2] Cyber operations have also targeted critical national infrastructure, such as the December 2023 attack on Kyivstar, Ukraine's largest mobile network.[3]

However, despite expectations, cyber has not yet been decisive in the Russo-Ukrainian War in the way many analysts anticipated. Cyber operations have nonetheless been a persistent and consistent feature of Russian activity. Notably, the deployment of X-Agent malware against Ukrainian artillery units between 2014 and 2016 is assessed to have contributed significantly

1 House of Lords, International Relations and Defence Committee, 'Ukraine: A Wake-up Call', HL Paper 10, First Report of Session 2024–26, September 2024.

2 National Cyber Security Centre, 'Russia Behind Cyber Attack with Europe-Wide Impact An Hour Before Ukraine Invasion', news release, 10 May 2022, <https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion>, accessed 28 February 2026.

3 Alexander Kott et al., 'Russian Cyber Onslaught was Blunted by Ukrainian Cyber Resilience, not Merely Security', arXiv preprint, arXiv:2408.14667, 26 August 2024.

to the attrition of D-30 howitzer units,[4] suggesting meaningful tactical and operational effects in the earlier phase of the conflict. The picture of cyber's decisiveness is therefore more contested than the full-scale invasion alone implies. This is largely thought to be due to Ukraine's strong cyber defences, supported by a broad coalition including the NCSC,[5] other UK government agencies, Allied intelligence partners and commercial technology firms. With Russia considered 'the greatest single source of ongoing cyberattack against the UK', [6] the strength of UK cyber defences could carry major implications in future conflict.

EW has been used in Ukraine to detect, track and disrupt enemy systems, for example by identifying drone electronic signatures and jamming[7] their communication links. Electronic decoys have also been employed to mislead sensors.[8] Recent Russian military analysis characterises Ukraine as a transitional war fought on a transparent battlefield. There, massed drones, space and drone-based ISR and networked fires render traditional concentrations of force instantly targetable.[9] Future warfare will probably centre on how to command and control mass numbers of uncrewed systems with legacy military capabilities, and achieve information dominance – in narrative and in the electromagnetic (EM) spectrum – under conditions of near-constant surveillance.[10]

Beyond their individual effects, Russia has used increasingly integrated cyber and EM operations to blind Ukrainian command and control, degrade ISR – particularly using drones – and sharply reduce the effectiveness of precision munitions, directly shaping the tempo and outcome of key battles since 2022. This integration lets Russia synchronise jamming, spoofing and cyber

4 Thomas Withington, '68 Guns', *Armada International*, 2 December 2021, <https://www.armadainternational.com/2021/12/russian-cyber-warfare/>, accessed 8 March 2026.
5 Foreign, Commonwealth & Development Office, 'UK Boosts Ukraine's Cyber Defences with £6 Million Support Package', 1 November 2022, <https://www.gov.uk/government/news/uk-boosts-ukraines-cyber-defences-with-6-million-support-package>, accessed 28 February 2026.
6 House of Lords, International Relations and Defence Committee, 'Ukraine: A Wake-up Call'.
7 Jamming is a technique to overpower a legitimate signal to disrupt or deny those communications.
8 House of Lords, International Relations and Defence Committee, 'Ukraine: A Wake-up Call'.
9 Oscar Jonsson, 'A New Face of War: Russian Military Strategy Post-Ukraine', *NDC Outlook* (Vol. 2-26, February 2026).
10 Maria Engqvist (ed.), 'The Future of Warfare in Russian Military Thinking', *FOI-R* (No. FOI-R--5806--SE, 2026).

disruption with fires and manoeuvre, turning control of the EM spectrum into a foundational enabler of operational initiative and making it harder for Ukraine to sustain coherent, networked operations at scale.[11]

It is against this backdrop that the Strategic Defence Review (SDR) decision to integrate cyber and EM operations into a single, coordinated domain becomes clear. Within the proposed structure, the National Cyber Force (NCF) continues to deliver offensive cyber effects in support of Defence and wider national security objectives. However, its operational priorities are now set by the CyberEM Command on behalf of the Chief of the Defence Staff. The SDR proposed a CyberEM Command to coordinate, not execute, cyber and EM operations across Defence. This was later announced as the Defence Cyber and EM Force (DCEMF). The NCF is already operating at the intersection of the cultural tensions this chapter examines. The NCF's relationship with DCEMF will shape what that command becomes in practice. This chapter addresses the central question that treating cyber and EM as one domain raises: how can the UK develop a warfighting culture in a relatively new, multi-organisational domain?

## What DCEMF Actually Is: Capabilities, Distinctions and the Case for Integration

The SDR states that the cyber and electromagnetic (CyberEM) domain is to include offensive and defensive cyber operations as well as EW.

EW should not be confused with cyber capabilities. The two are doctrinally and technically distinct. Cyber operations are activities 'intended to preserve friendly freedom of action in cyberspace and/or to create effects to achieve commanders' objectives'.[12] EW, by contrast, uses directed energy to deny access to the EM spectrum, disrupting the signals that connect technologies and rendering them ineffective. While EW can interfere with digital infrastructure

11 Pasquale Iorillo and Rosario Maria Simonetti, 'Electromagnetic Operations in Ukraine: Lessons Learned, Capability Development and Future Implications', *RUSI Journal* (Vol. 170, No. 6/7, 2025), pp. 90–98.

12 NATO Standardization Office (NSO), 'Allied Joint Doctrine for Cyberspace Operations', Allied Joint Publication AJP-3.20, Edition A, Version 1, January 2020.

and therefore influence activity in cyberspace, the two disciplines operate through fundamentally different mechanisms.[13]

It should be clear that the CyberEM domain is an organisational construct for integration purposes, not due to the two disciplines being the same type of activity. This chapter uses EW for activities in the EM spectrum, 'offensive' and 'defensive' cyber for activities in and through cyberspace, and CyberEM only for the integrated UK construct that will cohere these capabilities across Defence. This is important. While the differences that this chapter explores matter for doctrine and governance, they should not obscure the tactical convergence between cyber and EW and the requirement for shared domain awareness. Proximal cyber techniques, which exploit physical proximity rather than network access, make early career literacy in these convergence areas a tactical necessity for warfare. The analysis now turns to a more detailed examination of these differences.

The UK NCF is 'responsible for operating in and through cyberspace to counter and contest those who would do harm to the UK or its allies'. [14] Unlike conventional military organisations, the NCF functions as a joint defence and intelligence partnership, with accountability shared between the foreign secretary and defence secretary.[15] Its blend of operational, intelligence and security expertise is intended to provide the UK with a competitive advantage over adversaries. Because NCF activities span government and are deeply intertwined with the intelligence community, they must align with wider national strategic priorities. This unique positioning also requires distinct legal and policy frameworks that differ from those governing traditional military operations.[16] The NCF is therefore not simply one component among others within the broader CyberEM landscape; it is the organisation whose professional identity, governance constraints and institutional origins most

13 NATO, 'Electromagnetic Warfare', updated 22 March 2023, <https://www.nato.int/en/what-we-do/deterrence-and-defence/electromagnetic-warfare>, accessed 15 February 2026.

14 National Cyber Force, 'National Cyber Force: Responsible Cyber Power in Practice', April 2023, <https://www.gov.uk/government/publications/responsible-cyber-power-in-practice>, accessed 2 January 2026.

15 National Cyber Force, 'About Us', Gov.uk, <https://www.gov.uk/government/organisations/national-cyber-force/about>, accessed 2 January 2026.

16 HM Government, 'National Cyber Strategy 2022: Pioneering a Cyber Future with the Whole of the UK', December 2022.

clearly embody the cultural challenge the whole command must navigate. But these are not the only differences.

Cyber impacts grow, along with their complexity, through the operational and strategic levels of war. For instance, Stuxnet's true value lay in the strategic undermining and delaying of a state's nuclear programme,[17] rather than tactically degrading centrifuges. Aaron F Brantly and Nataliya D Brantly's analysis of offensive cyber operations during the Russia–Ukraine conflict found that cyberattacks typically targeted soft systems and, particularly in the full-scale invasion phase, proved less suited to generating reliable short-term tactical effects than many anticipated.[18] This picture however does not reflect earlier operations where the deployment of X-Agent against Ukrainian artillery units before 2022[19] suggests that precision cyber operations can produce meaningful tactical effects when conditions are right. Moreover, cyberattacks have been used to support air defence suppression missions such as during Operation *Orchard*, an Israeli Air Force operation, where cyber and EW capabilities are reported to have been used to compromise the Syrian air defence radar system, allowing airstrikes to proceed[20] by presenting radar operators with a false picture.[21]

It is important to note that such tactical examples are rare and sometimes contested in detail. Nonetheless, the point stands that, as Paul Withers states, offensive cyber effects for military gain do not replace air, land and maritime activities but are best employed by supplementing them.[22] So offensive cyber operations exhibit a distinctive duality; they can deliver profound

17 Claudia Emilie Aanonsen, 'Stuxnet, Revisited (Again): Producing the Strategic Relevance of Cyber Operations', *Journal of Cyber Policy* (Vol. 10, No. 1, 2025), pp. 68–84.

18 Aaron F Brantly and Nataliya D Brantly, 'The Bitskrieg That Was and Wasn't: The Military and Intelligence Implications of Cyber Operations During Russia's War on Ukraine', *Intelligence and National Security* (Vol. 39, No. 3, 2024), pp. 475–95.

19 Withington, 'Russian Cyber Warfare'.

20 NATO Cooperative Cyber Defence Centre of Excellence, 'Operation Orchard/Outside the Box (2007)', International Cyber Law: Interactive Toolkit, last modified 17 September 2021, <https://cyberlaw.ccdcoe.org/wiki/Operation_Orchard/Outside_the_Box_(2007)>, accessed 1 February 2026.

21 *Airforce Technology*, 'The Israeli "E-tack" on Syria – Part II', 10 March 2008, <https://www.airforce-technology.com/features/feature1669/>, accessed 1 February 2026.

22 Paul Withers, 'Do We Need an Effects-Based Approach for Cyber Operations?', in Tim Stevens and Joe Devanny (eds), *Research Handbook on Cyberwarfare* (Cheltenham: Edward Elgar Publishing, 2024), pp. 205–22.

operational and strategic effects, but can also be critical to the manoeuvre and survivability of tactical air, land and maritime operations during conflict.

In the model set out in the SDR,[23] DCEMF acts as the central authority for CyberEM activity incorporating NCF into a coherent, joint Defence portfolio, setting Defence-wide priorities and allocating limited DCEMF resources. At the same time, the NCF continues to 'operate' offensive cyber capabilities as a joint Defence Intelligence organisation, accountable to both the Foreign, Commonwealth & Development Office and the Ministry of Defence (MoD) under its principles of being 'accountable, precise, and calibrated'.[24]

In contrast, EW is most commonly integrated at the tactical level in support of air, land and maritime operations. This is where much of its immediate value lies. Examples include disrupting drone control signals[25] to protect ground forces or injecting false data to disrupt an adversary's maritime situational awareness.[26] However, sustained EM operations can generate effects at the operational and strategic levels. For example, during Operation *Desert Storm*, coalition EW, particularly in support of air operations, was a key enabler of the coalition's ability to achieve and sustain air superiority, contributing directly to the campaign's outcome.[27] Lessons from Ukraine further underscore its critical role and the importance of integrated EW for future conflicts.[28]

With defensive cyber operations, warfighting capabilities also enable tactical air, land, maritime and space missions. Larger nations such as the US have also invested in defensive strategic campaigns of persistence, to compete and contest with adversaries.[29] In this context, US Cyber Command

23 Ministry of Defence (MoD), 'The Strategic Defence Review 2025: Making Britain Safer: Secure at Home, Strong Abroad', June 2025, p. 121.
24 National Cyber Force, 'National Cyber Force: Responsible Cyber Power in Practice', p. 14.
25 House of Lords, International Relations and Defence Committee, 'Ukraine: A Wake-up Call'.
26 Dom, 'Emerging Cyber Threats in the Maritime Domain: AIS Spoofing and Infrastructure Vulnerabilities', *Spheira*, 24 April 2025, <https://www.spheira.ca/emerging-cyber-threats-in-the-maritime-domain-ais-spoofing-and-infrastructure-vulnerabilities/>, accessed 28 February 2026.
27 Thomas A Keaney and Eliot A Cohen, *Gulf War Air Power Survey: Summary Report* (Washington, DC: US Government Printing Office, 1993).
28 Daniel Sullivan, Riley Murray and Rylan Neely, 'Lessons from the Frontlines: Ukrainian SEAD Operations and Their Implications for Western Special Operations Forces', Irregular Warfare Initiative, 6 February 2025, <https://irregularwarfare.org/articles/ukrainian-sead-operations-lessons-for-western-sof/>, accessed 4 January 2026.
29 US Government Accountability Office, 'DOD Cyberspace Operations: About 500 Organizations

(USCYBERCOM) operates as a centralised mission authority which sets missions down to tactical units within the military commands. However, US military commands still retain a separate and larger number of their own personnel to service their own tactical priorities which are not centralised.[30] While this model works for the US because of its vast resources,[31] it would be far more difficult for smaller nations to implement with limited capacity.

The US approach of retaining substantial cyber and EW capability within military commands alongside centralised strategic missions reflects the inherently domain-specific character of EW and defensive cyber operations, which depend on deep air, maritime and land expertise. For instance, air defensive cyber operators must assess mission-system air safety risks while maritime defensive cyber operators are experts in operational technology to ensure ships remain mission capable. Land EW teams concentrate on intercepting and jamming command and control networks, artillery radios and IED triggers, also factoring in terrain and power constraints,[32] and airborne EW operators conduct missions across wider areas and understand key limitations such as aircraft endurance. In the maritime environment, EW plays a critical role in detecting and countering radar-guided anti-ship missiles,[33] where the speed of engagement leaves little margin for error. Counter-UAV and Global Navigation Satellite System denial have also become core EW mission sets across the land[34] and maritime domains, as adversaries increasingly exploit low-cost uncrewed systems and precision navigation. Ultimately, effective integration of cyber and EW capabilities for military advantage depends on robust air, land and maritime domain expertise.

Have Roles, with Some Potential Overlap', GAO-25-107121, September 2025, <https://www.gao.gov/assets/gao-25-107121.pdf>, accessed 5 January 2026.

30 Jacquelyn G Schneider et al., *Ten Years In: Implementing Strategic Approaches to Cyberspace*, Newport Papers No. 45 (Newport, RI: US Naval War College Press, 2020).

31 Out of 61,000 Department of Defense cyberspace operators, 14,542 were aligned to USCYBERCOM. The rest served the single services. See US Government Accountability Office, 'DOD Cyberspace Operations'.

32 John R Hoehn, 'Defense Primer: Electronic Warfare', CRS In Focus, IF11118, version 13, updated 14 November 2022, <https://www.congress.gov/crs_external_products/IF/PDF/IF11118/IF11118.13.pdf>, accessed 20 March 2026.

33 Defence Science and Technology Laboratory, 'Transforming the Royal Navy's Electromagnetic Warfare Capabilities', case study, Gov.uk, 13 May 2025, <https://www.gov.uk/government/case-studies/transforming-the-royal-navys-electromagnetic-warfare-capabilities>, accessed 21 March 2026.

34 Jack Watling and Noah Sylvia, 'Competitive Electronic Warfare in Modern Land Operations', *RUSI Occasional Papers* (January 2025).

As Withers argues, this necessitates a workforce model in which deep cyber specialists are embedded within air operations, alongside airpower professionals who progressively build cyber awareness over the course of their careers.[35]

The rationale for integrating offensive and defensive cyber operations and EW under a single command is worth stating explicitly, since it is not self-evident given that these disciplines are doctrinally and technically distinct. Two main drivers appear to underpin the SDR's decision. First, coherence: by setting Defence-wide priorities across CyberEM from a single authority, the command enables integrated effects that would otherwise require complex inter-service coordination. Coherence is particularly significant for the NCF, whose dual accountability to the foreign secretary and the defence secretary means its operational priorities have historically been set partly outside the Defence chain of command. DCEMF's role in setting NCF's Defence priorities is therefore not merely administrative; it is the mechanism by which offensive cyber effects are brought into genuine alignment with joint warfighting requirements. Second, and perhaps most significantly, representation: placing DCEMF at the command level within Defence signals institutional parity with air, land, maritime and space, giving the domain a political and budgetary voice it has historically lacked. DCEMF is therefore less an operational executor than an orchestrator and advocate, a distinction that has direct implications for the kind of culture it needs to cultivate.

## How Military Organisational Cultures Form and Why DCEMF Is Different

Military domains originally emerged to reflect the geographical separation of military operations. They shaped military structures that were optimised for tactical excellence. Today, an 'operational domain' is defined by NATO as 'an artificial construct intended to aid understanding and to reflect Defence perceptions on how things should be organised'.[36] The term 'Cyber and Electromagnetic domain' was first seen in 2018 in conceptual work on UK Information Advantage (JCN 2/18). In 2022, it was formalised into UK Defence

35 Paul Withers, 'Integrating Cyber with Air Power in the Second Century of the Royal Air Force', *Air Power Review* (Vol. 21, No. 3, Autumn/Winter 2018), pp. 132–59.

36 MoD, 'Cyber Primer', 3rd edition, 4 October 2022.

Doctrine (JDP 0-01, 6th edition). It is described as 'a domain comprising of capabilities which enable activities that maintain freedom of action by creating effects in and through cyberspace and the electromagnetic spectrum'.[37] However, the designation of the EM spectrum as a warfighting domain in its own right remains contested in some quarters.[38] Some argue that the EM spectrum is better understood as a cross-cutting operational enabler than a domain equivalent to air, land or maritime.[39] The UK's SDR position is taken here as the working framework, but this chapter's cultural argument does not depend on resolving this doctrinal question.

Before proceeding, it is necessary to be precise about what 'culture' means in this context, as the chapter uses the term in three related but distinct senses. 'Organisational culture', following the work of Edgar Schein, refers to the shared assumptions, values and artefacts that shape behaviour within a specific institution which is the primary lens applied to the RAF, Space Command and DCEMF in this section. 'Strategic culture', drawn from Elizabeth Kier's work, operates at a higher level of abstraction. It describes the historically embedded assumptions within a military or national security establishment about the utility of force and the nature of threat. Such assumptions shape what options appear politically and institutionally possible. This is the focus of the following section. 'Warfighting culture', the normative goal of this chapter's argument, describes the operational disposition for the acceptance of bounded risk, the prioritisation of mission effect, and the mindset that distinguishes combat-oriented organisations from those oriented around compliance and risk reduction. These concepts are related but not the same, and the chapter flags where the analysis moves between them.

The NCF illustrates why this precision matters. As a joint defence and intelligence organisation accountable to two secretaries of state, it occupies a position in which strategic culture – the institutional assumptions about the legitimate use of offensive cyber effects – directly shapes what operational culture is permitted to look like within it. Understanding how these three levels

37 *Ibid.*

38 John A Tirpak, 'EMS Not Its Own Domain of Warfare, Strategy Implementer Says', *Air & Space Forces Magazine*, 15 November 2020, <https://www.airandspaceforces.com/ems-not-its-own-domain-of-warfare-strategy-implementer-says/>, accessed 8 March 2026.

39 Garrett K Hogan, 'The Electromagnetic Spectrum: The Cross Domain', *Joint Air Power Competence Centre (JAPCC) Journal* (No. 21, November 2015), pp. 11–16.

interact is therefore an essential precondition for designing a DCEMF that can articulate a clear demand signal to the NCF without either eroding the NCF's distinctive character or allowing its pre-existing culture to become the default model for the wider command.

Parallels for DCEMF can be drawn with the declaration of space as a domain. In 2019, NATO designated space as an operational domain, and the UK subsequently established the MoD Space Directorate and UK Space Command in 2021 to protect national space interests. The SDR 2025 states that the CyberEM domain should be led similarly, centralising authorities and decision-making to reduce duplication and increase efficiency.[40] Forming a DCEMF will probably face institutional challenges similar to Space Command's and those encountered during the formation of the RAF in 1918, when fundamental questions emerged about the purpose of airpower and how it differed from Army and Navy aviation.

The RAF was created by merging the Royal Flying Corps (RFC) and the Royal Naval Air Service (RNAS). Before becoming an independent force, control of the air already played a vital enabling role, supporting ground reconnaissance, artillery observation and land attack.[41] However, poor coordination between the British Army and Royal Navy led to inefficiencies in the allocation of aircraft in the war and in the procurement of new aircraft. In response, the prime minister appointed Field Marshal Jan Smuts to conduct an independent review. Drawing heavily on the ideas of the first commander of the RFC, Smuts endorsed the creation of a separate air force that could support maritime and land operations, but also deliver independent air effects.[42] Today, airpower operates as both a supporting function and a strategic instrument capable of independent impact, including providing capabilities such as deep strike and deterrence. The relevance for DCEMF is not that it should emulate airpower, but that cultural identity, once embedded, defines how an organisation perceives risk, authority and legitimacy in war.

40 MoD, 'Strategic Defence Review 2025', p. 122.

41 David Jordan, 'Learning to Fly: The Royal Flying Corps and the Development of Air Power', *British Journal for Military History* (Vol. 4, No. 2, 2018), pp. 8–31.

42 Sebastian Cox, 'The Birth of the Royal Air Force', *History of Government* blog, 1 April 2018, <https://history.blog.gov.uk/2018/04/01/the-birth-of-the-royal-air-force/>, accessed 20 March 2026.

Structural changes were undoubtedly necessary when the decision to form the RAF was made but authors such as Ross Mahoney assess that it was ultimately the cultivation of a distinct RAF culture that ensured the organisation's long-term survival.[43] Edgar Schein's influential model describes organisational culture as functioning across three levels.[44] The first level comprises visible artefacts. These are tangible and observable features, such as uniforms or the RAF's early specialist training pipelines at RAF Halton and the RAF College Cranwell. The second level of Schein's model consists of espoused beliefs and values, reflected in the RAF's emerging sense of professional pride and Hugh Trenchard's[45] advocacy for an 'Air Force Spirit', which helped to distinguish the service from its naval and army origins.[46]

The third level, basic underlying assumptions, encompasses the deeply embedded beliefs that unconsciously shape behaviour. In the early RAF, these assumptions were inherited from the RFC and the RNAS. The RFC carried forward broader Army cultural norms, while the RNAS brought a more innovation-driven identity shaped by its experimental naval heritage. Despite differences, both communities shared a growing 'aviator' identity rooted in risk-taking and a perception of elite status. When the services merged, these service assumptions persisted, creating friction visible in reactions to the new uniform and with tensions among senior leaders.[47] This illustrates how underlying assumptions can influence actions even when they conflict with an organisation's stated beliefs or values.

A similar dynamic can be seen in the development of UK Space Command which, although conceived as a joint organisation, had nearly 70% of its

43 Ross Mahoney, 'Trenchard's Doctrine: Organisational Culture, the "Air Force Spirit" and the Foundation of the Royal Air Force in the Interwar Years', *British Journal for Military History* (Vol. 4, No. 2, 2018), pp. 143–77.

44 Edgar H Schein, *Organizational Culture and Leadership*, 3rd edition (San Francisco, CA: Jossey-Bass, 2004), pp. 10–11.

45 Hugh Trenchard (1873–1956), first Chief of the Air Staff and founding commander of the RAF, is widely regarded as the 'Father of the RAF'. As the RAF's dominant figure during the interwar period, he shaped its doctrine, culture and institutional identity through sustained advocacy for air power as an independent strategic instrument.

46 Fin Monahan, 'The Origins of the Organisational Culture of the Royal Air Force', PhD thesis, University of Birmingham, 2018, <https://etheses.bham.ac.uk/id/eprint/8306/1/Monahan18PhD.pdf>, accessed 20 March 2026.

47 Mahoney, 'Trenchard's Doctrine'.

workforce drawn from the RAF.[48] The organisation fostered a new culture by introducing visible artefacts such as the 'Space Operator' badges and specialised stable belts, to differentiate its personnel from the wider Defence community.[49] In an interview in March 2021, the inaugural commander of Space Command characterised its espoused beliefs and values as centred on collaboration and enablement.[50] Space Command also contends with a broader cultural context; while UK doctrine recognises space as both a domain and an enabler, Defence still tends to treat it as the latter.[51]

Similarly, during the First World War, control of the air was primarily understood as an enabling function, supporting ground reconnaissance, artillery observation and land attack.[52] It was only after the war, most notably through Giulio Douhet's 1921 advocacy of an independent air command and autonomous effects such as strategic bombing,[53] that wartime experience translated into meaningful organisational reform. By contrast, cyber and EM operations are already active and contested, both above and below the threshold of armed conflict, as illustrated by both the Russo-Ukrainian War and by UK parliamentary warnings on the rising frequency of attacks to the UK homeland outside of traditional conflict.[54] As DCEMF is designed and formed under the SDR, the opportunity therefore exists to shape organisational culture deliberately from the outset, rather than allowing inherited assumptions to take hold.

## Strategic Culture and Institutional Inertia

The analysis now moves from organisational culture, the internal dynamics of how institutions form and sustain shared assumptions, to strategic culture, a distinct concept that operates at the level of established national and

48 Juliana Suess, 'Between Ambition and Reality: How Space Fits into the UK Defence Framework', *RUSI Emerging Insights* (July 2024).

49 RAF, 'UK Space Command Officially Launched', news article, 30 July 2021, <https://www.raf.mod.uk/news/articles/uk-space-command-officially-launched/>, accessed 20 March 2026.

50 War Studies KCL, 'In Conversation with the UK's Leading Space Commanders', YouTube, <https://www.youtube.com/watch?v=kbP_L9jKXJM>, accessed 2 February 2026.

51 Suess, 'Between Ambition and Reality'.

52 Jordan, 'Learning to Fly'.

53 Giulio Douhet, *The Command of the Air*, translated by Dino Ferrari (Maxwell Air Force Base, AL: Air University Press, 2019).

54 House of Commons Defence Committee, 'Defence in the Grey Zone', HC 405, Fifth Report of Session 2024–25, July 2025.

institutional dispositions towards the use of force. Elizabeth Kier's foundational argument is that facts are always interpreted through cultural lenses, and that military organisations act on the worldview that their culture provides, determining what options appear possible while rendering others invisible.[55] Applied to DCEMF, this insight has immediate force: the question is not only what kind of organisation DCEMF should be, but what the surrounding institutional culture will permit it to become.

The US EW enterprise illustrates this directly. Despite sustained advocacy in parts of the enterprise for organisational reform,[56] the US has not established a dedicated combatant command for Electromagnetic Spectrum Operations equivalent to USCYBERCOM. Viewed through Kier's lens, this is not primarily a resource or capability failure. It reflects the fact that the military commands – which have long regarded EW as domain-specific rather than joint, taking a 'platform-by-platform approach'[57] – have not recognised a centralised EW command as a legitimate or necessary option. The institutional worldview that EW belongs to the military service, not to a joint command, has rendered the alternative functionally invisible. The UK's decision to coalesce CyberEM under a single command therefore represents a structurally bolder departure from the US approach and one that directly challenges that inherited assumption.

The US debate over establishing a dedicated Cyber Force reveals the same dynamic operating at a different level. Senior practitioners caution that this approach risks treating the symptoms rather than the underlying issue: cyber is not the top priority for any existing military service, resulting in inconsistent recruitment, training standards and, subsequently, retention.[58] Similarly in the UK, cultural prioritisation has been observed to be the primary barrier to the

55 Elizabeth Kier, 'Culture and Military Doctrine: France Between the Wars', *International Security* (Vol. 19, No. 4, Spring 1995), pp. 65–93.

56 US Government Accountability Office, 'Electromagnetic Spectrum Operations: DOD Needs to Address Governance and Oversight Issues to Help Ensure Superiority', GAO-21-64, December 2020, <https://www.gao.gov/assets/720/711469.pdf>, accessed 21 March 2026.

57 John Knowles, 'Congressional Electromagnetic Warfare Working Group Discusses EMSO Priorities', *Journal of Electromagnetic Dominance*, 24 July 2023, <https://www.jedonline.com/2023/07/24/congressional-electromagnetic-warfare-working-group-discusses-emso-priorities/>, accessed 21 March 2026.

58 Shaun Waterman, 'Can the Latest Plan for CYBERCOM Stave Off Calls for a New Service?', *Air & Space Forces Magazine*, 16 November 2025, <https://www.airandspaceforces.com/cybercom-force-generation-plan-new-service/>, accessed 16 February 2026.

Army's adoption of EW.[59] In both cases, the constraint is not technical but cultural; existing services interpret the problem through a lens that does not register cyber or EW as a primary mission, and so consistently underweight it in competition for resources and talent.

John Fernandes and others extend this analysis to the individual level. They compare traditional Army culture with an emerging cyber culture across factors such as physical fitness norms, expendability and austere living. Their work argues that forming a Cyber Force from five services would require deliberate and sustained effort to build a cohesive culture.[60] The difficulty is precisely that personnel arrive already shaped by institutional worldviews and they carry with them assumptions about what military service looks like, what counts as operational success, and what risks are acceptable. These assumptions do not dissolve on transfer; they persist as the basis from which any new organisation must build.

This persistence is what Thomas U Berger's study of post-Second World War Germany and Japan makes concrete: deeply embedded identities shape decisions as 'common sense' for generations, long after the conditions that produced them have changed.[61] Once a service is organised around a domain, its identity becomes entrenched and resistant to reform. This is not inherently negative; shared cultural symbols foster unit cohesion, strengthen morale and reinforce belief in the mission. However, the consequence is that historical decisions have done much more than define organisational structures. They have established cultural identities that still fundamentally shape military behaviour today, creating long-term patterns of behaviour that are difficult to alter: what is commonly called path dependence. The formation of the NCF in 2020 provides a clear illustration. Established by bringing together personnel from GCHQ, the MoD and the Secret Intelligence Service, the NCF pre-dates the announcement and creation of a DCEMF. As such, its cultural foundations were shaped independently of any joint warfighting framework. Applying Kier's argument, the issue is therefore not

59 Watling and Sylvia, 'Competitive Electronic Warfare in Modern Land Operations'.

60 John Fernandes, Erica D Lonergan and Alexander Master, 'Why Culture Matters: Organizational Culture and Force Generation for the Cyber Domain', *Cyber Defense Review* (Vol. 10, No. 3, 2025), pp. 127–45.

61 Hans W Maull, review of *Cultures of Antimilitarism: National Security in Germany and Japan*, by Thomas U Berger, *Pacific Affairs* (Vol. 73, No. 1, Spring 2000), pp. 118–19.

whether the NCF possesses a culture. Rather, it is whether the worldview that culture provides – and the assumptions about governance, risk and what operational success looks like – is the right one for the integrated domain the SDR now demands.

The potential for institutional inertia becomes even clearer when examining how different organisational subcultures interact. James Q Wilson's 'Bureaucracy' identifies operators, executives and managers as distinct subcultures,[62] with managers bridging the gap between operators and executives. In the military, officers often play this bridging role. The NASA Challenger disaster illustrates what happens when the bridge between subcultures collapses: operator warnings about O-ring failures never reached the executives who authorised the launch.[63] This was an organisational failure later attributed to path dependence and the 'normalisation of deviance',[64] a direct consequence of a cultural worldview that had made certain warning signals effectively unreadable to decision-makers.

Path dependence does not operate only within organisations; it is also reinforced externally by society and by the nature of the threats a nation faces. Philip Davies and Toby Steward warn that, before the Russo-Ukrainian War, UK and US doctrine was shaped heavily by counterterrorism and counterinsurgency (COIN), leaving both countries poorly prepared for high-intensity conflict with strategic peers.[65] Decades of focus away from peer-level threats created a peacetime mindset oriented around safety, certainty and risk avoidance. Even with the shift towards multidomain doctrine, some analysts argue that the UK has simply applied multidomain labels retrospectively to COIN practices rather than reorienting its force structure for great power competition.[66] In Kier's terms, the espoused beliefs changed, the

62 James Q Wilson, *Bureaucracy: What Government Agencies Do and Why They Do It* (New York, NY: Basic Books, 1989).

63 US House of Representatives, Committee on Science and Technology, 'Investigation of the Challenger Accident', House Report 99-1016, 99th Congress, 2nd Session, 29 October 1986.

64 Joseph Lorenzo Hall, 'Columbia and Challenger: Organizational Failure at NASA', *Space Policy* (Vol. 37, No. 3, 2016), p. 127.

65 Philip H J Davies and Toby J Steward, 'The Trouble with TESSOC: The Coming Crisis in British and Allied Military Counterintelligence Doctrine', *Defence Studies* (Vol. 24, No. 2, 2024), pp. 234–56.

66 David Morgan-Owen, Aimée Fox and Alex Gould, 'Sources of Military Change: Emulation, Politics, and Concept Development in UK Defence', *British Journal of Politics and International Relations* (Vol. 26, No. 3, 2024), pp. 864–85.

language updated but the underlying assumptions, and with them the option space available to commanders, did not.

This is precisely the danger that now faces DCEMF. Cultural dynamics often become most visible where different professional communities intersect, and in cyber and EM, this is where assurance-driven norms meet the requirements of a warfighting mindset. If the institutional worldview that shapes DCEMF is drawn primarily from assurance and compliance cultures, then Kier's argument predicts the result: not outright failure, but a quiet narrowing of what appears possible. The result is a cultural fault line that reveals why integrating cyber and EM is uniquely challenging, and why these tensions may undermine military effectiveness more profoundly than any technical barrier.

