Ministry
of Defence

Cyber Primer

Third Edition

Cyber Primer

Cyber Primer, 3rd Edition, dated October 2022,
is promulgated as directed by the Chiefs of Staff

Head Doctrine

Conditions of release

Authorisation

The Development, Concepts and Doctrine Centre (DCDC) is responsible for publishing strategic trends, joint concepts and doctrine. If you wish to quote our publications as reference material in other work, you should confirm with our editors whether the particular publication and amendment state remains authoritative. We welcome your comments on factual accuracy or amendment proposals. Please contact us via email at: DCDC-DocEds@mod.gov.uk

Copyright

If contacting Defence Intellectual Property Rights for authority to release outside of the UK government and MOD, the Patent Officer should be informed of any third party copyright within the publication.

Crown copyright and Merchandise Licensing, Defence Intellectual Property Rights, Central Legal Services, MOD Abbeywood South, Poplar 2 #2214, Bristol, BS34 8JH. Email: DIPR-CC@mod.gov.uk

Distribution

All DCDC publications can be demanded from the LCSLS Headquarters and Operations Centre.
LCSLS Help Desk: 01869 256197 Military Network: 94240 2197

Our publications are available to view and download on defnet at: https://modgovuk.sharepoint.com/sites/IntranetUKStratCom/SitePages/development-concepts-and-doctrine-centre-dcdc.aspx

This publication is also available on the Internet at: www.gov.uk/mod/dcdc

Preface

> We will adopt a comprehensive cyber strategy to maintain the UK's competitive edge in this rapidly evolving domain. We will build a resilient and prosperous digital UK, and make much more integrated, creative and routine use of the UK's full spectrum of levers – including the National Cyber Force's offensive cyber tools – to detect, disrupt and deter our adversaries.
>
> *Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy*, 2021

Purpose

1. The purpose of the *Cyber Primer* is to introduce the subject of 'cyber', primarily within the Defence context, but also encompassing everyday aspects of life both at work and home. It is the foundation to reading UK Defence's cyber and electromagnetic concepts and doctrine.

Context

2. Cyber capability is vital to our national security and prosperity, playing an integral role in protecting the UK and our interests against external and internal threats. Cyber activity cannot be the responsibility of one government department or agency alone, each will have their own experiences and expertise; Defence is just one partner in a whole of society effort.

3. Cybersecurity and resilience are vital within Defence as our Armed Forces depend on digital technology, platforms, data, information and communication systems, both in the UK and on operations around the world. Our adversaries' activities present a real and rapidly developing threat to these systems and to our operations.

4. Cyberspace, and the associated technologies, are full of opportunities for improving the way we work and live; they contribute substantially to our economy and prosperity, but they also introduce new hazards of which we need to be aware. The impact of cyber activities, positive and negative,

on military activity requires Defence personnel, and those associated with Defence, to understand the depth of our dependence on ‘cyber’.

5. The primer has a deliberate cyber focus. Although mention is made of the wider electromagnetic environment, this is to provide contextual reference as necessary.

Audience

6. The *Cyber Primer* seeks to inform a wide audience. As an introduction to cyber it will be of use to all Defence personnel.

Structure

7. The publication is divided into four chapters and is supported by a lexicon and resources section. A breakdown of the chapter contents is below.

a. **Chapter 1 – Cyber fundamentals.** Chapter 1 introduces the essential terminology and covers cyber from a national policy and strategy perspective. The chapter explains the nature and characteristics of cyberspace and the cyber and electromagnetic domain. The chapter also highlights applicable laws and concludes by looking at the importance of international engagement.

b. **Chapter 2 – Cyber threats.** Chapter 2 outlines: the threats from cyberspace; the range of threat actors; the characteristics of a cyberattack and the different tools and techniques used; and cyber threat mitigation. The chapter concludes with Annex 2A detailing seven case studies.[1]

c. **Chapter 3 – Cyber functions.** Chapter 3 looks at the four military cyber operations roles – influence, defend, enable and inform – which are delivered by cyber capabilities through offensive and defensive cyber

[1] The examples and case studies included in this primer contain reports selected from various external sources by the Strategic Command Cyber Reserve, a cadre of cyber-industry experts who are also Tri-Service Reservists. All of this information is publicly available online and provided for understanding only; sources quoted and opinions expressed do not necessarily reflect those of the Ministry of Defence (MOD). Similarly, where alleged perpetrators are identified they have been done so through public sources and not through any investigations or conclusions conducted by the MOD. The names of the operations associated with the examples have been assigned by the international cyber security community.

operations, cybersecurity and cyber threat intelligence.[2] It also examines information management and finally looks at the relationship between cyber and other closely linked military functions.

