INSTITUTE FOR DEFENSE ANALYSES

# U.K. National Cyber Force, Responsible Cyber Power, and Cyber Persistence Theory

Richard J. Harknett
Michael P. Fischerkeller
Emily O. Goldman

April 2023



IDA Non-Standard D-33461

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22305

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.


**About This Publication**

This work was conducted by the IDA Systems and Analyses Center under contract HQ0034-19-D-0001, Project C5224, "Review and Editorial Prep for Non-sponsored Articles and Essays for External Publication," for the IDA. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

**Acknowledgements**

USCYBERCOM Public Affairs Office, Commander, NCF (UK)



**For More Information**

Michael P. Fischerkeller, Project Leader
mfischer@ida.org, 703-845-6784

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782




Rigorous Analysis | Trusted Expertise | Service to the Nation

**UK National Cyber Force, Responsible Cyber Power, and Cyber Persistence Theory**

Richard J. Harknett, Michael P. Fischerkeller, Emily O. Goldman

This week the United Kingdom's National Cyber Force (NCF), a defense and intelligence partnered organization between the Government Communications Headquarters (GCHQ) and elements of the UK Ministry of Defense, released "The National Cyber Force: Responsible Cyber Power in Practice." The document builds on the UK's 2022 National Cyber Strategy, and provides details about how the NCF is operating now, and doing so responsibly, given its rapidly accumulating knowledge and understanding of cyberspace strategic realities.

The document's description of the cyber strategic environment and the UK's operational approach for exercising responsible cyber power closely align with US insights about cyberspace embodied in the strategy of Defend Forward and the operational approach of persistent engagement. The fact that the UK and US came to the same strategic and operational revelations independently is a testament to the explanatory power of Cyber Persistence Theory (CPT) and to a paradigm change unfolding before our very eyes.

**From Misalignment to Persistence**

*Cyber Persistence Theory: Redefining National Security in Cyberspace* introduces the logic of initiative persistence, explains how such logic aligns to the structural realities of the cyber strategic environment and creates an imperative for all cyberspace actors. The explanatory framework of CPT redefines security as seizing and sustaining the initiative in exploitation; that is, anticipating the exploitation of your own digital vulnerabilities before they are leveraged against you, exploiting others' vulnerabilities to advance your own security needs, and sustaining the initiative in this exploitation dynamic. States may choose not to abide by this logic or not operationalize it well. The consequence will be cyber insecurity and a loss of relative power for those not persisting. States may also abide by the logic but do so in irresponsible ways that threaten peace and security. The UK has provided a helpful framework for distinguishing such irresponsible cyber behavior.

In *Cyber Persistence Theory* we posited that if our theory is correct, we should see more states explicitly adopting strategies of cyber persistence to seize and sustain initiative in their behaviors. The Biden Administration's 2023 National Cybersecurity Strategy and now the NCF's operational primer align with that expectation. The UK NCF's document, essentially an "operational primer," offers a model for how states with significant cyber capability and capacity may pursue initiative persistence and do so in a responsible manner. Specifically, responsible cyber operations and campaigns are a recognition that the "UK cannot leave cyberspace an uncontested space where adversaries operate with impunity." The NCF must be "agile in developing and seizing opportunities" while contributing "daily" to a "whole of society" approach to a secure cyberspace in which the UK thrives. This is a paradigmatic shift away from the UK's 2016 cyber strategy wherein security would be achieved with offensive cyber capabilities employed as deterrent threats to malicious activity—a paradigm that in the United States has also begun to recede.

**NCF Operational Approach and Principles**

Although it is a relatively new UK organization, the NCF's operational approach is based on years of cyber operations experience, and the experience of its partners. It is important to note that both the UK and the United States independently arrived at some common understandings of an operational approach for the cyber strategic environment. These include: proactively and continuously operating and linking continuous operations into campaigns to generate enhanced cumulative effects of strategic import; campaigning to counter and contest, disrupting the capacity of the adversary to act or achieve their objectives; seizing opportunities to both advance security in competition with others and to set favorable conditions for managing crisis conditions and prevailing in conflict; layering cyber effects operations with information operations to amplify cognitive effects by sowing confusion and friction amongst threat actors; and combining such campaigns with other levers of national power to create longer-term strategic impact.

The NCF offers a foundation of three operational principles upon which all British cyber operations and campaigns rest: they must be conducted in line with domestic and international law (accountable); they must be timed and targeted with precision (precise); and their intended impact must be carefully assessed (calibrated). The document goes to important lengths to emphasize that UK operational planning has robust oversight ("one of the strongest in the world") and is guided by established processes, authorizations and clear doctrine with a feedback loop so that the principles of being accountable, precise and calibrated are reinforced in the operational planning cycle.