## The Assurance–Operations Fault Line

Warfighting culture, the operational disposition that accepts bounded risk and prioritises mission effect over procedural conformity, is most clearly understood by examining where it is absent. While EW in the UK has long sat within the military's operational community, responsibility for cyber naturally emerged within the J6[67] community because of its technical grounding in communications and networks. Today, most military cyber specialists originate from assurance roles outside of operational planning functions (J3-Operations, J35-Operations Planning, J5-Strategic Planning).[68] As a result, any new organisational construct will probably inherit a compliance background which contrasts with a warfighter mindset.[69]

EW and offensive and defensive cyber operations require highly skilled operators who are normally limited in number and must be carefully prioritised. Their focus is not on protecting or enabling everything (an impossible task) but on achieving mission success for priority missions across the air, land, maritime and space domains. When the NCF was established in 2020, bringing together personnel from GCHQ, the MoD and the Secret Intelligence Service, it formalised the shift towards operational offensive cyber activity.

67 Specialists in communications, computers and signals.

68 Operations-focused roles: J3 – operations; J35 – operations and planning; J5 – planning.

69 Alan Mears and Wayne Loveless, 'Beyond Cyber Security – Integrated Defensive Cyberspace Operations', *Wavell Room*, 14 April 2022, <https://wavellroom.com/2022/04/14/beyond-cyber-security-integrated-defensive-cyberspace-operations/>, accessed 20 March 2026.

Tensions were anticipated at the NCF's inception, noting the probable friction associated with integrating personnel from different professional cultures and accountability frameworks into a single joint organisation.[70] Yet since then, there has been little public visibility of how MoD staff from assurance backgrounds adapted to operational roles, or how these cultural frictions were managed during the transition.

This distinction with the NCF reflects a broader structural pattern across NATO doctrine, which similarly separates effect-generating cyber roles from communications, information and security (CIS) assurance functions. NATO's Allied Joint Doctrine 3.20 describes cyberspace operations designed to generate effects that support a commander's objectives, while CIS focuses on safeguarding systems through confidentiality, integrity and availability. However, while separated doctrinally, AJP-6 positions defensive cyber and CIS together under the broader C5i[71] construct, which is organisationally placed under J6 enabling staff responsible for assessing CIS and cyber requirements within the Operational Order.[72]

Why does it matter? While it may not manifest as acutely in peacetime, lessons from the war in Ukraine indicate that military planning is strengthened by adopting agile methodologies that enhance responsiveness.[73] In wartime, conventional management approaches quickly become insufficient; under the pressures of conflict, risk-taking becomes a driver of adaptation and transformation rather than something to avoid.[74] Assurance culture, however, is oriented towards minimising risk through compliance and standardisation, with success measured by audits and incident reduction. Operational warfighting cultures differ fundamentally: they accept bounded risk, prioritise agility, and measure success by mission outcomes rather than procedural conformity. The practical difference between these cultures is often visible in

70 Joe Devanny et al., 'The National Cyber Force That Britain Needs?', KCL Cyber Security Research Group, April 2021.

71 Covering defensive cyber, command, control, communications, computers and information.

72 NSO, 'Allied Joint Doctrine for Communication and Information Systems', Allied Joint Publication AJP-6 Edition B, Version 1, with UK national elements, April 2024, pp. 85–92.

73 Ionuț-Alexandru Radu, 'Using Agile Project Methodologies in Military Action Planning', *Bulletin of 'Carol I' National Defence University* (Vol. 14, No. 2, 2025), pp. 311–25.

74 Mykola Pugachov et al., 'Effectiveness of the Management System in the Conditions of Military Operations and Crisis Situations', *Design, Construction, Maintenance* (Vol. 3, 2023), pp. 152–59.

planning outputs: compliance-oriented teams tend to open briefs with what others must provide, rather than with what they themselves can do to posture effectively. The contrast between asking 'what do we need from others?' and 'what can we do?' is a reliable indicator of whether a warfighting mindset has taken hold.

If the cultural balance is misjudged, the operational consequences could be severe. A DCEMF shaped by assurance-oriented mindsets would approach cyber and EW effects through the lens of risk reduction rather than mission delivery. Actions that should be pre-delegated may instead remain subject to high-level approval. In the UK, NCF activities already require ministerial authorisation, with joint accountability held by the defence secretary and the foreign secretary, one of the most stringent governance regimes globally.[75] While appropriate in peacetime, such processes would impede operational integration during peer conflict unless authorities were delegated in advance. Michael P Carvelli highlights similar challenges in the US, where limited delegation of cyber authorities creates operational hesitation and delays.[76] Similar observations about risk perception and the cultural constraints on offensive cyber have been made elsewhere,[77] suggesting this is a recognised pattern rather than a UK-specific pathology.

This risk-averse framing stands in stark contrast to the expectations of EW operators, who must be enabled at the tactical level to respond rapidly to emerging threats.[78] As seen in Ukraine, timely deconfliction of CyberEM activities is essential, yet an assurance-driven culture may slow these processes by prioritising safety and compliance over mission tempo. These delays are not abstract concerns. On a transparent battlefield where Russian practice has shown that targeting cycles are measured in minutes,[79] bureaucratic friction will quickly translate into tactical defeat.

75 National Cyber Force, 'The National Cyber Force: Responsible Cyber Power in Practice', p. 22.

76 Michael P Carvelli, 'A Smarter Approach to Cyber Attack Authorities', *Joint Force Quarterly* (No. 91, 4th Quarter 2018), pp. 67–73.

77 Juliet Skingsley, *Offensive Cyber Operations: States' Perceptions of Their Utility and Risks* (London: Chatham House, 2023), Chapter 3.

78 Conner Bender, 'Rebuilding Combat Electromagnetic Warfare for U.S. Ground Forces', Irregular Warfare Initiative, 19 August 2025, <https://irregularwarfare.org/articles/combat-electromagnetic-warfare-us-ground-forces/>, accessed 20 March 2026.

79 Kateryna Bondar, 'How Russia Is Reshaping Command and Control for AI-Enabled Warfare', Center for Strategic and International Studies, February 2026, <https://www.csis.org/analysis/

The SDR signals a practical shift towards separating operational effects from assurance functions. It places support, Defence Digital[80] and service-agnostic capabilities under the responsibility of the National Armaments Director (NAD), while assigning DCEMF responsibility for cohering offensive and defensive cyber operations and EW.[81] Although this is an important step forward, it does not eliminate the risk that a new DCEMF could still inherit an assurance-oriented culture after years of cyber activity being embedded within the J6 community. Such a shift could create challenges for EW operators, who bring decades of tactically integrated experience from their respective military commands.

An equally concerning risk is cyber missions being led by operators who lack an understanding of the computer-science fundamentals that underpin cyber operations, or who treat cyber as a supporting function confined to annexes of the Operational Order.[82] This problem is less acute in EW, where physics is embedded from the outset.[83] This exposes the central dilemma: whether it is easier to train operators in technical fundamentals or to shift assurance-focused personnel towards an operational mindset. Current cyber training pipelines prioritise technical proficiency, but proficiency and operational disposition are not the same. Optimising for the former risks repeating the cultural error this chapter identifies and the unresolved challenge of how to develop senior leaders and a culture that embodies a genuine CyberEM warfighting mindset.

To return to Kier's argument, a leader shaped by an assurance-driven worldview may not only move more slowly through a decision cycle, but they may also fail to recognise viable operational options altogether. The issue is therefore not just speed, but awareness of the full spectrum of choices. A commander whose career has been built within a compliance-oriented

how-russia-reshaping-command-and-control-ai-enabled-warfare>, accessed 28 February 2026.

80 Responsible for making sure that effective digital and information technology is put into the hands of the military and business frontline. See Gov.uk, 'Defence Digital', <https://www.gov.uk/government/groups/defence-digital>, accessed 20 March 2026.

81 MoD, 'The Strategic Defence Review 2025'.

82 Mears and Loveless, 'Beyond Cyber Security'.

83 Inzpire, 'Inzpire Delivers a Fresh Approach to Electromagnetic Warfare Training', News & Insights, 11 June 2024, <https://www.inzpire.com/news/inzpire-delivers-a-fresh-approach-to-electromagnetic-warfare-training>, accessed 25 January 2026.

culture may instinctively treat offensive capabilities as risks to be contained rather than effects to be directed, meaning high-risk, high-reward opportunities may not even register as legitimate courses of action.

This risk becomes particularly acute if J6 personnel form the recruitment baseline for a DCEMF, as they are accustomed to answering questions which were designed for a different problem set. Consequently, the earlier question of whether it is easier to teach operators computer science fundamentals or to retrain assurance specialists for operational roles becomes secondary to a more fundamental issue: who defines what 'good' looks like in the domain, and what problem is the organisation ultimately trying to solve? Answering that question requires deliberate cultural design. While many of the organisational and strategic tensions described above ultimately manifest along a single cultural fault line, history offers clear guidance on what deliberate cultural design demands.

## How Culture is Built and How it Goes Wrong

Meaningful cultural change, as Trenchard demonstrated with the formation of the RAF, depends on three core elements. First, personnel must understand the purpose behind the change – the 'why' – which requires a clearly articulated organisational mission. Trenchard's concept of an Air Force Spirit provided this clarity, giving personnel a distinctive identity that superseded loyalty to their parent organisations. Second, the organisation must invest in its people and capabilities so that stated intentions are matched by visible, practical action. Trenchard achieved this through the creation of specialist training pipelines at RAF Cranwell and RAF Halton. Third, leaders must consistently model the behaviours and identity those they seek to instil. Trenchard's 1925 Cambridge Address[84] exemplified this approach, as he championed the centrality of airpower to national defence to the wider public, rather than it just being a supporting function for the Army and Navy. Importantly, he shaped the RAF's culture from the outset,

84 Graham Wilf Taylor (wilf_san), 'The Royal Air Force at 7: Trenchard's Cambridge Address', post on Air Cadet Central, The Staff Mess forum, 29 December 2012, 6:23 pm, <https://forum.aircadetcentral.net/t/the-royal-air-force-at-7-trenchards-cambridge-address/265>, accessed 20 March 2026; Sophy Gardner, 'Whitehall Warriors: The Political Fight for the Royal Air Force, 1917–29', PhD thesis, University of Exeter, August 2019.

establishing deliberate foundations before inherited assumptions could take root.

The consequences of failing to do so are now illustrated by analysing what happened when a culturally embedded doctrine was transplanted from one theatre to another without anyone first asking whether it still fit the problem.

The period following the Anbar Awakening in Iraq (2006–08), and the subsequent transition to operations in Afghanistan, illustrate the risks of allowing culturally embedded doctrine to dominate military thinking. The perceived success of COIN in Al-Anbar produced a belief that 'population-centric' warfare was the correct model for modern conflict.[85] This shifted attention away from confronting or defeating an enemy and towards shaping civilian behaviour. When the US formalised this approach in its 2006 doctrine, it did more than codify a method; it created a professional identity. COIN was described as 'the graduate level of war',[86] implying that those who mastered COIN possessed a superior intellectual and professional standing compared with those who questioned it. This sense of confidence and identity became as influential as the doctrine itself.

Tim Bird and Alex Marshall observe that when operations shifted from Iraq to Afghanistan, COIN was applied as a template, with US commanders assuming that its apparent success in Iraq would translate to the Afghan context, despite the two theatres presenting fundamentally different problem sets.[87] The approach that had proved effective in Al-Anbar was therefore transplanted into Afghanistan without first questioning whether COIN was suited to the conditions it encountered there. Having experienced success in Iraq, commanders rotating into Afghanistan were likely to interpret the new theatre through the same conceptual lens, shaped by prior victory rather than by the demands of the emerging environment. Bird and Marshall illustrate this through a senior commander's reflection, recounted in the context of the Afghan campaign, that success in Iraq had felt like winning the

85 Niel A Smith and Sean MacFarland, 'Anbar Awakens: The Tipping Point', *Military Review* (March–April 2008), pp. 41–52.

86 David H Petraeus and James F Amos, *Counterinsurgency: FM 3-24* (Boulder, CO: Paladin Press, 2007).

87 Tim Bird and Alex Marshall, *Afghanistan: How the West Lost Its Way* (New Haven, CT: Yale University Press, 2011), p. 254.

national championships,[88] a remark that captures how prior victory shaped the conceptual lens through which the new theatre was interpreted.

There is a direct parallel here for CyberEM. Personnel arriving from assurance backgrounds bring a readymade set of answers, compliance processes, risk registers and incident reduction frameworks, shaped by careers spent solving a fundamentally different problem. These approaches are entirely appropriate for assurance and peacetime system protection, just as population-centric metrics and governance tools were appropriate within the COIN context in Iraq. But just as COIN concepts and culture were carried from Iraq into Afghanistan without reconsidering their suitability, cyber and EM operations risk being viewed through an assurance-focused lens they were never designed for. Unlike COIN, however, this mismatch may be far less visible, subtle, quieter and harder to attribute, yet still capable of narrowing the operational options presented to commanders. The result is a persistent cultural drag that does not match the tempo or risk tolerance required on a transparent battlefield.

## Conclusions and Recommendations: Creating a CyberEM Warfighting Culture

The window for deliberate cultural design in DCEMF is now, before institutional gravity makes the choice for Defence. The analysis presented in this chapter leads to five recommendations for designing a command capable of meeting the demands of the SDR. First, assurance functions must be fully separated from operational roles. Although the SDR's separation of digital functions to the NAD is a positive step, it will be insufficient if the new command adopts a J6-driven approach. Second, single-service military domain expertise, spanning EW and cyber, must be preserved and protected, as effective tactical integration cannot be delivered by CyberEM generalists. Third, a leadership development pathway is required that cultivates a warfighter identity from early career stages rather than attempting to retrofit operational culture later, echoing the success path of the development of RAF identity. A CyberEM Operational Leader designation would incentivise individual investment in warfighting competence and distinguish operational

88 Robert D Kaplan, 'Man Versus Afghanistan', *The Atlantic*, April 2010; Bird and Marshall, *Afghanistan*, 254.

CyberEM activity from J6 and digital personnel, clarifying that they require fundamentally different identities.

Fourth, the command must develop warfighting-focused metrics to prevent a drift back towards compliance- and assurance-based measures. Finally, leadership should be drawn from the J3, J35 and J5 communities, as these are the leaders best placed to define what 'good' operational performance looks like. Leadership is the mechanism by which this warfighting culture will either deliberately be constructed or accidentally imported. This cultural ambition should extend beyond the CyberEM community itself. A baseline level of 'cyber and electromagnetic mindfulness' should extend across the UK's national defence enterprise. Even where personnel are not directly involved in these activities, they should understand the potential and limitations in the same way that a general appreciation of sea, land, air and space power is considered a professional norm.

Declaring CyberEM as a domain will not, on its own, deliver military advantage. Culture will, and once culture is formed it is extraordinarily difficult to redirect. The importance of this distinction is illustrated by the NCF itself. As a joint defence and intelligence organisation accountable to two secretaries of state, it occupies a position where strategic culture – the institutional assumptions about the legitimate use of offensive cyber effects – directly shapes what operational culture is permitted to look like within it. While the SDR assigns DCEMF responsibility for articulating Defence's demand signal to the NCF, it grants no authority over the NCF's internal structure, governance or cultural formation. Appreciating how strategic, organisational and warfighting cultures interact is therefore a necessary condition for designing a DCEMF that can shape NCF activity without either eroding the NCF's distinctive character or allowing its pre-existing culture to become the default model for the wider command.

For CyberEM, the most significant cultural risk is that an assurance-experienced culture will quietly narrow the option space available to commanders, institutionalising hesitation, framing offensive effects as risk issues and proving structurally unable to operate at the tempo that a transparent, sensor-rich battlefield demands. The cost of failing to act will not appear in an audit; it will appear on a battlefield where decision cycles are measured in seconds, and where the adversary has long since stopped waiting.

## About the Author

### Carolyn Swinney

Carolyn Swinney is a Wing Commander and cyberspace officer within the RAF. She holds a PhD in Electronics Engineering and is an Executive Fellow with the University of Essex. Her main research interests are signal processing, uncrewed aerial vehicles, neural networks, machine learning and cyber security. The views expressed in this chapter are those of the author, and do not reflect official government policy.

CHAPTER 3

# Friction and Initiative in Cyberspace Through the Doctrine of Cognitive Effect

**Monica Kello and Richard Harknett**

The Doctrine of Cognitive Effect (DCE), a pioneering set of ideas publicly introduced by the UK National Cyber Force (NCF) in 2023,[1] encompasses important mechanisms that can have sustained effects on an adversary with the potential to impact strategic outcomes through cyberspace. The doctrine's central premise is that it is possible to gain or lose strategic advantage by structuring adversaries' assessments of the operating environment. It therefore recognises that to achieve advantage in cyberspace, you need to create an unfavourable operating environment for your adversary while simultaneously creating a favourable one for yourself. This assertion is consistent with a campaigning mindset and posture that, combined, seek to affect the adversary's ability to gain initiative in cyberspace.

Moreover, the doctrine notes that changes in perception should generally be introduced subtly and over time, highlighting the unique value proposition of cyber operations linked as a campaign.[2] The often covert and clandestine nature of cyber operations means that they are particularly well suited to the execution of slow, patient and, potentially, low-intensity effects. These are uniquely calibrated to erode trust within key relationships between people, as well as between people and their technology and organisations. In the latter case, this erosion emanates from the technology not working (full disruption of capability) or not working as effectively or efficiently as assumed. This may

1 National Cyber Force, 'National Cyber Force: Responsible Cyber Power in Practice', April 2023, <https://www.gov.uk/government/publications/responsible-cyber-power-in-practice>, accessed 16 December 2025.

2 Richard J Harknett and Max Smeets, 'Cyber Campaigns and Strategic Outcomes', *Journal of Strategic Studies* (Vol. 45, No. 4, 2020), pp. 534–67.

be blamed on the technology itself or raise questions about the competency of operators and, thus, reverberate back to the people-to-people trust relationship. Overall, the erosion of trust is a key objective of sustained, cumulative cyber operational effects. Adversaries have shown to be adept in their recognition of key relationships in Western societies, for example in Russia's interference in the US presidential election in 2016. The onus is now on Western democracies to determine adversarial pressure points and how they can best leverage them with cyber means.

In this chapter, we posit that at the heart of the DCE is the mechanism of friction. Friction consists of: a technical level – the complication of operations and the generation of distrust in data and systems; an organisational level – the complication of standard operating procedures and adaptability; and a psychological level – the manipulation of the perceptions of people within the organisation and its wider ecosystem to create affective-cognitive consequences. At each imposition of friction there is the potential to induce a loss of trust: at the technical level, in data and systems; at the organisational level, in standard operating procedures; and at the psychological layer, in people and how people view the technical and organisational levels. The DCE can be applied beyond a single organisation to affect trust within a wider community or ecosystem.

The chapter starts with the premise of Cyber Persistence Theory: that cyberspace is an environment of constant contact that requires states to persistently set and maintain the conditions of security in their favour through campaigns of linked operations. Second, applying the logic of initiative persistence, we develop the concept of friction as a mechanism central to cyber campaigning. Third, we illustrate, heuristically, the potential of friction with a case study of UK law enforcement's Operation *Cronos*, drawing from official National Crime Agency (NCA) publications, media reporting, cyber threat intelligence analysis, and interviews with senior NCA officials involved in the operation. Although *Cronos* was an operation that was independently designed by the NCA and not guided formally by the DCE, it converged on a similar logic. Thus, as an avowed cyber campaign, *Cronos* offers a rare, empirically accessible case through which to examine the mechanism of friction. We conclude that the DCE applied through friction campaigns enables optimised cyber resource allocation for strategic advantage and contingency preparation.

## Cognitive Effect Through Friction Campaigns

In and through cyberspace, states and non-state actors seek continuously to exploit the technical and user vulnerabilities to unauthorised access and action that are inherent in networked computing environments. Securing against such exploitation ideally requires anticipating those exploits before they occur. This requires a shift in mindset and organisational posture to a proactive and persistent approach based on the logic of initiative persistence.[3] When operationalised, this logic requires a move away from viewing cyber resources as best used as episodic options to be taken 'off-the-shelf' when conditions arise that require a response. The logic of initiative persistence requires the operational artform captured in a campaigning mindset that views cyber resources best employed through linked operations that create cumulative effects on the operational environment that adversaries seek to exploit. If one cedes the initiative to the adversary in a global interconnected network environment where speed, scale and scope of effects are exponentially increasing, one is accepting risk to one's political, economic, military and social sources of national power.[4]

Cyber campaigning, thus, is a baseline for 21st century national security and needs to be conducted to secure strategic advantage and prevent strategic loss.[5] It is an everyday persistent activity anchored on protecting national interests, because there is some salient threat actor seeking exploitation every day, whether that be another country seeking economic advantage through intellectual property theft or an organised crime group seeking ransom through encrypted extortion. Basic cybersecurity practices need to be understood as an element of cyber campaigning both organisationally and nationally – they are not isolated technical controls that the IT department is responsible for and everyone else forgets about (or grumbles over when they must watch a compliance video once a year). Creating a favourable

3 Michael P Fischerkeller, Emily O Goldman and Richard Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (Oxford: Oxford University Press, 2022).

4 This analytical framework for cyber campaigning is developed in Michael P Fischerkeller, Emily O Goldman and Richard J Harknett, *Cyber Persistence and Campaigning: The Logic and Art of Securing Cyberspace* (forthcoming 2026).

5 Michael P Fischerkeller, Emily O Goldman and Richard J Harknett, 'Setting the Stage: Cyber Contingency Campaigning', *Lawfare*, 28 August 2025, <https://www.lawfaremedia.org/article/setting-the-stage--cyber-contingency-campaigning>, accessed 16 December 2025.

operational environment in one's own national space is the first essential element of cyber campaigning.

Cyber initiative must also be sustained through two other essential campaigning elements: managing third-party influences; and structuring unfavourable circumstances for your adversaries. Managing influences can involve influence campaigns against third parties to create positive effects but also must be understood more broadly as policies and strategies involving key alignment of private sector activity with national security objectives.[6]

The DCE through campaigning is salient both in setting favourable conditions in one's own systems and in managing third-party influences. However, its greatest potential is in structuring unfavourable circumstances for adversaries by adjusting the operational environment,[7] both in real terms and misperceived terms, proactively. The objective is to have adversaries operate in conditions and circumstances that you have set to your relative advantage. In football, a team whose offence relies on quick passing wants as slick a pitch as possible – short cut grass and well-watered. An untimely (and intentional) breakdown in the lawn-cutting machinery or watering system right before a match can have a direct impact on the efficiency of a passing team, undermine the confidence of players as passes are misplaced, and create a potential relative advantage if the opposing team relies on counterattack long-ball tactics. A strategic outcome of loss for the other side becomes enhanced through these actions taken *before* the players ever got out on to the pitch.

This hints at another critical facet of cyber campaigning: you can pursue it for day-to-day advantage, but also link it to key national security over-the-horizon contingencies such as the prospect of militarised crisis or armed conflict before the emergence of such geopolitical conditions. If you understand what it takes for the adversary to consider that 'today is a good day for war', you can cyber campaign to ensure that such circumstances never align for them to make that judgement. If you disrupt the watering system of your opponent's training ground, they never get a good practice in, the manager never trusts his players to win. Countries cannot only campaign for strategic

6 Fischerkeller, Goldman and Harknett, *Cyber Persistence and Campaigning*, Chapter 2.

7 Michael Fischerkeller, Emily Goldman and Richard Harknett, 'NATO Must "Contingency Campaign" in Cyberspace', Book Binder, 16 December 2025, <https://bindinghook.com/nato-must-contingency-campaign-in-cyberspace/>, accessed 10 January 2026.

advantage in competition but can use those campaigns concurrently as cyber contingency campaigning[8] against very specific national security threats (not every country poses a threat of war or militarised crisis for the UK). There is an additive quality to this use of cyber resources as more use enhances capacity to introduce cumulative effects on a diminishing marginal return (access begets access; operators become more skilled by operating; and cognitive effects can cumulate as they limit, frustrate and disrupt organisational efficiencies and personnel confidence). It takes effort to introduce friction (interfere with watering the grass), but less effort to sustain its effects as frustration and limits are introduced (players' performance degrades over time when challenged with continuous complication – the watering system still does not work at half time).[9]

Structuring unfavourable operational circumstances in a sustained manner requires campaigns that leverage cognitive effects purposefully to maximise each increment of friction introduced through cyber means. Cognitive impacts become an effects multiplier when layered onto the technical and organisational levels of operational friction that cyber campaigns can unleash.

## Unpacking the Mechanism of Friction

Friction is the intentional manipulation of an adversary's environment to impede its normal functioning.[10] Its objective is to create unfavourable circumstances for the adversary in its own space, whether by introducing new complications or amplifying existing ones. Cyber campaigns are particularly well suited

8 Fischerkeller, Goldman and Harknett, *Cyber Persistence and Campaigning*, Chapter 1.

9 Although never fully developed analytically, the phrase 'limit, frustrate, disrupt' is found in the Joe Biden administration's US National Cybersecurity Strategy, published in 2023. This document advocated for disruption campaigns 'to make malicious actors incapable of mounting sustained cyber-enabled campaigns that would threaten the national security or public safety of the United States'. See White House, 'National Cyber Security Strategy 2023', 2023, p. 14.

10 This definition closely aligns with John Boyd's conception of friction whereby actors intentionally generate it to disrupt an adversary's organisational coherence and decision-making. This contrasts with Clausewitzian and Luttwakian treatments that frame friction primarily as an inherent feature of complex systems, rather than a deliberate instrument of strategy. Our definition includes both. See John Boyd, 'Key Concepts', <https://www.coljohnboyd.com/static/documents/1986-12__Boyd_John_R__Patterns_of_Conflict__PPT-PDF.pdf>, accessed 16 December 2025.

to introducing friction as they can be carefully calibrated to achieve subtle effects over an extended period.[11]

Friction need not have a cognitive effect as an intentional outcome. One can simply drop a spanner into the works and disrupt operations for the sake of disrupting operations. One generates distrust through that disruption, but one does not seek to amplify it further. The real potential of the UK's DCE lies in treating the psychological and emotional dimension as a default prioritised layer built into cyber operations and campaigns. Introducing friction into the operational environment of adversaries is not easy but doing so in a manner that emphasises the cognitive effect beyond the technical and organisational impact is a value proposition for cyber resource allocation.

In considering friction campaigns that leverage the DCE, it is useful to recognise the difference between complicating the adversary's operational environment and disrupting it. Disruption is a sub-set of complication that is more directly noticeable to the adversary – it knows it has been disrupted when things do not work. Complication, as a broader construct, enables us to consider operational effects in campaign planning that are more subtle, cumulative and potentially psychologically more potent (frustration may flow more from the uncertainty of why things are not achieving the ends one wants than from failing to achieve the expected outcome). Ultimately, we suggest that friction is inclusive of both dropping a spanner into the works (disruption) and throwing sand in the gears (complication) in colloquial terms.

Cyber operations can introduce friction at two principal levels: technical; and organisational. The first level complicates computer system operations through *technical* effects. It includes actions such as disrupting command and control servers, exposing or removing adversary malware, cutting operators' internet access or even damaging data and IT infrastructure. More subtly, it may involve introducing what appear as typical computing issues, such as system upgrades that go poorly, software updates that get blamed for system disruptions, or data manipulation that appears as simple user input error. The second level is *organisational*: the complication of standard operating procedures and organisational adaptability. In a situation of technical

11 The advantage of linking operations into campaigns is acknowledged in the National Cyber Force, 'The National Cyber Force: Responsible Cyber Power in Practice'.

disruption, an organisation is forced to reallocate time and resources away from its own operations and towards isolating compromised systems, shutting down accounts and servers, investigating intrusion vectors and malware, and eventually restoring and remediating their systems. If the operation is subtle and long term, and appears more like system administrator mistakes and user errors than effects from attacks, these investigations can take extended effort to resolve, generating significant costs. Compromises of communication infrastructure may lead to inefficiencies in personnel coordination as well. This friction undermines standard operating procedures. In turn, this creates barriers, real and imagined, to restoring organisational efficiency.

In isolation, cyber operations to introduce technical and organisational friction can be effective but are not the optimised use of cyber resources. A layered cyber campaign – in which such friction is amplified with a focus on cognitive effects as integral to planning – leverages cyber means at their most efficient. Cyber campaigns can take technical and organisational operations and link them to the psychological. This involves amplifying the misperceptions of people within the organisation and its wider ecosystem to create affective-cognitive consequences including sustained distrust, frustration, anger, fear and shame. In other words, the psychological effect can be layered onto the technical and organisational. The prioritisation of this layer becomes the distinguishing nature of operations and campaigns conducted under the DCE.

In practice, once distrust takes hold at the technical and organisational level, it can be used as an almost universal lens through which personnel interpret all interactions, leading to a broad loss of confidence in the entire operating environment.[12] The malfunctions may generate suspicion of other workers – questioning their motives or competency – which fuels hypervigilance, erodes cooperation and eventually breeds paranoia.[13] Hypervigilance and rumination

12 Branko Božič and Sabina Keston-Siebert, 'The Profession That Came in from the Cold: Trust and Distrust in Espionage', *Journal of Professions and Organization* (Vol. 11, No. 3, 2024), p. 198; Jamie MacColl and Tim Stevens, 'Countering Non-State Actors in Cyberspace', in Tim Stevens and Joe Devanny (eds), *Research Handbook on Cyberwarfare* (Cheltenham: Edward Elgar Publishing, 2024).

13 Steven Fein, 'Effects of Suspicion on Attributional Thinking and the Correspondence Bias', *Journal of Personality and Social Psychology* (Vol. 70, No. 6, 1996), p. 1165; Steven Fein and James L Hilton, 'Judging Others in the Shadow of Suspicion', *Motivation and Emotion* (Vol. 18, No. 2, 1994), p. 169.

are understood to have a cyclical relationship: hypervigilant assessment of social information produces additional 'raw data' for the sceptical individual to ruminate upon, while rumination fosters the development of scepticism-ladened hypotheses that incite further vigilant examination of the situation and particularly of others' actions.[14] In this way, trust cultivated over years of working relationships can become significantly destabilised.[15]

Anger appears when individuals start to attribute negative events, either to one another or to an external party. It belies a belief that there is an ability to redress the wrongdoing and thus primes the individual for confrontation or retaliation.[16] Fear arises from a heightened sense of vulnerability and anticipatory anxiety on whether the adversary has been fully ousted from systems. Feelings of shame are often associated with cybersecurity breaches, as they tend to be viewed as preventable, and are compounded when a particular incident violates core identity traits.[17] In organisations specialising in cyber operations, feelings of shame arising from a suspected foreign interference are likely to be particularly strong. Invulnerability to security breaches, credibility and secrecy are part of their professional identity and organisational mission. A cyber incident ruptures this self-understanding. It also bears consequences for their legitimacy and reputation when it is exposed to allies, competitors/adversaries, and the general public.[18] Surfacing compromised information, such as divulging that a hacker is in the systems of their own enablers, or they are attacking vectors that they are not supposed to be attacking, could undermine legitimacy. This is particularly true if this behaviour contravenes the hacker's declared code of conduct. Reputation is important to cyber operators, who want to be seen as skilled experts at their craft. The loss of reputation can be so significant as to discredit the organisation among key audiences, generating sustained friction through

14 Roderick M Kramer, 'Paranoid Cognition in Social Systems: Thinking and Acting in the Shadow of Doubt', *Personality and Social Psychology Review* (Vol. 2, No. 4, 1998), p. 254.

15 Roy J Lewicki and Barbara Benedict Bunker, 'Developing and Maintaining Trust in Work Relationships', in Roderick M Kramer and Tom R Tyler (eds), *Trust in Organizations: Frontiers in Theory and Research* (London: SAGE Publications, 1996), p. 127.

16 Richard S Lazarus, *Emotion and Adaptation* (Oxford: Oxford University Press, 1991); Laurie J Barclay, Daniel P Skarlicki and S Douglas Pugh, 'Exploring the Role of Emotions in Injustice Perceptions and Retaliation', *Journal of Applied Psychology* (Vol. 90, No. 4, 2005), pp. 629–43.

17 W E Douglas Creed et al., 'Swimming in a Sea of Shame: Incorporating Emotion into Explanations of Institutional Reproduction and Change', *Academy of Management Review* (Vol. 39, No. 3, 2014), pp. 275–301.

18 *Ibid.*

persistent distrust that complicates partnerships and increases scrutiny, thus impeding the planning and coordination of new operations.

In addition, negative emotions and attitudinal orientations deplete cognitive capacities and divert attention away from productive, future-focused activities.[19] They can also lead to the erosion of a shared sense of mission and lower employee morale, leading individuals to eventually leave the organisation.[20] Importantly, the psychological effects of friction introduced by interfering with technology are amplified. This is because IT systems are meant to be friction-reducers; their very purpose is to make organisations more efficient. In campaigning for friction, the core purpose of network computing is turned on its head. In countering adversaries, a high-end campaign would be one that turns that network infrastructure against the adversary itself. Law enforcement's Operation *Cronos* was one such campaign.

## Illustrating Friction: Operation *Cronos*

In early 2024, a campaign by several law enforcement agencies, led by the UK's NCA, successfully disrupted what was at that point the most prolific ransomware-as-a-service (RaaS) group in the world, known as LockBit. The group had operated on an affiliate model, allowing partners to use its ransomware in exchange for a percentage of their earnings. LockBit had targeted over 2,500 victims (with 7,000 ransomware builds) and extorted over 500 million dollars, creating disruption costs of billions of dollars.[21] Operation *Cronos* illustrates the application of friction at both the technical and organisational level and the prioritisation of psychological effect for long-term impact.

At the technical level, law enforcement acted in three stages: infiltration and compromise; infrastructure takedown and control; and data and asset

19 Rosalind Searle, Karen V Renaud and Lisa van der Werff, 'Shaken to the Core: Trust Trajectories in the Aftermaths of Adverse Cyber Events', *Journal of Intellectual Capital* (Vol. 25, No. 5/6, 2024), p. 1168.