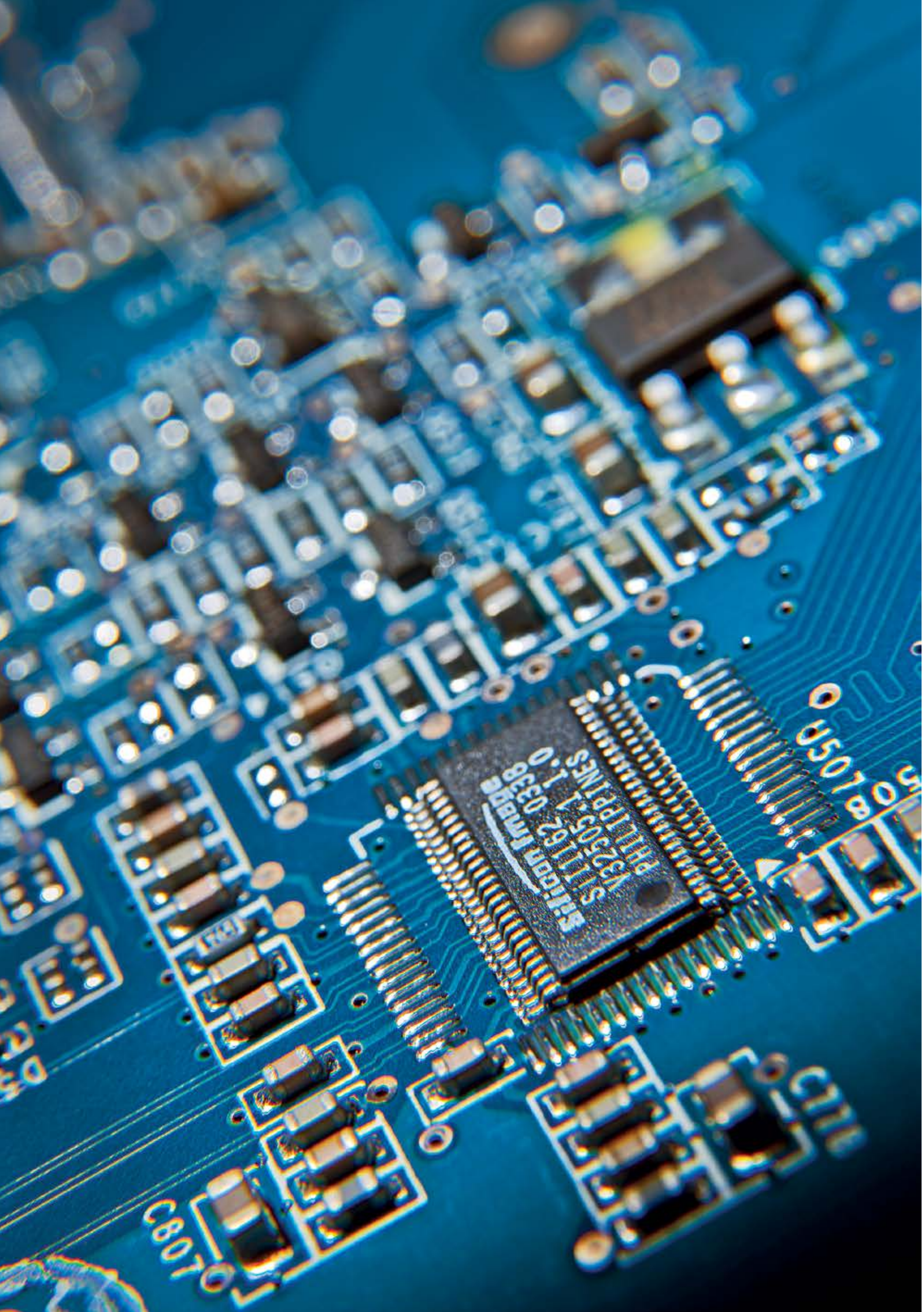
d. **Chapter 4 – Cyber operations.** Chapter 4 looks at how cyber capability is currently organised and integrated with military operations and provides some detail concerning cyber command and control.

