# The UKâ??s New Take on Cyber

## Description

From its 2010 inception to its most recent 2022 publication, the primary focus of the United Kingdomâ??s National Cyber Strategies (NCS) evolved from a security-focused approach to a broader, more ambitious vision of â??cyber power.â?? The United Kingdom views cyber power as the projection of cyber security. With aims to act as â??a leading responsible and democratic cyber power â?• and strategies steeped in the language of both national power and big-picture thinking, the United Kingdom understands cyberspace as a battleground for Great Power Competition and a platform to export values, knowledge and norms. While it redefined its approach to cyber, its objectives remain ambiguous and require further refinement.

### How Does the United Kingdom Define Cyber Power?

In the 1990s, American political scientist Joseph Nye first coined the term â??soft powerâ?• as a means to counteract the prevailing theories of hard, coercive and militaristic power projection. Specially, soft power proposes the benefit of projection via co-option: to influence â??others by ideas and attraction that sets the agenda for others or gets them to want what you want.â?• Nye describes the power as more than the capacity to do things or to have things; rather, it is the ability to influence the adversary to achieve the outcomes one wants.

The United Kingdom applies both Nyeâ??s soft and traditional military power theories to cyber, defining cyber power as â??the ability to protect and promote national interests in and through cyberspace.â?• This â??ability to protectâ?? suggests the ability to defend the UK government, private organizations, and citizens against attacks in cyberspace, manifested in the strategyâ??s focus on resilience and â??detecting, disrupting and deterringâ?• cyber threats through hard power. Securing the state against cyber threats and continuing to emphasize cybersecurity, therefore, remains an important component of the United Kingdomâ??s cyber power.

The United Kingdom also makes it clear that cyber power is the ability to do more than just secure and protect the state. Instead, the United Kingdom must deploy and promote cyber capabilities through cyber diplomacy. This aligns with Nyeâ??s concept of soft power, reflected in the NCSâ??s emphasis on leveraging instruments such as education and intellectual capacity to increase diversity of thought internationally through exchange of ideas. This second element, the promotion of national interests abroad, elevates cyber from a matter strictly of security to a power projection ability.

### Cyber Power with â??Responsible and Democraticâ?? Characteristics

What does it mean for the United Kingdom to be responsible and democratic in cyberspace? With new domains of power projection come increased requirements for responsibility and regulation. States seldom agree on how responsibility and democracy apply to international security. Cyberspace also uniquely transcends geopolitical borders and challenges traditional notions of state sovereignty, adding to the complexity. The United Kingdom seeks â??to promote a free, open, peaceful, and secure cyberspace,â?• using soft power to gain influence through democratic principles as opposed to offensive activities. In light of this approach, the UK government is highly critical of Russian, Chinese, and North Korean use of â??cyber operations to disrupt or destroy critical infrastructure, and directing or [harboring] cybercriminals.â?•

For a country like the United Kingdom, which prioritizes responsible conduct in cyberspace, achieving its cyber objectives requires a disproportionate investment of time, resources, and effort compared to countries that do not prioritize ethical, normative, and collateral considerations.Therefore, the effort and resources directed toward the pursuit of responsibility and democracy in cyberspace presents a particular â??handicap,â?•as it may detract from the resources needed to develop and maintain the United Kingdomâ??s cyber power ambitions.

### Democratic Does Not Equal Defenseless: Cyber Power as a Weapon

While the United Kingdom strives for responsible and democratic use of cyber power, its policy does not necessarily make the nation an easy mark for cyber coercion and exploitation. The United Kingdom subscribes to a contested understanding of the meaning of sovereignty in cyberspace that enables it â??to engage in cyber operations that, in its interpretation, do not violate other statesâ?? sovereignty and therefore do not violate international law.â?• According to the United Kingdomâ??s interpretation of non-intervention, the act of breaching another stateâ??s digital sovereignty through offensive cyber actions (e.g. disrupting a targetâ??s networks or disinformation campaign), does not itself constitute a violation of international law. Under the international law of countermeasures, the UK government argues that states whose sovereignty is violated by cyber intrusions have the right to take action that would otherwise be considered illegal. Ambiguity surrounding responsible and democratic behavior in cyberspace are thus considered to create an unstable environment in which an action perceived as minor and insignificant by one state may result in unnecessary escalation.