**Mechanisms of Effect**

CPT expects the unilateral exercise of cyber power to be the dominant form of cyber activity in which actors set and reset the conditions for their own security directly. This expectation is fully manifested in the NCF operational approach, which sees its core role "to make it harder for adversaries to use cyberspace and digital technologies to achieve their ends." Recognizing that cyberspace is a contested space (in line with the implication of CPT's notion of constant contact), the NCF seeks to make adversary technology work less effectively or cease functioning, disrupt those seeking to harm by impacting their ability to communicate and organize (and in the case of terrorists to disseminate extremist views), impede access to data for decision-making, undermine criminal platforms, and, when needed, support and enable military operations. Combinations of these activities create an advantage over adversaries "by affecting their perception of the operating environment and weakening their ability to plan and conduct activities effectively", what this operational primer refers to as the doctrine of cognitive effect. Operating in cyberspace, where security rests on anticipation of exploitation in an environment in which speed, scale, and scope of effects can be exponential and near instantaneous, requires mechanisms to set advantage. The NCF document suggests one solution is introducing precise and calibrated friction (this is our word and interpretation of what the doctrine of cognitive effect ultimately entails) into an adversary's operational environment, both technically and perceptually.

Based on experience, the document concludes that "we 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. This may be described as a "bend-but-do not-break approach," one informed by observations that destructive effects can often be rapidly countered by replacing

equipment or moving to different infrastructure. The document also argues that "while the immediate effect of a particular cyber operation may be relatively short lived, the cognitive impact—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." We agree with the NCF that the operational art of compounding friction to reduce functionality and confidence, by introducing doubt and complexity, is aided by cyber operations' great capacity for ambiguity—a lack of clarity about whether lost functionality is a technical glitch or a consequence of an unknown but intentional act.

**Measuring Value and Strategic Impact**

The NCF primer acknowledges the need to develop new approaches to measure effect, and to convey these to senior political leaders who rightly want to see a return on their investment. One obstacle to be surmounted is the incorrect reflex made by some analysts and policymakers to focus on the technical (and often transitory) effects of a singular operation and conclude that they fall short of exerting an independent and decisive impact. Some academic literature is wedded to this narrow understanding and fails to recognize the independent strategic impact of cyberspace campaigns in competition and enabling role in crisis and conflict. Viewing each cyber operation as a discrete act, and particularly cyber effects operations as a substitute for kinetic effects, has fostered unrealistic expectations for measuring impact.

Technical effects on systems or data can produce tactical outcomes and often short-term effects (to include cognitive) on targets and actors. Over time, when combined with information operations, the cumulative impact of tactical actions can have an operational impact on the adversary's military campaign and a strategic impact on their broader goals. Moreover, military cyber operations can advance broader allied strategic goals by enabling demarches, indictments and arrests, sanctions, and other partner activities. US and UK cyber forces have pivoted from thinking in terms of discrete targets toward understanding how cyber operations contribute to campaigning for strategic impact. This remains a work in progress and a fruitful area for US-UK collaboration.

**An Area for Further Research**

We have argued that academic research in the field of cyber security studies will need to address with greater fidelity the operational nuances that are likely to emerge as states anchor their cyber strategies on initiative persistence. The NCF has provided grist for that academic research mill with its inaugural operational principles document, just as US Cyber Command did in 2018 with the introduction of persistent engagement. Both documents leveraged expertise from the academic community. This should broaden and the NCF operational primer identifies an area that is ripe for academic research—how continuous campaigns that introduce organizational and decision-making friction disrupt an adversary's ability to leverage speed, scale, and scope. Slowing down the other side has the knock-on potential to reinforce one's own advantage in a fluid environment of contested initiative. This is a fascinating way and means of cyber persistence, which the British have illuminated.

Ultimately, the UK and the United States share a vision of cyberspace that remains global, interoperable, secure, and anchored responsibly around democratic principles. The release of this NCF operational

primer on responsible cyber power should encourage support and confidence from the UK public and government and become an important pillar in an effective whole of society cyber approach. Internationally, the document makes an invaluable contribution to defining what the responsible exercise of cyber power in the pursuit of defense and security looks like when it is aligned with the strategic realities of cyberspace.

*The views expressed are those of the authors and do not reflect the official position of any US government agency.*

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE (DD-MM-YY) | 2. REPORT TYPE | 3. DATES COVERED (From – To) |
|---|---|---|
| 00-04-23 | Non-Standard | |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| U.K. National Cyber Force, Responsible Cyber Power, and Cyber Persistence Theory | HQ0034-19-D-0001 |
| | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBERS |

| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
|---|---|
| Richard J. Harknett, Michael P. Fischerkeller, Emily O. Goldman | C5224 |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |

| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES | 8. PERFORMING ORGANIZATION REPORT NUMBER |
|---|---|
| Institute for Defense Analyses<br>730 East Glebe Road<br>Alexandria, VA 22305 | NS D-33461 |

| 9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR'S / MONITOR'S ACRONYM |
|---|---|
| Institute for Defense Analyses<br>730 East Glebe Road, Alexandria, VA 22305 | IDA |
| | 11. SPONSOR'S / MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Michael P. Fischerkeller

14. ABSTRACT

In April 2023, the United Kingdom's National Cyber Force released a primer describing how it would operate. This essay examines that primer from the perspective of cyber persistence theory and finds that the UK's strategic approach is closely aligned with the theory's strategic prescriptions.

15. SUBJECT TERMS

Cyberspace, cyber strategy, UK National Cyber Force

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | Institute for Defense Analyses |
| Unclassified | Unclassified | Unclassified | Unlimited | 4 | 19b. TELEPHONE NUMBER (Include Area Code) |