Linkages

8. The *Cyber Primer* is underpinned by a number of policy, strategy and doctrinal publications. In addition, there are number of other publications that provide further context and greater detail on aspects introduced. Links to these data sources can be found within the resource section at the end of this publication.

[2] Full details of these roles and the activities that are conducted within them are detailed within Joint Doctrine Publication 0-50, *UK Defence Cyber and Electromagnetic Doctrine*, 2nd Edition, which is due to publish in 2023.

Contents


Silicon Image
SiI1162 0338
Y32503.1 1.0
PHILIPPINES
U507
C807
C711

Chapter 1

Cyber fundamentals

Chapter 1 introduces the essential terminology and covers cyber from a national policy and strategy perspective. The chapter explains the nature and characteristics of cyberspace and the cyber and electromagnetic domain. The chapter also highlights applicable laws and concludes by looking at the importance of international engagement.

Cyber definitions

1.1. There are no universally accepted definitions for cyber but, for the purpose of this primer, the current UK definitions will be used. The definitions for cyber and cyberspace[1] are below.

A–Z

cyber
Relating to information technology, the Internet and virtual reality.
(*Concise Oxford English Dictionary*)

cyberspace
The global environment consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data.
(Joint Doctrine Publication (JDP) 0-50, 2nd Edition draft)[2]

[1] The North Atlantic Treaty Organization (NATO) refers to cyberspace as a sub-set of the information environment. NATO Military Committee Policy – MC 422/4.

[2] Proposed new definition that will be added to JDP 0-01.1, *UK Terminology Supplement to NATOTerm* on ratification of JDP 0-50, *UK Defence Cyber and Electromagnetic Doctrine*, 2nd Edition.

National context

1.2. The *Integrated Review*[3] in 2021 identified four overarching and mutually supporting objectives set within a Strategic Framework. Summarised, these are:

- sustaining strategic advantage through science and technology;
- shaping the open international order of the future;
- strengthening security and defence at home and overseas; and
- building resilience at home and overseas.

1.3. The UK's *National Cyber Strategy 2022*[4] builds on the *Integrated Review* by placing a strong strategic emphasis on cyber and, as set out by the *Integrated Review*, details five pillars of cyber capability. These are detailed below.

a. Pillar 1. Strengthening the UK cyber ecosystem, investing in our people and skills and deepening the partnership between government, academia and industry.

b. Pillar 2. Building a resilient and prosperous digital UK, reducing cyber risks so businesses can maximise the economic benefits of digital technology and citizens are more secure online and confident that their data is protected.

c. Pillar 3. Taking the lead in the technologies vital to cyber power, building our industrial capability and developing frameworks to secure future technologies.

d. Pillar 4. Advancing UK global leadership and influence for a more secure, prosperous and open international order, working with government and industry partners and sharing the expertise that underpins UK cyber power.

e. Pillar 5. Detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace, making more integrated, creative and routine use of the UK's full spectrum of levers.

[3] HM Government, *Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy*, 2021.

[4] HM Government, *National Cyber Strategy 2022*.

1.4. Defence supports this national strategy by ensuring that our Armed Forces:

- have strong cyber defences and capabilities that are secure by design;
- are able to project power in and through cyberspace (just as they do in the other operating environments);
- are ready to assist the wider UK in the event of a significant cyber incident; and
- can respond to a cyberattack as they would respond to any other attack – using whichever capability is most appropriate.

1.5. Defence's ability to conduct protective operations in cyberspace is mission critical, demands resilience and facilitates decision superiority. Our adversaries will contest our freedom of manoeuvre in cyberspace so we need to have capabilities that can identify, protect, detect, respond and recover from attacks against our digital systems and communication networks.

1.6. Defence's activities in cyberspace and digital capabilities are continuously evolving. The basics of well implemented cybersecurity go a long way in protecting Defence's data, supply chains and capabilities but there will always be vulnerabilities in digital systems. To defend itself, Defence must ensure cybersecurity policies are continuously reviewed, enforced and, where risk is tolerated, the full impact of that risk is completely understood.

There will always be vulnerabilities in digital systems

© Sergey Nivens / Shutterstock.com

1.7. Cyberspace can act as an information source in its own right. Information gained from cyber activity can be used to strengthen our own cyber defences but can also form the basis of further intelligence analysis. This might support cyber operations or more 'traditional' military activity above or below the threshold of armed conflict.