20 David L Weakliem and Stephen J Frenkel, 'Morale and Workplace Performance', *Work and Occupations* (Vol. 33, No. 3, 2006), pp. 335–61.

21 National Crime Agency, 'LockBit Leader Unmasked and Sanctioned', 7 May 2024, <https://www.nationalcrimeagency.gov.uk/news/lockbit-leader-unmasked-and-sanctioned>, accessed 18 November 2025.

acquisition. Having 'hacked the hackers',[22] it maintained its silent presence in LockBit's systems for an extended period of time, allowing it to design the 'most impactful international collaborative disruption possible'.[23] The NCA took control of LockBit's primary administration environment – the platform that enabled affiliates to build and carry out ransomware operations – and the group's public leak site on the dark web, which it had used to threaten victims and post their data.[24]

In the second stage, the operation focused on disabling LockBit's operational tools and acquiring data and assets. The allies took down 34 LockBit servers across several countries, seized 11,000 domains, gained access to over 1,500 decryption tools and disabled LockBit's data exfiltration infrastructure known as Stealbit.[25] It also froze over 200 LockBit-linked cryptocurrency accounts.[26] The technical compromise yielded access to the platform's source code and intelligence from LockBit's systems, including the identities of affiliates, and access to chats and negotiations with victims.[27] The technical friction introduced by *Cronos* created a loss of capability and introduced distrust of LockBit's IT and financial infrastructure.[28] This technical friction plausibly halted the group's attack operations, forcing it to move into crisis management and attempted remediation.[29]

22 National Crime Agency, 'International Investigation Disrupts the World's Most Harmful Cyber Crime Group', 20 February 2024, <https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group>, accessed 18 November 2025.

23 Remarks made by William Lyne in Chainalysis, 'Operation Cronos: Infiltrating the LockBit Ransomware Syndicate', *Public Key Podcast*, Episode 122, 6 August 2024, <https://www.chainalysis.com/blog/operation-cronos-lockbit-takedown-ep-122/>, accessed 16 December 2025.

24 National Crime Agency, 'International Investigation Disrupts the World's Most Harmful Cyber Crime Group'.

25 Tim Bradshaw, 'Royal Mail Hackers LockBit Hobbled by Global Law Enforcement', *Financial Times*, 20 February 2024.

26 Europol, 'Law Enforcement Disrupt World's Biggest Ransomware Operation', 20 February 2024, <https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation>, accessed 18 November 2025.

27 Chainalysis, 'Operation Cronos'.

28 Christopher Boyton, 'Unveiling the Fallout: Operation Cronos' Impact on LockBit Following Landmark Disruption', Trend Micro, 3 April 2024, <https://www.trendmicro.com/en_gb/research/24/d/operation-cronos-aftermath.html>, accessed 18 November 2025.

29 Chainalysis, 'Operation Cronos'.

While the technical level of *Cronos* depended on highly unique access and advanced capabilities, technical takedowns tend to achieve only short-term impact.[30] The NCA's objective was not only to disrupt LockBit's operations, but to derail the trajectory of the group.[31] To this end, it was in its prioritisation of the psychological layer within the organisational level that the operation was most innovative. To complicate organisational procedures, *Cronos* focused mainly on two elements: disrupting standard operating procedures at the core of the RaaS affiliate model; and depriving members of their anonymity, including its leadership. The latter instigated powerful psychological effects, which significantly undermined the organisation's efforts to adapt, evolve and recover from the campaign. This chapter examines each element in turn.

To complicate standard operating procedures, *Cronos* compromised LockBit's primary administration environment, internal communication infrastructure and the affiliate management system.[32] Members of the group were consequently not able to securely communicate with affiliates to issue urgent guidance and coordinate migration to new infrastructure. Law enforcement also seized a significant amount of data, including affiliate accounts and histories, chat logs, victim databases and revenue records.[33] Combined, these actions had a significant impact on disrupting the processes which the organisation would have used to reconstruct their operational capability. Although LockBit constructed a new leak site within a week of *Cronos*, it quickly became evident that this was a Potemkin exercise with victims recycled from previous breaches.[34]

The second element combined organisational complication and psychological layering to target LockBit's legitimacy and credibility. According to Graeme Biggar, the NCA's director general, these were based on secrecy and

30 Author interview with Gavin Webb, Regional Head of Investigations, Multi-Threat and Borders at the National Crime Agency and UK lead for Operation *Cronos*, Microsoft Teams, 8 January 2026.

31 *Ibid*.

32 National Crime Agency, 'International Investigation Disrupts the World's Most Harmful Cyber Crime Group'.

33 Boyton, 'Unveiling the Fallout'.

34 Resecurity, 'LockBit 3.0's Bungled Comeback Highlights the Undying Risk of Torrent-Based Data Leakage', 4 March 2024, <https://www.resecurity.com/blog/article/lockbit-30s-bungled-comeback-highlights-the-undying-risk-of-torrent-based-data-leakage>, accessed 18 November 2025.

anonymity (a similar sentiment had also been expressed by the group itself in a rare interview).[35] In a highly consequential move, in May 2024, the leader of LockBit, known as LockBitSupp, was publicly unmasked as Dmitry Khoroshev and sanctioned by the UK, the US and Australia.[36] Law enforcement also revealed the usernames of LockBit's entire network of 194 affiliates and carried out several international arrests of its members.[37] Importantly, the NCA consciously leveraged psychological factors in this element of the operation. It sought to break trust between all the nodes within the LockBit community: the owners of the malware strain and the coders; the owners and the affiliates; and the owners and the victims.[38] Once LockBitSupp as the central leadership figure became vulnerable to law enforcement, the financial resilience and predictability of the LockBit system – a major point of attraction for affiliates – collapsed.

In another creative twist, the operation sought to take advantage of the animosity towards Khoroshev already present within the cybercriminal community, which viewed him as arrogant and extractive.[39] Khoroshev himself had been so confident in his anonymity that he had offered a $10-million reward to anyone who could uncover his identity, and repeatedly taunted law enforcement.[40] As a result, his unmasking triggered ridicule and distancing within the cybercriminal community.[41] Distrust and the erosion of morale therefore spread organically, without the NCA having to control the narrative.

35 National Crime Agency, 'International Investigation Disrupts the World's Most Harmful Cyber Crime Group'; KELA Cyber, 'LockBit 2.0 Interview with Russian OSINT', 24 August 2021, <https://www.kelacyber.com/blog/lockbit-2-0-interview-with-russian-osint/>, accessed 18 November 2025.

36 Searchlight Cyber, 'A Timeline of Events: Operation Cronos and LockBit', 14 May 2024, <https://slcyber.io/blog/a-timeline-of-events-operation-cronos-and-lockbit/>, accessed 18 November 2025.

37 *Ibid.*; National Crime Agency, 'International Investigation Disrupts the World's Most Harmful Cyber Crime Group'; US Department of Justice, 'Two Foreign Nationals Plead Guilty to Participating in LockBit Ransomware Group', press release, 18 July 2024, <https://www.justice.gov/archives/opa/pr/two-foreign-nationals-plead-guilty-participating-lockbit-ransomware-group>, accessed 18 November 2025.

38 Author interview with James Babbage, Director General (Threats) at the National Crime Agency, Microsoft Teams, 11 December 2025.

39 Author interview with Gavin Webb.

40 National Crime Agency, 'New Year Honours: King Awards Eight National Crime Agency Officers', 29 December 2025, <https://www.nationalcrimeagency.gov.uk/news/new-year-honours-king-awards-eight-national-crime-agency-officers>, accessed 9 January 2026.

41 Author interview with Gavin Webb.

The loss of credibility also hollowed out the group's brand, which Khoroshev had cultivated with unusual intensity, at times encouraging overt displays of loyalty such as paid LockBit tattoos.[42] In a later interview, he revealed that 'I felt like I was being hunted, like they were trying to destroy me … They were trying to inflict maximum reputational damage to make me stop working'.[43] The operation also intentionally revealed that one of the five countries most hit by LockBit malware was China,[44] introducing a geopolitical element, possibly to attract the attention of the Russian government.

The psychological dimensions of *Cronos'* organisational complication did not end there. The operation publicly exposed LockBit's failure to delete victim data after a ransom had been paid, puncturing a promise that had been fundamental to the group's reputation and business model.[45] Convincing victims to pay up was to become untenable.[46] Law enforcement also revealed that, despite Khoroshev's claims that the group did not target hospitals, it routinely did so, and provided encryption keys that did not work.[47] Finally, in a symbolic reversal of ransomware coercion, law enforcement sought to cause the group public embarrassment and shame. It took control of LockBit's leak site on the dark web and posted a splash page stating that it was 'now under control of law enforcement', including a taunting countdown timer for the revelation of the leader's identity.[48] It went on to post daily updates exposing the group's capabilities and operations.[49]

42 Dina Temple-Raston, '"Ransomware Diaries:" Going Undercover with the Leader of LockBit', *The World from PRX*, 30 January 2023, <https://theworld.org/stories/2023/01/30/ransomware-diaries-undercover-leader-lockbit>, accessed 18 November 2025.

43 Dina Temple-Raston and Sean Powers, 'Exclusive: After LockBit's Takedown, Its Purported Leader Vows to Hack On', *The Record*, 15 March 2024, <https://therecord.media/after-lockbit-takedown-its-purported-leader-vows-to-hack-on>, accessed 18 November 2025. Note, the interview is with the LockBit leader who claims he is not, in fact, Dmitry Khoroshev.

44 Lawrence Abrams, 'LockBit Ransomware Admin Identified, Sanctioned in US, UK, Australia', *BleepingComputer*, 7 May 2024, <https://www.bleepingcomputer.com/news/security/lockbit-ransomware-admin-identified-sanctioned-in-us-uk-australia/>, accessed 18 November 2025.

45 National Crime Agency, 'International Investigation Disrupts the World's Most Harmful Cyber Crime Group'.

46 Max Smeets encapsulates this logic in the 'ransomware trust paradox' where ransomware actors must cultivate trust among victims if they are to succeed in their business model. See Max Smeets, *Ransom War: How Cyber Crime Became a Threat to National Security* (London: Hurst, 2025).

47 Author interview with Gavin Webb.

48 Bradshaw, 'Royal Mail Hackers LockBit Hobbled by Global Law Enforcement'.

49 National Crime Agency, 'International Investigation Disrupts the World's Most Harmful Cyber Crime Group'.

After Operation *Cronos*, LockBit never recovered effectively. Introducing friction that prioritised its cognitive dimensions eroded key trust relationships within the collective. It structured an unfavourable environment for actors in a way that made it impossible for LockBit to rebuild its legitimacy, credibility and brand. Crucially, because *Cronos* interrupted its operational trajectory, LockBit could not evolve into what 'it could have been' – an even more damaging criminal actor.[50] The campaign's cognitive effects also percolated into the wider cybercriminal community, with cyber threat intelligence analysts noting declining trust and collaboration between ecosystem actors and some adaptation of RaaS practices.[51]

Large, highly prolific groups, such as LockBit, no longer exist.[52] The ransomware landscape has fragmented and actors generally display more prudence in their targeting and payment demands, keeping a lower profile.[53] Ransom payments have also declined, both in terms of the share of victims who paid and the size of payments among those who did pay.[54] All of these observations indicate the presence of sustained friction and an environment that is less favourable to the adversary: heightened uncertainty among members of the criminal community following a high-profile law enforcement operation and victims' lack of faith that attackers will deliver on their promises. *Cronos* demonstrated that creative cyber campaigns, which combine technical and organisational complication while amplifying cognitive effects, offer a means to maximise cyber resources and achieve lingering outcomes.

## Conclusion

Cyber campaigns have innate qualities that can be replicated across different threat actors and threat environments. Anticipating, complicating and

50 Author interview with Gavin Webb.

51 Boyton, 'Unveiling the Fallout'; Thorsten Rosendahl and Hazel Burton, 'The LockBit Story: Why the Ransomware Affiliate Model Can Turn Takedowns into Disruptions', Cisco Talos blog, 15 March 2024, <https://blog.talosintelligence.com/ransomware-affiliate-model/>, accessed 18 November 2025.

52 Author interview with William Lyne, Deputy Director at the National Crime Agency, Microsoft Teams, 9 January 2026.

53 Author interview with James Babbage.

54 Coveware, 'Insider Threats Loom While Ransom Payment Rates Plummet', 24 October 2025, <https://www.coveware.com/blog/2025/10/24/insider-threats-loom-while-ransom-payment-rates-plummet>, accessed 16 December 2025.

disrupting the operating environments, and, thus, the campaigning capacity of state actors – which seek security advantages over relative national power – and non-state actors – which seek profit through criminal activity – share common features. Operation *Cronos* is a case study of interest not only for the NCA; it is revealing of what is possible when adopting a campaign mindset and posture that contains the NCF's DCE outcomes.

Intriguingly, in the conduct of our research, we came to conclude that the UK's NCA and the NCF appear to have landed on the importance of cyber-enabled cognitive effects independently. There may be various reasons for this, including the stove-pipe bureaucratic separation between national security and law enforcement agencies in the UK (also prevalent in the US and other Western democracies). This chapter cannot solve that structural gap (which state adversaries exploit by blurring the false compartmentalisation of national security and crime through use of criminal proxies to advance state interests at arm's length). However, we do propose that cross-agency learning is possible and should be regularised.

*Cronos* is an interesting use case. It reveals the importance of building campaigning muscle memory through doing. The actual operation was built on previous operations that may have been more limited and focused (the 'take-down' era of counter-cybercrime operations)[55] and, as such, can be seen as an evolution towards cyber campaigning. It highlights that the psychological layer can be impactful and it shows the prospect of what more can be done for sustained effect, if such a layer is prioritised in campaign planning. We conclude that friction campaigns leveraging cognitive effects can be an optimisation of cyber resourcing in a persistently engaged threat environment.

55 For example, the takedown of criminal Dark Web markets including Silk Road, in 2013, and AlphaBay and Hansa, in 2017.

## About the Authors


### Monica Kello

Monica Kello is a Lecturer in War Studies (Cyber Security) and Co-Director of the Cyber Security Research Group at King's College London. Her work examines cyber strategy and conflict. Monica holds a PhD in Cyber Security from the University of Oxford.

### Richard J Harknett

Richard J Harknett is Professor and Director of the Center for Cyber Strategy and Policy and Co-director of the Ohio Cyber Range Institute at the University of Cincinnati. He served as an inaugural Fulbright Scholar in Cyber Studies at Oxford University and as the inaugural Scholar-in-Residence at US Cyber Command. He is co-author *of Cyber Persistence Theory: Redefining National Security in Cyberspace* (Oxford University Press, 2022).



### Acknowledgements

The authors would like to thank James Babbage, Gavin Webb and William Lyne for taking the time to share their insights about Operation *Cronos*. This contribution also benefited from participant feedback at a closed-door workshop at RUSI in December 2025. We thank Jamie MacColl for inviting us to present our initial findings there.

CHAPTER 4

# The Illusion of Restraint
## Precision, Accountability and Calibration in the Cognitive Contest

**Charl van der Walt, Zohra Hamila, Richard Derbyshire and Adam Ridley**

Cyberspace has become a central arena of geopolitical competition. What began as a domain associated primarily with espionage and technical disruption is now embedded within broader competition over perception, legitimacy and political influence.

In the UK, the National Cyber Force (NCF) has sought to respond to this changing environment in a responsible manner, including imposing guiding principles of precision, accountability and calibration (PAC) on its offensive cyber operations.[1] Precision emphasises limiting unintended consequences and tailoring actions to specific objectives. Accountability requires that operations be attributable within government and consistent with legal and ethical standards. Calibration seeks to manage escalation by ensuring that cyber effects are proportionate, reversible where possible, and politically attuned. Together, PAC is presented as a means of aligning cyber power within an institutional framework informed by democratic values and international law, while preserving strategic utility.

Adversaries also consider PAC, but in different ways. Adversary precision lies in tailoring messages to maximise distrust and political instability at scale. Adversary accountability is authoritarian and political, obscuring links between state and proxy. Adversary calibration seeks dominance, overwhelming and controlling the narrative through timing and amplification.

1 National Cyber Force, 'National Cyber Force: Responsible Cyber Power in Practice', April 2023, <https://www.gov.uk/government/publications/responsible-cyber-power-in-practice>, accessed 25 February 2026.

Recognising these fundamental, paradigmatic contrasts is essential for competing on equal terms.

In this context, responsibility in cyberspace, and PAC in particular, has often been portrayed in contemporary commentary as an inhibitor of effectiveness. Critics argue that legal oversight, proportionality and evidentiary requirements slow decision-making and favour technically bounded actions over influence-oriented operations,[2] suggesting that PAC might pose a genuine disadvantage. This chapter challenges that narrative by arguing that the perceived limitations of PAC stem less from the principles themselves than from the way cyberspace and conflict are framed within UK doctrine. The problem is not that PAC constrains action, but that it is applied within a conceptual model that remains rooted in technical control rather than cognitive competition.

The chapter proceeds in three stages. It first examines the doctrinal and policy foundations of UK, Russian and Chinese approaches to cyber operations and statecraft. The two latter states were selected because they were highlighted as the two principal state adversaries in the National Cyber Security Centre's Annual Review 2025.[3] It then analyses how PAC functions within these different strategic frameworks, showing that adversaries also practise analogous forms of it, but orient them towards deniability, narrative dominance and audience effects. Finally, it reframes cyberspace as a sociotechnical and cognitive environment and argues that PAC can act as an enabler rather than a constraint when aligned with this reality. In doing so, the chapter suggests that a commitment to being a responsible cyber power need not be a source of strategic weakness. Instead, it can serve as a force multiplier in contemporary political competition by clarifying strategic objectives, defining guardrails and reducing operational friction.

2 An Anonymous European Intelligence Official, 'Can Lawyers Lose Wars by Stifling Cyber Capabilities?', Binding Hook, 23 July 2024, <https://bindinghook.com/can-lawyers-lose-wars-by-stifling-cyber-capabilities/>, accessed 25 February 2026.

3 National Cyber Security Centre (NCSC), 'NCSC Annual Review 2025', 14 October 2025, <https://www.ncsc.gov.uk/collection/ncsc-annual-review-2025>, accessed 25 February 2026.

## Background and Doctrinal Foundations

Competing doctrines of cyber power reflect different assumptions about the purpose of cyber operations and the nature of contemporary conflict. This section examines the policy and doctrinal foundations of UK, Russian and Chinese approaches to cyber operations to clarify how each integrates cyber activity into broader political and strategic competition.

### UK Doctrine and Cyberspace as a Technical Domain

UK cyber policy has sought to formalise responsible offensive cyber operations through the principles of PAC.[4] These principles are embedded in doctrine, legal interpretation and operational oversight mechanisms that shape how cyber power is authorised and employed. In this way, the UK aligns its cyber strategy with wider Western commitments to international law, democratic values and escalation management.[5]

The NCF's 2023 publication, 'Responsible Cyber Power in Practice',[6] makes clear that cyber operations are not limited to technical disruption. It sets out the 'doctrine of cognitive effect', under which influencing adversary confidence, decision-making and behaviour is treated as a legitimate and, in some cases, primary objective of cyber activity, rather than solely targeting digital systems and infrastructure. Nevertheless, the UK National Cyber Strategy 2022 defines 'cyberspace' in technical terms as 'the interdependent network of information technology that includes the internet, telecommunications networks, computer systems and internet-connected devices'.[7] The framing of the doctrine tends towards affecting an adversary's perception of the operating environment and weakening their ability to plan and act effectively. Rather than a broad contest of narratives, engagements under the doctrine of cognitive effects have been historically characterised as 'pinprick' operations intended to disrupt carefully selected targets. The few publicised cyber operations that may be considered examples of this doctrine have involved

4 National Cyber Force, 'National Cyber Force: Responsible Cyber Power in Practice'.
5 Suella Braverman, 'International Law in Future Frontiers', speech given at Chatham House, London, 19 May 2022, <https://www.gov.uk/government/speeches/international-law-in-future-frontiers>, accessed 25 February 2026.
6 National Cyber Force, 'National Cyber Force: Responsible Cyber Power in Practice'.
7 HM Government, 'National Cyber Strategy 2022: Pioneering a Cyber Future with the Whole of the UK', December 2021.

deterring specific adversaries such as LockBit[8] or the Islamic State[9] by disrupting their systems or seeding distrust or dissent. These are cognitive impacts, but still within a technical framing of cyberspace.[10]

At the same time, the NCF document acknowledges the difficulty of defining what responsible use of cyber power entails in practice. It also highlights the challenge of assessing the effects of cyber operations when those effects are indirect, cumulative or perceptual rather than technical. This tension between ambition, definition and measurement has become a central feature of contemporary cyber policy debate in the UK.[11]

Western national doctrines and thinking have been shaped by international legal and normative frameworks that reinforce this responsible cyber power narrative. The Tallinn Manual process has provided structured interpretations of how international law applies to offensive cyber operations, including principles of sovereignty, non-intervention, proportionality and state responsibility.[12] Speeches by UK attorneys general in 2018[13] and 2022[14] reaffirmed the UK government's position that existing international law governs state behaviour in cyberspace and that offensive cyber operations must be conducted within these legal bounds. Together, these developments reinforce the role of PAC as defining characteristics of legitimate state cyber activity and establish law and norms as central reference points for operational design.

8 National Crime Agency, 'The NCA Announces the Disruption of LockBit with Operation Cronos', <https://www.nationalcrimeagency.gov.uk/the-nca-announces-the-disruption-of-lockbit-with-operation-cronos>, accessed 25 February 2026.

9 Alexandra Ma, 'GCHQ has been Messing with ISIS Communications and Making it "Almost Impossible" for Them to Operate', *Business Insider*, 12 April 2018, <https://www.businessinsider.com/gchq-breaks-down-how-its-been-messing-with-isis-communications-2018-4>, accessed 25 February 2026.

10 Tim Stevens et al., 'Evaluating the National Cyber Force's "Responsible Cyber Power in Practice"', *RUSI Commentary*, 14 April 2023 , <https://www.rusi.org/explore-our-research/publications/commentary/evaluating-national-cyber-forces-responsible-cyber-power-practice>, accessed 25 February 2026.

11 National Cyber Force, 'National Cyber Force: Responsible Cyber Power in Practice'.

12 NATO Cooperative Cyber Defence Centre of Excellence, 'International Law Applies to Cyber Operations, Tallinn Manual 2.0 Reaffirms', 2017, <https://ccdcoe.org/news/2017/international-law-applies-to-cyber-operations-tallinn-manual-2-0-reaffirms/>, accessed 26 February 2026.

13 Jeremy Wright, 'Cyber and International Law in the 21st Century', speech given at Chatham House, London, 23 May 2018, <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>, accessed 24 February 2026.

14 Braverman, 'International Law in Future Frontiers'.

### Restraint and Effectiveness in the UK Debate

The Western emphasis on law and norms has also influenced strategic culture in indirect ways, including within the UK. Policy discussions frequently centre on thresholds, attribution, escalation management and proportionality.[15] Offensive cyber operations are often framed around the risks they must avoid, including civilian harm, unintended spillover and damage to critical infrastructure. While this approach has strengthened international credibility and coalition cohesion, it has also generated criticism that Western cyber power is overly constrained by legal and procedural caution.

This critique has emerged in recent debates over whether legal oversight and normative commitments reduce operational tempo and strategic effectiveness. Commentators have argued that adversaries exploit ambiguity, deniability and proxy actors to pursue political objectives without incurring the same constraints, thereby gaining the initiative in cyber conflict.[16] In response, UK institutions have maintained that legality and responsibility are not obstacles to effective cyber power, but necessary foundations for sustained competition, alliance cooperation and public trust.[17] These exchanges illustrate an unresolved tension between responsibility understood as restraint and responsibility understood as strategic discipline.

### Adversary Doctrines and Competing Conceptions of Cyber Conflict

While this debate unfolds, adversarial states approach cyber operations through different doctrinal traditions. Russian and Chinese doctrines conceptualise cyberspace fundamentally as a political and informational environment. In contrast, the UK's 'doctrine of cognitive effects' takes effect within a largely technical conceptualisation of cyberspace. This shapes how cyber operations are integrated into broader statecraft.

In contrast with Western rule-of-law restraint or the UK's specific 'responsible cyber power' model, analyses indicate that for cyber operators in Russia[18] and

15 Juliet Skingsley, *Offensive Cyber Operations: States' Perceptions of their Utility and Risks* (London: Chatham House, 2023).

16 An Anonymous European Intelligence Official, 'Can Lawyers Lose Wars by Stifling Cyber Capabilities?'.

17 GCHQ, 'Cyber Operations and the Law', <https://www.gchq.gov.uk/information/cyber-and-law>, accessed 24 February 2026.

18 Foreign, Commonwealth & Development Office, 'Russia's FSB Malign Activity: Factsheet', 7 December 2023, <https://www.gov.uk/government/publications/russias-fsb-malign-cyber-

China,[19] constraints emerge from authoritarian command-and-control and political regulation in the form of hierarchy, political control and internal discipline.

An examination of how adversarial states such as Russia and China understand cyberspace, conflict and the organisation of offensive cyber operations is essential. This provides a comparative basis for critically examining the strengths and weaknesses of PAC within UK offensive cyber operations.

### *Russia*

Russia conceptualises 'cyber' not as a discrete technical domain but as a global information space encompassing social, political and cultural dimensions. In statements to the UN, Russia describes not only 'computer attacks' on information resources as threats but also information deemed harmful to a state's sociopolitical and socioeconomic foundations, including its spiritual, moral and cultural environment.[20]

Russia's doctrine, 'Information Confrontation', treats cyberspace as a continuous form of competition.[21] Analysts have asserted that 'Russian military theorists generally do not use the terms cyber or cyberwarfare'. Instead, 'they conceptualise cyber operations within the broader framework of information warfare, a holistic concept that includes computer network operations, electronic warfare, psychological operations, and information operations'.[22] Technical intrusions are employed primarily to shape perceptions, erode trust and influence political outcomes. These operations target not only networks but also military and political leadership, armed forces and civilian populations

activity-factsheet/russias-fsb-malign-activity-factsheet>, accessed 24 February 2026.

19 *Reuters,* 'China Sets up Powerful Information Warfare Force to Support "Military Struggles"', 11 April 2024.

20 UN Office for Disarmament Affairs, 'Updated Concept of the Convention of the United Nations on Ensuring International Information Security – Proposal of the Russian Federation', unofficial translation, 2021, <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_convention_on_ensuring_international_information_security.pdf>, accessed 23 February 2026.

21 Janne Hakala and Jazlyn Melnychuk, *Russia's Strategy in Cyberspace* (Riga: NATO Stratcom COE, 2021).

22 Michael Connell and Sarah Vogler, 'Russia's Approach to Cyber Warfare', CNA, 2017, <https://nsarchive.gwu.edu/sites/default/files/documents/3728883/Michael-Connell-and-Sarah-Vogler-Center-for.pdf>, accessed 24 February 2026.

through information technologies, often without a formal declaration of war.[23] In this model, cognitive effects are central – rather than incidental – as influencing democratic decision-making, undermining trust and exacerbating social divisions are pursued as enduring strategic objectives within an ongoing information struggle.

Contemporary analysis describes this approach as deliberately operating below the threshold that would trigger NATO's Article 5. It combines psychological and propaganda activity, offensive cyber operations, electronic warfare, covert action and economic coercion into a continuing campaign of pressure rather than discrete wartime episodes.[24]

Russia directs its cyber operations through a system of vertical state control and internal security discipline, which Western assessments characterise as a presidentially centred governance model.[25] Cyber operations are reportedly coordinated through reporting channels that run from operational units within the Russian General Staff (GRU) and the Federal Security Service (FSB) to the Presidential Administration and Security Council, rather than through a unified cyber command.[26] Within the GRU, units operate under a defined chain of command in which senior officers direct operational details, and junior officers are paired with experienced handlers for operational training. Within the FSB, the Information Security Center (TsIB) sits inside the operational directorate, under supervisory control. Criminal hackers have been incorporated into these structures through recruitment or coercion, placing their capabilities under formal state oversight.[27]

Accountability is oriented upward to the executive and security leadership, combining centralised political control with distributed operational

23 *Ibid.*

24 Seth G Jones, 'Russia's Shadow War Against the West', Center for Strategic and International Studies, 18 March 2025, <https://www.csis.org/analysis/russias-shadow-war-against-west>, accessed 23 February 2026.

25 *Ibid.*

26 Regional Cyber Defence Centre, 'Report on the Russian Use of Offensive Cyber Capabilities in the Course of Military Aggression in Ukraine', 2022, <https://www.nksc.lt/doc/rkgc/Report_Russian_Use_of_Offensive_Cyber_Capabilities_in_UA.pdf>, accessed 23 February 2026.

27 Andrei Soldatov and Irina Borogan, 'Russian Cyberwarfare: Unpacking the Kremlin's Capabilities', CEPA, September 2022, <https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/>, accessed 24 February 2026.

responsibility across agencies. One description of inter-agency conflict within the Russian apparatus argues that each 'tries to prove to the Kremlin that it is more useful than the others and thus to secure greater access to the Kremlin's levers of power and patronage, but also increased funding and privileges'.[28]

Russian offensive cyber operations are frequently conducted through proxies such as criminal organisations, NGOs, diaspora networks, local recruits or companies, which enables deniability and complicates attribution. This delegation is treated as integral to Russia's ability to sustain pressure, while managing escalation risk and creating ambiguity, particularly when cognitive effects are sought.[29]

### *China*

In official discourse, China defines 'cyberspace' as a state-governed social and political domain in which security encompasses control over infrastructure, data and online content.[30] Government white papers emphasise 'law-based cyberspace governance', presenting it as an arena to be managed in support of national security, social order and development through state regulation of platforms, online activity and information flows.[31] This framing is closely linked to China's concept of 'cyber sovereignty', which asserts each state's right to regulate and secure the internet within its borders, including content and the broader digital ecosystem. This concept is also reflected in China's 'community with a shared future in cyberspace' vision and associated governance principles.[32] China's cybersecurity concept has developed into a comprehensive national security and governance

28 Nicu Popescu and Stanislav Secrieru (eds), 'Hacks, Leaks and Disruptions: Russian Cyber Strategies', *Chaillot Papers* (No. 148, October 2018).

29 Justin Sherman, 'Untangling the Russian Web: Spies, Proxies, and Spectrums of Russian Cyber Behavior', Atlantic Council, 19 September 2022, <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/untangling-the-russian-web/>, accessed 25 February 2026.

30 Niels Nagelhus Schia and Lars Gjesvik, 'China's Cyber Sovereignty', NUPI Policy Brief 2/2017, 2017, <https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/NUPI-Policy_Brief_2_17_Schia_Gjesvik.pdf>, accessed 25 February 2026.

31 State Council, People's Republic of China, 'Full Text: China's Law-Based Cyberspace Governance in the New Era', 16 March 2023, <https://english.www.gov.cn/archive/whitepaper/202303/16/content_WS6489542ec6d0868f4e8dcd56.html>, accessed 24 February 2026.

32 Dakota Cary, 'Community Watch: China's Vision for the Future of the Internet', Atlantic Council, December 2023, <https://www.atlanticcouncil.org/in-depth-research-reports/report/community-watch-chinas-vision-for-the-future-of-the-internet/>, accessed 25 February 2026.

project that encompasses ideological and public-opinion security, platform governance and technical security.[33]

Within this context, China's 'Three Warfares' doctrine structures influence as a coherent strategy aimed at achieving 'discursive power' by shaping perceptions and constraining adversary choices in both peace- and wartime.[34] The doctrine seeks to create conditions favourable to China without recourse to physical conflict, or, if force becomes necessary, to prepare the narrative and legal context needed to legitimise its use. Offensive cyber activity operates within this model as an enabling layer for cognitive contest rather than as an isolated 'computer-on-computer' activity. Technical operations can serve diverse ends. Reported examples include: long-term cyber espionage against the Uyghur diaspora to identify politically active individuals; 'network coercion to compel the cessation of perceived pro-independence activities or deter any perceived moves by Taiwan towards independence';[35] and evidence of email-access and surveillance services being procured from third party contractors.[36]

Institutionally, the People's Liberation Army (PLA) has centralised cyber, electronic warfare and psychological operations through the creation of the Strategic Support Force (SSF) – a unified structure responsible for information-domain operations. Subsequent reforms placed a newly configured information warfare support force directly under the top-level command authority, the Central Military Commission (CMC). Official commentary frames this as consistent with the Party's 'absolute leadership' over the armed forces, embedded within political discipline and anti-corruption oversight mechanisms. Chinese sources also link unified command structures to

33 DigWatch, 'China's National Cyberspace Security Strategy', December 2016, <https://dig.watch/resource/chinas-national-cyberspace-security-strategy/>, accessed 24 February 2026.

34 John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era, China Strategic Perspectives*, Vol. 6 (Washington, DC: NDU Press, 2018).

35 Insikt Group, 'From Coercion to Invasion: The Theory and Execution of China's Cyber Activity in Cross-Strait Relations', Recorded Future Research Report, November 2022, <https://www.recordedfuture.com/research/from-coercion-to-invasion-the-theory-and-execution-of-china-cyber-activity>, accessed 24 February 2026; Ben Nimmo, C Shawn Eib and L Tamora, 'Cross-Platform Spam Network Targeted Hong Kong Protests', 25 September 2019, <https://graphika.com/reports/spamouflage>, accessed 24 February 2026.

