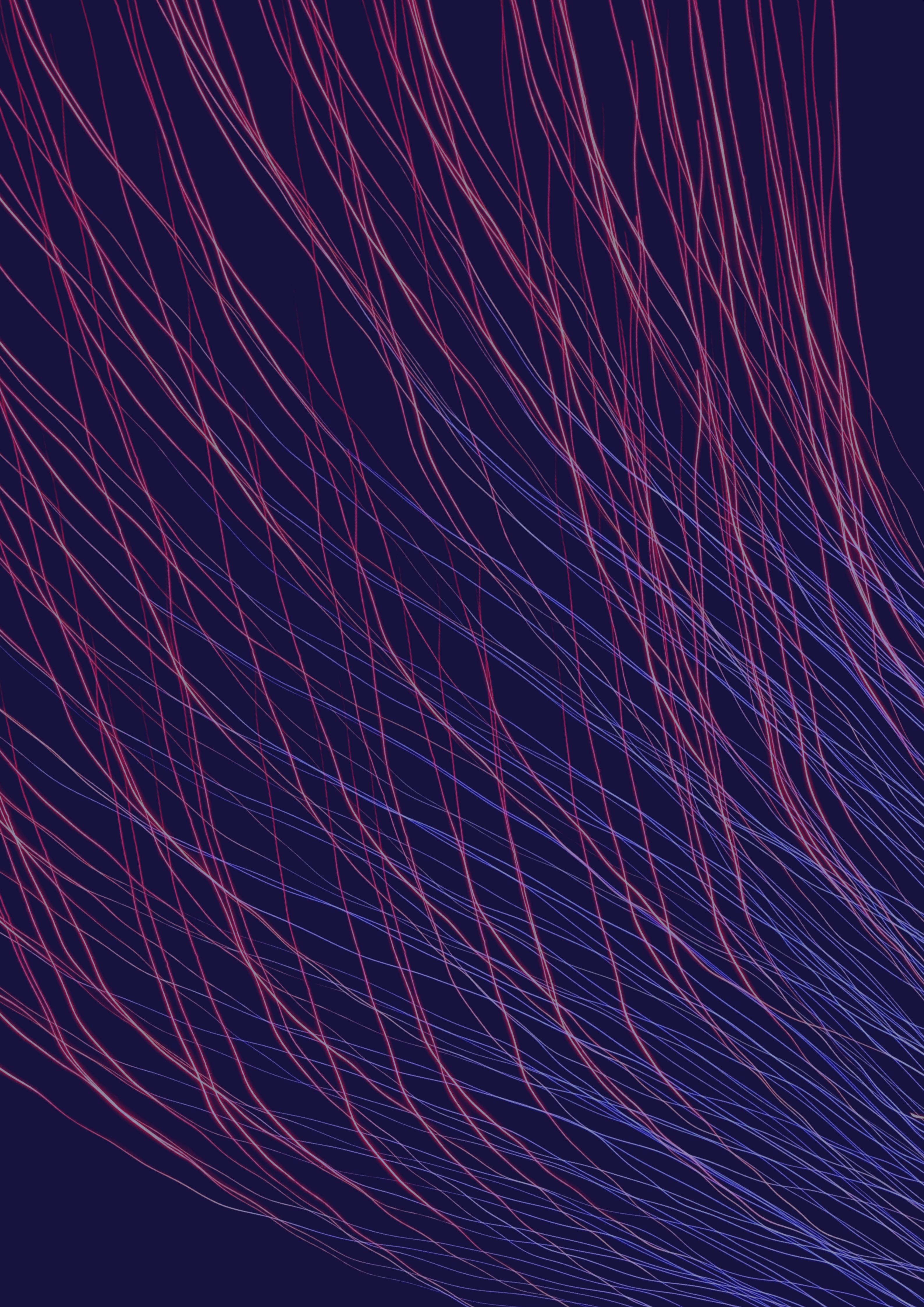
National
Cyber Force

A Defence and Intelligence Partnership

The National Cyber Force:

Responsible Cyber Power in Practice



Contents

Foreword

The vision of the UK's National Cyber Strategy (NCS) 2022 is that the UK will continue to be a leading, responsible and democratic cyber power, able to protect and promote its interests in and through cyberspace in support of national goals. The NCS 2022 set out how the UK will continue to adapt, innovate, and invest in order to pioneer a cyber future with the whole of the UK.