1.8. Cyber capabilities must be integrated with all areas of military planning, preparation activities and budgeting across the Defence Operating Model. A range of support and implementation is required, covering the following activities.

a. **Direct** – governance, organisation, budgeting, policy, thought leadership, strategy, and concepts and doctrine. Alignment with allies, national bodies and other government departments.

b. **Develop** – research and development, capability planning and cyber-industry engagement.

c. **Deliver** – acquisition and through-life management of cyber capabilities.

d. **Generate** – fielding deployment of those capabilities (across the Defence lines of development), personnel recruitment, talent development, education and training.

e. **Operate** – the command, control and execution of effects in and through cyberspace by dedicated cyber force elements; the inclusion of cyber activity with other operational domain capabilities to achieve integrated action.

Cyberspace

1.9. Cyberspace is complex and interdependent with the electromagnetic spectrum[5] and is a uniquely dynamic human-made operating environment. It is essential to all military operations and includes far more than just the Internet or protecting an information technology system. Cyberspace is broad and pervasive, covering digital, information technology and operational technology,

[5] Electromagnetic spectrum is defined as: the entire and orderly distribution of electromagnetic waves according to their frequency or wavelength. Note: the electromagnetic spectrum includes radio waves, microwaves, heat radiation, visible light, ultraviolet radiation, x-rays, electromagnetic cosmic rays and gamma rays. NATOTerm.

for example, aircraft traffic control systems, medical life-support systems, physical device controllers,[6] industrial control systems and national distribution systems for water, gas and electricity, which are often termed critical national infrastructure. Cyberspace is all encompassing and forms a consideration for all environments and operational domains.

1.10. Cyberspace is less geographically definable or constrained than other environments. Devices and systems may have physical location and identifiable electronic boundaries; however, globalised cloud computing and hyper-connectivity mean that many digital systems are both geographically dispersed and accessible globally. They may also appear to be in more than one territory simultaneously. The notion that Defence systems are not reachable via the public Internet and World Wide Web is increasingly false. Location, distance, reach and accessibility must be viewed differently to traditional environments when considering cyberspace operations. The interconnectedness of cyberspace means that it is almost impossible to segregate cyber risks either geographically, or by organisation, unlike in other operating environments.

1.11. Access by people to cyberspace is possible via many means, although most often through desktop computers, laptops, tablets and mobile phones. Connectivity may be achieved via wireless connections, for example, Wi-Fi or third, fourth and fifth generation mobile communications networks, or physical cables of copper and optic fibre. Cyberspace is created by and dependent on physical assets – power sources, computers, cables, network infrastructure, data centres – as well as the people who operate and manage them. Some of the 'fabric' of cyberspace is created automatically by computers without human intervention.

1.12. Increasingly, machine to machine communication is becoming a dominant use of cyberspace as digital automation, robotics and artificial intelligence technologies mature. From home assistants, such as Amazon's 'Alexa', to more simple devices including domestic appliances, security cameras, lighting controls and thermostats, machines are forming a mesh of connected devices known as the 'Internet of things'. Many of these devices rely on near-permanent data centre connectivity via the Internet to function.[7] Internet of things devices are often less sophisticated than traditional personal

[6] Devices such as computer-controlled pumps, avionics, engine management systems and robotic manufacturing systems.

[7] In December 2021 an Amazon Web Services data centre outage caused thousands of doorbells and robot vacuum cleaners to stop working across the United States. BBC News, 'AWS: Amazon web outage breaks vacuums and doorbells', 26 November 2020.

computers and smartphones and so can be harder to secure but they are cheap, offer convenience and are proliferating. Poorly engineered Internet of things devices can therefore offer a vector into an otherwise well-defended computer network.

1.13. Most digital technologies and information systems have cyber vulnerabilities,[8] although not all are readily exploitable.[9] They range in severity from minor to critical, with a persistent process of discovery increasing the number known about each year. We might consider a minor vulnerability that caused short-term loss of the Internet or connectivity in our homes as an irritant and a risk worth tolerating, but one that allowed hacking into our email account and stealing personal information to be more serious and needing attention. A cyberattack leading to a prolonged loss of the electricity grid or Defence's logistic capabilities, on the other hand, could have severe consequences, including loss of life. As such, a cyberattack could have comparable effects to a physical attack.

1.14. Action within cyberspace can occur at very high speed; a packet of data or an email can circle the globe in milliseconds and, consequently, decision-making timelines can be significantly compressed compared to other operational domains. This has implications for delegation of authorities to those who defend networks and extends beyond Defence's traditional hierarchical command and control.