36 Ryan McMorrow, 'Leak Shows China Uses Private Company to Hack Citizens and Foreign States', *Financial Times*, 22 February 2024.

escalation control, presenting centralised command and control as a means of imposing organisational restraint.[37]

Although China's use of proxies[38] differs from that of Russia, it similarly relies on layered deniability and ecosystem mobilisation. Threat-intelligence reporting identifies China-nexus clusters that blur state and non-state boundaries, including 'dual' espionage-criminal groups and broker-style access actors.[39] In addition, government and industry reporting describes a contractor marketplace where private firms supply intrusion tooling and operational services to Chinese government customers. For example, the i-Soon document leak depicts offensive capabilities and government creating a commercial proxy ecosystem.[40] US law enforcement further asserts that a commercial entity controlled a large botnet used to conceal operator identities.[41]

### *Technical and Cognitive Integration in Russian and Chinese Doctrine*

Across both Russia and China, offensive cyber operations and influence operations function as mutually reinforcing elements of a single competitive approach. Within this approach, technical access, disruption and reconnaissance enable cognitive effects. By framing accusations of misconduct through terms such as 'insufficient', 'unprofessional' or 'political manoeuvring',[42] narrative, psychological and legal framing shape how those technical actions are perceived, interpreted and contested. This integration

37 Lincoln Davidson, 'China's Strategic Support Force: The New Home of the PLA's Cyber Operations?', Council on Foreign Relations, 20 January 2016, <https://www.cfr.org/articles/chinas-strategic-support-force-new-home-plas-cyber-operations>, accessed 24 February 2026.

38 Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press, 2018), pp. 107–20.

39 Nalani Fraser et al., 'APT41: A Dual Espionage and Cyber Crime Operation', Threat Intelligence, 17 August 2019, <https://cloud.google.com/blog/topics/threat-intelligence/apt41-dual-espionage-and-cyber-crime-operation>, accessed 24 February 2026.

40 Dakota Cary and Aleksandar Milenkoski, 'Unmasking I-Soon: The Leak that Revealed China's Cyber Operations', SentinelLabs, 21 February 2024, <https://www.sentinelone.com/labs/unmasking-i-soon-the-leak-that-revealed-chinas-cyber-operations/>, accessed 24 February 2026.

41 US Department of Justice, 'Court Authorised Operation Disrupts Worldwide Botnet Used by People's Republic of China's State Sponsored Hackers', press release, 18 September 2024, <https://www.justice.gov/archives/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state>, accessed 24 February 2026.

42 *Reuters*, 'China Calls Hacking Allegations by US, UK "Political Manoeuvring"', 26 March 2024.

allows offensive cyber operations to be employed as part of a broader grey-zone strategy, where coordinated actions pursue strategic objectives below the threshold of open armed conflict, collectively generating a sustained and 'cohesive pressure system' on Western adversaries.

Breaches, hack-and-leak operations, DDoS campaigns, defacements and cyber extortion serve both technical and psychological purposes. Beyond immediate disruption, they generate fear, humiliation, loss of trust and deterrence through uncertainty. Even where technical damage is limited or rapidly remediated, the primary strategic effects are realised in the cognitive and informational environment. Such incidents can undermine trust in democratic institutions and contribute to wider social and political disruption. Beyond these potential impacts, downstream consequences can include reduced confidence in public services, heightened perceptions of vulnerability and increased political cynicism.[43] Assessments of the alleged 2007 Russian attacks against Estonia, for example, assert that 'the psychological effects on Estonian decision-makers and the population at large can be considered as the most significant consequence of the 2007 cyberattacks'.[44]

Individual cyber actions therefore impose economic or psychological costs on their targets, regardless of whether they are technical or cognitive in character or conducted by state, proxy or criminal actors. When such actions accumulate over time, even if each appears isolated, they generate distraction, disunity and distrust, ultimately producing a significant weakening of the target state.

## PAC in Practice Across the UK and Adversaries

The doctrinal and policy differences outlined above shape how PAC is interpreted and applied in practice. The application of PAC in the UK operates within a strategic framing that appears to treat cyberspace largely as a technical domain where threats need to be 'disrupted' or 'deterred',[45] and

43 Ryan Shandler and Miguel Alberto Gomez, 'The Hidden Threat of Cyber-Attacks – Undermining Public Confidence in Government', *Journal of Information Technology & Politics* (Vol. 20, No. 4, 2023), pp. 359–74.

44 Popescu and Secrieru, 'Hacks, Leaks and Disruptions'.

45 National Cyber Force, 'National Cyber Force: Responsible Cyber Power in Practice'.

remains anchored in escalation management, legal restraint and technical control. By contrast, adversarial doctrines place cognition, perception and influence at the centre of cyberspace and competition by employing cyber operations as one element within broader campaigns designed to generate sustained, cumulative pressure on an opponent.

This divergence produces an asymmetry that is often attributed to PAC itself, without considering the interaction between governance mechanisms and deeper strategic assumptions about cyberspace and conflict. But while no equivalent to the UK's 'responsible cyber power' can be identified in adversary policy, adversaries still operate under constraints expressed as strategic discipline and control, centralised tasking, internal political accountability and incentives. Those constraints typically align with their theories of cyberspace and competition. The apparent divergence thus cannot be explained fully by PAC as a restriction; the way cyberspace is conceptualised, how competition is understood, and how command-and-control arrangements are structured must be considered.

The question that then arises is whether the UK's approach to cyber competition adequately captures the character of cyberspace and cyber conflict, while remaining consistent with the democratic values that demand a mechanism such as PAC in the first place. How can the UK design its cyber strategy and structures to counter the hybrid approaches of its adversaries by increasing operational flexibility and speed while still safeguarding the liberal-democratic principles that PAC is intended to uphold?

Evaluating the strategic value of PAC requires examining how it is interpreted and operationalised in UK cyber practice. It also requires comparing this with the implicit restraint mechanisms shaping adversary operations, and assessing whether indeed values, law and governance necessarily constrain operational effectiveness.

### UK Orientations of PAC and Their Consequences

Although UK strategy and official guidance recognise cyberspace as a socio-technical construct[46] and the NCF has articulated a doctrine of cognitive

46 HM Government, 'National Cyber Strategy 2022'; and NCSC, Helen L, 'Sociotechnical Security Group Problem Book v4-0', September 2022, available at National Archives, <https://

effect,[47] UK offensive cyber operations remain primarily oriented towards technical intervention. Democratic values are expressed through responsible cyber power and embedded in operational tactics and processes. While PAC enhances credibility and reinforces lawful, responsible practice, it also exacerbates the procedural and temporal burdens associated with planning and authorising cyber operations. As a result, UK operators may be structurally nudged towards technical interventions in digital systems – as publicised UK offensive cyber operations appear to suggest[48] – since 'computer-on-computer' effects are easier to justify, measure and defend. These tendencies may be compounded by institutional arrangements that constitute the NCF as a cyber-operations body, structurally distinct from strategic communications and other influence functions,[49] as well as by risk-averse delegation structures.[50] Taken together, these features can narrow the effective mission space available to operators, reduce operational tempo, and make certain forms of grey-zone competition structurally more difficult to pursue.

By contrast, Russia and China lack a public policy framework that directly mirrors PAC. That said, it would be inaccurate to suggest they operate without constraints on cyber activity. As described earlier, cyber and information operations are instead embedded within highly centralised state or party security systems that integrate technical, informational, psychological and legal measures into continuous strategic competition. Within these systems, operators contribute to enduring campaigns of political influence, rather than executing isolated technical actions.

In competition with adversaries such as Russia and China, this contrast places the UK at an asymmetric disadvantage, increasing operational friction and narrowing operational choice towards infrastructure-adjacent effects. The NCF's explicit contrast between PAC-governed operations and adversary

webarchive.nationalarchives.gov.uk/ukgwa/20220901131647/https://www.ncsc.gov.uk/files/StSG-Problem-Book-v4-0.pdf/>, accessed 23 February 2026.

47 National Cyber Force, 'National Cyber Force: Responsible Cyber Power in Practice'.

48 Ma, 'GCHQ has been Messing with ISIS Communications and Making it "Almost Impossible" for Them to Operate'.

49 National Cyber Force, 'About Us', <https://www.gov.uk/government/organisations/national-cyber-force/about>, accessed 23 February 2026.

50 Stevens et al., 'Evaluating the National Cyber Force's "Responsible Cyber Power in Practice"'.

'large-scale disinformation', alongside its acknowledgement of the utility of ambiguity and cognitive effects, illustrates this tension.[51]

In addition to these operational considerations, the UK faces a fundamental dilemma. UK cyber power must reconcile democratic responsibility with effectiveness in a contested environment, requiring not only careful application of PAC, but also policy, strategy and organisational designs that align operational practice with the democratic values that PAC seeks to protect.

### Governance as a Strategic Enabler

One should not accept that values, laws and other constraints must inevitably introduce operational friction. When properly designed, they can enable tempo by reducing uncertainty and decision latency. Rules of engagement and authorisation frameworks can function as pre-established guardrails, allowing operators to act decisively within an agreed policy rather than seeking ad hoc permission for each action. This logic is demonstrated in NATO joint doctrine,[52] which can be read to link speed and freedom of action to mission command, suggesting that action can follow swiftly when intent, boundaries and delegation are clear.

PAC creates friction only when treated as a compliance layer applied to narrowly defined technical actions. It does not inherently slow operations. Applied within an appropriate strategy, PAC can enable faster action. Clear political intent, agreed boundaries, defined escalation limits and established evidentiary standards reduce uncertainty and the need for repeated approvals. Operators who understand the mission and its limits can act confidently within pre-authorised parameters. If governance, strategy and operations are aligned in advance, PAC functions as a guardrail that supports tempo rather than restricting it.

Successful competition against adversaries such as Russia and China therefore requires a strategy that reflects the broad conceptualisation of cyberspace, revised measures of effect that capture cognitive outcomes,

51 National Cyber Force, 'National Cyber Force: Responsible Cyber Power in Practice'.

52 NATO Standardization Office, 'Allied Joint Doctrine', AJP-01, Edition F, Version 1, December 2022; Ministry of Defence, 'UK Defence Doctrine', Joint Doctrine Publication 0-01, 6th Edition, November 2022.

and delegated authorities that allow operators to act within clearly defined policy guardrails. The challenge for the UK is therefore not whether to retain PAC, but how to situate it within a conceptual and doctrinal understanding of cyberspace and conflict that aligns governance, strategy and operations, rather than allowing governance alone to define what is operationally feasible.

## Reframing Cyberspace and Values as Strategic Assets

Addressing the friction and dilemmas associated with PAC requires re-analysis of the context from which PAC emerges. This raises two key questions. First, does the UK's prevailing conception of cyberspace adequately reflect the sociotechnical and cognitive character of the competition with adversaries such as Russia and China? Second, can the democratic values expressed through PAC function as sources of operational advantage rather than constraints?

### Reframing Cyberspace as a Sociotechnical and Cognitive Environment

Although UK strategy and guidance acknowledge the sociotechnical nature of cyberspace, NCF documentation such as 'Responsible Cyber Power in Practice' and publicly reported operations suggest that cyberspace is frequently operationalised primarily in technical terms, with access, disruption and deterrence at the forefront. By contrast, key adversaries appear to integrate cognition and social dynamics directly into operational design, treating influence and perception as intrinsic components of cyber competition rather than downstream effects.

This broader sociotechnical framing aligns with existing thinking, including NATO Allied Command Transformation's doctrine[53] on cognitive warfare, which treats competition as spanning public opinion, psychological operations, legal instruments and technical capabilities in an integrated manner. However, unless this wider understanding of competition is internalised and reflected in operational design, governance mechanisms such as PAC cannot realise their enabling potential. Guardrails can accelerate action only when they are calibrated to the full spectrum of effects being pursued. If competition is framed narrowly in technical terms, then pre-agreed categories of acceptable

53 NATO, 'Cognitive Warfare', <https://www.act.nato.int/activities/cognitive-warfare/>, accessed 25 February 2026.

action, escalation thresholds and evidentiary standards will also be narrowly defined, limiting rather than expanding operational latitude. Improved tempo therefore depends not simply on clearer guardrails, but on ensuring that those guardrails are aligned with an accurate understanding of the character of contemporary competition.

While NATO's exploratory doctrine is not directly comparable to a national policy document, it nonetheless demonstrates how psychological, legal and informational instruments can be treated as co-equal with technical capabilities in operational design. By contrast, although 'Responsible Cyber Power in Practice' acknowledges cognitive effects, these are framed largely as consequences of technical operations, with the document's structure and case studies centred on access, disruption and deterrence. This suggests that sociotechnical integration is recognised in UK articulation but not foregrounded as an organising principle of operational design.

### Reframing UK Democratic Values as Operational Strengths

In a cognitive conflict centred on defending democratic values, some of the asymmetry disadvantaging the UK could be offset by deliberately exploiting those same democratic values as an advantage. Openness, transparency and accountability can themselves serve as tools for mitigating the cognitive impact of adversary activity. Timely, evidence-based public communication, clear attribution where possible, and transparent institutional accountability are key levers for a democratic government. Leveraged correctly, these measures can also limit adversaries' ability to shape narratives and thus reduce space for coercion.[54] Rather than being a vulnerability, such practices can blunt the psychological leverage adversaries seek to derive from disruptive incidents. Openness and participation could be organised into a national capability, with civil and institutional components, that helps society to absorb and neutralise hostile influence.

UK government policy increasingly frames hostile information activity as a national security concern and a threat to democratic institutions. This approach is reflected in the Government Communication Service's RESIST

54 NATO, 'NATO's Approach to Counter Information Threats', 3 February 2025, <https://www.nato.int/en/what-we-do/wider-activities/natos-approach-to-counter-information-threats>, accessed 25 February 2026.

toolkits, which explicitly discuss misinformation and disinformation as threats to democratic values and recommend building resilience through effective communication rather than emulating adversary behaviour.[55] Although RESIST focuses on misinformation and disinformation, its logic could be extended to address the cognitive impacts of cyber incidents, by addressing the narrative elements of cyber events and applying similar principles of preparation, rapid factual communication and trust stabilisation.

The European External Action Service (EEAS)[56] leads the EU's efforts to protect information integrity and counter 'Foreign Information Manipulation and Interference' efforts by foreign state or state-linked actors to distort information environments and influence democratic processes. Through reports and tools, the EEAS maps hostile networks and patterns, supporting coordinated EU responses that strengthen detection, resilience and democratic integrity across member states.

These examples illustrate efforts to leverage democratic strengths as a way to address asymmetries in cyberspace conflict without relaxing the accountability and restraint that PAC is intended to uphold. This line of thought suggests that democratic values can provide an advantage in cognitive competition. Rather than mirroring adversaries' coercive methods, this advantage comes from using the strengths of democratic systems to build societal cohesion and resilience, reduce audience receptivity, and increase the reputational and political costs for attackers.

## Conclusion

Debates about UK offensive cyber operations often treat PAC as sources of strategic restraint in a contest against adversaries perceived to operate with fewer limits. Such a diagnosis misidentifies the problem. The apparent asymmetry does not arise from PAC itself, but from the interaction between

55 Government Communications Service, 'RESIST 3: Building Resilience to Information Threats', <https://www.communications.gov.uk/publications/resist-3-building-resilience-to-information-threats/>, accessed 25 February 2026.

56 EU External Action Service, 'Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI)', Strategic Communications, March 2026, <https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en>, accessed 23 February 2026.

governance mechanisms and an inherited conceptual framing that treats cyberspace primarily as a technical domain in the context of offensive cyber operations. When cyber competition is understood instead as a sustained cognitive contest conducted largely in the grey zone, PAC appears less a constraint and more as a potential organising framework for effective action.

Comparing UK doctrine with Russian and Chinese approaches shows that adversaries are not unconstrained. They also operate within systems of PAC, but orient these principles towards narrative dominance, deniability and sustained pressure on political and social targets. Their integration of technical and cognitive effects within continuous campaigns highlights that the strategic question is not whether constraints exist, but how they are aligned with underlying theories of conflict. The UK dilemma is therefore one of alignment: ensuring that governance structures, operational practice and conceptual models of cyberspace reinforce rather than undermine one another.

Operationalising a sociotechnical and cognitive understanding of cyberspace within the design and conduct of offensive cyber operations, and treating democratic values as operational assets rather than liabilities, suggest a path forward. Pre-agreed authorities, integrated campaign design and clearer measures of cognitive effect can increase tempo without sacrificing legality or legitimacy. At the same time, transparency, attribution and civic resilience can reduce the psychological leverage that adversaries seek to exploit. In this sense, responsible cyber power is not a defensive posture but a strategic choice about how to compete effectively.

The central implication is that PAC should be engineered around the contest that the UK is actually in. When embedded within a doctrine that recognises cyber operations as instruments of political competition, PAC can function as force multipliers. The challenge is not to relax these principles, but to apply them to a broader understanding of cyber conflict where people, perceptions and institutions are the primary terrain.

## About the Authors

### Charl van der Walt

Charl van der Walt leads the global Security Intelligence and Research team at Orange Cyberdefense, spanning four countries. He co-founded a penetration testing firm in 2000 and later transitioned to corporate cyber defence leadership. His work combines technical assessments, data analysis, social science, geopolitics and systems thinking.

### Zohra Hamila

Zohra Hamila is a Junior Security Researcher at Orange Cyberdefense where she focuses on cybercrime and the effect of law enforcement activity on cybercrime ecosystems. She has experience in international business and is interested in how cybersecurity, commercial dynamics, and social contexts intersect with and influence one another.

### Richard Derbyshire

Richard Derbyshire is a Principal Security Researcher at Orange Cyberdefense and an Honorary Researcher at Imperial College London. His work spans offensive and defensive cybersecurity, with a focus on operational technology and critical national infrastructure. He takes a pragmatic approach, bridging technical and policy perspectives.

### Adam Ridley

Adam Ridley holds a PhD in Comparative Politics and Public Policy from Flinders University, Australia. He works at Orange Cyberdefense as both a Team Lead in the Reporting and Data Analytics Team, and as a Continual Improvement Manager. His research interests include the geopolitics of cybersecurity, anti-discrimination policymaking and multiculturalism.

CHAPTER 5

# Legal Mechanisms for Scaling UK Offensive Cyber Capabilities Through the Private Sector

**Pia Hüsch and Charles Coventry**

States across the globe are preparing their cyber capabilities for competition, crisis and conflict. Some do this with more transparency than others: some are comfortable speaking about 'offensive cyber' operations and capabilities;[1] others are less direct in their language.[2] The need to scale offensive cyber capabilities is triggered by an ever-evolving threat landscape, enhanced by increased digitisation and geopolitical tensions. States face the need to scale their cyber capabilities to retain options to respond to adversarial activities in and through cyberspace.

National contexts around permissions, public perception and funding for enhancing these capabilities vary widely, but most states face one common challenge: much of the capacity and expertise on cyber operations sits within the private sector. In order to scale their cyber capabilities, public

1 US Cyber Command, 'CYBER 101 – Cyber Mission Force', news, 1 November 2022, <https://www.cybercom.mil/Media/News/Article/3206393/cyber-101-cyber-mission-force/>, accessed 30 January 2026. US Cyber Mission Force und US Cyber Command explicitly list 'offensive cyber operations' as one of their three primary forms of operations. See also Tim Starks and Mark Pomerleau, 'Trump and Others Want to Ramp Up Cyber Offense, But There's Plenty of Doubt about the Idea', Cyberscoop, 13 January 2025, <https://cyberscoop.com/aggressive-cyber-offense-trump-administration-us-strategy-debate/>, accessed 30 January 2026.

2 The Republic of South Korea speaks of 'offensive cyber defence'. See Ji da-gyum, 'S. Korea Announces "Offensive Cyber Defense" Strategy', *Korea Herald*, 1 September 2024, <https://www.koreaherald.com/article/3465045>, accessed 30 January 2026. Japan has passed a new law in 2025 to enable 'Active Cyber Defense'. Japan House of Representatives, 'サイバー安全保障を確保するための能動的サイバー防御等に係る態勢の整備の推進に関する法律案' ['Draft Act on Promoting the Development of Active Cyber Defense'], <https://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g21306007.htm>, accessed 30 January 2026.

sectors are therefore highly dependent on cooperation with the private sector for skilled people, capabilities and tools.

The UK cyber ecosystem is no exception to this. The National Cyber Force's (NCF) Responsible Cyber Power primer has publicly acknowledged that the UK conducts cyber operations against the adversary, yet does not explicitly call these 'offensive cyber operations'.[3] It has also reconfirmed that the UK is doing so in a responsible manner in compliance with domestic and international law.[4] But like in other states, the UK's ambitions are dependent on collaboration with the private sector. Such collaboration can take many forms, from informal exchanges to formal subcontracting.

Two main questions arise in this context:

1. What legal mechanisms are available to the public sector to effectively leverage skills and capabilities in the private sector to scale up its offensive cyber capabilities in times of competition, crisis and conflict?
2. What legal challenges and considerations under domestic and international law arise in this context?

This chapter answers these research questions from a perspective of the UK cyber ecosystem by providing an overview of the legal models and practised mechanisms that allow states to work with the private sector to leverage the latter's expertise on offensive cyber. It then dives deeper into the legal aspects covered in one specific legal mechanism: contracted capabilities/services requiring a warrant. Finally, it explores legal considerations under domestic and international law before a conclusion summarises the state of debate in the UK.

3 The primer speaks of 'the ability to take disruptive cyber action' or 'make it harder for adversaries to use cyberspace and digital technologies to achieve their ends'. National Cyber Force, 'National Cyber Force: Responsible Cyber Power in Practice', April 2023, p. 6, <https://www.gov.uk/government/publications/responsible-cyber-power-in-practice>, accessed 30 January 2026.

4 *Ibid.*, p. 14.

This chapter relies on literature review, including grey literature, combined with findings from a UK Cyber Effects Network's (UKCEN) research workshop on the role of the private sector in the UK's offensive cyber ecosystem, and anonymous informal follow-up conversations with members of the UKCEN.

This chapter by no means provides a comprehensive legal analysis of this complex area of law. Instead, it offers legal context to a debate that is often conducted behind closed doors and/or from a policy or technical angle, leaving the legal issues to government's tight-lipped legal advisers and corporate legal departments. Academia and the broader public policy debate have few insights into the legal considerations that arise in this context. Where they do, such debate is often US dominated,[5] focusing on concepts such as 'letters of marque'[6] or 'deputisation'[7] that are of limited relevance to the UK. This chapter provides an overview of the legal context to scaling offensive cyber capabilities with the help of the private sector from a UK perspective.

5 For example, on whether US offensive cyber operations in support of Ukraine met legal thresholds such as the use of force, see Kim Zetter, 'What It Means that the U.S. Is Conducting Offensive Cyber Operations Against Russia', Zeroday, 17 June 2022, <https://www.zetter-zeroday.com/what-it-means-that-the-us-is-conducting/>, accessed 30 January 2026. For the legal questions on subcontracting private sector entities for offensive cyber operations, see Adam Sella, 'U.S. Weighs Expanding Private Companies' Role in Cyberwarfare', *New York Times*, 14 January 2026; and Sezaneh Seymour and Brandon Wales, 'Partners or Provocateurs? Private-Sector Involvement in Offensive Cyber Operations', Lawfare Research Report 25-5, June 2025, <https://s3.documentcloud.org/documents/26000607/partners-or-provocateurs-seymour-wales.pdf>, accessed 30 January 2026.

6 For instance, Juan Zarate argues that 'Congress has the right to issue letters of marque and reprisal'. See *Washington Post*, 'Juan Zarate: "Absolutely" Ok for Private Companies to Hack Nation-state', 6 October 2016; David DiMolfetta, 'An 18th-century War Power Resurfaces in Cyber Policy Talks', Nextgov, 22 May 2025, <https://www.nextgov.com/cybersecurity/2025/05/18th-century-war-power-resurfaces-cyber-policy-talks/405526/>, accessed 30 January 2026.

7 Gareth Mott, 'Deputising UK Counter-Cybercrime Operations', *RUSI Insights Papers* (February 2026).

We faced two key challenges in writing this chapter. First is the lack of access to classified information and the lack of publicly available information on the topic, due to statutory restrictions on what information can be disclosed with respect to warrants and authorisations.[8] There are some public acknowledgments that it may be appropriate for UK government bodies to work with third-party contractors for activities – such as covert surveillance falling under the Investigatory Powers Act,[9] or reports by the Intelligence and Security Committee on the relationship with contractors.[10] However, publicly available information remains limited (and primarily focused on defensive cyber or surveillance) and often hidden in long, legal documents. Daniella Lock concludes that 'we are far from having a full picture of the current arrangements' of how the Single Intelligence Account subcontracts private tech companies for their services.[11] The approaches discussed in this chapter therefore need to be seen in light of the lack of wider publicly information on the topic. A second challenge is the lack of an authoritative definition of what constitutes 'offensive cyber'. While it is not our aim to provide such a definition, we are working with a narrow interpretation, focusing primarily on destructive operations. Supporting activities, such as training or mere espionage, would therefore not fall under the definition of offensive cyber used here.

8 For example, as per Section 57 of the Investigatory Powers Act 2016, and Section 4 of the Officials Secret Act 1989.

9 Home Office, *Covert Surveillance and Property Interference: Revised Code of Practice* (London: Home Office, 2018), para. 4.32.

10 For a useful summary that 'traces' the evidence of expanded reliance on subcontractors by the UK's Security and Intelligence Agencies, see Daniella Lock, 'Public Power and Private Hands: Outsourcing in UK National Security Law', *King's Law Journal* (Vol. 36, No. 3, 2025), pp. 571–602.

11 Lock, 'Public Power and Private Hands', p. 581.

## Legal Mechanisms and Practised Models to Work with Private Sector Offensive Cyber Capabilities

There are a range of models and legal mechanisms through which public entities conducting offensive cyber operations could potentially engage with the private sector. They differ across a number of variables – including on formality, risk levels and scalability – and have varying benefits and downsides. Some are more applicable to a UK context than others, and only a few of them truly focus on 'offensive cyber operations' in the stricter sense. Table 1 provides an overview of different mechanisms that could be feasible, their upsides and downsides and (where information is available) to what extent these are currently practised in the UK. These categories are not necessarily mutually exclusive and can overlap depending on exact understanding or could be used concurrently.

**Table 1:** Potentially Feasible Mechanisms

| Mechanism | Explanation | Offers | Comes with Downside/Risk |
|---|---|---|---|
| **Industry Schemes (for example, i100[12])** | • In the UK, the NCSC-run i100 scheme offers secondment of private sector individuals to work with public sector, for example, once a month or more regularly.<br>• Participants remain paid by the private sector but get government contacts, insights and security clearance in return.<br>• Potential to copy a similar model for offensive cyber currently under-explored. | • Closer ties between individuals in industry and government.<br>• Allows government to recruit skilled individuals for limited time.<br>• Offers security clearance to private sector participants. | • Current model in the UK focused on the larger cyber security sector, not on offensive cyber community – therefore remains largely defensive and outside genuinely offensive cyber scope.<br>• Perception that government is exploiting skills and not paying adequately.<br>• Difficulties getting participants cleared to adequate/higher level for offensive cyber. |
| **(Sub) Contracted Capabilities/ Services not Requiring Warrant** | • Can include activities such as training for Cyber Capacity Building (CCB) which fall outside the scope of criminal activities, including the scope of the Computer Misuse Act (CMA).<br>• Do not require secretary of state to provide warrant against criminal/civil liability.<br>• Currently understood to be used for non-offensive cyber activities. | • Standardised practice to subcontract private sector for certain activities, for example, incident response.<br>• Establishes working relationships.<br>• Can provide services in support of offensive cyber even when activities fall short of offensive cyber. | • Depending on definition, does not cover offensive cyber given that it is below the threshold requiring warrant. |

| | | | |
|---|---|---|---|
| **(Cyber) Reserves** | • Existing models in uniform, for example, under existing structures of UK armed forces.[13] | • Individuals able to conduct offensive cyber operations as a reservist (not under private sector function).<br>• Allow individuals to contribute skills developed in private sector to armed forces.<br>• Can provide them with operational experience and security clearances.<br>• Legal certainty that this falls under state's responsibility. | • Mixed assessments of usefulness for offensive cyber purposes.<br>• Proper use requires significant investment, including time from standing forces to meaningfully integrate reserves.<br>• Lack of attraction / unclear why requirement for individuals to be in uniform. |
| **Embedded Private Sector Reps** | • Perceived as a relatively common model used by government authorities to rely on private sector skills and capabilities.<br>• Typically done via time contracts as opposed to specific tasks/services.<br>• Unclear to what extent used for 'truly' offensive cyber operations or just referring to providing wider technical skills. | • Skilled workforce closely embedded into ways of working of public sector.<br>• Established model of cooperation.<br>• Company maintains reputational and other risks for individuals. | • Limited ability to scale given it is costly.<br>• Challenge to retain public sector staff working next to better paid equivalent. |



12 National Cyber Security Centre, 'Industry 100', <https://www.ncsc.gov.uk/section/industry-100/about>, accessed 30 January 2026.
13 HM Government, 'Joint Cyber Reserve Force', Gov.uk, <https://www.gov.uk/government/groups/joint-cyber-reserve-force>, accessed 30 January 2026.

| Mechanism | Explanation | Offers | Comes with Downside/Risk |
|---|---|---|---|
| **Retainer Model** | • Retainer agreements with private sector companies which could mobilise private sector staff for specific capabilities based on commercial arrangements.<br>• Speculated that this is not currently used in the UK for offensive cyber capabilities. | • Skilled workforce from private sector.<br>• Ability to scale quickly when required.<br>• Practised in other areas. | • Ongoing costs while private sector not used.<br>• Relatively high costs for commercial agreement. |
| **(Sub) Contracted Capabilities/ Services Requiring Warrant Issued by Secretary of State** | • Authorised individual, for example, secretary of state, can issue warrant for capabilities and services otherwise in violation of existing domestic law, such as CMA.<br>• Would allow contracting of private sector for development of tools or provision of services typically reserved for public sector but for which it may not have scale or capacity.<br>• Some indications that this is, to some extent, practised in the UK already, for example, on surveillance, but no public evidence with respect to 'truly' offensive cyber operations. | • Provides companies/individuals with assurance they do not carry liability under specific statutes of domestic criminal and at times civil law.<br>• Risk-averse contracting authority may retain control over key aspects and shape warrant in line with their red lines. | • Difficulty setting out compliance with international and domestic legal obligations.<br>• Moral, ethical and potentially legal considerations in how far offensive cyber operations should/can be subcontracted to private sector. |

| | | | |
|---|---|---|---|
| **Letter of Marque (LoM, loose terms)** | • Mostly understood as a loose agreement/instruction for private sector to go after a more or less well-defined threat actors, potentially in exchange for plunder (for example, crypto).<br>• Still perceived as a no-go in the UK context and currently unlikely to be used in the UK, but discussions resurfacing in the US.<br>• Practices in North Korea and Russia seen as potential examples of letter-of-marque-style relationship between governments and cybercriminals. | • A fast option to scale private sector involvement for offensive cyber.<br>• Potentially possible to instruct private sector generically without triggering state's responsibility for activities if instruction below control threshold.<br>• Could provide more detailed instructions mirroring a contract but, in our understanding, would then no longer be a LoM. | • Typical understanding of LoM is loose and provides little control for instructing authority.<br>• Requires large risk appetite from both instructing authority (loses ability to control) and company (loses protection against certain risks).<br>• Likely to require legislation in the UK. |
| **Hacktivists and other voluntary supporters** | • Informal model to leverage capabilities from private individuals and hacktivist communities without providing contract, merely relying on loose instructions.<br>• Most prominently used in Ukraine via Ukrainian IT Army.<br>• Individuals are not exempt from liability, including under international criminal law.<br>• Sentiment that this is unlikely to be used in UK context but no public evidence on UK government position. | • Allows government to draw on talent from private and third sector.<br>• Provides ability to scale.<br>• May provide ability to avoid state responsibility if instructions sufficiently vague. | • Unclear how much control government authority can exercise, balancing potential desire not to trigger state responsibility.<br>• Requires high-risk appetite from government. |

***Source:*** *The authors.*

### Legal Considerations for Private Sector Services Requiring a Warrant

Agreements for services requiring a warrant, as mentioned in Table 1, currently seem the most relevant mechanisms in the UK to subcontract private sector companies to scale offensive cyber operations. However, there is limited to no publicly available information to what extent and for which activities these currently exist.

In the context of this chapter, agreements for services requiring a warrant are essentially a 'tasking contract' between the public sector entity and a private company. Such agreements succeed a warrant issued by the secretary of state which renders certain otherwise unlawful activities lawful for all purposes, thereby negating the criminal and civil liability of said company. It then can conduct otherwise unlawful activities on behalf of the state.

Due to the freedom of contract, the exact agreements can principally be of varying length, specificity and scope. In a very loosely defined form, an agreement for services requiring a warrant could be seen as a letter of marque. However, these are not currently representative of UK practice and we therefore treat them separately. Instead, such an agreement would likely resemble a more detailed contract. These agreements would be attractive to private sector companies as a guarantee that (due to the existence of a warrant) their activities would not trigger criminal liability while allowing public sector authorities to set the scope and retain control. We are currently unaware of any public examples of such contracts. In the absence of public examples, Table 2 illustrates what legal considerations could be relevant when hypothetically concluding an agreement for services requiring a warrant.

We focus on this particular type of mechanism – instead of the others listed in Table 1 – as the most suitable to scale the UK's offensive cyber capabilities through the private sector. Several mechanisms – such as i100 in its current form – are only suitable to cyber activities that do not fit a narrow definition of offensive cyber. Others – such as letters of marque – are not currently used in the UK nor do they seem adequate to describe the relationship that UK authorities would feasibly pursue in a current context.

Table 2 highlights several key legal considerations that a 'tasking contract' for services requiring a warrant may include. Some of these may already be covered in the warrant itself.