One year on, the National Cyber Force (NCF) is taking the opportunity to illustrate aspects of how the UK is being a responsible cyber power in practice. The NCF is one of the exciting and transformational elements which contribute to the NCS. Created in 2020, by building on the previous National Offensive Cyber Programme, the NCF operates continually to support the armed forces and foreign policy of the UK and disrupt a variety of threats: some enabled by the internet and others that put at risk our own ability to benefit from a free, open, peaceful and secure cyberspace.

It draws together personnel from GCHQ, the Ministry of Defence (MOD), including Defence Science and Technology Laboratory (Dstl), and SIS under one unified command. Since its establishment, it has played its part in creatively developing a much more integrated and routine use of a full spectrum of capabilities to maintain the UK's strategic advantage. The integration of the NCF into both Defence and the intelligence agencies is a key part of its unique offer.

Responsible Cyber Power In Practice provides more detail about how NCF is operating now. Although the field remains relatively new, with much still to be discovered about how these capabilities can be deployed to best advantage, the level of knowledge and understanding has developed quickly in the NCF. Cyberspace is a dynamic environment, and therefore the NCF needs to be agile in developing and seizing opportunities.

> *Cyberspace is a dynamic environment, and therefore the NCF needs to be agile in developing and seizing opportunities.*

In outlining its current thinking, the NCF aims to promote constructive debate and contribute to demonstrating the UK's commitment to being a responsible cyber power. It may also potentially contribute to deterrence. Much has been achieved since the NCF's creation; in particular, stakeholders appreciate the versatility of its offer, and the utility of learning together across its diverse missions, from supporting military operations and countering a wide range of state threats, to addressing terrorism and serious crime. NCF derives strength from the diversity of its participants, and the wide range of partners both in the UK and internationally that it cooperates with. In demonstrating the clear value, relevance, and potential of these capabilities, NCF is already helping to show how the whole of society and whole of cyber vision set out in the NCS is the right one for the UK.

Sir Jeremy Fleming
Director GCHQ

General Sir Jim Hockenhull
Commander UK Strategic
Command

Introduction

Cyberspace and digital technology are a fundamental part of daily life. They are central to how we communicate with each other, develop our understanding of what's happening in the world, conduct business and enjoy our free time. They are also key to how governments and armed forces across the world operate today.

An inevitable consequence of this digital revolution is that cyberspace is a significant environment where global security issues are increasingly played out. In today's digital age, the UK's ability to operate securely and effectively in cyberspace has become necessary to delivering our national goals. At the same time, the UK's adversaries, including both state threats and non-state actors, are increasingly using cyberspace and digital technology to do us and others harm.

The Government believes the UK cannot leave cyberspace an uncontested space where adversaries operate with impunity. In the Integrated Review 2021 the UK Government set out the intent to have the ability to take disruptive cyber action that exploits an adversary's own dependence on digital technology. It also committed to shaping new rules so that offensive cyber tools are developed and used responsibly, in accordance with international law and with due regard to voluntary and non-binding norms such as those endorsed by the UN General Assembly.

The UK cannot leave cyberspace an uncontested space where adversaries operate with impunity.

It is the role of the NCF to make it harder for adversaries to use cyberspace and digital technologies to achieve their ends. This guide to the NCF provides more detail on the background to the NCF and the context in which we operate. It describes our fundamental operational principles, how we go about our work and provides some operational examples. And it sets out that **how** we function is key to being consistent with our democratic values and the principles of a responsible cyber power.

The Challenge

The digital technologies that constitute cyberspace are a transformational global force for good with societies increasingly reliant on them. They also act as a critical enabler for actions in the physical world. Modern armed forces worldwide use sophisticated digital capabilities for command and control, situational awareness and as an integral component of weapons systems; in military operations, where the side that most effectively uses digital systems to its own advantage, whilst reducing the ability of their enemy to do so, has a critical edge. These technologies also offer malicious actors new and more effective ways to cause harm in the UK and throughout the world.