How offensive operations should be calibrated to be proportionate in practice is unclear. Joe Devanny and Tim Stevens from Kingâ??s College London suggest that the UK National Cyber Force, which is responsible for leading and coordinating UK cyber defense, needs to be more explicit about prioritizing counter-force over counter-value targeting, pursuing adversariesâ?? military infrastructure instead of

civilian targets such as energy and transportation facilities to avoid escalations against noncombatants.Furthermore, the United Kingdomâ??s legal position on coercion and non-intervention needs clarification, especially regarding the extent to which, in its view, international law is applicable to offensive cyber operations conducted during peacetime. In an article published by *Lawfare* in 2022, Andrew Dwyer and Ciaran Martin explained that, by advocating for an expanded use of coercion, the United Kingdom grants the National Cyber Force greater operational flexibility. This, in turn, may be seen as a threat to other states. Such individual understanding and application of coercion to cyberspace is especially problematic because, in the cyber domain, such concepts cannot be bound by geographical borders.

At the same time, the National Cyber Force faces scrutiny over transparency. According to Dr. Dan Lomas, Assistant Professor in International Relations at the University of Nottingham, â??an ongoing challenge for the [Force] is demonstrating accountability and legitimacy around its â??license to operate,â?? and how far officials can go in telling us what it does.â?• Policymakers find offensive cyber operations an attractive option as â??they are largely covert [â?¦] and donâ??t have to be disclosed to or debated in Parliament or the press.â?• Yet, this is in direct opposition with the United Kingdomâ??s vision of adhering to democratic principles in cyberspace.

**Democracy Versus Freedom: Contradictions of Control**

The United Kingdomâ??s current vision to promote a free and open global cyberspace clashes with the NCSâ??s pillar of advancing UK global leadership and influence for a secure and prosperous international order. The United Kingdom wants cyberspace to be free and open but also under its control to facilitate regulation. This contradiction raises questions about political sovereignty. Specifically, it reflects the tension between the view that the sovereign nation state should have absolute authority over the cyberspace within its territorial borders, versus the view that this cannot occur because cyberspace is an inherently transnational and open space. If there is authority over where data exists and where data travels, then political and physical geography still matter in cyberspace; if not, then political borders, physical geography, and the traditional meaning of sovereignty become irrelevant.

**Public and Private Protection**

While the United Kingdom dictates the need to proliferate the range and number of public-private partnerships to increase information sharing, their ideal structure and method of operations remains unclear. The public and private sectors disagree about their roles and responsibility in cyberspace.The former believes that it is solely responsible for providing national security and therefore rejects liability for private networks. The latter, however, contends that some networks, particularly privately owned

critical national infrastructure networks, are also central to national security. Such conflicting expectations between the government and private enterprises about roles and responsibilities can lead to a dangerously fragmented approach to cyber power.

After the 2017 WannaCry attack, which targeted British healthcare systems and corporations worldwide, UK government officials and cybersecurity experts sought to determine responsibility for the vulnerability. According to former chairman of NHS Digital, Kingsley Manning, â??a failure to upgrade old computer systems at a local level within the NHS had contributed to the rapid spread of the malware.â?• However, cybersecurity experts agree that addressing attacks like WannaCry hinges largely on management rather than technology. WannaCry revealed that no party was fully prepared to shoulder responsibility. For public-private partnerships to work, they must be based on shared accountability and trust. Therefore, to increase the range and number of public-private partnerships in cyberspace, the United Kingdom must start by establishing clear parameters and frameworks that define roles, responsibilities, and expectations for both sectors.

## A New Vision for Cyber

The United Kingdomâ??s third-generation national cyber strategy suggests that cyber is a core component of national power. But what cyber power means for the United Kingdom, especially when it is exercised â??responsibly and democratically,â?• requires clarification and greater specificity.

Due to competing narratives, strategic cultures, and the natural progression of technology, states will inevitably adopt their own understandings of not only cyber power but also what it means to operate responsibly and democratically. In a geopolitically contested battleground, where nations attribute different meanings to the concept of cyber and cyber power, the most important effect will be the balance of players, not the balance of power. Ultimately, the United Kingdom must be clear about its own understanding of cyber power if it is to lead by example and remain a key participant in cyberspace.

---

*Abaigeal Lorge is a National Security Research Analyst at Karve International. She holds a BA in International Relations from the Kingâ??s College London Department of War Studies. Her research areas of interest include cybersecurity, Russian geostrategic ambitions and the role of emerging technologies in warfare.*

*Image Credit: UK Government Communications Headquarters. May 14, 2024.*

***Acknowledgment:*** *Portions of this article are heavily influenced by the course BA3 â??Cybersecurity: Policy, Politics and Practiceâ?• taught by Dr. Danny Steed, Department of War Studies, Kingâ??s*

*College London.*

*If you value reading the Irregular Warfare Initiative, please consider supporting our work. And for the best gear, check out the IWI store for mugs, coasters, apparel, and other items.*

**Date Created**
2025/03/04