**Table 2:** Legal and Contractual Considerations for 'Tasking Contracts'

| Aspect | Legal/Contractual Considerations |
|---|---|
| **Legal Basis** | Some laws allow for certain state organs to issue warrants and authorisations, for example, under Section 7 of the Intelligence Services Act 1997. This Act states that 'a person [that] would be liable in the United Kingdom for any act done outside the British Islands, he shall not be so liable if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under this section'. Additional requirements spelled out in the Act need to be fulfilled. For example, acts must be done for the function of an Intelligence Service/GCHQ. Other legal bases include the Regulation of Investigatory Powers Act 2000 (RIPA) Part II, Part III, for example, for intrusive surveillance.[14] |
| **Authority** | Signature requirement from a senior official to issue a warrant. In the UK, a warrant under the Intelligence Services Act requires approval by the secretary of state. |
| **Scope of Contracted Work under Agreement over Services Requiring a Warrant** | Determines scope of activities or tools covered by the agreement, including the target set, such as who exactly should be targeted by the operation or activity in question. Could also determine who is covered under the agreement (for example, specific individuals) to conduct said activities. |
| **Temporal Aspects** | Covers the timeline over which the private company enjoys exemption from liabilities, but could also be tied to a fulfilment of a specific service as opposed to time. Typically, such agreements require renewal after a maximum of six months. |
| **Domestic Criminal Liabilities** | Certain, normally unlawful, activities (for example, under Computer Misuse Act) can be rendered lawful. A warrant renders certain activities conducted in accordance with the warrant 'lawful for all purposes', which negates criminal liability for these under domestic criminal law. This does not apply to foreign domestic criminal law, however. Where the activities are in violation of another state's criminal code, individuals may still be liable under the relevant law, and may face consequences, for example when travelling to said state on holiday. |

14 For a useful overview see, Mark Waller, *Report of the Intelligence Services Commissioner for 2014*, HC 225 (London: The Stationery Office, June 2015), pp. 7–8.

| Aspect | Legal/Contractual Considerations |
|---|---|
| **Civil Liabilities** | Similarly to activities raising criminal liability, states can also negate civil responsibility for activities conducted in accordance with the warrant which renders the activity in question 'lawful for all purposes', for example, for unintended harm to innocent third parties. |
| **Intellectual Property Considerations** | Covers aspects such as who holds intellectual property rights over capabilities/tools developed under the agreement. |
| **International Legal Liabilities** | No government can exclude liability under international law. Most international law does not directly apply to individuals, but certain provisions such as international criminal law do. Similarly, if a state exercises sufficient control over the activities of a private sector company it will still be responsible under international law for such activities. However, a contract may encourage or even make compliance with international legal norms a requirement or encourage adherence to certain standards or policy. These include voluntary norms, for example, UN norms on responsible cyber behaviour or the NCF's Responsible Cyber Power in Practice.<br><br>In addition, an agreement may include provisions for financial indemnity that the company may have to provide to the contracting state where exceeding instructions attracts the international liability of the contracting state. |
| **Degree of Control Versus Risk** | On the one hand, agreements for services requiring a warrant will balance the degree of control the contracting authority will want to exercise – both to have control over the kind of activities conducted under the agreement but possibly also to avoid a certain degree of control that could trigger international legal responsibility for the activities – and the risk the contracting authority is comfortable with. On the other hand, the private company may not want to take on the risk of conducting activities without certain provisions, such as a warrant negating civil or criminal liability for its employees, in place. |

***Source:*** *The authors.*

## Legal Implications and Challenges

### Legal Implications and Challenges under Domestic Law

In the UK, there are some established legal bases under which the relevant secretary of state might issue warrants to private companies. As listed above, these include Section 7 of the Intelligence Services Act 1997. However, the offensive cyber community in the UK largely perceives current signals from government as reflecting a highly risk-averse mindset that is reluctant to make extensive use of such provisions. Although there is a recognition of the need to scale offensive cyber capabilities – or at least to prepare for scaling to ready for scenarios of conflict – the current risk appetite to subcontract sensitive tasks to the private sector remains limited. However, such appetite may change depending on the geopolitical context and could open the door to further warrants being granted or looser mechanisms, as outlined in Table 1, to find more relevance in the UK context.

This apparent risk aversion also means that the debate on domestic legal challenges has been somewhat limited, particularly in terms of a lack of government statements and positions on the matter. While more active with respect to the application of international law (as will be discussed) to cyberspace, domestic law, including the legal basis for providing warrants, is rarely discussed in public by government officials, particularly with respect to offensive cyber operations. This also includes thorny questions such as the risk of an intelligence agency acting outside of its statutory purposes or the Ministry of Defence acting outside the scope of the Royal Prerogative if subcontracting what are the most inherent of government tasks. These issues are rarely discussed in the wider public, at least by representatives of the government.

Private sector representatives and academics have been more vocal about the need to reform certain domestic legal provisions, primarily the Computer Misuse Act (CMA) of 1990, often seen as a restrictive and outdated piece of domestic legislation that constrains offensive cyber operations and forms of research.[15] In an opinion piece from January 2026, Lord Holmes – co-author

15 Richard Walton, 'The Computer Misuse Act', *Information Security Technical Report* (Vol 11, No. 1, 2006), pp. 39–45; Audrey Guinchard, 'The Criminalisation of Tools under the Computer Misuse Act 1990. The Need to Rethink Cybercrime Offences to Effectively Protect Legitimate Activities and Deter Cybercriminals', in Tim Owen and Jessica Marshall (eds), *Rethinking Cybercrime: Critical Debates* (Cham: Springer, 2020), pp. 41–61; Chris Holmes, 'Computer Misuse Act

of several Lords Select Committee reports on digital technologies – describes the CMA as doing 'damage to our cyber professionals … while simultaneously holding our cyber industry back'.[16] Reform of the CMA has therefore long been a subject matter in policy circles – and under governmental review since 2021.[17] At the end of 2025, the UK government renewed its pledge to review the act, increasingly under pressure to keep up with international counterparts such as Portugal, where legislation recently added additional protections for cyber security researchers.[18]

Detailed recommendations for reform of the CMA are beyond the scope of this chapter. However, attention should be drawn to some of the key challenges that have been raised in this context. First, the list of offences under the CMA criminalises a wide range of activities conducted by malign and benign actors. This specifically includes Section 3A, referring to 'making, supplying or obtaining articles for use in computer misuse offences'. Such wide scope can include tools developed for legitimate purposes. Related to this point is the availability of defences under the Act, which many would like to see extended to provide protection for activities such as critical vulnerability research or other threat intelligence activities undertaken by ethical cyber security professionals and researchers.[19] Second, it may be difficult for a smaller company without an existing warrant in place to develop offensive cyber-relevant tools to pitch to the UK government as a customer. Without a warrant it may be difficult – or even unlawful – for them to prove their relevant capabilities in the first place – a chicken-and-egg situation that makes it particularly difficult for smaller or newer companies to collaborate with the government.

Finally, the CMA has extraterritorial application where there is a 'significant link' to the appropriate jurisdiction in the UK, making it 'possible to prosecute a person in this country for an act committed abroad' if an offence is

Reform is Overdue – Not all Anniversaries Should be Celebrated', *Computer Weekly*, 9 January 2026, <https://www.computerweekly.com/opinion/Computer-Misuse-Act-reform-is-overdue-not-all-anniversaries-should-be-celebrated>, accessed 23 January 2026.

16 Holmes, 'Computer Misuse Act Reform is Overdue'.

17 *Ibid.*

18 Joe Fay, 'UK Finally Vows to Look at 35-year-old Computer Misuse Act', *The Register*, 9 December 2025, <https://www.theregister.com/2025/12/09/uk_computer_misuse_act/>, accessed 23 January 2026.

19 Holmes, 'Computer Misuse Act Reform is Overdue'.

committed under Sections 1–3 of the CMA.[20] If there is no significant link to the UK, a UK national may still be prosecuted provided the offence in question is also an offence 'in the country where it took place'.[21] This can raise challenges for British companies seeking to sell services or tools to foreign allies. UK government authorities would be unlikely to provide a warrant for said service if they are not the customer, but a foreign government is – which could provide a warrant. This may pose challenges to British companies seeking to commercially scale and export offensive cyber services/tools, thereby not just enhancing commercial value but also the offensive cyber capabilities of UK allies.

Beyond UK domestic law, private companies conducting such operations also remain subject to the risk of legal consequences under the domestic law of foreign states. For example, if a British company were to conduct offensive cyber operations against State A under a warrant provided on behalf of the British state, the UK-issued warrant would exempt the company and its personnel from liabilities under UK criminal law. However, these activities might still be in violation of State A's criminal law. State A may have challenges enforcing such law against the company and its employees while located in the UK, but next to the psychological impact of being charged by a foreign state's criminal law enforcement system, employees of the company could still face challenges when travelling, either to State A directly or another allied state that has an extradition treaty in place with State A. For example, in November 2025, a Russian suspected of cybercrime was arrested in Thailand, facing extradition to the US for his alleged crimes.[22] This may have consequences for employees' travel plans and personal lives, and would influence a company's risk assessment of whether to accept such work.

Alongside domestic legal considerations, there are also voluntary, non-binding norms and policy standards that a government may impose on itself. In the UK, the NCF's 'Responsible Cyber Power in Practice' primer has set out key expectations for how the UK conducts offensive cyber operations but also how it conducts conversations with the wider public about these issues.[23]

20 'Serious Crime Act 2015 (UK)', Part 2: Computer Misuse, para. 137.
21 *Ibid.*
22 Laura Sharman, Helen Regan and Sean Lyngaas, 'Russian Alleged Cyber-hacker Faces Extradition to US after Arrest in Thailand', *CNN*, 15 November 2025.
23 National Cyber Force, 'National Cyber Force: Responsible Cyber Power in Practice', p. 6.

While not legal issues in the stricter sense, these voluntary standards shape the domestic debate on subcontracting private sector stakeholders for offensive cyber. They link to key democratic principles, such as the rule of law, and further shape perceptions about the ethical and moral implications of a government subcontracting private sector stakeholders for offensive cyber-related services. These include the risks of lack of supervision of private sector companies conducting such activities.[24]

For some, contracting private companies for these activities may be comparable to areas such as construction or similar, where it is common and uncontroversial for a government to hire private sector stakeholders. However, others point to the sensitivities of subcontracting tasks typically reserved as the prerogative of the state. Although some cyber security services may be seen as uncontroversial, truly offensive cyber operations arguably should remain within a state's remit, especially as a state has human rights and other obligations that are not necessarily shared by private companies.

Depending on these perceptions, the question of subcontracting carries many different connotations, from business-as-usual to comparisons to notorious private military contractors – and this shapes how the discussion is framed. The contemporary US debate is marked by stronger pushes towards permissive use of private sector offensive cyber capabilities.[25] In Germany, however, proposed legislative reform to allow federal intelligence services to conduct offensive cyber operations received considerable pushback, questioning the legitimacy of such reform.[26] While offensive cyber operations remain a highly sensitive, largely classified topic within the prerogative of the intelligence and defence communities, the UK's position is generally progressive in comparison. It stresses a need for transparency, accountability and dialogue with the wider public, for example via the Responsible Cyber Power in Practice primer. Public perception and narrative are, of course, also subject to wider context, for example, whether a given state is in a state of competition, crisis or conflict.

24 Lock, 'Public Power and Private Hands', p. 582ff.

25 Sella, 'U.S. Weighs Expanding Private Companies' Role in Cyberwarfare'.

26 Gabriel Rinaldi, 'Bundesregierung prüft neue Befugnisse im Cyberraum' ['Federal Government Examines New Powers in Cyberspace'], *Süddeutsche Zeitung*, 21 January 2026, <https://www.sz-dossier.de/tiefgaenge/bundesregierung-prueft-neue-befugnisse-im-cyberraum-c7f2fa2c>, accessed 30 January 2026.

## Legal Implications and Challenges under International Law

The international law dimension further adds to the complexity of subcontracting private sector entities for offensive cyber operations. Although international law primarily binds states, some provisions also raise consequences for private individuals.

This is the case for international criminal law, which holds individuals accountable for some of the gravest crimes they can commit, including genocide, war crimes or crimes against humanity. Although the bar for crimes prosecuted under international criminal law by domestic courts or the International Criminal Court (ICC) is high, it is applicable in cyberspace. In 2025, the office of the prosecutor published a draft policy on cyber-enabled crime under the Rome Statute, the founding treaty of the ICC, confirming that international criminal law also applies to cyber activities.[27] The articles referring to war crimes are particularly relevant, as the draft policy clarifies that 'A number of war crimes in the Statute may be committed by cyber means'.[28]

The offences in question would have to be committed during an international or non-international armed conflict, which means they do not apply in peacetime. Potential offences include intentionally directing an attack (and a cyber-attack can qualify as such) against the civilian population, against individual civilians or against civilian objects, or intentionally launching an attack in international armed conflict knowing that it will cause incidental harm to civilians or widespread, long-term and severe damage to the natural environment that is clearly excessive in relation to the concrete and direct overall military advantage anticipated.[29]

Although this area of law remains subject to further clarification and no one has so far been convicted for conducting cyber-enabled war crimes, the ICC has announced it is investigating cyber-attacks against Ukraine as possible war crimes.[30] Offensive cyber operations conducted by individuals could

27 International Criminal Court, Office of the Prosecutor, 'Draft Policy on Cyber-Enabled Crime under the Rome Statute', 6 March 2025, <https://www.icc-cpi.int/sites/default/files/2025-03/250306-OTP-Policy-on-Cyber-Enabled-Crimes-for-public-consultation.pdf>, 23 January 2026.

28 *Ibid*., p. 19.

29 *Ibid*., p. 20.

30 Anthony Deutsch, Stephanie van den Berg and James Pearson, 'Exclusive: ICC Probes Cyberattacks in Ukraine as Possible War Crimes, Sources Say', *Reuters*, 14 June 2024.

therefore, under specific circumstances, amount to international war crimes. The UK is a signatory and state party to the Rome Statute.[31] No warrant issued by a UK government authority could exclude liability for crimes committed under the Rome Statute.

States have more extensive rights and obligations under international law than individuals, both in peacetime and in times of conflict. Relating to the activities of a private company, the decisive question to trigger these is whether a state is responsible for the activities of a non-state actor.[32] This is determined by establishing whether the private actor in question has acted under the necessary instruction, direction or control of a state.[33] The detailed legal debate on what these terms mean exactly and when a threshold is met triggering state responsibility for cyber activities has been conducted elsewhere.[34] Yet, it primarily concerns non-state actors, such as cybercriminals, used as proxies.

The legal mechanism chosen to deploy private sector capabilities would provide indications as to the question of whether a state is responsible for an individual's or a company's conduct in cyberspace. For example, where the individual is a reservist of the armed forces, a state is assumed to exercise sufficient control over its state organs (such as the armed forces) to automatically trigger state responsibility. A loosely worded letter of marque or a voluntary IT army without specific instructions or a degree of control over individuals' activities, however, may not necessarily trigger state responsibility. A tasking contract for activities – as described earlier – that clearly sets out scope, tasks and instructions, in contrast, may be more likely to trigger responsibility, as it may qualify as providing specific-enough instructions, direction or control depending on its exact framing. The exact

31 For a full list of states parties, see International Criminal Court, 'The States Parties to the Rome Statute', <https://asp.icc-cpi.int/states-parties>, accessed 12 May 2026.

32 There may be other examples that do not require obligations pursuant to the laws of state responsibility to be triggered, for example, due diligence obligations, such as ensuring and promoting the rules of international humanitarian law.

33 International Law Commission, 'Draft Articles on the Responsibility of States for Internationally Wrongful Acts', Article 8.

34 Kubo Mačák, 'Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors', *Journal of Conflict & Security Law* (Vol. 21, No. 3, 2016). See also national statements by states on the application of international law to cyberspace.

legal thresholds, however, remain subject to academic and legal debate. Even public attributions of cyber operations to states provide little insight into attributing states' legal interpretation of when they are considering a state responsible for a non-state actor's cyber operations.

Assuming a state has responsibility over the activities in question, it has to comply with its obligations under international law. In peacetime, these include the adherence to thorny legal concepts such as the principle of non-intervention or the principle of sovereignty. The exact legal thresholds of which still remain subject to debate – not just between scholars but also between states.[35] This is despite an increased number of state statements seeking to clarify such thresholds in their respective national statements on the application of international law to cyberspace. The UK position on the legal thresholds of sovereignty, for example, has been more permissive than that of many other countries.[36] In times of conflict, the UK would additionally need to comply with international humanitarian law obligations, set out in the Geneva Conventions and customary international law.

Any agreement that UK authorities would conclude with a private sector company to conduct genuinely offensive cyber operations that require a warrant needs to comply with the UK's international legal obligations. However, it is less clear how this would work out in practice. International legal thresholds are often blurred or unsettled and difficult to navigate for government officials in the best of times. The main considerations here would relate to international human rights law including the right to privacy,[37] principles of international law such as sovereignty, the use of force or non-intervention, due diligence obligations, state responsibility and ultimately international humanitarian law applicable in an armed conflict. Typically, there are no easy instructions to pass on that explain to a cyber security professional where there are clear red lines – after all, any lawyer would answer clarification questions with an

35 Harriet Moynihan, *The Application of International Law to State Cyberattacks Sovereignty and Non-Intervention* (London: Chatham House, 2019).

36 Michael Schmitt, 'The United Kingdom on International Law in Cyberspace', EJIL:Talk!, 24 May 2022, <https://www.ejiltalk.org/the-united-kingdom-on-international-law-in-cyberspace>, accessed 30 January 2026.

37 On challenges for compliance with human rights safeguards by private contractors, see Lock, 'Public Power and Private Hands', p. 595ff. A detailed report also highlights government's response to allegations of misuse of data by contractors. See Waller, *Report of the Intelligence Services Commissioner for 2014*.

uncomfortable 'it depends'. This also explains why a government authority would be reluctant to broaden a scope of a warrant and why a risk-averse posture is the default position – particularly in peacetime without the pressing need to scale capacity occurring during a conflict.

If the application of binding international law already paints a complex picture, voluntary or evolving norms only add to these legal challenges. The Montreux Document, a joint initiative of the Swiss government and the International Committee of the Red Cross, sets out states' obligations under international humanitarian and human rights law with respect to activities of private military and security companies.[38] Concluded in 2008, the document, however, is not a new binding treaty such as the Geneva Conventions. Instead, it is the first document to reaffirm existing international legal obligations and sets out suggested best practices.

The UK was part of the group of states that jointly finalised the document and supported its content.[39] This means that, where the UK is a contracting party to security personnel conducting offensive cyber operations, it has a number of obligations. These include an obligation to investigate and, as appropriate, prosecute or extradite those suspected of having committed international crimes (para. A6). The UK is also responsible for violations of human rights and humanitarian law if a private sector party is acting on the instructions of the UK or under its direction or control (para. A7d). Additionally, the UK would have to pay reparations for violations of international humanitarian and human rights law if wrongful conduct of a private sector company is attributable to the UK (para. A8).[40]

However, these merely confirm obligations under existing international law and are not a progressive new approach to contracting private military or security companies, nor is the Montreux Document specific to cyberspace. Critics are sceptical that these frameworks provide sufficient legal protection in a digital age where many tech companies take over critical security

38 Swiss Federal Department of Foreign Affairs, 'The Montreux Document', 1 February 2026, <https://www.eda.admin.ch/en/the-montreux-document>, accessed 8 April 2026.

39 *Ibid.*

40 UN General Assembly Security Council, 'Informal Summary of the Montreux Document By Switzerland', A/63/467–S/2008/636, 6 October 2008.

services, even if not identifying as private military or security enterprises.[41] A broader interpretation of applicable norms has been put forward by the UN's working group on the use of mercenaries, chaired by South Africa. The fourth draft agreement offers an expansive interpretation of states' obligations in relation to private security companies including to strengthen accountability of those companies, to apply human rights obligations and to affirm that state parties should not contract private military and security companies, their personnel and subcontractors to carry out activities defined as prohibited under the UN Charter, including the use of force.[42]

The draft makes clear that the proposal also applies to security companies such as 'private business entities … which provides military and/or security services … in cyberspace'.[43] Some think that the current draft's wide remit would also apply to tech companies such as Palantir and other cyber security companies providing technologies and services to states, even where they do not see themselves as private military contractors.[44] Depending on interpretation, some of the services these companies provide are already used by the UK government or the UK government may be seeking to use these in the future. The UK representative to the working group stated in April 2025 that the UK supported a non-binding agreement before discussing a legally binding instrument.[45] Progress reports on the scoping of the regulatory framework reflect state representatives' arguments to widen or broaden the interpretation of the draft agreement. US and, to a lesser extent, UK representatives have argued for a narrower scope of interpretation.[46] While

41 Vincent Bernard, 'Symposium on PMSCs: Revisiting the International Regulation of Private Military and Security Companies in the Digital Age', *OpinioJuris*, 16 July 2025, <https://opiniojuris.org/2025/07/16/symposium-on-pmscs-revisiting-the-international-regulation-of-private-military-and-security-companies-in-the-digital-age/>, accessed 30 January 2026.

42 Office of the UN High Commissioner for Human Rights, 'Revised Fourth Draft Instrument on an International Regulatory Framework on the Regulation, Monitoring of and Oversight over the Activities of Private Military and Security Companies', p. 14, <https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/igwg-military/session6/IGWG-PMSCs-Revised%20fourth%20draft%20PMSCs-Track%20Changes%20version%20-%20Copy.pdf>, accessed 12 May 2026.

43 *Ibid*., pp. 8–9.

44 Bernard, 'Symposium on PSMCs'.

45 UN General Assembly, 'Progress Report on the Sixth Session of the Open-Ended Intergovernmental Working Group to Elaborate the Content of an International Regulatory Framework on the Regulation, Monitoring and Oversight of the Activities of Private Military and Security Companies', UN A/HRC/60/39, 9 July 2025, para. 7.

46 For example, paragraphs 34 and 36 in UN General Assembly, 'Progress Report on 6th Working

the proposal for a regulatory framework on the use of private military and security companies remains under revision, with a fifth draft instrument under development, the debate demonstrates the ongoing discussion on the international legal frameworks for subcontracting private security companies for offensive cyber operations.

## Concluding Observations

The public debate on the legal challenges and implications of using private sector skills, people and capabilities for UK offensive cyber operations remains very limited. Despite several pushes from the NCF and other actors in the community to enhance communication and transparency, legal considerations often remain classified, overlooked or limited to an international law angle. Instead, attention rests on doctrinal or strategic questions and, to a lesser extent, on technical capabilities. While the international law perspective is discussed more widely than domestic legal implications, it often risks being purely academic and detached from practical insights and operational realities.

In the absence of a more mature UK debate on the topic, the US conversation continues to provide the dominant narratives on private sector engagement in offensive cyber operations. This is particularly true for concepts such as deputisation or letters of marque. However, this chapter has demonstrated that the current, apparently risk-averse UK position means that these mechanisms are less relevant – if not practically irrelevant – to the current UK context.

A US-dominant conversation, based on different risk assessments and degrees of comfort with subcontracting private military and security companies for highly sensitive tasks typically reserved to states, risks brushing over decisive legal questions for the UK context. If the public perception is that the UK debate does not differ from that in the US, legal issues such as compliance with UK domestic law or alignment with the UK's international legal positions will not receive sufficient scrutiny. But with the US-born impression that the private sector is contracted for far more offensive cyber than is necessarily the case in the UK, legal

Group Meeting', UN A/HRC/60/39, 9 July 2025.

challenges may be overlooked and dismissed as niche cases. Yet these are highly relevant legal components of one of perhaps the most pressing questions: how to responsibly scale the UK's offensive cyber capabilities for situations of crisis and conflict.

In the UK, subcontracting the private sector, specifying carefully bounded limits for activities that require a warrant, seems the most suitable legal mechanism through which bodies – such as the NCF – could currently contract private sector entities to conduct and scale activities for UK offensive cyber. This chapter has offered insights into the legal implications and questions that arise both under domestic and international law when drafting these 'tasking contracts' once a warrant has been obtained. Without further public insights from the NCF or other government bodies that can obtain these warrants, it is impossible to say how commonly used these agreements are at the time of writing this chapter.

Many other mechanisms for working with the private sector, such as via contracts for activities not requiring a warrant, are discussed more widely, but likely fall outside the scope of truly offensive cyber operations or, as is the case for letters of marque, are currently not considered as reflecting potential mechanisms in the UK.

However, it is feasible that if the geopolitical context triggered a change in the risk appetite of government departments, other legal mechanisms might become more relevant to the UK – that includes versions of letters of marque, a different form of cyber reserves or engagement with hacktivists. Further research should examine the relationship between cyber/geopolitical threat perception and resulting risk appetite. It should also consider implications for the application of other legal mechanisms to leverage private sector expertise for UK offensive cyber capabilities. Further research should also clarify which part of offensive cyber capabilities a state should never contract to the private sector, even in conflict.

## About the Authors

### Pia Hüsch

Pia Hüsch is a Research Fellow in cyber, technology and national security at RUSI. Prior to joining RUSI, Pia conducted her doctoral research on offensive cyber operations in international law at the University of Glasgow.

At RUSI, Pia conducts research on disruptive technologies, including on how national security and geopolitical considerations shape countries' science, tech and innovation policy. Pia researches tech policy issues (including AI policy), offensive cyber operations and cyber policy in the Indo-Pacific. She is a recognised expert in her field and has contributed to inquiries of the UK Foreign Affairs Committee and the UK Science and Technology Committee as well as a broad range of media outlets, including *The Economist* and the *BBC*.

### Charles Coventry

Charles Coventry is a barrister and a legal officer in the British Army. He began his career in chambers, concurrently serving as a reservist cavalry officer, before commencing full-time service as a military lawyer. He has advised on live military operations worldwide, and has taught International Law at the US Military Academy, West Point.

Charles' interests include the pragmatic application of international and domestic law to modern operations. He writes in a purely personal capacity, and thus the views expressed in this chapter do not necessarily constitute those of the UK Ministry of Defence or the UK Government.

CHAPTER 6

# Military Cyber Operations and the Art of Manoeuvre in War

**Stefan Soesanto and Wiktoria Gajos**

At the 2026 Munich Security Conference, General Sir Rob Magowan, commander of the UK's Cyber and Specialist Operations Command, observed bluntly that 'we are in a hybrid war, and one can say we are on the losing side'.[1] His remark underscored a growing concern within British defence circles: that the UK's self-conception as a 'responsible cyber power', anchored in legal and ethical restraint, may impose operational constraints in an increasingly contested digital environment.[2] The UK's 2023 strategy for offensive cyber operations seeks to reconcile capability with principle.[3] Yet the volatile geopolitical climate, much of it now unfolding in cyberspace, including during the Russo-Ukrainian War, suggests that incremental adjustment may be insufficient. If hybrid conflict and war are becoming persistent conditions rather than the exception, the UK must reassess how it develops, integrates and deploys offensive cyber capabilities in order to retain the initiative.

Offensive military cyber operations conducted in war are largely understood to be enabling capabilities that are employed in support of kinetic operations rather than independent means of decisive military force.[4] To date, no

1 Monika Ermert, 'MCSC: Cyberdefense Alone is No Longer Enough', *Heise Online*, 14 February 2026, <https://www.heise.de/en/news/MCSC-Cyberdefense-alone-is-no-longer-enough-11176706.html>, accessed 19 February 2026.

2 Stefan Soesanto and Wiktoria Gajos, 'Offensive Cyber Operations and Combat Effectiveness After Ukraine', *Lawfare*, 3 November 2025, <https://www.lawfaremedia.org/article/offensive-cyber-operations-and-combat-effectiveness-after-ukraine>, accessed 19 February 2026.

3 National Cyber Force, 'The National Cyber Force: Responsible Cyber Power in Practice', April 2023.

4 Joshua Rovner, 'Warfighting in Cyberspace', *War on the Rocks*, 17 March 2021; Lennart Maschmeyer and Nadiya Kostyuk, 'There Is No Cyber "Shock and Awe": Plausible Threats

offensive cyber operation has ever stopped a tank in its tracks. No offensive cyber operation has ever conquered physical territory. And no offensive cyber operation has ever directly killed a human being. Unsurprisingly, to many military planners, offensive cyber is thus merely one of many substitutes that could be employed against a target when kinetic actions are either politically constrained or tactically undesirable. Scholars are, on the whole, equally on the fence on the subject. Some doubt the relevance of offensive cyber for kinetic warfare altogether, while others are still debating the conditions under which offensive cyber operations might unfold their hidden potential in armed conflict.[5] However, the question may not be *whether* and *what* might make offensive cyber operations meaningful in war, but *how* manoeuvre and campaigning in cyberspace are conceptually organised to conduct independent and double-tap combat operations.[6]

Traditional manoeuvre warfare theory privileges disruption over destruction. Its purpose is not the steady erosion of enemy forces, but the collapse of coherence. By generating successive, unanticipated dilemmas and exploiting speed, initiative and operational surprise, manoeuvre seeks to outpace the adversary's capacity to decide and respond.[7] In its most kinetic form, this logic is often associated with the armoured thrusts of Heinz Guderian, where tempo and concentrated force are combined to rupture defensive lines and induce systemic paralysis. Yet cyberspace does not conform neatly to either rapid breakthrough or static defence. Manoeuvre warfare in the digital domain is better understood as a synthesis of Guderian's operational velocity and Aleksandr Svechin's concept of positional warfare.[8] From Guderian,

in the Ukrainian Conflict', *War on the Rocks*, 8 February 2022; Matthias Schulze and Mika Kerttunen, 'Cyber Operations in Russia's War Against Ukraine', *SWP Comment* (No. 23, April 2023); Frederik A H Pedersen and Jeppe T Jacobsen, 'Narrow Windows of Opportunity: The Limited Utility of Cyber Operations in War', *Journal of Cybersecurity* (Vol. 10, No. 1, 2024).

5 See, for example, Lennart Maschmeyer, 'The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations', *International Security* (Vol. 46, No. 2, Fall 2021), pp. 51–90; Jason Healey, 'Cyber Effects in Warfare: Categorizing the Where, What, and Why', *Texas National Security Review* (Vol. 7, No. 4, Fall 2024), pp. 37–50.

6 Julian E Barnes and Adam Sella, 'How Computer Warfare Is Becoming Part of the Pentagon's Arsenal', *New York Times*, 27 January 2026.

7 G I Wilson et al., 'The Maneuver Warfare Concept', *Marine Corps Gazette* (Vol. 65, No. 4, 1981), pp. 49–54.

8 Barry R Posen, *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars* (Ithaca, NY: Cornell University Press, 1984); Aleksandr A Svechin, *Strategy*, edited by Kent D Lee (Minneapolis, MI: East View Press, 1992).

it borrows the premium placed on tempo, initiative and the creation of cascading dilemmas within an adversary's decision cycle. From Svechin, it adopts the recognition that durable advantage emerges from the deliberate occupation and consolidation of critical positions within a broader system. Manoeuvre in cyberspace thus unfolds in two intertwined movements. It involves rapid, adaptive actions that disrupt, confuse and dislocate, while simultaneously embedding persistent access, control and structural leverage within key digital terrain. Breakthrough and entrenchment operate together. Speed creates opportunity and positional consolidation converts opportunity into enduring advantage.

More fundamentally, cyber warfighting still lacks both a Clausewitzian campaigning theory that coherently links tactics, operations and political purpose, and a Jominian geometry that defines decisive points, lines of operation and spatial logic for manoeuvre in cyberspace.[9] Without such theoretical architecture, cyber operations are often conceived as technical events rather than as elements of sustained campaigns with cumulative strategic effects.[10] But when conceptualised as a mix of positional accumulation and operational acceleration, cyber manoeuvre becomes a coherent mode of warfare in its own right, capable of shaping conditions, tempo and leverage across all phases of war.

To achieve some clarity on these issues, this chapter outlines six distinct cyber campaigning archetypes: (1) a manoeuvre campaign that solely focuses on adversarial military assets and command-and-control structures (Mil-Strike); (2) a campaign that specifically goes after critical infrastructures that support adversarial military operations (Base-Lock); (3) a campaign that aims to disrupt and cripple adversarial military production, maintenance and innovation facilities (Forge-Blight); (4) an economic warfighting campaign that is solely directed against an adversary's civilian economy (Val-Crash); (5) a campaign that seeks to dismantle an adversary's civilian bureaucracy

9 Carl von Clausewitz, *On War*, edited by Beatrice Heuser, translated by Michael Howard and Peter Paret (Oxford: Oxford University Press, 2007). Antoine Henri de Jomini, *The Art of War*, Restored edition, translated by G H Mendell and W P Craighill (Kingston: Legacy Books Press Classic, 2018).

10 There have been good attempts. See, for example, Gregory Conti and David Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict* (Kopidion Press, 2017).

and judiciary (Civ-Stasis); and (6) a campaign that targets assets and infrastructures that are central to population survival (Viv-Threat).

Having established these six archetypes, the chapter then maps them across seven distinct operational phases of cyber warfighting: (0) Intelligence Contest; (1) Reconnaissance; (2) Intelligence Overmatch; (3) Pre-positioning; (4) Assault; (5) Kinetic Support; (6) Warfighting and Destabilisation; and (7) Domination. Rather than treating offensive cyber operations as episodic actions in war, this phase model conceptualises them as components of sustained warfighting with varying levels of intensity and shifting concentrations of dedicated capabilities. This comparative mapping clarifies when particular campaigning logics are likely to dominate, when they operate in support of others, and how they evolve as conflict transitions from intelligence competition to war and post-conflict consolidation (Figure 1). Given the UK's commitment to being a responsible cyber power, the chapter also provides a Law of Armed Conflict (LOAC) compliance matrix for all phases of war and campaign archetypes. This outlines the UK's legal constraints and inability to effectively campaign in cyberspace (Figure 2). This analysis demonstrates that the UK's current approach imposes normative constraints that limit its tactical flexibility. As a result, less constrained adversaries can exploit legal ambiguities, placing the UK at a relative disadvantage. Overall, the chapter aims to answer two crucial questions: What type of warfighting should the UK National Cyber Force conduct? And what type of cyber campaigns are strategically and tactically relevant to win a war?

