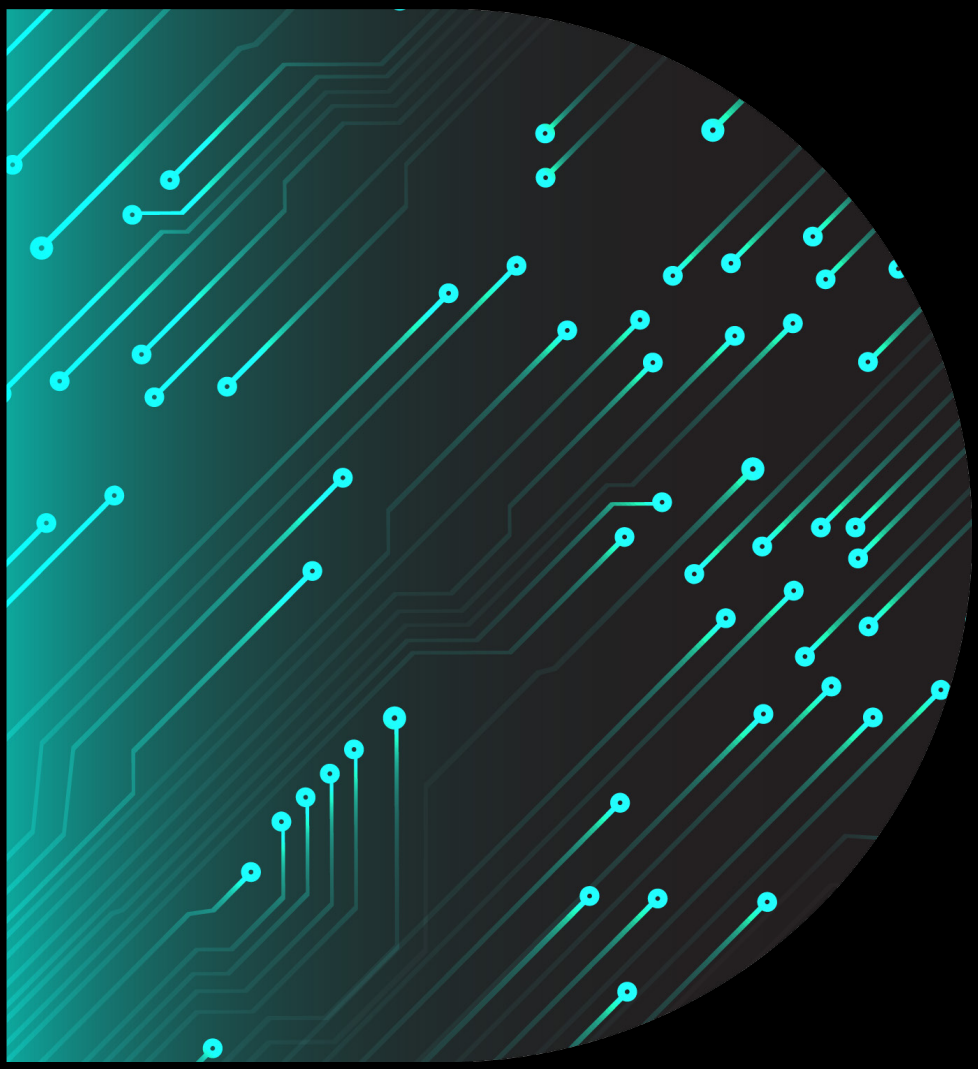
The Advantages of "Hunt Forward" Extend Beyond the Hunt

Nick Beecroft & Toby Gilmore



Digital Intelligence

BAE SYSTEMS

Introduction

Hunt Forward Operations (HFOs) have risen to prominence as the most tangible demonstration of US Cyber Command's intent to pursue threats in cyberspace. Since its initiation in 2018, the HFO programme has attracted increasing demand for its services, with 47 operations conducted on over 70 networks in 22 countries[1].

Yet the purpose of these operations is often **misinterpreted**, usually by association with offensive cyber operations[2], leading to **poor understanding of the value of the capability and its potential application for other countries**. This paper aims to clarify the nature of HFOs and introduces some considerations for how other nations could employ similar capabilities.