Countries such as Russia and Iran routinely carry out cyber operations of different kinds in order to spread disinformation, attempt to undermine democratic processes, disrupt the ability of democratic governments to carry out their day-to-day functions and even to prevent key pieces of critical infrastructure from functioning, without any regard for the consequences.

International organised crime groups have developed whole new classes of criminal activity – in particular ransomware – that exploit our dependence on digital technology to make them money. Terrorist organisations use the internet extensively to spread propaganda and to co-ordinate their attacks.

And the Russia-Ukraine conflict has seen cyber criminals and hacktivists explicitly aligning themselves with each side's political objectives and carrying out cyber-attacks targeting foreign interests for political purposes. This demonstrates the potential growth of ideologically driven cyber-attacks outside of any state influence or control at all.

Cyberspace has become an environment that hostile actors are seeking to exploit as much as they can. This very dependency opens up new opportunities to disrupt threat actors, reduce their ability to do us harm and further the interests of the UK and its allies.

The Response

The UK and its allies have a wide range of levers available to tackle serious security threats, including those that are dependent on, or enabled by, cyber capabilities. Depending on the context, these can involve measures such as cyber resilience, law enforcement action, sanctions, diplomatic intervention, and military activity including, where necessary, the use of force. Alongside these measures, the NCF provides options for the UK to use cyber capabilities as part of the response to serious threats from states and other hostile actors.

Where traditional responses are best placed to deal with the challenge effectively, NCF would rarely if ever get involved. We use existing prioritisation and objective setting structures across government to ensure that we focus our efforts where the nature of the problem means that cyber operations can make a important contribution.

Cyber operations offer particular advantages, depending on the circumstances. They provide an opportunity to reach adversaries irrespective of geography and without the need for individuals to be physically present. They can sometimes provide the only practical

means of disrupting an adversary's ability to exploit the internet and digital technology. They can be precisely targeted with specific effect and can avoid the challenges of using other, potentially physically destructive, interventions. They can create a range of cognitive effects – such as undermining an adversary's confidence in the data they are receiving or in the ability of their information systems to function effectively – that may be harder to achieve with other approaches.

For all this, there remain questions over the role of cyber operations as a part of modern deterrence. Much has been written about cyber and deterrence, without distinguishing between deterring cyber activity, or using cyber effects to deter other activities. The complexity of the many contributing factors to deterrence means it is not straightforward to read across concepts and lessons directly from the fields of conventional or nuclear deterrence, or seek to build a standalone concept of deterrence without thinking holistically across these broader aspects.

Whilst evidence is limited for cyber operations being a primary contributor to deterrence, they can form a secondary or supporting element in an integrated approach.

> *To be secure in cyberspace also requires actively tackling the cyber dependencies of adversaries.*

The UK's resilience in cyberspace needs to be at the heart of the UK's defence against adversaries looking to exploit the internet to cause harm. That is why the Government has invested significant resources and energy into improving the UK's cyber security as set out in the 2022 NCS. However, to be secure in cyberspace also requires actively tackling the cyber dependencies of adversaries. Thus, the National Cyber Security Centre (NCSC) and the NCF are both integral to the strategy.

National Cyber Force

Established in 2020, the NCF is responsible for operating in and through cyberspace to counter and contest those who would do harm to the UK or its allies, to keep the country safe and to protect and promote the UK's interests at home and abroad. We operate at the direction of a democratically elected government within a robust oversight framework.

Once the currently planned growth is complete, we will be made up of a roughly equal share of personnel from the MOD and the intelligence agencies, bringing together expertise, resources, and authorities under a single command structure. We are building on significant experience in cyber operations, stretching back over two decades. This has included disrupting terrorist command and control and propaganda distribution, supporting military objectives on the battlefield, and disrupting the activities of hostile actors seeking to do us harm.