## Cyber Campaign Archetypes

The aim of a Mil-Strike[11] strategy is to produce discernible cyber effects that directly impact the kinetic battlefield – either through the disruption of adversarial data flows (including injection of false data and military orders) or a reduction in the combat effectiveness of adversarial military assets. Offensive cyber operations that target adversarial command-and-control infrastructure and military assets are the hardest to execute. However, in most cases, these are completely acceptable targets under LOAC. If we take the concept of functional autonomy – that is to say, how much a military asset is

11 Short for 'Military Strike'.

reliant on external data streams to perform its primary combat role – then we can broadly discern between two categories.

The first is independent mobile military platforms (IMMPs) that possess organic lethality, such as armoured fighting vehicles, self-propelled artillery, combat aircraft and combat vessels. While these all benefit from outside data, their primary fire-control, navigation and defensive systems are integrated on-board. If the external data link is cut, they can still manoeuvre and fight using their internal sensors. Touching IMMPs in and through cyberspace is extremely difficult – if not impossible – without conducting either close-access hacking operations or complex supply-chain infections that are planned years in advance to insert exploitable pathways.

Based on open source information, to date, no offensive cyber operation in the wild has ever succeeded in significantly degrading the combat effectiveness of an IMMP. It is equally unknown whether any defence industry tests or military red-teaming exercises have ever been executed to prove whether a manipulated microchip, embedded system vulnerability or malware injection via radio-waves could reliably trigger system failures to stall a tank, bring down a fighter jet or deactivate a ship's manoeuvring, sensing and attacking capabilities. Given current open source knowledge, the available evidence that a cyber operation could significantly degrade the combat effectiveness of an IMMP is extremely limited. Most coverage of this topic is based on non-technical reporting, speculation (for instance Israel's Suter use against Syrian radar[12]), and solely reliant on undisclosed military sources (such as German Patriot battery malfunction in Turkey[13]). Despite this lack of open source information, military experimentation in this area is highly likely ongoing – if not even already operational today. Offensive cyber operations against IMMPs are the holy grail for campaigning and manoeuvring on the digital battlefield of tomorrow. If a reliable and responsive foothold can be established within an IMMP, then other operational questions will naturally arise. These will include whether the most effective path is to manipulate an IMMP's sensing capabilities, targeting processes or the munition itself.[14]

12 Richard B Gasparre, 'The Israeli 'E-tack' on Syria – Part II', *Airforce Technology*, 10 March 2008, <https://www.airforce-technology.com/features/feature1669/>, accessed 19 February 2026.

13 Zulfikar Abbany, 'Has Germany's Patriot Missile System been Hacked?', *Deutsche Welle*, 7 August 2015.

14 Inspector General, US Department of Defense, '(U) Audit of Cybersecurity Requirements

Second are non-independent military platforms (NIMPs). These are essentially network-dependent nodes whose main function is to conduct remote sensing, data collection, and transferring orders and signals to other military assets – including radar stations, satellites, remote-piloted aircraft, electronic warfare jammers, missile defence systems, and the whole suite of military command-and-control infrastructure. Notably, NIMPs do not operate independently, and will lose their primary battlefield function when their cycle of signal intake, analysis and data transfer is disrupted. For example, electronic warfare jammers need real-time signals intelligence to match enemy frequency hopping, and missile defence systems cannot engage a target effectively without data from a distant radar or command-and-control node. Double tapping NIMPs – hitting them kinetically and disrupting them in cyberspace – is the definite way to take an asset off the battlefield. However, ultimately, the strategic objective of campaigning against NIMPs is rarely the physical destruction of the hardware itself. Rather, it is to degrade the asset's analytical processing capability or sever its data-transfer connection at a critical juncture in time and space. By doing so, an attacker can achieve a dual effect: creating windows of opportunity for kinetic exploitation on the battlefield elsewhere; and potentially inducing a state of institutional friction and a degradation in system trust to create a residual level of cognitive paralysis.[15] The possibility of exploiting the latter crucially depends on the level of persistence, stealth and the number of established footprints across a variety of NIMPs at the same time.

A Base-Lock[16] strategy deliberately targets critical infrastructure assets whose disruption would constrain an adversary's ability to mobilise, transport and sustain its military forces. Importantly, this strategy prioritises the targeting of critical infrastructure assets with high centrality, low tolerance for fluctuations, long recovery times, and strong cross-sector coupling, rather than by their immediate operational function. This campaign strategy targets dual-use infrastructure and deliberately exploits the absence of a clear, universally

for Weapon Systems in the Operations and Support Phase of the Department of Defense Acquisition Life Cycle', DODIG-2021-051, February 2021, <https://media.defense.gov/2021/Feb/12/2002581936/-1/-1/1/DODIG-2021-051.PDF>, accessed 19 February 2026.

15 Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York, NY: Simon & Schuster, 2017); Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York, NY: Crown, 2015); P W Singer and August Cole, *Ghost Fleet: A Novel of the Next World War* (New York, NY: Mariner Books, 2016).

16 Short for 'Basing and Sustainment Lock'.

recognised legal definition in international humanitarian law. This ambiguity allows attackers to operate in a grey zone between civilian and military targets. Three sectors are of particular interest. First, the telecommunications sector, including cellular networks, fibre backbones and satellite internet infrastructure. Second, logistic hubs and networks, such as railways, airports, maritime ports and cargo terminal facilities. Third, energy and power systems, spanning from electric power generation, petroleum refining and fuel production, to fuel storage and distribution assets.[17] Reconnaissance, access and pre-positioning malware are must-have capabilities for Base-Lock to unfold its full potential. Overall, we can broadly discern between four manoeuvre strategies: an asset approach; a functional approach; a fluctuation approach; and a volatility and dependency approach.[18]

An asset approach aims to target central systems within the three sectors that concentrate network risks regardless of their functional role. On an abstract level, this includes hubs, exchanges, control centres and terminals. Of particular interest are assets that sit between systems to, for example, conduct organisational handoffs, deal with different standards on each side, or are assets whose ownership and responsibilities are ambiguous.[19] More broadly speaking, an asset approach also takes advantage of identifying widespread and structurally similar systems, either through shared vendors, shared software or shared regulatory requirements.[20]

The functional approach targets organisational stress points within these three sectors. For example, when it comes to airports, attacks would aim at

17 James X Dempsey and Andrew J Grotto, 'Ensuring the Cyber Resilience of Critical Infrastructure Serving Domestic Military Installations: Questions for Senior Leadership', *Cyber Defense Review* (Vol. 10, No. 2, 2025), pp. 115–30; Michaela Lee, 'Beyond the Fence Line: Operationalizing Civil-Military Cyber Coordination at U.S. Military Installations', *Cyber Defense Review* (Vol. 10, No. 2, 2025), pp. 23–38.

18 The asset approach reinterprets Clausewitz's centre of gravity through the lens of network centrality. The functional approach applies Svechin's operational art by prioritising systemic disruption over the destruction of physical forces. The volatility approach extends Boyd's OODA (observe, orient, decide, act) loop by targeting the infrastructure conditions that enable decision-making. And the dependency approach weaponises Schelling's concept of the 'power to hurt', exploiting asymmetric interdependencies to create coercive leverage and manipulate strategic risk.

19 For example, Skylogic's role in the ViaSat hack. See Katrina Manson, 'The Satellite Hack Everyone Is Finally Talking About', *Bloomberg*, 1 March 2022.

20 Robert Plummer and Tom Gerken, 'CrowdStrike and Microsoft: What We Know About Global IT Outage', *BBC News*, 19 July 2024.

air traffic management and coordination – including systems responsible for flight scheduling, slot allocation, sequencing and safety systems that default to grounding. Since airports are deeply interdependent ecosystems, stress points also include continuous electric power flows, aviation fuel and supply, and networked systems for security, logistics and operations. The easiest and often overlooked functional weak points include manipulating credentialing and access management systems, workforce scheduling and regulatory compliance systems. Small disturbances or failures in these areas have a high chance of inducing legitimate, cascading shutdowns. Overall, airports fail as systems before they fail as runways.[21]

The fluctuation approach is somewhat similar to the functional approach in that it creates small disturbances to trigger outsized, system-wide effects. Specifically, it aims to target low-tolerance assets that have narrow operational thresholds, hard safety cutoffs and respond in non-linear ways to disturbances. These systems do not smoothly degrade but snap from nominal to unusable. As such, the asset disruption does not have to be large, just well-timed. Rhythm-dependent systems – such as systems that depend on continuous flow – are of similar interest. These can include railway timetables, fuel logistics, port operations and air traffic coordination, which all exhibit properties of high throughput, low buffering, just-in time coordination, and where cascading delays amplify. In essence, temporal disruptions matter more than duration. Another category of assets that are of interest is slow to recover assets. System traits include complex restart procedures, regulatory and safety gating, and their interdependence with other systems. Overall, assets with long recovery times exert strategic weight even if their disruption is brief.[22]

A volatility and dependency approach is aimed at figuring out how stress propagates between systems. Cross-sectoral accelerants can include power dependencies, data dependencies and fuel dependencies. So, we are not

21 Florian Piekert et al., 'Mitigation of Operational Impacts on Airports by Early Awareness of Malicious Events Impacting Linked Critical Infrastructures', *Journal of the Air Transport Research Society* (Vol. 2, June 2024).

22 Ignacio Fariza and Álvaro Sánchez, 'The Five Seconds that Plunged Spain into Darkness', *El País*, 1 May 2025, <https://english.elpais.com/spain/2025-05-01/the-five-seconds-that-plunged-spain-into-darkness.html>, accessed 19 February 2026; CERT-PL, 'Energy Sector Incident Report – 29 December', 30 January 2026, <https://cert.pl/uploads/docs/CERT_Polska_Energy_Sector_Incident_Report_2025.pdf>, accessed 23 February 2026.

searching for weak assets, but those that can spread instability the fastest. Another category of assets that fit into this approach is allocation systems that determine who gets resources first, and credential and access systems that can shut out users instantly. Even more abstractly, an attack can also aim to target psychological volatility nodes: assets whose disruption carries high symbolic visibility, erodes public trust, and triggers disproportionate political, social or behavioural responses. The disruption of these assets might thus produce second- or even third-order effects disproportionate to their physical role.

Forge-Blight[23] is a cyber campaigning strategy aimed at destroying and disrupting an adversary's ability to manufacture, assemble and repair military assets. It does so by targeting the industrial ecosystems that underpin wartime production and sustainment. Its objective is to degrade the production speed, output and material viability of military systems by impairing the processes that transform designs, components and damaged equipment into deployable battlefield assets. Rather than focusing on immediate frontline effects, Forge-Blight treats military production and sustainment as decisive terrain in their own right.

Contemporary military production relies heavily on networked IT environments that support design, logistics, quality control, scheduling and coordination across geographically dispersed actors. These functions are distributed across complex networks of prime contractors, subcontractors and specialised suppliers, all of which depend on the integrity, availability and synchronisation of shared data. Disruption within these environments can generate cascading effects that extend far beyond the initially targeted organisation, propagating delays, errors and uncertainty throughout the production ecosystem.

Within this system, small and medium-sized defence contractors represent particularly critical points of failure. While large defence firms attract attention due to their scale and visibility, smaller suppliers often provide specialised components, materials or services that are difficult to replace quickly. Their limited redundancy, constrained resources and lower resilience mean that disruptions at these nodes propagate upward through supply chains, amplifying impact and producing disproportionate strategic effects.

23 Shorthand for 'Systemic Production Decay'.

A central feature of Forge-Blight is its emphasis on military design and engineering bureaus. These institutions function as intellectual chokepoints where specifications, revisions, tolerances and upgrade pathways converge. Disruptions at this level propagate widely. Compromised design baselines, falsified tolerance data, or interference in revision control can result in scrapped components, failed assemblies, unsafe systems and costly rework across multiple production and repair facilities simultaneously.

Drone, robotic and automated manufacturing facilities occupy a similarly prominent position within the target set.[24] Uncrewed systems and industrial robotics depend on precise software control, calibration and sequencing. Forge-Blight could exploit these dependencies to induce misalignment, accelerated wear or catastrophic faults that damage machinery, destroy in-process inventory or render assembly lines inoperable. In these cases, offensive cyber operations are explicitly aimed at physical loss rather than mere degradation of performance.

Maintenance and repair infrastructure forms another critical axis of effort. Modern forces depend on rapid refurbishment to offset battlefield attrition and sustain force availability.[25] By corrupting maintenance records, diagnostic software, parts histories or certification logs, Forge-Blight could seek to cause repair efforts to fail, misfire or irreversibly damage platforms under refurbishment. Repair hubs are thus transformed from engines of recovery into sites of additional attritional loss.

Across all these target sets, Forge-Blight places particular emphasis on degrading data integrity. The insertion, alteration or desynchronisation of critical data creates logistical and organisational strain without requiring continuous system outages. Erroneous inventory records, corrupted maintenance logs, or manipulated production schedules force organisations to halt operations for verification, revalidation or manual reconciliation. This generates managerial overload and erodes trust in institutional processes.[26]

24 Daryna Antoniuk, 'Ukraine-aligned Hackers Claim Cyberattack on Major Russian Drone Supplier', *The Record*, 16 July 2025, <https://therecord.media/ukraine-hackers-claim-attack-russia-gaskar-group-drone-maker>, accessed 23 February 2026.

25 Marinko Aleksic et al., 'Analysis of Land Army Maintenance Techniques in the War in Ukraine', *Military Review* (May–June 2023).

26 For example, a much more advanced version of this Fancy Bear campaign would fit. See

Crucially, Forge-Blight blends overtly destructive actions with ambiguity. Production, assembly and repair may continue, but under degraded and hazardous conditions. Over time, industrial efficiency, morale and institutional confidence may collapse. In sum, Forge-Blight reframes offensive cyber operations as campaigns against an adversary's industrial time, capacity and survivability. When forges, assembly halls and repair facilities are degraded together, battlefield losses outpace restoration, and industrial output becomes a decisive determinant in war. Although targeting these sites offers a definite strategic benefit, it may be considered irresponsible because of the potential resulting harm to the civilian population.

Val-Crash[27] is an economic warfighting strategy. Its primary objective is to systematically degrade an adversary's economy and undermine social cohesion. Rather than seeking decisive military effects, Val-Crash targets the economic foundations that sustain a state's capacity, public confidence and political stability. Central to the strategy is the continuous collection and analysis of business and economic intelligence in order to determine where pressure should be applied, at what scale, and at what moment in time within an adversarial economic ecosystem. The scale, effects and coercive nature of a cyber operation determine its legality. If a disruptive attack reaches a high threshold of severity – meaning it causes substantial damage or permanently disables critical infrastructure – it may be deemed unlawful. Val-Crash conceptualises this pressure through three complementary manoeuvres.

The first manoeuvre focuses on identifying and exploiting economic centres of gravity. In cyberspace, these are rarely the largest or most visible corporations. Instead, they are smaller firms that sit at the intersection of vulnerability, dependency and asymmetry. Such companies provide niche software, data services, compliance tooling, logistics platforms, payment processors, or regulatory infrastructure that quietly sustain entire sectors of the economy, including financial activity.[28] Often operating below strategic

National Security Agency et al., 'NSA and Others Publish Advisory Warning of Russian State-sponsored Cyber Campaign Targeting Western Logistics and Technology Entities', Joint Cybersecurity Advisory, 21 May 2025, <https://media.defense.gov/2025/May/21/2003719846/-1/-1/0/CSA_RUSSIAN_GRU_TARGET_LOGISTICS.PDF>, accessed 19 February 2026.

27 Short for 'Value System Crash'.

28 For example, see David Maynor, Matt Olney and Yves Younan, 'The MeDoc Connection', Cisco Talos Blog, 5 July 2017, <https://blog.talosintelligence.com/the-medoc-connection/>, accessed 19 February 2026.

visibility and outside rigorous security investment cycles, these entities represent critical chokepoints. Disruption at these nodes propagates outward, generating cascading effects across supply chains, markets and institutional coordination, while obscuring attribution and intent.

The second manoeuvre targets large corporations whose scale directly drives economic output, employment and public confidence. These firms function as economic anchors within national and regional economies. Offensive cyber operations against them are designed to disrupt user access, corrupt or destroy critical data, and undermine operational continuity. Even temporary impairment can result in lost revenue, market instability, regulatory scrutiny and erosion of consumer trust.[29] Because these organisations are deeply intertwined with everyday economic life, disruptions are highly visible and socially salient, amplifying psychological and political impact beyond their immediate financial cost.

The third manoeuvre consists of calibrated, time-bound disruption of specific digital assets within targeted sectors and regions. This approach relies on selectively applied denial-of-service activity to temporarily disable platforms, services or interfaces at moments of heightened economic or political sensitivity.[30] The intent is not permanent damage, but precise interruption. By aligning disruption with key commercial periods, regulatory deadlines or public events, Val-Crash magnifies uncertainty, strains incident response capacity, and reinforces perceptions of instability.

Crucially, Val-Crash is not a blunt instrument. It is designed to operate below the threshold of outright economic collapse while steadily increasing friction, volatility and distrust. The cumulative effects are economic drag, institutional fatigue and social anxiety. Over time, reduced growth, recurring disruptions and declining confidence weaken an adversary's ability to mobilise resources,

29 For example, see Veon, 'Kyivstar Completes Preliminary Assessment of the Financial Impact of the Cyberattack', 18 January 2024, <https://www.veon.com/newsroom/press-releases/kyivstar-completes-preliminary-assessment-of-the-financial-impact-of-the-cyberattack>, accessed 19 February 2026.

30 For example, see Daryna Antoniuk, 'Ukraine's Intelligence Claims Cyberattack on Russia's State Tax Service', *The Record*, 12 December 2023, <https://therecord.media/ukraine-intelligence-claims-attack-on-russia-tax-service>, accessed 23 February 2026; A J Vicens and James Pearson, 'Suspected Israeli Hackers Claim to Destroy Data at Iran's Bank Sepah', *Reuters*, 17 June 2025.

govern effectively and sustain popular legitimacy. In this way, Val-Crash reframes cyber operations as campaigns against economic resilience itself, turning markets, platforms and trust into contested terrain.

Civ-Stasis[31] is a cyber campaign strategy designed to induce administrative paralysis as a strategic effect. Rather than targeting military forces or economic productivity, it focuses on governance itself, specifically an adversarial state's ability to regulate, adjudicate and respond to citizens' needs. By degrading bureaucratic processes and authoritative records, offensive cyber operations undermine institutional credibility, delay decision-making and generate systemic uncertainty that persists long after the technical systems are restored.[32] The objective is sustained dysfunction that erodes legitimacy, not immediate administrative collapse.

The primary targets of Civ-Stasis are functional administrative systems that sustain day-to-day governance. This campaign strategy is highly coercive and focuses on manipulation and destruction, which violates sovereignty and potentially constitutes a use of force if it causes severe civilian consequences. These include tax administrations, judicial infrastructure, civil registries, e-governance platforms, emergency response call centres, and civil protection alert mechanisms.[33] Together, these systems form the procedural backbone of state authority. When digital governance applications become unresponsive or unreliable, routine activities such as filing taxes, registering property, accessing benefits, submitting legal documents or requesting emergency assistance stall. The resulting administrative gridlock directly affects daily life and reinforces perceptions of institutional failure.

31 Short for 'Civilian Stasis'.

32 Ryan Shandler and Miguel Gomez, 'The Hidden Threat of Cyber-attacks – Undermining Public Confidence in Government', *Journal of Information Technology & Politics* (Vol. 20, No. 4, 2023), pp. 359–74; Kelly Jackson Higgins, 'DigiNotar Hacked Out of Business', *Dark Reading*, 20 September 2011, <https://www.darkreading.com/cyberattacks-data-breaches/diginotar-hacked-out-of-business>, accessed 25 February 2026.

33 *BBC News*, 'Ukraine Cyber-attack: Russia to Blame for Hack, Says Kyiv', *BBC*, 14 January 2022; Daryna Antoniuk, 'Attack Claimed by Pro-Ukraine Hackers Reportedly Erases a Third of Russian Court Case Archive', *The Record*, 15 May 2025, <https://therecord.media/russia-court-system-hack-third-of-case-files-deleted>, accessed 23 February 2026; Adam Goldman, Glenn Thrush and Mattathias Schwartz, 'Russia Is Suspected to Be Behind Breach of Federal Court Filing System', *New York Times*, 12 August 2025.

Strategic timing and sequencing are central to the effectiveness of Civ-Stasis. Early deployment of destructive malware, including wipers, can rapidly undermine perceptions of state functionality at the outset of conflict, inducing institutional paralysis and reactive governance.[34] A coherent campaign prioritises central administrative systems located in capital regions that function as mobilisation hubs and industrial centres. Disruption at this level will likely produce immediate nationwide reverberations. From this core, operations could expand outward in an irregular and deliberately unpredictable pattern, targeting regions with existing vulnerabilities such as susceptibility to extreme weather events, strained administrative capacity, or ethnic, religious and social fragmentations. By jumping unpredictably between regions and institutions, Civ-Stasis complicates response prioritisation and generates feedback effects that propagate back towards the central authorities in the capital.

A defining feature of Civ-Stasis is the deliberate corruption of administrative truth. Courts and civil registries derive authority from the assumption that their records are accurate and final. Cyber operations that generate fake judicial summonses, altered hearing notices, contradictory rulings or mass administrative communications will overwhelm institutional capacity and create legal confusion. Manipulation of civil registry data – such as birth dates, addresses, marital status, gender markers or even falsely pronouncing individuals deceased – undermines the state's role as the arbiter of legal identity.[35] These distortions could even cascade across voting systems, pensions, healthcare access, inheritance claims and law enforcement databases, producing procedural chaos with deep social and psychological consequences.

Past campaigns have often overemphasised symbolic ministries rather than functional regional administrative systems.[36] Ministries embody political authority. However, courts, registries, tax agencies and emergency coordination centres sustain governance through routines that cannot be

34 MSP Threats Security Team, 'WhisperGate Malware Targets Ukrainian Government Sites', Acronis Threat Research Unit, 16 March 2022, <https://www.acronis.com/en/tru/posts/whispergate-malware-targets-ukrainian-government-sites/>, accessed 19 February 2026.

35 Shaun Walker, 'Romanian Court Tells Man He Is Not Alive', *The Guardian*, 16 March 2018.

36 ESET Research, 'A Year of Wiper Attacks in Ukraine', 24 February 2023, <https://www.welivesecurity.com/2023/02/24/year-wiper-attacks-ukraine/>, accessed 19 February 2026.

improvised or bypassed. Damage to these systems produces lingering effects that are difficult to reverse.

Ultimately, Civ-Stasis seeks to transform governance from a source of order into a generator of instability. By degrading the state's ability to tax, adjudicate, identify, protect and communicate, administrative disruption weakens legitimacy and forces reactive, often coercive, state responses. Integrated into a broader conflict strategy, Civ-Stasis functions as a force multiplier, slowing state response, amplifying internal tensions and undermining public confidence long after systems come back online.

Viv-Threat[37] is a cyber campaign that targets population-sustaining systems, representing the most coercive form of non-kinetic warfare. Unlike operations aimed at military forces, economic performance or administrative capacity, Viv-Threat focuses on infrastructures that sustain everyday life and human security. Water treatment facilities, sewerage systems, rubbish collection, traffic control networks, food supply chains and hospitals constitute the material foundations of population welfare.[38] Interference in these systems directly challenges the state's core obligation to protect life and maintain social order.

The strategic purpose of Viv-Threat is compelled submission rather than destruction.[39] The tactical objective is not genocide or permanent national annihilation, but to demonstrate that the state cannot fulfil its protective role. Central to the strategy is the principle of systemic collapse. Isolated disruptions can often be managed, but near-simultaneous failures across multiple life-sustaining systems overwhelms institutional coping mechanisms. When water, healthcare, transportation, food distribution and emergency services fail altogether, the state's inability to coordinate recovery or communicate effectively becomes visible. Governance itself appears to unravel under cumulative stress.

37 Short for 'Vital Infrastructure Vulnerability Threat'.

38 Cybersecurity and Infrastructure Security Agency, 'IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities', Cybersecurity Advisory, AA23-335A, 18 December 2024, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a>, accessed 19 February 2026.

39 Inspired by Thomas C Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966).

A secondary effect, population herding, exploits selective targeting by degrading infrastructure in some regions while leaving others functional. Populations migrate to the spared zones, overloading housing, medical services and logistics, pushing stable areas towards administrative and social failure. Depopulated regions suffer economic collapse and loss of control.[40] Herding multiplies pressure by forcing the state to manage simultaneous humanitarian inflows and governance breakdown, making subsequent attacks on life-sustaining infrastructure far more devastating.

The operational impact of Viv-Threat is shaped by identified threshold dynamics. The key question is not whether harm occurs, but where disruption crosses from tolerable suffering into humanitarian crisis or long-term depopulation pressures. Thresholds vary depending on factors such as climate, geography, infrastructure redundancy and social resilience. In energy- or water-scarce environments, limited interference can escalate rapidly, whereas more resilient systems absorb shocks with less immediate effect. This campaign strategy violates all principles of LOAC, since it is focused on attaining the maximum harm to human life.

Viv-Threat can be employed at two strategic extremes. Early in conflict, simultaneous disruption of multiple systems produces immediate shock, collapsing confidence before adaptation. Late in conflict, it can serve as a final coercive lever when negotiations stall or the adversary nears submission. Targeting the capital likely amplifies impact, as its failure signals systemic collapse radiating outward from the administrative core. Ultimately, Viv-Threat is an instrument of coercive dominance, not attritional destruction. Its strategic purpose is to accelerate political outcomes by converting civilian vulnerability and population movements into leverage.

## Seven Phases of Cyber Warfighting

The operationalisation of the seven cyber campaign archetypes unfolds across a sequential and interdependent set of phases in war, each marking a distinct intensity of digital warfighting. These phases determine how access,

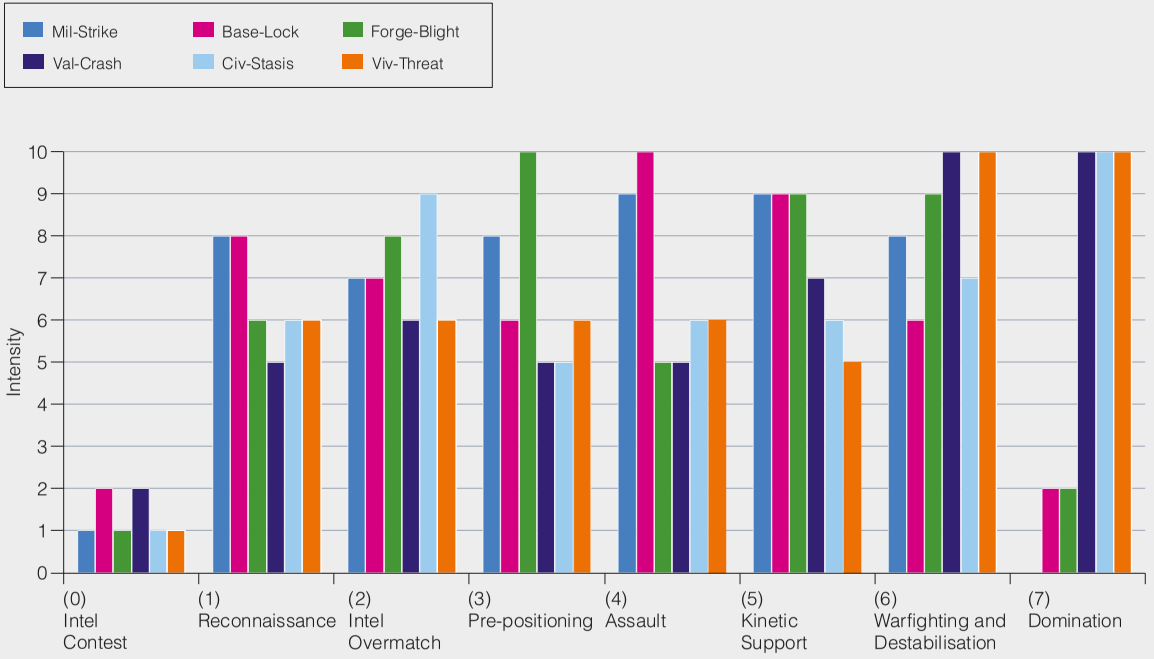
40 Similar to this example, Peter Dickinson, 'UN Report: Russia Targets Civilians in Systematic Bid to Depopulate Ukraine', Atlantic Council, 28 October 2025, <https://www.atlanticcouncil.org/blogs/ukrainealert/un-report-russia-targets-civilians-in-systematic-bid-to-depopulate-ukraine/>, accessed 24 February 2026.

control, and effects accumulate over time. Far from isolated operations, they form a continuous campaign flow, revealing when strategies take the lead, support others or combine to shape the trajectory of battle in cyberspace.

Figure 1 assumes that each manoeuvre strategy operates under a fixed resource ceiling of 50 intensity points distributed across seven phases of cyber warfighting. The constraint is deliberate. It reflects the reality that offensive cyber operations are limited by scarce resources such as operator workload, intelligence collection, available access, and more. Allocating more intensity points to one phase necessarily means allocating fewer points to others. The figure therefore does not depict what is possible in the abstract, but what is prioritised under conditions of scarcity. Intensity represents both strategic emphasis and operational volume. A high value indicates that a given strategy consumes a disproportionate share of cyber offensive capacity in a particular phase. The figure views cyber campaigning as a problem of portfolio management and target focus over time.

The capacity ceiling can be expanded by turning to allied forces, the private sector or by mobilising civilian hackers. Civilian hackers are easiest to integrate in Val-Crash, Civ-Stasis and Viv-Threat strategies. The private sector would preferably be leveraged in Mil-Strike, Base-Lock, Forge-Blight, Val-Crash and Civ-Stasis campaigns. And allied forces – constrained by LOAC – could provide surge capabilities to run Mil-Strike, Base-Lock and Forge-Blight campaigns.

**Figure 1:** Intensity of Cyber Campaign Manoeuvre Across the Phases of War




***Source:*** *The authors.*

### Phase 0: Intelligence Contest

The intelligence contest phase is the baseline condition of geopolitical contests and intelligence operations inside and outside of cyberspace.[41] In the intelligence contest phase, the level of intensity is minimal across all strategies. No signs of war have yet emerged, and no decision to go to war has yet been taken. Capacity is being conserved. Early investments focus on access cultivation and option preservation rather than sustained effect creation. Base-Lock and Val-Crash receive slightly higher allocations than Mil-Strike or Forge-Blight, reflecting the long lead times required to map civilian, financial and infrastructural systems. Heavy allocation here would prematurely consume scarce access and political capital.

### Phase 1: Reconnaissance

In the reconnaissance phase, the intensity of operational conduct in and outside of cyberspace increases sharply across all strategies as access validation, targeting refinement and dependency mapping accelerate. The reconnaissance phase is a critical first step that consists of passive and active intelligence collection to identify potential vulnerabilities in adversarial systems and networks. Mil-Strike and Base-Lock rise prominently, reflecting their reliance on precise targeting and junction identification. Forge-Blight and Civ-Stasis also expand, driven by the need to map industrial, bureaucratic and civilian-facing infrastructures before escalation. This phase reflects the transition from abstract intelligence competition to campaign preparation, where informational asymmetries begin to solidify.

### Phase 2: Intelligence Overmatch

In the intelligence overmatch phase, the decision to go to war in cyberspace has been taken. The planning for designating targets in cyberspace is now in full swing. This phase shows the first real divergence. Forge-Blight and Civ-Stasis peak or near-peak as informational dominance over complex production and administrative systems becomes decisive. Mil-Strike remains high, but begins to plateau, while Val-Crash and Viv-Threat continue a steady ascent. This distribution highlights that intelligence overmatch in cyber

41 Our definition of intelligence contest is much narrower than the one used in Robert Chesney and Max Smeets (eds), *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest* (Washington, DC: Georgetown University Press, 2023).

conflict is less about battlefield awareness and more about deep structural comprehension of adversarial systems and processes.

### Phase 3: Pre-positioning

The pre-positioning phase marks a critical divergence among strategies. Its purpose is to ensure that when conflict arises, actions can be taken immediately. Forge-Blight reaches its maximum intensity, reflecting the heavy investment required to manipulate complex supply chains and production networks ahead of open conflict. Mil-Strike and Base-Lock remain elevated but begin reallocating capacity towards imminent execution. Civ-Stasis and Val-Crash stabilise at moderate levels, emphasising latent disruption over immediate effect. This phase illustrates the cumulative nature of cyber manoeuvre: earlier investments condition later outcomes. Not all designated targets need pre-positioned malware. Commanders must find a balance between maintaining access and payloads being discovered prematurely.

### Phase 4: Assault

The war in cyberspace commences. Base-Lock consumes its largest share of points, peaking decisively. The priority is immobilisation of the adversary: transport, fuel, energy and communications become decisive constraints. Mil-Strike also peaks, tightly coupled to future kinetic manoeuvre. Forge-Blight drops sharply, reflecting a conscious reallocation away from long-term industrial effects towards immediate operational payoffs. Capacity scarcity forces a clear choice: constraining adversarial force movements and command structures takes precedence over targeting military production.

### Phase 5: Kinetic Support

Kinetic warfighting commences. The strategic intensity in cyberspace is being redistributed. Mil-Strike and Base-Lock begin to decline, having largely exhausted their allocated capacity. Forge-Blight rebounds modestly, while Val-Crash and Civ-Stasis increase, reflecting a shift towards economic pressure, governance disruption and resilience erosion. Viv-Threat remains constrained, signalling its limited utility during conventional force-on-force engagements. This phase captures the transition from decisive entry effects to sustained pressure.