The Logic of Hunt Forward

HFOs are a unique approach developed by the US Cyber Command Cyber National Mission Force (CNMF), as part of its mission to **"deter, disrupt, and defeat adversary cyber and malign actors"**[3]. In simple terms, HFOs extend the well-established cybersecurity activity of threat hunting to include overseas deployment of personnel to investigate foreign networks. They are described as purely defensive operations[4], but the label of "hunt forward" can lead to them being misunderstood as offensive – i.e. involving covert penetration of adversary networks. In order to understand the purpose and advantages of HFOs, it is necessary to briefly examine the concepts that serve as the foundation for Cyber Command operations.

The most influential concept is the doctrine of **"persistent engagement"**, which is based on the idea that the interconnectedness of cyberspace creates a state of continual competitive interaction between adversaries, below the level of armed conflict[5]. In this environment, effective defence and strategic advantage rely on seizing and maintaining the initiative[6]. This logic led to the strategy of **"defend forward"**, which emphasises sustained, proactive measures to disrupt threats before they can harm the US.

Defending forward therefore relies on early and detailed identification of adversary activity, and the role of HFOs is to provide an enhanced capability for identifying and assessing threats early in their development. This is accomplished through the deployment of CNMF personnel to receptive countries, where they are provided with the necessary access to **"observe and detect malicious cyber activity on host nation networks"**[7]. The aim is to operate **"as close to the origin of adversary activity as possible"**[8], which in practice means the **"near abroad"** of the highest priority adversaries[9].

These operations have been credited with discovering previously unknown malware[10], but it is possible that similar results could have been achieved through remote threat hunting. The most distinctive contribution of a HFO could lie not in the tactical aim to discover threats on given networks, but in more enduring benefits created through networks of trusted partners and a tangible commitment to collective defence.

There is a risk that HFOs could be perceived as the US exploiting its leverage over partners for its own benefit[11], and Cyber Command has consistently emphasised its intention to create mutual benefit with host nations through enduring relationships and shared insights. HFO teams do not undertake security activity to mitigate threats they find on host networks, but they do share the intelligence gained and assist in identifying vulnerabilities[12]. Deployed teams also aim to build relationships of trust and familiarity with their hosts that endure beyond an operation and promote ongoing intelligence sharing and assessment. This operational collaboration has been credited with deepening the bilateral relations between the US and the host nation[13], and HFOs have been aligned with broader cyber capacity building objectives aimed at enhancing collective cyber defence[14]. The partnership model has also been extended to a joint operation with an ally, through a mission to Latvia with the Canadian cyber task force in early 2023[15].

Public reporting of the results of HFOs has necessarily been limited, but Cyber Command evidently judges that HFOs have made a valuable contribution. The Command's budget estimate for financial year 2024 included a provision for a significant increase in operational tempo of up to 22 HFOs per year, albeit involving only a relatively modest (in the context of the total budget) **$15 million** increase in financial commitment[16].

Modifying "Hunt Forward" for Wider Application

The concept of deploying cyber expert teams to work with foreign partners has attracted interest beyond the US – for example, the EU has established a capability under the leadership of Lithuania for the deployment of "Cyber Rapid Response Teams" [17]. However, the HFO model involves a major commitment of specialist resources dedicated to the mission of one agency, and it benefits from the global influence of the US to secure the cooperation of partners.

Other countries will not be able to call on the same advantages, and will need to develop alternative approaches. Modification of the HFO model should therefore be founded on a broader range of objectives, to maximise the benefits gained from a deployment, and an emphasis on partnerships to make the most efficient use of resources. This article uses the label **"deployed cyber defence"** (DCD) to distinguish this broader approach from the intelligence-gathering focus of HFOs.

The aim of DCD would be to retain the benefits of deployed working with partners and the threat-focused, proactive approach of HFOs, but apply it to a wider range of public policy objectives. Intelligence gathering for the purposes of defeating/disrupting threat actors would be supplemented by activities to mitigate vulnerabilities, assess risks, develop resilience and build cyber capacity.