The NCF combines MOD's operational and planning expertise, Dstl's scientific and technical capabilities, GCHQ's global intelligence and SIS's skills in recruiting and running agents alongside delivering clandestine operational technology. This mix of operational, intelligence and security experience provides the UK with a diversity of perspectives and thinking that we believe gives us an edge over our adversaries.

The NCF carries out cyber operations on a daily basis to protect against threats to the UK, further the UK's foreign and national security policy, support military operations, and prevent serious crime (such as countering child sexual exploitation and abuse). NCF operations are conducted against both state and non-state threats (such as terrorism).

> *This mix of operational, intelligence and security experience provides the UK with a diversity of perspectives and thinking.*

We are establishing a new permanent base at Samlesbury in Lancashire, which will enable the NCF to increase its operational output. The new headquarters will also contribute to the levelling up agenda and bring economic stimulus and other tangible benefits to the region.

The NCF is responsible for operating in and through cyberspace to counter and contest those who would do harm to the UK or its allies.

What this means in practice

In practical terms the NCF develops and uses cyber capabilities to carry out operations including disrupting adversary ability to make use of cyberspace and digital technology, influencing adversaries away from doing harm, and exposing hostile activity and wrongdoing.

Our work can include covert operations against the IT networks or technology used by adversaries and employing techniques to make that technology function less effectively or cease to function altogether.

> *Our work can include covert operations against the IT networks or technology used by adversaries.*

It might involve disrupting an adversary's ability to use different forms of digital communications systems, so they are unable to contact each other at critical times. Or affecting systems an adversary depends on for access to data or to enable their decision making. Techniques may be used to reduce the ability of terrorists to spread extremist media online, or to make it harder for states to use the internet to spread disinformation. Operations may undermine the ability of adversaries to use the internet for criminal purposes by disrupting their use of online platforms and services. Or support the UK's current military operations and future planning.

Operations may also be conducted to try to influence hostile actors. Intelligence capabilities may be used covertly to gather data about a hostile actor's activities and then used to demonstrate that their actions are known about and understood. Or covert techniques may be used to reach out to individuals who pose a significant threat to the UK or our allies to seek to influence their actions in a positive way.

We may also use a combination of technical and information operations against hostile actors in a mutually supportive way, for example, to sow distrust in groups such as criminal gangs or terrorist cells.

This document outlines, from NCF's perspective, some of the fundamental operational principles that lie behind these activities, the requirements of responsible cyber operations and some of the challenges that we face as a new organisation.

The UK's Principles And Operational Approach

Operational principles

Cyber operations are complex and challenging. As a responsible democratic cyber power, the UK is expected to operate in a legal, ethical and responsible way. With that in mind, the NCF designs its operations in accordance with the following core principles:

- Accountable
- Precise
- Calibrated

Accountable

Operations are conducted in a legal and ethical manner, in line with domestic and international law and our national values.

Precise

Operations are based on a deep understanding of the cyber environment and are designed to be timed and targeted with precision.

Calibrated

The impact of operations is carefully assessed, taking into account the wider context. This is a dynamic process that responds rapidly to any changes in the operational environment. Consideration is given to a wide range of factors including those that might affect wider escalation and de-escalation.

The operational approach

We have developed an operational approach drawing on the UK's experience of and lessons derived from conducting cyber operations over many years, as well as the use of cyber by others. Our thinking and approach will inevitably continue to evolve as we reflect and learn from the operational impact. The main elements are as follows:

Cyber operations and cognitive effect

Our objective is to change adversary behaviour by exploiting their reliance on digital technology. Sometimes our operations will simply aim to remove the adversary's ability to act. For example, preventing a terrorist group from publishing pieces of extremist media. While it may not be possible to prevent such actions indefinitely, there is advantage in disrupting activity at key points.

Other operations seek to have a more wide-ranging effect on the adversary's ability to carry out their intentions. We do this through various means including affecting an adversary's ability to acquire, analyse and exploit the information they need to advance their objectives. We may also limit their ability to communicate and co-ordinate with others. And we may seek to affect their confidence in their digital technology and the information it is providing them.