### Phase 6: Warfighting and Destabilisation

This phase absorbs the largest cumulative share of capacity across most strategies. Forge-Blight, Val-Crash, Civ-Stasis and Viv-Threat all reach high

or near-maximum intensity, reflecting the prolonged, systemic character of modern conflict. Rather than seeking immediate operational collapse, cyber effects are applied to degrade endurance, complicate recovery and amplify internal strain. The model emphasises persistence, compounding disruption and strategic exhaustion as defining features of this phase.

### Phase 7: Domination

In the final phase, remaining capacity is fully concentrated among Forge-Blight, Val-Crash, Civ-Stasis and Viv-Threat, all of which reach maximum intensity. Mil-Strike and Base-Lock fall to minimal levels, having front-loaded their effects earlier in the campaign. The allocation reflects a decisive shift from contesting forces to shaping post-conflict conditions through sustained disruption of production, governance and social coherence. Domination, in this model, emerges not from cyber-enabled battlefield success, but from the long-term denial of an adversary's ability to reconstitute power.

Figure 2 shows how each cyber campaign maps when it comes to their likely compliance with LOAC. The figure highlights where operations align with, or risk breaching, international humanitarian law – and by extension the UK's commitment to being a responsible cyber power. Civilian-focused strategies naturally score lower, especially in the later phases of war, while military-focused campaigns generally score higher.

**Figure 2:** Law of Armed Conflict (LOAC) Compliance Matrix

| Campaign Strategy | Primary Object of Attack | Distinction Risk | Proportionality Risk | Military Necessity Argument Strength | Precaution Complexity | Relative LOAC Compliance |
|---|---|---|---|---|---|---|
| **Mil-Strike** | Military assets (IMMPs and NIMPs) | **Low** (if strictly military targets) | **Moderate** (depending on cascading effects) | **Strong** (direct battlefield advantage) | **High** (technical precision required) | **High** (when tightly targeted) |
| **Base-Lock** | Dual-use critical infrastructure (telecoms, logistics, energy) | **High** (civilian character risks) | **High** (forseeable civilian harm) | **Contested** (depends on sustainment linkage) | **Extremely Complex** (cascading effect) | **Low to Medium-Low** |
| **Forge-Blight** | Defence-industrial ecosystem and supply chains | **Medium to High** (dual-use industry | **High** (physical and workforce impact risk) | **Moderate to Strong** (if tied to military production) | **High** (indirect civilian labor effect) | **Medium** (context dependent) |
| **Val-Crash** | Broader economic systems and major corporations | **Very High** (primarily civilian objects) | **High and Diffuse** (economic and social harm) | **Weak** (unless direct war sustainment link) | **Difficult** (economic unpredictability) | **Low** |
| **Civ-Stasis** | Civil governance systems (courts, registries, tax) | **Very High** (civilian objects) | **High** (societal and procedural harm | **Weak** (rarely direct warfighting relevance) | Nearly impossible to isolate civilian impact | **Very Low** |
| **Viv-Threat** | Population-sustaining infrastructure (water, hospitals, food) | **Extremely High** | **Extremely High** (severe civilian harm forseeable) | **Very Weak** under LOAC | Civilian harm largely unavoidable | **Near-Zero** / Presumptively unavoidable |

***Source:*** *The authors.*

## Conclusion

The modelling of the six cyber campaign strategies tried to demonstrate that the UK can conceptualise offensive cyber operations as stand-alone instruments of manoeuvre warfare, and that these can be governed by their own logics of operational intensity, capacity concentration and endurance across the seven phases of cyber warfighting. By imposing explicit capacity constraints, the chapter showed that cyber effectiveness emerges from sustained, phase-aligned pressure rather than isolated and transient effect operations. The model suggests that UK offensive cyber operations can be most decisive when they systematically degrade an adversary's ability to generate, sustain and regenerate power across the military and political economy of war. The core implication is that UK offensive cyber operations do not have to derive their strategic value from their proximity to kinetic force. Rather, they can generate independent effects that determine the tempo, pressure and outcome of modern war.

The chapter also reaches an uncomfortable conclusion: the UK's commitment to being a responsible cyber power risks becoming a strategic constraint in future wars. If the National Cyber Force seeks decisive outcomes, it cannot rely on excessive caution. The battlefield will reward speed, persistence and ruthless prioritisation. To dominate, the UK must degrade adversary military, industrial and governance capacity while exploiting systemic vulnerabilities to multiply pressure. Adversaries will not show reciprocal restraint. In cyber warfighting, self-limitation invites exploitation. Power will accrue to those prepared to impose systemic disruption faster and at a greater scale than their opponent can absorb.

## About the Authors


### Stefan Soesanto

Stefan Soesanto is the former head of the cyber defence team at the Center for Security Studies at ETH Zurich.

### Wiktoria Gajos

Wiktoria Gajos is a researcher at the Center for Security Studies at ETH Zurich. She focuses on civil–military integration and critical infrastructure cyber security, with particular attention to the role of digital operations in conflict settings.


### Disclaimer

Generative AI tools were used in a limited editorial capacity to support drafting and phrasing. All substantive analysis, arguments and conclusions are the authors' own.

CHAPTER 7

# Adapting the UK's Approach to Responsible Cyber Effects for the 2030s

**DW**

Since publishing its National Cyber Strategy in 2022,[1] the UK government has positioned itself as a responsible cyber power, defined (to an extent) by the UN's 13 cyber norms,[2] and the Tallinn Manual on Cyber International Law.[3] Yet there is no internationally agreed definition of what it means to be a responsible cyber power, despite significant policy and academic literature on the topic.[4]

As a follow up to the UK's 2022 National Cyber Strategy, in 2023, the National Cyber Force (NCF) published 'Responsible Cyber Power in Practice' (RCPiP), a public explanation of what it considers responsible cyber effects operations to be, and how they are conducted. Within the document, the NCF lays out three operational principles: accountability; precision; and calibration. It further explains how it applies these to all cyber effects operations it carries out. [5]

1 HM Government, 'National Cyber Strategy 2022', December 2022.
2 Bart Hogeveen, 'The UN Norms of Responsible State Behaviour in Cyberspace', *ASPI Policy Brief* (March 2020).
3 Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).
4 Marcus Willett, *Cyber Operations and Their Responsible Use* (Abingdon: Routledge, 2024), p. 212; Louise Marie Hurel, 'New Ways to Frame Responsible Cyber Behaviour Beyond the UN', *RUSI Occasional Papers* (May 2025), p. 10; Gatra Priyandita and Louise Hurel, 'Responsible Cyber Behaviour in the Indo-Pacific: Views from Cambodia, Fiji, India, Indonesia, Japan, Pakistan and Taiwan', *ASPI Policy Brief* (January 2025), p. 4.
5 National Cyber Force, 'National Cyber Force: Responsible Cyber Power in Practice', p. 14.

The UK has, until now, been able use its permanent membership of the UN Security Council to promote its responsible approach to cyber activity.[6] However, technological innovation and rising multipolarity mean that the context for responsible cyber operations is changing. Without adaptation, there is a risk that the current understanding and concepts of responsibility in cyberspace become irrelevant or even constraining for the UK.

This chapter seeks to challenge the UK's current operational principles of cyber effects operations, and aims to suggest changes to the principles of accountability and precision to meet the challenges of the future. First, it envisions three plausible futures in 2035, and their impact on cyber effects operations. It then compares those plausible contexts with the approach taken by the UK and, specifically, the NCF. Finally, this chapter suggests policy adaptations to ensure that the UK's approach, and specifically the operational principles stated within RCPiP, remain relevant into the next decade.

To focus the discussions, the chapter states some assumptions and constraints up front. The chapter focuses on cyber effects delivered over/on the internet, rather than considering proximal or electromagnetic-delivered operations. It also assumes that the UK maintains technical ability to conduct effective cyber operations against emerging technologies. It is reasonable that for every exploitative opportunity that evolves, there will be a security patch or protection. However, to focus considerations on policy rather than technology, the chapter keeps the discussion to what we might be able to do, rather than what we might not. Finally, this analysis focuses on the likely, rather than all plausible, technological advancements over the next decade.

## Taking a Scenario Approach

The future is impossible to predict. Given the high levels of uncertainty and limited agency over what lies ahead, this chapter uses a scenarios methodology to develop and consider several alternative options.[7]

6 World Economic Forum, 'Global Cooperation Barometer 2025', January 2025, pp. 15, 20–22.
7 *Futures Workshop* podcast, 'Bill Sharpe on Three Horizons', Episode 1, 25 July 2024, 54:29.

The methodology used in developing this analysis is a combination of Peter Schwartz's scenario approach,[8] and that proposed by David Wright, Bernd Stahl and Tally Hatzakis.[9] There are a range of driving forces of change.[10] These include international consensus on what is or is not responsible, the connectivity of the internet of things, and the challenge between decentralised and cloud-based visions of the future internet. These all present changes, opportunities and challenges to the status quo.[11] However, two stand out as being particularly opaque and impactful.

The first is the form of future global tech leadership – whether a multipolar state-centric or a globalised non-state-led order is pre-eminent. While these alternatives are not necessarily in direct opposition, they were chosen to draw out the challenges which emerge from state versus commercial leadership. The logical opposites to multipolar/globalised leaderships (either a single hegemonic state leader, or no state leadership whatsoever), were deemed to be implausible futures and so discounted.

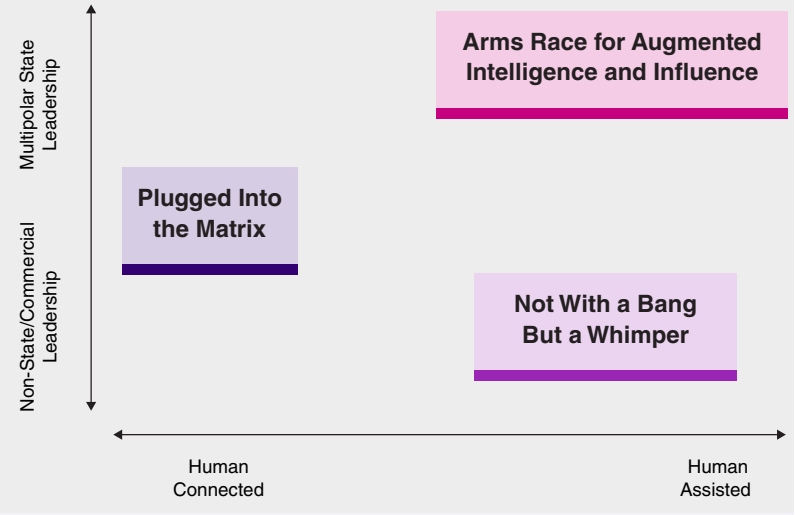
The second is the level of integration between humans and computers, scaling from a limited level of human augmentation through to physical brain/human-to-computer interfaces. RCPiP states the role of cyber effects operations is 'to change adversary behaviours by exploiting their reliance on digital technology' – therefore the relationship between adversaries and technology is a crucial variance to understand.[12]

Traditional futures methods place key drivers on an X–Y chart, resulting in four potential future scenarios. In developing scenarios for this study, these were refined using the plausibility and legitimacy factors defined in Wright, Stahl and Hatzakis to give the three scenario logics shown below in Figure 1.[13] I discounted potential futures combining human–computer connectivity and either sole-state or sole-commercial leadership, which felt

8 Peter Schwartz, *The Art of the Long View: Planning for the Future in an Uncertain World*, 2nd edition (New York, NY: Doubleday, 1996), pp. 241–48.
9 David Wright, Bernd Stahl and Tally Hatzakis, 'Policy Scenarios as an Instrument for Policymakers', *Technical Forecasting and Social Change* (Vol. 154, February 2020).
10 Schwartz, *The Art of the Long View*, p. 243.
11 Development, Concepts and Doctrine Centre, 'Global Strategic Trends', 7th edition, Ministry of Defence, September 2024.
12 National Cyber Force, 'National Cyber Force: Responsible Cyber Power in Practice', p. 14.
13 Wright, Stahl and Hatzakis, 'Policy Scenarios as an Instrument for Policymakers', p. 4.

implausible, instead settling for a mid-value. While the other two scenarios feature both commercial and state leadership, plausible and legitimate logics could be drawn to explain why one or the other had the pre-eminence of leadership.

**Figure 1:** Scenario Logics




***Source:*** *The author.*

## Scenario 1: Plugged into the Matrix

The first scenario is built on a future with increased connectivity between humans and computers, featuring norms and standards set by non-state actors, such as tech giants and industry.

The world is optimistic in 2035, having emerged from a very chaotic late 2020s. The 2028 war between the US and China over Taiwan was short but destructive, a pyrrhic victory for China following Taiwanese capitulation. However, it was relegated to the history books as a warmup for the destruction caused by a global pandemic in 2029. The effects of this pandemic were greatly exacerbated by a lack of leadership from states still trying to recover from war. Major corporations were the only group emerging positively from the chaos of the late 2020s, curing

the pandemic and driving economic growth. The targeting of Western web and cloud infrastructure as part of the Taiwan conflict led to the emergence of a new order of technology giants, primarily with bases in China and the Middle East.

Scarred by the second pandemic in a decade, industry capitalised on an increasingly health-conscious consumer base. Evolving from medical experiments and strategies published in the 2010s, the 2020s sees connected technologies grow from simple health status monitoring to personalised applications tracking emotions and stress and providing wearers with advice and remote interventions.[14] By 2033, human–computer interfaces have further developed, commercialising human links to the Internet of Things, with elites racing to be the first to demonstrate their control and connectivity at home.

Some ethical discourse has challenged the increasing connectivity of these systems, although the preoccupation of state leadership with recovering from conflict and financial challenges meant major corporations were able to overwhelm and discredit those challenging human–computer integration. That has not stopped some investigative reports emerging from authoritarian states claiming that alleged dissidents are being forcibly fitted with implants, enabling authorities to track their movements and activity as part of a second generation of Smart City technologies.

In this future, the reduced distance between people and computers could make cyber effects operations aimed at influencing decision-making even more impactful than today. In the UK, unlike in some other states, particularly China,[15] the thinking on the implications of brain–computer interfacing has yet to be thoroughly considered.[16] As a result, understanding how to calibrate operations exploiting brain–computer interfaces against their potential intended and unintended impacts is challenging. Without any legal or ethical accountability mechanisms, the UK is not only unable to use these opportunities, but is also on the conceptual back foot compared with potential future challengers.

14 Daria Impiombato et al., 'Persuasive Technologies in China: Implications for the Future of National Security', *ASPI Policy Brief* (November 2024).

15 *Ibid*.

16 Regulatory Horizons Council, 'Neurotechnology Regulation', November 2022.

## Scenario 2: The Arms Race for Augmented Intelligence and Influence

The second scenario moves away from direct connectivity, with computing augmenting and automating decision-making. China benefited from a late 2020s 'surge' in leadership and technological capability. It 'won' the AI implementation race in 2027–28 and was able to enact an increasingly assertive global foreign policy following the peaceful annexation of Taiwan in 2031.

Meanwhile, controversial US elections in 2028 and ensuing violence and financial instability led to an industrial slowdown in the West. Faced with turmoil and inward-looking policies, global audiences and technology giants sought to coordinate through regional organisations and structures, although the funding and global convening power of China meant that, by 2035, Beijing was regarded as *the* global leader, if not quite the hegemon.

Towards the end of the 2020s, China began to capitalise on its position of global leadership, exploiting its 'China Standards 2035' strategy to export control and influence across the world.[17] In 2032, the UN adopted the BRICS-led 'International Principles on Cyber Sovereignty', enshrining total state sovereignty of a state's cyber infrastructure into international law and challenging any form of intervention against a third party.

Alongside securing the legal basis for Smart Cities and Regions, the largely peaceful annexation of Taiwan enabled a commercially savvy Chinese Communist Party to demonstrate, enhance and export the concept to the increasing number of paranoid autocratic leaderships across emerging states.

Powered by the commercialisation of 6G in the late 2020s and increasingly powerful but economical generative AI tools, the scope of Smart City operations has gradually moved from city to provincial and regional levels.[18] Complete connectivity at a national level, able to fuse and forecast

17 Matt Sheehan, Marjory S Blumenthal and Michael R Nelson, 'Three Takeaways from China's New Standards Strategy', Carnegie Endowment for Peace, 28 October 2021.

18 Sanjeev Sharma et al., 'The Role of 6G Technologies in Advancing Smart City Applications: Opportunities and Challenges', *Sustainability* (Vol. 16, 2024).

environmental data, vessel and people movements and real-time surveillance across entire states is now available to security-conscious regimes.[19] The operationalisation of this approach caused significant consternation in the US, when in 2033 Huawei unveiled a concept for the 'Panama National Brain' – a fully connected system providing national-level awareness to Panama's leadership.

The high levels of speed and connectivity in these Smart Cities have also driven an explosion in targeted influence and censorship. Emerging in the early 2020s, the concept of hypersuasion has become a reality – pairing machine learning tools and generative AI models to shape, exploit and provide content to users at speed and driven by state censoring and manipulation.[20]

The connectivity and accessibility of information in the linked Smart City brain concepts provide obvious targets for operations to disrupt or alter the situational awareness of decision-makers. Conducting precision operations against these targets will be challenging as adversaries focus on securing these vital systems. Furthermore, the UK's ability to conduct operations against Smart Cities has been challenged by the new global leadership, legislation and standards on cyber effects operations. Accountability to international law, which the UK has found itself signed up to, increasingly denies the legal freedoms to conduct operations, and calibrating the impact and escalatory reactions of adversaries is increasingly challenging given growing international consensus on concepts of cyber statehood which do not align with those of the UK.

## Scenario 3: Not with a Bang, but with a Whimper – Corporate Leadership in an AI-sceptical World

The final scenario is one where technological advances are slowed by a sceptical public, despite industry's attempt to drive advances.

19 Valentin Webber, 'China's Smart Cities and the Future of Geopolitics', LSE Strategic Update, May 2023.

20 Impiombato et al., 'Persuasive Technologies in China'; Floridi Luciano, 'Hypersuasion – On AI's Persuasive Power and How to Deal with It', *Philosophy and Technology* (Vol. 37, May 2024), pp. 64–74.

Faced with disagreement, diverging priorities and ineffective cooperation while AI commercialisation emerged in the late 2020s, the international state structure stalled and failed to provide coherent guardrails and incentives against the misuse and exploitation of generative AI tools. An unregulated and uncontrolled industry stepped into the void, but the misuse and exploitation of early AI undermined public confidence and acceptance.

Emerging in the late 2020s, the industrial metaverse became a driver in enhancing the efficiency and safety of commercial operations.[21] By virtually modelling and mirroring industrial processes, factories were able to anticipate where processes were likely to fail. This concept was also adopted in medicine, enabling virtual testing of medicines on models, or digital twins, of real patients.[22] However, these groundbreaking achievements have been undermined by misuse of the underpinning technologies. In 2031, a global advertising consortium was bankrupted by a digital-twin scandal when it was discovered it was creating huge models of target populations containing sensitive individual data to test and tailor campaigns of hypernudging advertisements.

Computer augmentation has also been developed in other fields. Most business intelligence teams are now augmented by some degree of machine intelligence, protected to an extent by the incorporation of machine-behavioural science and ethics into the occupational health profession. There have been commendable attempts to make these agentic AI capabilities more personable through the incorporation of emotionally intelligent models. However, advances in this field have been misused, and increasingly convincing organised fraud using realistic AI-driven persona models have become the costliest form of crime in the 2030s.

The advances in AI testing and augmentation in this scenario would bring additional opportunity in the cyber effects space. Being able to develop virtual models of audiences, particularly key influence targets, might allow the testing or rehearsal of approaches and messages in a sandbox environment,

21 MIT Technology Review Insights, 'The Emergent Industrial Metaverse', *MIT Technology Review*, 2024, <https://www.technologyreview.com/2023/03/29/1070355/the-emergent-industrial-metaverse/>, accessed 28 November 2025.

22 Mickaël Ringeval et al., 'Advancing Health Care with Digital Twins: Meta-Review of Applications and Implementation Challenges', *Journal of Medical Internet Research* (Vol. 27, 2025).

increasing the eventual likelihood of success (and supporting the calibration principle of RCPiP).

## Adapting the UK's Responsible Approach to Operations

The three scenarios discussed here are by no means exhaustive, exclusive or independent. While the crises and technologies discussed are all plausible, the challenge remains to identify the commonalities which will impact the UK's current approach to cyber effects operations. All three scenarios identify changing global leadership at varying levels, an increasing dependence of decision-makers on computer representations of the world and the speeding up of decision-making. Based on the issues highlighted in these scenarios, I propose some changes to the operational principles within RCPiP, specifically on precision and accountability.

The focus on precision within the UK's operational principles is the first element of the UK's approach which needs adapting. Instead, the focus needs to be on proportionality. In cyber, as in more traditional domains, operations and the weapons developed to conduct them have concentrated on achieving precision and accuracy. However, this drive for accuracy means that should an operation miss, or not be able to affect its intended target, an entire new cycle of target development and strikes, with their associated costs – both financial, and creeping breadth and employment of cyber tools – must be conducted. In conventional operations this challenge has been termed the precision paradox,[23] and the premise behind it is equally applicable to the world of cyber effects operations. It is potentially of even more importance in cyber operations, where an attempted attack vector could be patched or protected against in a matter of hours.[24] Incorporating the use of AI tools to rapidly adapt or reattack targets, where the initial intent was or could not be met, would reduce the potential impact of this.

23 Amos C Fox, 'Precision Paradox and Myths of Precision Strike in Modern Armed Conflict', *RUSI Journal* (Vol.169, Nos 1–2, 2024), pp. 62–74.

24 Matthias Schulze, 'Cyber-Operationen in Den Kriegen in Der Ukraine Und Im Gazastreifen: Noch Keine Revolution Der Kriegsführung' ['Cyber Operations in the Wars in Ukraine and the Gaza Strip: Not Yet a Revolution in Warfare'], *Zeitschrift Für Außen- Und Sicherheitspolitik* (Vol. 18, No. 2, 2025), pp. 229–50.

In technological terms, emerging AI capabilities have already demonstrated the ability to increase the speed of understanding and subsequent delivery of cyber effects activities, both for influence and disruptive ends.[25] The scenarios also highlight the increasing connectivity and interdependence between computer and internet systems, opening up increasing numbers of accesses which adaptable cyber effects operations would be able to rapidly exploit. However, in policy terms, the UK does not yet seem ready to remove some of these constraints. Defence's own guidance on the implementation of AI and automation tools focuses on safety, and the *augmentation* of humans. The Ministry of Defence policy position suggests that 'rigorous human control over AI-enabled systems' does not always need 'some form of real-time human supervision' – however this is couched in the context of defensive, rather than offensive activities.[26]

Adapting the operational principles to include proportionality rather than precision in no way implies that UK cyber effects operations should become irresponsible or indiscriminate. Indeed, the Tallinn Manual's own definition of proportionality makes clear the factors that planners would need to consider.[27] But engendering an approach which bounds a target and encourages adaptability and flexibility will enhance the UK's approach to cyber effects operations in the futures considered earlier.

Giving cyber effects operators the boundaries of what is or is not proportional and allowing them to develop and employ autonomous and intelligent tools, which can rapidly switch from planned targets to emerging or fleeting proportionate opportunities, will increase the effectiveness of access to a target and reduce the potential for the 'precision paradox' against cyber targets. Redefining the UK's operational principles now to include 'proportionate' rather than 'precise' will help to engender the flexible and opportunistic mindset needed in the planners of cyber effects operations – while ensuring that they remain cognisant of accountability to legal and policy constraints.

25 Alex Moix, Ken Lebedev and Jacob Klein, 'Detecting and Countering Misuse of AI', Anthropic Threat Intelligence Report, 27 August 2025, <https://www.anthropic.com/news/detecting-countering-misuse-aug-2025>, accessed 8 January 2026.

26 Ministry of Defence, 'Ambitious, Safe, Responsible: Our Approach to the Delivery of AI Enabled Capability in Defence', Policy Paper, June 2022.

27 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, pp. 470–73.

The principle of accountability is the second area within the UK's operational principles that will be challenged by the futures envisioned above. Rather than a change in entirety, there are two areas where more nuanced adaptation will be required. This will ensure that the UK is able to conduct impactful cyber effects operations in the future.

The first is the centrality of the rules-based system to the UK's national values, and what is considered responsible. The UK's views on conducting cyber operations responsibly emerge from the rules-based order, a system in which 'the UK has been able to secure for itself a position enabling it to punch above its weight internationally'.[28] However, many argue that the rules-based international order has been superseded,[29] and even UK policy – such as the 2025 National Security Strategy – removed references to it.[30]

In all the scenarios explored, the various international systems departed from today's status quo. If this continues to be the case, the legal and technical leadership the UK perceives that it enjoys on defining and exploiting the definition of responsible cyber operations may well be challenged.

Currently, the UK's views on elements of responsibility defined in law, such as state sovereignty, differ from many others in the international community. While the UK considers that concepts associated with state sovereignty do not necessarily translate to cyberspace,[31] others, including traditional allies such as France, do.[32] This approach is also echoed by other states. China, for instance, makes it clear that infringing on its cyber infrastructure is 'a violation

28 Nicholas Wright, 'The UK and the International Rules-Based System', Foreign Policy Centre, 8 September 2020, <https://fpc.org.uk/the-uk-and-the-international-rules-based-system/>, accessed 12 January 2026

29 Fangyin Zhou, 'The Changing United States Policy and the Dissolving Liberal International Order', *China International Strategy Review* (Vol. 7, November 2025), pp. 181–94; Amitav Acharya, 'The Decline of the West and the Rise of "The Rest" Will Lead to a New World Order', *World Today*, 16 December 2025.

30 HM Government, *National Security Strategy 2025: Security for the British People in a Dangerous World*, CP 1338 (London: The Stationery Office, 2025), p. 14.

31 Foreign, Commonwealth & Development Office, 'Application of International Law to Conduct in Cyberspace', Policy Paper, 3 June 2021.

32 French Ministry of Defence, 'Droit international appliqué aux operations dans le cyberespace' ['International Law Applicable to Operations in Cyberspace'], Policy Paper, September 2019.

of the principle of sovereignty, which will constitute a wrongful act under international law'.[33]

The UK's views on responsibility are also defined in ethical and social norms. Here, the UK may also find itself in a position of irrelevance in the scenarios where increasing corporate leadership identifies and defines what is and is not ethically or socially (rather than legally) responsible. Mega corporations increasingly have impacts well outside of their traditional remit, leading changes in the norms of social responsibility. These may not align with the direction of the UK's responsible cyber principles.[34]

In a world with increasingly alternative leadership in cyber norms and legislation, there is a risk that the UK becomes an 'antipreneur' if it does not take internationally defensible but operationally advantageous policy positions. The operational principle for cyber effects operations to remain accountable will likely remain valid across all the scenarios developed earlier. However, the scenarios all identify that what shapes these values and norms is likely to change. In this case, rather than technical challenges to the UK's approach, policymakers and diplomats will need to ensure that the UK's concept and definition of responsible cyber operations continue to prove operational freedoms, in a world where the rules and norms are increasingly derived and defined from outside the traditional rules-based system.

In addition to national values, the principle of accountability also identifies international law as a factor in how cyber effects operations are conducted responsibly. Legislation relating to interventions and influence is an area of legislation that has potential to be particularly impacted across all the scenarios explored.

States have long engaged in operations to influence others. While current research suggests that long-term influence operations can have successful

33 People's Republic of China Ministry of Foreign Affairs, 'China's Views on the Application of the Principle of Sovereignty in Cyberspace', UN Office for Disarmament Affairs, 11 October 2021, <https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf>, accessed 16 January 2026.

34 Eviatar Matania and Udi Sommer, 'Tech Titans, Cyber Commons and the War in Ukraine: An Incipient Shift in International Relations', *International Relations* (Vol. 39, No. 4, 2025), pp. 586–611.

outcomes in terms of influencing populations,[35] others suggest that authoritarian regimes, whose behaviours the UK is likely to seek to change in the future, are far less likely to be influenced by their own domestic pressures.[36] Instead, by interfering with the collation, evaluation and integration of data provided to senior leaders, operations could be conducted to shape adversary decision-making and policymaking more directly than the broad influence operations conducted today. The increasing connectivity between computing and decision-makers, and the draw of security-centric Smart Cities for authoritarian leaders – explored particularly in Scenarios 1 and 2 – make these opportunities more likely and potentially effective in the future.

However, to exploit these opportunities, how the UK holds itself accountable to international legal norms over the definition of influence and control may need to adapt. Currently, the UK limits operations to conducting 'routine and legitimate … influencing activities'.[37] Contrast this with the (illegal) concept of coercion, which is currently understood as using means which are 'forcible, dictatorial, or otherwise coercive, depriving a State of its freedom of control over matters which it is permitted to decide freely'.[38] The scenarios offer worlds where the accesses and technologies exist to control and distort almost all the key channels of information presented to a state's leadership. Using these capabilities, operations could be developed with the intention of significantly altering the target's perception of reality to the point that it takes a path it would not consider otherwise. There is a school of thought that doing so would cross the line that separates influence from coercion, specifically coercion by control (rather than force).[39] Under this approach, such actions would therefore be considered illegal and contravene the principle of accountability set out in the RCPiP operational principles. This

35 Jon Bateman et al., 'Measuring the Effects of Influence Operations: Key Findings and Gaps from Empirical Research', Carnegie Endowment for International Peace, 28 June 2021.

36 Feruza Madaminova, 'Foreign Policy Change Under Authoritarian Leaders: Analysis of Uzbekistan's Foreign Policy in the Post-Cold War Era', *Politologija* (Vol. 111, No. 3, 2023), pp. 113–62.

37 Suella Braverman, 'International Law in Future Frontiers', speech given at Chatham House, London, 19 May 2022, <https://www.gov.uk/government/speeches/international-law-in-future-frontiers>, accessed 3 December 2025.

38 *Ibid.*

39 Marko Milanovic, 'Revisiting Coercion as an Element of Prohibited Intervention in International Law', *American Journal of International Law* (Vol. 117, No. 4, 2023), pp. 601–50.

level of impact on behaviours would also likely impact a second element of the concept of coercion, specifically seeking to change adversary domestic or foreign policies. Doing so could constitute an unlawful intervention as defined currently by both the UK[40] and within the Tallinn Manual.[41]

Yet the UK has publicly stated that the concept of illegal interventions, an element of customary international law, could 'develop over time' and 'adapt to new frontiers'.[42] Indeed, unilateral sanctions, another method used by states to coerce and change another state's foreign or domestic policies, are used by the UK to further its foreign policy objectives. Again, these are designed to coerce an adversary and were envisioned to be used multilaterally within a UN-led framework. However, they now exist in an increasingly challenged legal space, and are increasingly used in a way which is counter to the original intent.[43]

The scenarios all identify worlds where the political appetite to change adversary behaviours and the technological opportunities to do so are increasing. However, the UK's understanding of where the line is drawn between responsible and illegal may limit any potential advantage. Rethinking the concept of control, and whether the UK seeks to use cyber effects to exercise it over adversaries will take policy, legal and mindset adaptation over the next decade. It will also require adaptations to publicly stated approaches and policy positions, as the UK will have to justify its position on influence or control to others.

While the futures explored earlier have not directly drawn out significant adaptations to the final operational principle, that of calibrated operations, it is worth noting the changes in the social acceptability flagged in the scenarios.

In social and ethical terms, the scenarios developed above – particularly Scenarios 1 and 2 – highlight a future where the use of AI tools is 'taken for granted', with the public encountering (wittingly or unwittingly) these technologies daily. Even in Scenario 3, a sceptical population is unable to

40 Braverman, 'International Law in Future Frontiers'.
41 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.
42 Braverman, 'International Law in Future Frontiers'.
43 Patrick Butchard, 'Sanctions, International Law and Seizing Russian Assets', Research Briefing No. 10034, House of Commons Library, 7 November 2024, pp. 16–18.

completely remove themselves from the commercial benefits of autonomous and intelligent technologies. While targeting augmented reality tools such as those explored in Scenario 3 may be within current responsible boundaries, the ethical impacts of interfering directly with an adversary's 'brain' – as described in Scenario 1 – through a connection to the internet seem significant today but, again, may be far less novel and contentious within a decade.

Away from the rapid turn-around of operational planning, those involved in developing long-term capabilities should note the potential for changing attitudes to alter how adversaries respond and escalate (or not) to cyber effects operations. Developing capabilities to interfere with brain–computer interfaces will be lengthy and challenging. In the current context, their use might feel uncalibrated and escalatory. However, by the time capabilities mature enough to be used in an operational context, social attitudes – and therefore an adversary's response – towards these tools may be quite different from the attitudes of today. Shying away from developing capabilities because the idea of employing them may seem excessive today may place cyber operations at a technical disadvantage in the future.

## Conclusion

The UK draws influence and moral confidence from its position as a leader in the concepts and use of responsible cyber operations. However, the technological, social and geopolitical changes over the next decade, while not forecastable or defined, seem likely to challenge the position and approach the UK takes today.

In principle, the idea of continuing to promote the concept of responsible cyber operations seems sound, but only if the guidance and principles which make up that approach ensure cyber effects operations can be successfully achieved. Ensuring that future operations are accountable to international law and national values, proportionate to the value of the target envisioned and calibrated to the social and adversary context will give future planners and operators the freedoms to ensure that the UK's cyber effects operations provide maximum impact to wider UK government objectives.

Without these adaptations, however, the world will advance technically and socially, leaving the UK's cyber effects approach unnecessarily constrained and archaic, and irrelevant to allies and adversaries alike.

## About the Author

### DW

DW is is a serving official in the National Cyber Force.

The views expressed in this chapter are those of the author, and do not reflect official government policy.

# Conclusion: A British Way of Cyber Operations?

**Conrad Prince, Andrew C Dwyer and Emily O Goldman**

This roundtable conclusion reflects on the analytical threads that run throughout the volume, as three international experts on cyber operations highlight some of the key characteristics that make up the UK's approach to cyber operations.