A simple way to illustrate the concept is by evaluating its relevance to the aims of the UK National Cyber Strategy 2022.

With a more flexible remit, including but not limited to intelligence gathering to inform deter/disrupt/defeat operations, DCD could serve objectives within three of the five pillars of the strategy, as shown below:

Pillar	Objective	DCD direct or indirect contribution
Cyber Resilience	Understand cyber risk	Direct
	Prevent and resist cyber attacks	Direct
	Prepare, respond and recover	Indirect
Global Leadership	Strengthen collective action and mutual cyber resilience	Direct
	Shape global governance of cyberspace	Indirect
	Leverage and export UK capabilities in cyber	Direct
Countering threats	Detect, investigate and share information on threats	Direct
	Deter and disrupt threats	Direct
	Take action in and through cyberspace to counter threats	Direct

Cyber Command HFOs have been credited with contributing to all of these objectives, but the specialised role of the CNMF means that operations would be prioritised and planned against the objective to deter and disrupt threats, with other considerations likely to be subordinate to this aim.

The US has the capacity to deploy other specialist resources overseas for objectives outside the CNMF remit. By contrast, the DCD concept of operations would allow any of these objectives to form the central, or an equally weighted, justification for deployment. This should establish DCD as a flexible capability that could deliver a range of outcomes.

Nevertheless, detailed scrutiny of the potential value and the costs/risks involved would be required to justify any investment in the capability. Below we introduce the main benefits and challenges that would warrant further investigation:

Benefits	
UK National Cyber Strategy Pillar	Detail
Cyber Resilience	Deeper understanding of emerging threats; opportunities for joint analysis with partners/hosts.
	Early interdiction of threats, before they proliferate and harm the UK.
Global Leadership	Creation of professional networks in countries likely to be targeted.
	Improved security and resilience of critical networks in recipient countries.
	Strengthened bilateral relations with recipient countries.
	Prevention of adversaries' attempts to exert influence through cyber operations, creation of opportunities to expose irresponsible/illegal activity.
	Identification of requirements for/effectiveness of capacity building measures.
	Introduction of UK cyber capabilities to new markets.
Countering threats	Enhanced intelligence collection opportunities against high priority targets.
	Early exposure of adversary tactics, techniques and procedures (TTPs), thus reducing/eliminating their effectiveness and imposing costs on adversaries.

Challenges	
Category	Detail
Resources	Requires highly skilled technical specialists; they would be diverted from other tasks or recruited for new roles. DCD would be an attractive proposition for these specialists, but they are in short supply and are highly sought after.
Budget and political considerations	Allocation of budget to assisting foreign partners to improve the cybersecurity of their networks may be controversial if it diverted funds from home defence or other forms of overseas assistance.
Administrative burden	May be significant if constituted as a permanent unit within a government department/agency.
Dependency/ moral hazard	There could be a risk of creating dependency with recipients, or disincentivising investment in cybersecurity in recipient countries.

The benefits illustrate how DCD would offer a range of advantages as a policy tool, complementing cyber capacity building (which is aimed at long term development objectives) and cyber crisis response (which is aimed at capability reinforcement and damage remediation during or after cyber-attacks).

By taking a proactive approach to identifying threats to, and strengthening the resilience of, partners' networks, DCD could negate the need for crisis response and provide a foundation for targeted capacity building. It could also enhance national cyber defence through insight to networks outside the normal scope of intelligence and security operations, and early interdiction of threats.

Nevertheless, the challenges could be prohibitive, especially in the commitment of specialist personnel and prioritisation of budgets to assist foreign countries. A public-private partnership delivery model could provide access to larger pools of resources and, with careful design of objectives and reporting requirements, could allow detailed assessment of the effectiveness and value for money of operations.

Precise operational design, drawing on multidisciplinary expertise and collaboration with recipients, would be essential. But this model has been used successfully for other cybersecurity operations, and it has promise for enabling DCD in a sustainable, cost effective way.