Taken together, these kinds of techniques have the potential to provide advantage over adversaries by affecting their perception of the operating environment and weakening their ability to plan and conduct activities effectively. We refer to this as the doctrine of cognitive effect. It is aligned with UK military doctrines of multi-domain and integrated action, which seek to combine capabilities across the domains to have an effect on an adversary's understanding, capability and willpower to change its behaviour.

From operational experience, we find 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 (as in some cases they can be quickly replaced). However, operations to have destructive effect remain an option where that is the most appropriate solution.

A high degree of planning is required to achieve optimal impact and, in some cases, getting the precise timing right is essential. 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. Combining several operations, alongside other levers of power, into a campaign for cumulative effect also supports longer term outcomes.

Our operations are covert, and the intent is sometimes that adversaries do not realise that the effects they are experiencing are the result of a cyber operation. The ambiguity involved can help to amplify the cognitive effect. As a general rule we cannot and do not avow cyber operations, as to do so undermines the benefits of ambiguity and risks enabling adversaries to develop better defences.

Influence activity

We use various techniques to influence hostile actors to change their behaviours, including engaging with them directly online. Other operations covertly expose information to a range of audiences highlighting, for example, unlawful activities or the fact that a state actor is behind certain disinformation sites. It is our accountable, precise, calibrated and therefore proportionate operations that distinguish us from the large-scale disinformation activities practised by certain of our adversaries.

Dynamic, targeted operations

Cyberspace is a dynamic operating environment that demands constant effort to identify opportunities and threats. We use a range of operational styles, tailored to particular circumstances and objectives. 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. Under most circumstances, our operations are dynamic. They focus on a range of priority targets with highly tailored and calibrated actions designed to achieve specific outcomes.

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. In the military context, cyberspace is frequently a

We may seek to affect their confidence in their digital technology and the information it is providing them.

key enabler of operations in other domains.

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.

Sometimes operations can be conducted specifically to respond to a particular action by a hostile actor – disrupting a state's disinformation campaign, for example. At other times they 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.

Military integration

NCF is integrating cyber with other UK military capabilities to help protect our forces, engage our allies and constrain our adversaries to prevent conflict developing.

We are supporting the development of better understanding of the cyber and electro-magnetic domain and its integration with the other operational areas of the military – maritime, land, air and space – to be able to synchronise effects across the tactical, operational and strategic levels. Conducting operations in cyberspace is a critical part of driving the conditions and tempo of strategic activity; a key plank of the military's approach to increased nation-state competition, and to warfighting, where that is necessary.

> *Conducting operations in cyberspace is a critical part of driving the conditions and tempo of strategic activity.*

Capability development

We develop cyber capabilities that are relevant to circumstances across the continuum from competition through crisis to conflict.

Our operational approach is flexible and agile in order to be ready when needed. Our capabilities combine people, technology and infrastructure. In general, cyber capability development is most efficiently achieved by developing 'blocks of capability' that can be deployed against a range of different requirements with the minimum necessary tailoring, while still enabling us to deliver operations that are precise and calibrated.

This is essential to enable a timely response against a variety of threats, many of which cannot easily be predicted and where there is simply not the time to develop bespoke capabilities from scratch. We avoid investing significant resource into niche and specific capabilities unless deemed critical. Maintaining skills through constantly operating, while continually developing capabilities, is our main way of ensuring we are postured for crisis and future contingencies.

Our operational approach is flexible and agile in order to be ready when needed.

Responsible Cyber Power In Action

Types of operation

The NCF has a remit to use cyber operations in the interests of national security, the UK's economic wellbeing or in support of the prevention or detection of serious crime. There are three broad categories of NCF operations:

Countering threats from terrorists, criminals and states using the internet to operate across borders in order to do harm in the UK and elsewhere.

Countering threats which undermine the confidentiality, integrity and availability of data, and effective use of systems by users. This can involve conducting cyber operations, when necessary, alongside the range of other mitigations available to counter threats to our cyber security, including improved cyber resilience, coordinated action with allied governments, and collaboration with the private sector.