## The Unique Origins of the UK Approach

**Conrad Prince**

Decoding national approaches to cyber effects operations is a challenging task, perhaps especially so when it comes to democratic nations such as the UK and like-minded countries. There are far fewer examples of their cyber operations available in the public domain than is the case with states such as Russia, China, Iran or North Korea. And, inevitably, nations are rather circumspect as to what information they release on this highly secretive subject.

That said, there are indicators out there as to the characteristics of the British approach to cyber effects, not least in the groundbreaking 2023 National Cyber Force (NCF) publication Responsible Cyber Power in Practice (RCPiP). Contributors to this volume have demonstrated that it is possible to draw out some key elements of a British approach.

### A Long Journey

An important starting point is to recognise that the UK – and the UK's cyber intelligence and security agency, GCHQ, specifically – has extensive experience in the delivery of cyber effects operations. The creation in 2020 of the NCF – the body that draws together people from GCHQ, the Ministry

of Defence (MoD) and the Secret Intelligence Service to deliver cyber effects operations – was a major development but by no means the start of the UK's journey on cyber effects.

In 2018, Jeremy Fleming, the then director of GCHQ, noted in his speech at that year's CyberUK conference that 'for well over a decade … GCHQ has pioneered the development and use of offensive cyber techniques'. While in 2023, RCPiP stated that the NCF was 'building on significant experience in cyber operations stretching back over two decades'.[1] It is worth recalling that the legislation that put GCHQ on a statutory footing over 30 years ago, the Intelligence Services Act 1994, explicitly authorises GCHQ to 'interfere with electromagnetic emissions'.[2]

Over those decades of delivering cyber effects operations, a particularly British approach has evolved, rooted in a number of characteristics peculiar to the UK experience.

### The GCHQ Heritage

In the present day, GCHQ provides a core component of the NCF. GCHQ has a number of features that have influenced the evolution of UK cyber effects operations. It is a civilian intelligence and security agency, a stand-alone department responsible to the foreign secretary. And while it has always had a close relationship with the UK armed forces, its leadership is civilian.

All this sits in contrast both to US Cyber Command and the National Security Agency, GCHQ's close US counterpart, which is part of the US Department of Defense and is always led by a serving military officer.

GCHQ's culture and mindset are not rooted in military thinking. It has a broad strategic remit, able to conduct operations in the interests of national security, economic wellbeing (where national security is engaged) and for the prevention and detection of serious crime. The breadth of these missions is repeatedly emphasised in RCPiP, which cites examples of cyber effects

1 National Cyber Force, 'National Cyber Force: Responsible Cyber Power in Practice', April 2023, p. 11, <https://www.gov.uk/government/publications/responsible-cyber-power-in-practice>, accessed 9 April 2026.
2 'Intelligence Services Act 1994 (UK)'.

operations ranging from support to military operations, to counterterrorism, preventing serious crime as well as countering 'other threats posed by states'.[3]

So the British approach to the application of cyber effects operations goes well beyond a single sphere, such as military operations. Nor is it simply rooted in a focus on countering cyber threats to the UK. The NCF is specifically an organisation for delivering cyber effects operations. Unlike US Cyber Command, it has no cyber security remit, and the UK approach does not particularly emphasise counter-cyber operations.

The roots of the UK's cyber effects capability in a civilian strategic intelligence agency with a broad remit significantly influences the breadth and range of application the UK sees for these capabilities. For the UK, cyber effects is a full-spectrum capability with broad application to achieving strategic advantage for the UK in multiple areas.

## Learning by Doing

The roots in GCHQ have influenced the UK approach in other ways. Neil Ashdown notes in this volume that UK agencies such as GCHQ tend not to be particularly focused on establishing theoretical constructs for their operational work. There is no equivalent to the many volumes of military doctrine that govern the operations of the armed forces. Instead, it could be said that a certain 'learning by doing' culture, against a strict oversight and compliance backdrop, has tended to drive operational evolution. It is a mindset rooted in practical pragmatism rather than theory.

The UK cyber effects story is one of evolution. It starts with GCHQ's pioneering work, that becomes more formalised through the National Offensive Cyber Programme reportedly initiated in 2014, in partnership with the MoD,[4] and then to the establishment of the NCF in 2020. The publication of RCPiP three years later is striking. It sets out, for the first time, some thinking of a more doctrinal nature. But this is thinking based on years of experience and can be seen as a distillation of practical lessons learned rather than purely theoretical construct. This is where a lot of the strength of the NCF approach lies.

3 National Cyber Force, 'National Cyber Force: Responsible Cyber Power in Practice', p. 21.

4 See, for example, Intelligence and Security Committee of Parliament, *Annual Report 2016-2017*, HC 655 (London: The Stationery Office, 2017), p. 43.

## Cognitive Effect and Other Doctrine

What RCPiP describes as the doctrine of cognitive effect is the most eye-catching element of NCF thinking set out in the document. Several contributors (for example, Ashdown, and Monica Kello and Richard Harknett) to this volume have considered different dimensions of the cognitive effect thinking and how it is reflected operationally. It seems clear that the central place of cognitive effect in RCPiP is intended to signal one important element of a particular British approach to cyber effects operations, one that looks beyond the simple technical effect to be achieved and into how this can influence the mindset of the adversary.

There are clues in the document to other thinking that may differentiate the UK approach. RCPiP does not explicitly comment on US Cyber Command's doctrine of persistent engagement. But its emphasis on 'dynamic, targeted operations' includes the suggestion that 'If practical, repeated targeting of a particular adversary may at times be necessary, but there may also be situations where this serves only to encourage the adversary to better protect itself'.[5]

There may be a suggestion here that the more extreme end of persistent engagement – a relentless piling up of multiple actions against a particular target – is not a good fit with the UK approach. In part, this may be a question of resources. The UK's inevitably more limited capacity than that of the US means that it cannot rely on sheer scale of operational activity against a given target. It must be more selective and focused.

RCPiP reveals a pragmatic preference for 'a range of operational styles, tailored to particular circumstances and objectives'.[6] Arguably the UK's resource limitations promote the virtues of focus and agility – and make the UK more relatable to other medium-sized democratic nations seeking to develop responsible cyber effects capabilities.

## Responsibility

It is important also to recognise the NCF's focus on 'responsible' operations, with strict adherence not only to domestic and international legal obligations

5 National Cyber Force, 'National Cyber Force: Responsible Cyber Power in Practice', p. 16.
6 *Ibid.*, p. 16.

but also an ethical dimension. Some contributors to this volume have asserted that it is difficult to explain what 'responsible' operations are. But RCPiP speaks fairly extensively to the components of what it calls 'responsible operational planning'.[7]

The chapter by DW argues that such a commitment to responsible operations is likely to be a severe constraint in future, while others (particularly the chapter by Charl van der Walt, Zohra Hamila, Richard Derbyshire and Adam Ridley) have suggested it can, in fact, be seen as a strength.

It is surely a given that states that operate with very few constraints have more options open to them than those that take their legal and ethical obligations seriously. But it is the commitment to responsible behaviour that is the key differentiator between states such as the UK, on the one hand, and Russia or China, on the other. Such a commitment is essential for democracies to win the licence to operate cyber effects capabilities.

## The Future

The British approach to cyber effects is rooted in the work of a major civilian signals intelligence agency (albeit now in the NCF with a significant military partnership). It rests in an organisation purely focused on cyber effects operations, with no cyber defence component. It takes a broad approach to the application of cyber operations, across a full spectrum of national security, military and serious crime dimensions. It takes a pragmatic approach to the delivery of cyber operations, embracing a range of different approaches based on practical lessons learned over many years and matched to the UK's scale and capabilities. It emphasises flexibility and agility. And it has a deep commitment to acting responsibly.

The future is likely to bring challenges for the UK when it comes to evolving this approach. Some of these are structural. What fundamentally is the role of the NCF? It arguably has multiple identities – a national security covert action agency using cyber effects to achieve advantage for the UK across a range of areas, a force element of Defence, and an organisation using effects operations to help to protect the UK from threats, including those that are

7 *Ibid*., pp. 22–24.

cyber related. Is it possible to hold these different identities simultaneously or will there be a need to prioritise?

A related question is whether the NCF should be the centre of all cyber effects operations delivered by the UK, or more of a centre of excellence, enabling other parts of government to deliver cyber effects in their areas of responsibility. This may be particularly relevant at a time when the UK landscape is evolving, including with the recent creation of the Defence Cyber and Electromagnetic Force and the announcement of the new National Police Service. The full implications of these developments for the NCF remain to be seen.

Kello and Harknett illustrate how Operation *Cronos*, the UK cyber operation targeting LockBit, was led not by the NCF but by the National Crime Agency, reflecting in its own way some of the wider UK thinking on cognitive effect. Does such diversification represent a pragmatic approach to making the most of resources and expertise across government, or does it risk undermining the benefits of an NCF with a broad remit and expertise able to apply lessons from one target set or type of operations to another?

It is probably not possible for the NCF to try to be the sole UK government cyber effects organisation. A more realistic approach would be to act as a centre of excellence, supporting others as the spider in the centre of the web of UK cyber effects. But a key lesson from the NCF's signals intelligence heritage is the criticality of retaining flexibility, the ability to shift rapidly to focus on different objectives and adversaries as the wider context demands. To avoid becoming tied to one area of focus or set of operations. Retaining the NCF's strengths of range and breadth of approach should be an important part of its future.

In a highly unstable world, with ongoing warfare across Europe's eastern border and in the Middle East, the NCF must face the challenge of how best it orientates itself to be able to operate in competition, crisis and conflict. Is it feasible to deliver operational capability across all those dimensions? And, if resources preclude this, how best should the NCF focus its efforts, working with partners and allies?

Fundamental to that challenge is how the UK best scales its cyber effects capabilities and in particular how best to leverage the private sector. The private sector is already a fundamental partner to the UK's national cyber

effort, but there may be scope for more innovative ways for government to partner with the commercial sector as a way of delivering scale and capacity at pace.

Pia Hüsch and Charles Coventry explore in their chapter some of the options and potential concerns over that. It feels as though today's complex and unstable operating environment means that the nettle of scaling needs to be grasped as soon as possible. Doing so may potentially involve pushing some boundaries.

Finally, and perhaps most relevant to this volume, there is the question of how the UK further develops its doctrinal thinking on cyber effects. I have set out how the UK approach to cyber effects operations is one that has been driven by practical experience rather than theorising. But, over time, that experience has been distilled into something more closely resembling doctrinal thinking, expressed publicly in particular through RCPiP.

The NCF's creation with RUSI of the UK Cyber Effects Network, of which this volume is one product, represents a powerful commitment to encouraging new thinking on cyber effects with a UK dimension. Maintaining the momentum of that work will be essential if the UK is to tackle successfully the challenges that today's world poses for the delivery of responsible cyber operations.

RCPiP has shown it is possible to explore, in public, issues of cyber effects doctrine and strategy. We need to hear from the NCF how its thinking has developed in the years since publication, including on the balance between focus on competition, crisis and conflict, and on how the NCF's role is evolving across its various identities and with its various partners. Hearing the NCF's own perspective is a vital part of UK leadership in cyber effects thinking.

## Balancing Responsible Cyber Operations

**Andrew C Dwyer**

The UK's ability to enable, sustain and pursue its national interest across periods of competition, crisis and conflict require sustained cyber operational activity and campaigns to deliver lasting effect. Whether

to combat the harm from ransomware,[8] to limit attacks against critical and social infrastructure, or in conventional integration with military assets, cyber effects play a considerable role. However, this involves compromise, tension and opportunity for a range of 'middle powers' who must balance constrained resources across competing priorities in their statecraft. It is also what makes the contributions in this volume essential. They offer the first sustained British view on cyber effect – a range of outcomes from cyber operational activity – with a distinctive flavour and articulation to some of the pressing questions on strategic options, legal frameworks, responsible and ethical behaviour, as much as future technical developments for the UK.

The emphasis of this edited collection on cyber effects represents a gradual development of British thinking into a cohesive view of the utility of cyber operations: learning that cyber effects come about through integration with other capabilites, experimentation, and introducing friction to adversaries through 'cognitive' disruption. Public debate has likewise moved – albeit unevenly – beyond the early imaginaries of cyber war as discrete from other modes of warfare. Instead of misguided analogies between cyber weapons and nuclear arsenals, there is today a nuanced and complex appreciation of cyber operational capability. While such debates have been more prominent within the US, they often overshadow the experiences, capacities and political inheritances of middle powers such as the UK.[9] As a result, much of the intellectual terrain of cyber operations remains implicitly US-centric.

This poses challenges. The UK has it own unique history across its capabilities, culture and institutions. What may work for US institutions and priorities is unlikely to work elsewhere, and what may appear universal for

8 See House of Commons and House of Lords, Joint Committee on the National Security Strategy, 'A Hostage to Fortune: Ransomware and UK National Security', HC 194 / HL Paper 23, First Report of Session 2023–24, December 2023.

9 However, see examples of UK-centric thinking in Marcus Willett, *Cyber Operations and Their Responsible Use* (Abingdon: Routledge, 2024); Joe Devanny and Andrew C Dwyer, 'From Cyber Security to Cyber Power: Appraising the Emergence of "Responsible, Democratic Cyber Power"', in T Jančárková et al. (eds), *15th International Conference on Cyber Conflict: Meeting Reality*, International Conference on Cyber Conflict (CyCon) (Tallin: NATO Cooperative Cyber Defence Centre of Excellence, 2023), pp. 381–97; Joe Devanny et al., 'The National Cyber Force that Britain Needs?', Cyber Security Research Group, King's College London, April 2021.

cyber operations and strategic behaviour may be particular to the context in which it is created (see Ashdown's chapter for this argument). A core contribution of this volume, therefore, is to place British ideas and practice on their own footing. Such a British perspective is not in opposition to the significant contributions made by US thinking. Rather, it is in conversation with them. For the first time, we see sustained attention to core elements of British thinking on: 'cognitive effect'; investigation of the NCF's accountable, precise and calibrated principles from RCPiP; how the application of operational 'friction' works through a British case; speculative sociotechnical futures; and the legal tensions of enabling private organisations to contribute to UK cyber effect.

## A Productive Fudge

Long before the public avowal of the NCF in 2020, the foundations for a view on cyber effects rested on significant institutional engagement between intelligence and defence communities, and on capabilities nurtured through decades of signals intelligence expertise within GCHQ. This long period of development, with public references since 2011,[10] signals a significant 'pre-history' to cyber effect where many of the discussions in public today emerge as a result of significant 'hands on' experimentation. The potential for such learning, however, rests on a classic British 'fudge'. This fudge is commonplace across British governance due to the institutional realities of fiscal constraint (especially post-2008), a relative paucity of skills, as much as a culture of compromise. This is not to suggest that this itself is easy for those involved, and frustration is a significant component of such a fudge. Those who would like clearly articulated perspectives and institutional demarcations are unlikely to be satisfied by this British way of doing.

This fudge – as Ashdown describes – is a significant divergence from the US and benefits a British view on cyber effects. It also aids in reflecting on why discussions on cyber effects within the UK often emphasise integration rather than cyber operations as a standalone capability. The fudge thus both enables – and is a result of – adaptability, collaboration and experimentation as well as ensuring that there is pragmatic justification to ministers for investment. This

10 For example, 'a Joint Cyber Unit hosted by GCHQ at Cheltenham whose role will be to develop new tactics, techniques and plans to deliver military effects, including enhanced security, through operations in cyberspace'. Cabinet Office, 'The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World', November 2011, para. 4.9.

significantly restrains UK pursuit of 'grand' strategy and means that flexibility and adaptability to the operational environment are required. This is best exemplified by an explicit attention to the pursuit of 'cognitive effect' in the NCF's RCPiP publication in 2023. Here, a view on the structural potential of the environment is sidestepped for an attention on what can be pragmatically achieved for the UK. Rather than a deficit, this fudge is highly productive in ensuring that cyber operations – and thus their effects – develop and respond sensitively to questions of responsibility and ethics that are core to the principles that I turn to next.

## Responsibility and Organisation

If one accepts that there is a productive British fudge, this is also sustained both in the organisation of cyber effects as much as in the ambiguity and flexibility of RCPiP's three principles: *accountable*; *precise*; and *calibrated*. Within the institutional compromise of the UK system, the NCF is a result of multiple entities that span defence and intelligence, as much as the need for integrated effects with other areas of government. In doing so, the NCF also inherits a wide remit of activity making prioritisation challenging. Should the NCF focus on ransomware harm, adversarial state activity, or something else? Without any public evidence to the contrary, It is hard to imagine that the NCF could sustain cyber operational capability during conflict at the same time as dealing with, for example, cybercriminal activity. This is why a focus on cyber effects over cyber operational capacity alone is promising. As Van der Walt, Hamila, Derbyshire and Ridley note, there is a broad array of actors responsible for cyber effects. This is made most clear in the contribution by Kello and Harknett on the takedown of the ransomware group, Lockbit, in Operation *Cronos* by the National Crime Agency and in Hüsch and Coventry's piece on the capacity of private enterprise to contribute to cyber effects. This leads to a distribution of both capability and responsibility that extends beyond and through the NCF across competition, crisis and conflict.

In the pursuit of the principles of accountable, precise and calibrated capabilities outlined in RCPiP, Van der Walt, Hamila, Derbyshire and Ridley counter the argument that these principles may add unnecessary friction through comparison to internal frictions imposed on Chinese and Russian activity. In a convincing argument, the authors note that there is a productive element to friction to enable reflection, ensure proportionality and tailor effect. This is particularly important for states including the UK that have limited resources and need to optimise. However, it is also crucial in broader

domains of maintaining a 'licence to operate'[11] as much as demonstrating to other 'middle ground' states that cyber operations can be conducted responsibly, ethically and in accordance with international law. For the UK, a clearer articulation of accountable, precise and calibrated activity from the NCF is required to demostrate clearer operational benefits for others. This speaks to the contribution from Stefan Soesanto and Wiktoria Gajos that offers campaigning archetypes to structure thinking in this area. If the UK wishes to become a more pragmatic and activist responsible actor in a changing international system, sustained attention to developing operational frameworks is a clear priority. This is distinct from directly shaping the environment, as articulated in Cyber Persistence Theory,[12] to one that advocates for continued contribution to normative rules-making.

## Trust and Friction

If middle powers are unable to compete at scale – where campaigning can arguably narrow capability to achieve precision and calibration – cognitive effect offers one valve for integrating effects across multiple 'layers' (see Kello and Harknett's chapter). Due to the wide range of pulls on the NCF's time and resources, sustaining effect through technical means alone is unlikely to be sustainable (nor appropriate to the lessons learned by British activity). Instead, cognitive effect draws on the inheritance of intelligence and cyber operational experimentation to disrupt trust in oneself, devices, organisations and communities. This is closely associated with long-running trends in disrupting trust of adversaries in pursuit of national security and defence objectives. Friction as a result of cognitive effect appears across the volume, and I find it simpler to view it as a broader environmental variable that can also be strategically manipulated. Friction in this sense then becomes part of operational practice: understanding where to add and *reduce* friction at varying points according to need and adversary behaviour. This results in a highly interdisciplinary requirement to not only understand how to use cyber operations to establish technical capability, but a range of other disciplines to *calibrate* effect and to do so responsibly.

11 Ged Hiscoke, Stephen Ward and Daniel Lomas, ' Trust Without Knowledge? UK Intelligence Agencies and the Public Trust Conundrum', *Intelligence and National Security* (Vol. 40, No. 3, 2025), pp. 548–75.

12 Michael P Fischerkeller, Emily O Goldman and Richard J Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (Oxford: Oxford University Press, 2022).

Yet, who and what do we trust to enable such frictions? This tension is present in the contribution by Hüsch and Coventry on the role of private enterprise in producing cyber effects under national and international law. Within UK governance, the wider the range of actors engaged in cyber effects, the more the risk of poorly accountable, imprecise and weakly calibrated cyber effects grows. To its fullest extent, this also applies to the growing automation within cyber operations and broader technical environments, whether in research and development, through to potential deployment. As in the contribution by DW from the NCF examining speculative futures, how does technological development enable or constrain cognitive effect? How may AI systems be used responsibily according to the NCF's principles, and broader cyber effects beyond it be held to account? Automating and distributing cognitive effect must be carefully managed – as its calibration and precision require significant work to enable effectiveness. Otherwise, the UK's status as a responsible actor could come under strain.

## Beyond Cognitive Effect?

It is unlikely that a British view on cyber effect requires any 'grand' theory; it goes counter to its history and practice. This also reflects my own bias as a political geographer where structural interpretations of sociotechnical environments are inherently questioned (underlining Ashdown's note of the different backgrounds of those involved in British cyber effects debate and presented in this volume). As cognitive effect – as one derivation of cyber effect – demonstrates, there is an experimental requirement to delivering effects through cyber operations. However, there are three risks to the pursuit of cognitive effect that emerge in this volume: 1) In seeking to optimise for current need, the NCF becomes overly attuned to that which works in periods of competition rather than the speedier requirements during crisis and conflict; 2) The NCF and the UK government must be attentive to the danger of the misinterpretation of cognitive effect as a general condition of cyber effect through the promotion of calibration and precision; 3) As is clear in the 2026 US Cyber Strategy,[13] there are cyber effects from Caracas to Tehran that are beyond cognitive in form that are not well articulated in public UK thinking and strategy, limiting its claim

13 White House, 'President Trump's Cyber Strategy for America', 2026, <https://www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf>, accessed 9 April 2026.

to offer a responsible perspective on cyber effects. To affirm itself as a leading voice for responsible cyber operations and effects, the UK should seek to fully explicate how cyber effects can be conducted across the spectra of use with and beyond cognitive effect.

## Holistic Pragmatism

**Emily O Goldman**

The contributions to this volume provide an array of insights that paint a distinctive British approach to cyber effects operations – or what is often called 'offensive cyber operations' – that is pragmatic and holistic. From a US perspective, this pragmatic and holistic approach combines practical, action-oriented tactics (pragmatic) with a systemic, interconnected view of complex systems (holistic) to achieve strategic goals. This is an adaptable approach that bridges the gap between comprehensive understanding and efficient execution. Practicality allows for complementary tendencies to co-exist in the service of strategic utility. A holistic view of cyberspace is congruent with an integrated campaigning mindset across government, private sector and allies that aligns with the interconnected nature of the cyber strategic environment.[14]

The UK's practical approach to 'responsible cyber power' should be contrasted with other international efforts to define responsible cyber behaviour. The UN Group of Governmental Experts (GGE), for example, sought a status as the main forum for states and their diplomats to debate and propose guidelines for international cyber behaviour.[15] They produced sets of voluntary, non-binding rules aimed at enhancing security, stability and conflict prevention. Nevertheless, the vague, high-level and aspirational nature of these would-be UN 'norms' contrasts starkly with the clarity and specificity of the UK framework on responsible cyber power.

To date, the UK is the only state to formally articulate what it means *operationally* to be a responsible cyber power and to provide specific examples of NCF practices. Responsible cyber power means abiding by stated, consistent and just principles in all cyber operations and campaigns. Offensive operations

14 Fischerkeller, Goldman and Harknett, *Cyber Persistence Theory*.

15 UN General Assembly, 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security', A/76/135, July 2021.

must be accountable (legal and ethical), precise (timed and targeted against genuine threats, based on deep understanding of the cyber environment) and calibrated (adaptable and attuned to escalation risks and other political sensitivities). The framework aligns democratic values and international law with operational practice rather than outcomes. Thus, it has much greater utility as a practical guide to responsible cyber behaviour than do the GGE's non-binding norms. The UK framework also incorporates a feedback loop to reinforce the principles of accountability, precision and calibration in the operational planning cycle.

Pragmatism also manifests in a distinct UK approach to openness and accountability. The British have managed to preserve significant secrecy about the NCF's composition and activities while also being transparent about the goals and principles of offensive cyber operations. The NCF's formation as well as government deliberations on how to reshape cyber organisations remain shielded from public debate (see Ashdown's contribution to this volume). The NCF was officially revealed in 2020 as the entity conducting offensive cyber operations, yet its members still do not publicise their affiliation. In 2023, the UK government revealed the name of the head of the NCF (James Babbage), but individual operatives remain anonymous. At the same time, however, the NCF launched a public relations campaign to explain what it means to be a responsible cyber power in a democracy. Building public support for highly secret operations assured the NCF's licence to operate. Selective transparency is pragmatic, and it contrasts with vigorous, but sometimes ill-informed, public debates in the US over how to organise cyber forces and how to execute cyber operations.

Another example of cyber pragmatism is the UK's staunch adherence to international law while preserving strategic utility in specifics (see Van der Walt, Hamila, Derbyshire and Ridley's contribution). In his 23 May 2018 Chatham House speech, UK Attorney General Jeremy Wright outlined the UK's position on international law and cyberspace, and the nation's commitment to international law – even when other states were giving it mere lip service in denying their own cyberspace operations. On the then-hotly debated topic of sovereignty in cyberspace, Wright affirmed that:

> Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber

> activity beyond that of a prohibited intervention. The UK government's position is therefore that there is no such rule as a matter of current international law.[16]

Nor does the UK accept that international law requires prior notification of countermeasures because such a requirement might force the state to reveal intelligence sources and operational methods.[17] The UK was the first state to publicly make this pronouncement and doing so clarified that freedom of cyber manoeuvre is consistent with international law. Other states have followed suit.

The UK's approach to cyber operations is also holistic. By conceiving cyberspace as a sociotechnical system rather than a warfighting domain, this approach naturally promotes synergies across government entities and with the private sector. These manifests in integrated campaigning, both below the level of armed conflict and as an element in manoeuvre warfare (see Soesanto and Gajos's chapter). A tendency towards integration over stove-piped organisations has historically been well served by Britain's parliamentary system and committee approach to problem solving across cabinet departments, as well as by the NCF's own hybrid organisational structure (see Ashdown's chapter). A similar hybrid sharing of responsibility for defensive cyber operations is reflected in the National Cyber Security Centre, a government–industry partnership working closely with GCHQ.

Britain's pragmatic and holistic approach to cyber operations informs the 'doctrine of cognitive effect', which fuses technical and informational techniques for precise, calibrated, combined impact. NCF doctrine asserts that one 'can often achieve the greatest cognitive effect by affecting the functionality and effectiveness of an adversary's systems over a period of time, rather than denying them entirely (as in some cases they can be quickly replaced)'. This 'bend-but-do-not-break' approach goes beyond integration to a technical–cognitive synergy that employs a range of technical and informational techniques to 'affect an adversary's perception

16 Jeremy Wright, 'Cyber and International Law in the 21st Century', speech given at Chatham House, London, 23 May 2018, <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>, accessed 6 March 2026.

17 *Ibid*.

of their operating environment and weaken their ability to plan and conduct activities effectively'.

The US views cyberspace, by comparison, primarily as a technical domain. Reinforcing this view are long-running debates (in the military and across the departments) over organising information operations (IO), in addition to different cyber and IO processes and authorities. The net result is a challenging bureaucratic environment for integrating cyber and IO. On the opposite end of the spectrum are Chinese and Russian views of cyberspace as a political, informational and cognitive environment. Cyber operations are informational and cognitive contests (see Van der Walt, Hamila, Derbyshire and Ridley's chapter) that often involve large-scale disinformation activities, quite distinct from the UK's precise, calibrated, operational approach.

The UK implements its unique approach with nuance and precision, viewing cognitive effects as the primary objective of cyber activity rather than merely a secondary consequence of technical disruption (see Van der Walt, Hamila, Derbyshire and Ridley's chapter). Yet, the NCF appreciates the wider impact of disruption operations, which may be relatively short-lived in terms of 'immediate [technical] effect – including a hostile actor's loss of confidence in their data or technology – can often be longer term … [reinforced through] a campaign for cumulative effect'. The ability to incorporate layered effects thinking into planning, operations and assessments in competition as well as crisis and armed conflict is very mature in the UK. It aligns with the British view of cyberspace as a sociotechnical system, which depends on close collaboration of government with the private sector to achieve integrated effects.

In the US, these converged dynamics constitute friction, which results from the layering of technical, organisational and psychological effects (see Kello and Harknett's chapter). US military doctrine has long focused on joint, combined and integrated conventional operations. Recent events demonstrate successfully integrated cyber and non-cyber effects in armed conflict. But in strategic competition (below the use-of-force threshold), offensive cyber operations are still viewed by many as purveyors of discrete technical effects. The layering of cyber effects with non-cyber effects – let alone with non-military governmental tools of national power – outside of armed conflict has proven elusive.

The UK's guidance on responsible cyber power is clear on the meaning of coordinated action: 'As with any form of government or military action, individual cyber operations are not usually expected to be strategically decisive on their own. Often, they are at their most effective when combined and co-ordinated with the activities of partners to achieve a shared goal'.[18] It further establishes that:

> Operations often take the form of a series of related actions and are part of a wider set of activities (campaigns) involving other partners, including allies. Cyber operations can amplify activities in the physical world and vice versa. There are also situations where cyber operations can enable an action by a partner organisation in the physical world.[19]

In addition, at times, cyber operations 'form part of a much wider and more proactive set of actions, or campaigns, to help achieve a particular UK security or military objective, potentially over an extended period'.[20]

Despite differences in size, scale, resourcing and organisational structure, the UK and the US share an emerging understanding of how military cyber forces can help to create security in and through cyberspace. Both agree they 'cannot leave cyberspace an uncontested space where adversaries operate with impunity'.[21] Cyber forces must be 'agile in developing and seizing opportunities' while operating 'daily' to secure cyberspace.[22] For both, 'daily' does not mean being everywhere all the time, but rather a recognition there is always something happening, that constant contact is a condition of cyberspace, and that campaigning is the operationalisation of what it means to persist.

Cyber campaigning as an operational approach has benefited from UK–US interaction in an Operational Insights Dialogue that was initiated to discuss shared experiences and insights from the Russia–Ukraine conflict. The dialogue was an exercise in strategic–operational integration aimed at tightening the loop between strategic forums such as the Cyber Management

18 National Cyber Force, 'National Cyber Force: Responsible Cyber Power in Practice', p. 16.
19 *Ibid*., p. 18.
20 *Ibid.*
21 *Ibid*., p. 6.
22 *Ibid*., p. 4.

Review and operational art.[23] The dialogue included academics to iterate between theory and practice – a priority for both countries. Each country's representatives acknowledged nuanced differences, but were united in a shared view of cyberspace as a strategic environment that calls for a campaigning approach to cyber operations. UK participants defined a campaigning approach in terms of: aggregation (aggregation of changes over time and continuous adapting); integration (of all available levers, not just offensive cyber operations or technical effects); and persistence (constantly revisiting a problem and operating in a sustained fashion to shape adversary behaviour). This aligns with the US view of cyber campaigning as operating persistently to achieve national objectives; however, the US focus is on contesting malicious cyberspace activity and setting and resetting operational conditions in cyberspace to thwart adversary plans, rather than on cognitive effect.

The UK so far has been enabled by its pragmatic and holistic approach, which is not only fit for purpose for today's challenges, but for future crises and armed conflicts. Both the US and the UK will inevitably face new operational and policy circumstances, some of which are already here. These include the public and legal challenges and implications of using the private sector to conduct offensive cyber operations (see Hüsch and Coventry's contribution), and whether the principles of responsible cyber power can accommodate a world of AI capabilities and AI-enabled systems (see DW's chapter). Still, both allies will be better equipped to overcome them and more effectively gain advantage during competition, crisis and armed conflict thanks to the complementary nature of their approaches and the dialogue between them.

23 GCHQ, 'UK and US Intelligence Chiefs Commit to Enduring Combined Cyber Operations', news, 18 November 2021, <https://www.gchq.gov.uk/news/cyber-management-review-2021>, accessed 9 April 2026.

## About the Authors

### Conrad Prince

Conrad Prince is a RUSI Distinguished Fellow and senior adviser on cyber security, offensive cyber, and related intelligence and security issues. He was formerly the Director General for Operations and deputy head of the UK Government's signals intelligence and cyber security agency, GCHQ, and was subsequently the UK Government's Cyber Security Ambassador.

### Andrew C Dwyer

Andrew C Dwyer is a Lecturer in Information Security at Royal Holloway, University of London. His research examines the interconnected dynamics between geopolitics and embedded cyber security practices for cyber policy and strategy. Andrew has been active in exploring the role of British cyber operations and effect through the academic-focused UK Offensive Cyber Working Group that he co-founded in 2020. He has held research positions at Bristol and Durham universities, was an Associate Research Fellow (2023 to 2025) at the UK National Cyber Security Centre-funded Research Institute for Sociotechnical Cyber Security, and completed his DPhil at the University of Oxford in 2019.

### Emily O Goldman

Emily O Goldman is a cyber strategist and thought leader on cyber policy. She currently serves at the National Security Agency. Previous positions include Director for Cyber Strategy at the National Security Council; cyber strategist in the US Cyber Command Directorate of Operations; cyber adviser to the Director of Policy Planning at the Department of State; and Director of the US Cyber Command/NSA Combined Action Group. She was a professor of Political Science at the University of California, Davis for two decades and has published and lectured widely on strategy, cyberspace operations, and military innovation.

Disclaimer: The views expressed are those of the author alone and do not represent the official position of any US government agency.

# New Thinking on UK Cyber Effects

## An Edited Collection

Cyber effects operations are a key tool of contemporary statecraft. But what do they look like for the UK, and other medium powers? *New Thinking on UK Cyber Effects: An Edited Collection* is the first effort to ask about and discuss the British way of cyber warfare. Bringing together a community of practice that draws on academic and policy research, professional insights and multidisciplinary expertise, this volume aims to reframe our understanding of cyber effects operations and UK strategic culture.

ISBN: 978-1-0667172-0-0