The DCD concept of serving a broad set of policy objectives and stakeholder interests would create additional complexities to be navigated, compared to the HFO model of an organic unit serving a single organisational mission. But the capability appears to be proving its value, and if nations other than the US wish to harness it, they will need to develop innovative mechanisms founded on partnerships and flexibility.

Reference List

[1] https://www.cybercom.mil/Media/News/Article/3390470/shared-threats-shared-understanding-us-canada-and-latvia-conclude-defensive-hun/

[2] https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139

[3] https://www.cybercom.mil/About/Components/CNMF/

[4] https://www.cybercom.mil/Media/News/Article/3229136/before-the-invasion-hunt-forward-operations-in-ukraine/

[5] https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace

[6] Michael P. Fischerkeller, Emily O. Goldman and Richard J. Harknett, Cyber Persistence Theory (Oxford University Press, 2022), 86-87

[7] https://www.cybercom.mil/Media/News/Article/3218642/cyber-101-hunt-forward-operations/

[8] https://www.cybercom.mil/Media/News/Article/3218642/cyber-101-hunt-forward-operations/

[9] https://www.defense.gov/News/News-Stories/Article/Article/2078716/dod-has-enduring-role-in-election-defense/). Of the 22 countries cited by Cyber Command, eight have been publicly identified as Albania, Croatia, Estonia, Latvia, Lithuania, Montenegro, North Macedonia and Ukraine. (https://www.cybercom.mil/Media/News/Article/3390470/shared-threats-shared-understanding-us-canada-and-latvia-conclude-defensive-hun/)

[10] https://breakingdefense.com/2021/11/cybercoms-no-2-discusses-hunt-forward-space-cybersecurity-china/

[11] https://www.bbc.co.uk/news/uk-63328398

[12] https://www.cybercom.mil/Media/News/Article/3337717/committed-partners-in-cyberspace-following-cyberattack-us-conducts-first-defens/

[13] See for example the joint statement of the Estonian Ministry of Defence and Cyber Command following a HFO in late 2020: https://kaitseministeerium.ee/en/news/hunt-forward-estonia-us-strengthen-partnership-cyber-domain-joint-operation

[14] https://www.cybercom.mil/Media/News/Article/3390470/shared-threats-shared-understanding-us-canada-and-latvia-conclude-defensive-hun/

[15] https://www.cybercom.mil/Media/News/Article/3390470/shared-threats-shared-understanding-us-canada-and-latvia-conclude-defensive-hun/

[16] https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2024/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PART_1/CYBERCOM_OP-5.pdf

[17] (https://crrts.eu/)

We are Digital Intelligence

BAE Systems Digital Intelligence is home to 4,800 digital, cyber and intelligence experts. We work collaboratively across 16 countries to collect, connect and understand complex data, so that governments, nation states, armed forces and commercial businesses can unlock digital advantage in the most demanding environments. Launched in 2022, Digital Intelligence is part of BAE Systems, and has a rich heritage in helping to defend nations and businesses around the world from advanced threats.

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
19, Boulevard Malesherbes
75008 Paris
France
T: +33 (0) 1 55 27 37 37

BAE Systems
Mainzer Landstrasse 50
60325 Frankfurt am Main
Germany
T: +49 (0) 69 244 330 040

BAE Systems
Level 12
20 Bridge Street
Sydney
NSW 2000
Australia
T: +6 1290 539 304

BAE Systems, Surrey
Research Park, Guildford,
Surrey, GU2 7RQ, UK

E: learn@baesystems.com

W: baesystems.com/digital

linkedin.com/company/baesystemsdigital

twitter.com/BAES_digital

Copyright © BAE Systems plc 2023. All rights reserved.

BAE SYSTEMS, the BAE SYSTEMS Logo and the product names referenced herein are trademarks of BAE Systems plc.

BAE Systems Digital Intelligence Limited registered in England & Wales (No.1337451) with its registered office at Surrey Research Park, Guildford, England, GU2 7RQ.

No part of this document may be copied, reproduced, adapted or redistributed in any form or by any means without the express prior written consent of BAE Systems Applied Intelligence.

BAE SYSTEMS