Contributing to UK Defence operations and helping to deliver the UK's foreign policy agenda. Cyber operations can support the full range of Defence activity. And they can make a particular contribution in support of key foreign policy and security objectives.

Operational examples

NCF routinely plans and conducts operations to support and protect military operations and help ensure they safely meet their mission objectives. This can include disrupting physical threats, protecting supply chains, and disrupting hostile malware which could threaten operational readiness. Sometimes this involves deploying these cyber capabilities forward, to give a military Commander a wider set of options for force protection.

NCF counters threats posed by states in ways other than directly supporting the UK military. These operations have ranged from exposing activities and supporting systems, to disrupting networks and operational capabilities. We have also acted to counter terrorist radicalisation, state disinformation, and reduce the threat of external interference in democratic elections.

In countering sophisticated, stealthy and continuous cyber threats, known as Advanced Persistent Threats (APTs) in support of NCSC, NCF operations are informed by behavioural science insights to undermine the tradecraft used by specific APTs. This has enabled our constraining efforts on the APT to persist for longer than in earlier operations.

We have continued to disrupt terrorist activities and networks, combining technical disruption operations, with activities designed to foster distrust and decrease morale.

NCF has carried out a series of actions to counter serious crime. We have also supported HMG's counter proliferation objectives, for example disrupting activities connected to sanctions evasion.

We deliver persistent campaigns to remove child sexual exploitation and abuse material from the public spaces online and make it harder to find. We have removed large amounts of the most egregious imagery and disrupted illegal activity. These operations are undertaken as part of global efforts to counter this harmful activity and augment the physical reach of law enforcement with digital means.

Responsible operational planning

Fundamental to our work is the need to act at all times in line with the UK's values and its commitment to be a responsible, democratic cyber power. This requirement underpins the operational approach described earlier and we believe makes us more effective. Key factors that ensure responsible cyber operations include the following:

Strict adherence to robust legal and ethical frameworks

NCF operations are conducted in line with a well-established legal framework, which includes the Intelligence Services Act 1994 (ISA), the Investigatory Powers Act 2016 (IPA) and the Regulation of Investigatory Powers Act 2000 (RIPA).

The NCF always acts within the law. Decisions to approve operations are informed by legal advice on relevant domestic and international law. NCF operations must satisfy GCHQ's statutory functions and obligations set out in ISA and are the subject of warrants and authorisations under that Act, the IPA and RIPA, as appropriate. For situations of armed conflict, international humanitarian law (also known as the Law of Armed Conflict) is also relevant.

Furthermore, we build a strong ethical component into NCF operational planning. This is to ensure that our operations, as well as being legally compliant, are also the right thing to do. Part of this is ensuring that operations are consistent with our democratic values, and that they are in line with the principles of responsible behaviour in cyberspace we are setting out here.

Robust oversight and accountability

The NCF's activities are subject to approval by Ministers, judicial oversight and Parliamentary scrutiny, making the UK's governance regime for cyber operations one of the strongest in the world.

Accountability for our activities is held jointly by the Secretary of State for Foreign, Commonwealth and Development Affairs, and the Secretary of State for Defence. NCF responds to priorities set by the National Security Council and works closely with officials across several government departments to ensure outcomes support Ministerial departments' objectives and campaign plans.

The Investigatory Powers Commissioner keeps various statutory powers used in the conduct of cyber operations under review. The Intelligence and Security Committee provides Parliamentary oversight. NCF also falls within the jurisdiction of the Investigatory Powers Tribunal, an independent specialist tribunal with unique statutory powers.

Clear strategy, doctrine and the necessary underlying policies

The application of operational cyber capabilities in a responsible way is governed by a defined strategy and doctrine, so that there is clarity about what they are used for and a well-understood set of principles governing their operational application. We have developed a robust framework and while most of this must remain secret, this document has set out a number of the most significant principles.

Thorough and established processes to govern operations, including authorisations

There is a clear process for setting requirements for NCF operations that involves stakeholders across Government and which enables a clear linkage between specific operations and national-level requirements, endorsed by Ministers.

Cyber operations may often take a long time to plan but equally may require rapid real-time decision making when the time comes to proceed. We have robust processes in place to govern the practicalities of conducting cyber operations, with clarity about where responsibility lies for sign off at any given point. These processes are designed to be sufficiently agile to handle high tempo operations.

Processes are also in place to achieve effective co-ordination between our operations and the wider activities of which they often form a part.

Cyber capabilities that can be controlled effectively and that are predictable

A core part of responsible cyber operations is the design and use of capabilities in a way that is predictable and controllable, and where the risks are proportionate to the outcome required. We carefully design our capabilities to achieve this end.

Sophisticated planning processes to ensure the principles of accountable, precise and calibrated operations are maintained

A significant amount of preparation goes in to NCF operations to ensure that they are effective and can be conducted in a responsible way. This includes relevant technical reconnaissance of the cyber operational environment, to achieve the best possible understanding in advance of and during any operation being undertaken. Our operations are carefully designed in a way that focuses on the specific outcome to be achieved and weighs up the associated risks. There are multiple approval stages that consider the feasibility, operational plan, benefits and risks of an operation before it can be authorised. And we ensure we learn from all operational proposals, not just those that are approved and delivered, to continually improve future operations.

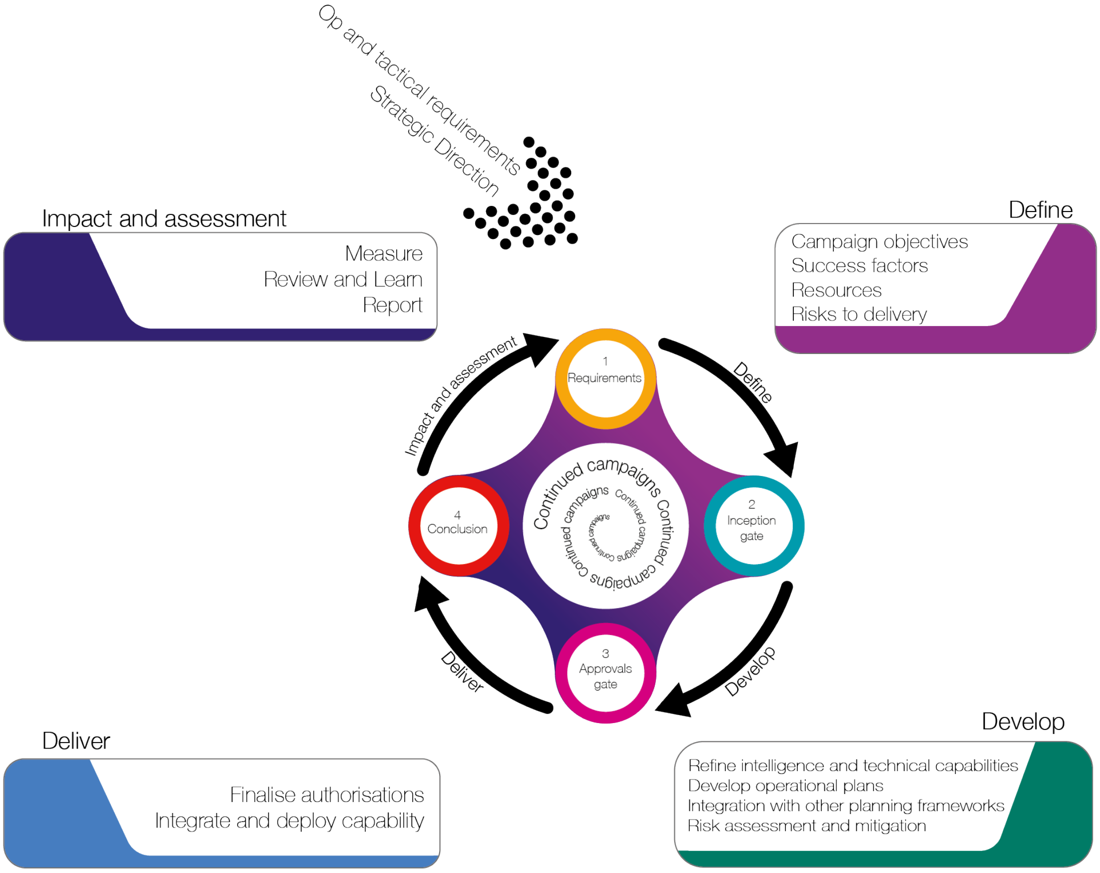


Figure 1: the NCF's operational planning cycle.

Next Steps In NCF Development

While it builds on years of UK experience with cyber operations, the NCF remains a relatively new construct. It is still in a period of growth and development as an organisation. Central to our further development are three key elements.

Scale

NCF needs to scale up to meet the requirements Government has of it. It is pursuing fast growth of personnel and capabilities to realise the potential of the force, whilst maintaining strong oversight and governance. In particular, this means recruiting and training people from across all our partners, as well as developing infrastructure, technology and associated capabilities.

Reach

Our adversaries are global and use a wide array of cyber and digital technologies. We need to have the technical ability and readiness to reach these adversaries wherever they are and irrespective of how they are using cyber technology. This requires significant capability investment to keep pace with the changing nature of technology, and which relies on enablers provided by key operational partners of the force: GCHQ, SIS and the MOD.

Integration

The force must integrate effectively with other parts of Government and with a wider range of partners and allies. This includes law enforcement, partners in the UK intelligence and security community, Government policy departments, and a growing number of international allies. More broadly we are working with the private sector, academia, think tanks and wider civil society to harness the best thinking available to enable our mission.

Challenges

In delivering our mission we inevitably face a number of challenges and risks, many of which we share with other organisations, agencies and departments. These are being carefully managed as the organisation develops, often as part of cross-government approaches under the National Cyber Strategy. They include:

People and skills

Success in cyber operations is fundamentally dependent on having sufficient of the right people with the necessary skills. That skill set is a broad one and, as well as core technology skills, includes intelligence analysis and operational planning. Many of these skills are in short supply, here and abroad.

Maintaining pace with cyber and digital technology

The NCF needs to be able to operate against adversaries using the full range of cyber and digital technologies. These technologies continue to evolve at a rapid rate. Fundamental changes to the future shape of the internet and the globalisation of technology could all raise significant complications. Against that backdrop, developing truly flexible cyber operational capabilities is a significant challenge.

Prioritisation — matching resources to where the impact is greatest

We have a broad remit to address threats including across national security, Defence, economic wellbeing (where this amounts to a national security threat) and serious crime. Inevitably a high degree of prioritisation is required to match available resources to those areas where not only is the need most significant, but where cyber operations have the greatest impact.

Measuring effect

Measuring the effect of covert operations, whether in the cyber or physical worlds, is often very hard. It can sometimes be difficult to say definitively that a particular outcome was the result of particular operations. While it may be relatively easy to measure whether a piece of technology is not functioning as intended, due to a cyber operation, it can be harder to measure the actual impact of this on the adversary's ability to achieve its objectives. We are working on new approaches to measuring effect, with partner assessment teams, in order to help address these challenges and to ensure that we can demonstrate an increasing return on the Government's investment in the NCF.

Organisational development

The NCF is a new organisation that is combining elements from both the intelligence community and the armed forces as well as wider Defence. This means investment in organisational development is important, not least given the often very different cultures, processes and professional experiences of the constituent organisations. The eventual location of the majority of the force, including its headquarters, at a new facility in Samlesbury presents an opportunity requiring a high degree of planning and preparation.

Licence to operate

The UK's approach to cyber operations has traditionally been kept highly secret. But this kind of work clearly prompts questions about how the UK can act in a responsible way that is consistent with its commitment to a free, open, peaceful and secure internet. With the creation of the NCF, and the degree of investment involved, it is right that we enable greater transparency and engage with the public more widely than has been done before. This document is part of that process. Doing so is a crucial part of assuring the force's 'licence to operate' in the public mind and demonstrating the UK's commitment to being a responsible and democratic cyber power. We do not take this for granted.

gov.uk/government/organisations/national-cyber-force

March 2023