1.15. Another factor related to timelines is the speed of evolution of technology which makes cyber capability planning, development and deployment challenging. A maritime, land or air platform capability may have a generational life cycle of 25 years or more. A single generation of information technology continues to last around 18 months and most information technology systems can be considered obsolete after five years. These factors have led to the idea of 'evergreen' technologies, whereby information technology systems are continually upgraded. Cyberspace is therefore never static, always changing and making it hard to 'map' and define.

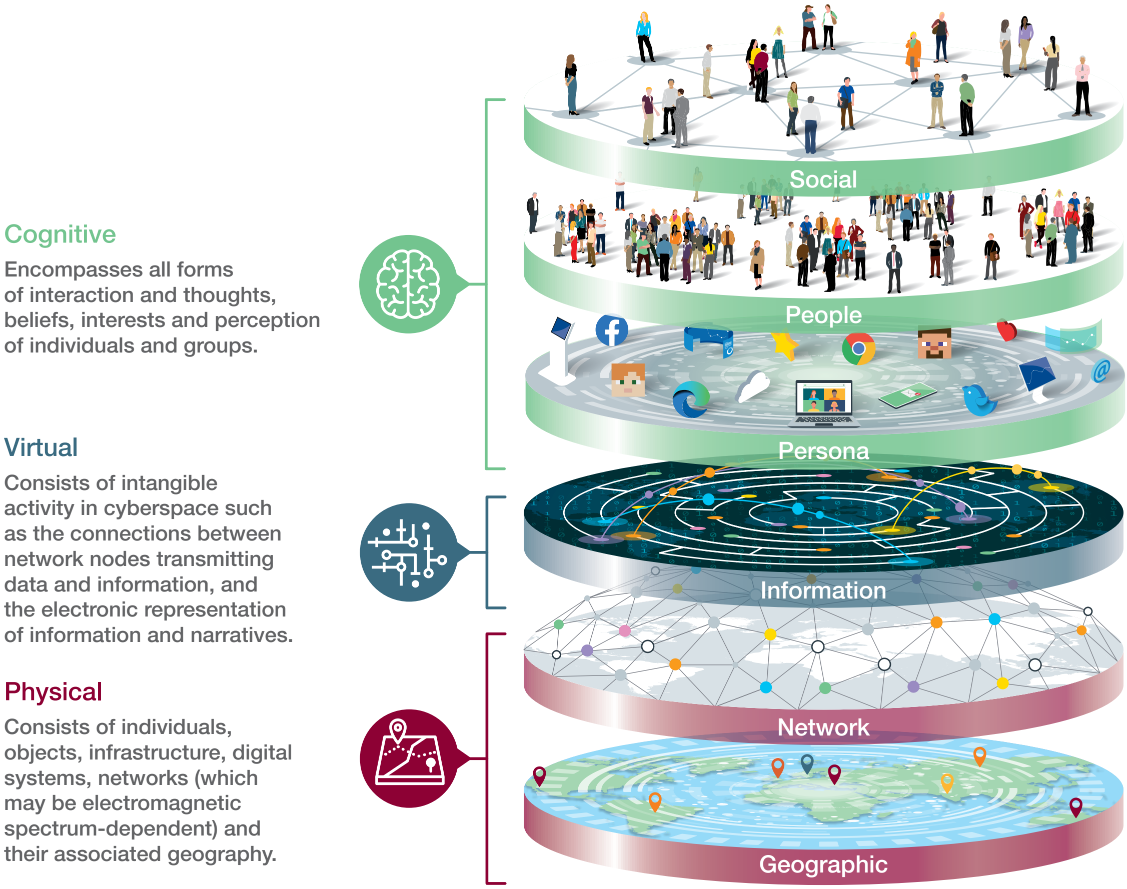
1.16. The technologies and systems that make up cyberspace have evolved from being partial enablers of modern life into being fundamental to how we live, work and prosper whether as Defence or as a society. We live in a

[8] A cyber vulnerability is simply a flaw or design feature in software that can be exploited to make the device running the software do something unintended or untoward.

[9] Such exploitation is normally via technical means, such as via remote network access, but it could equally be undertaken by human interference, for example, via connecting a device to a USB port or clicking on a hyperlink.

digital world and are ever more reliant on smartphones, office and home computers, conferencing and social media applications, the World Wide Web, messaging applications and email. In the military this dependency extends to our industrial supply chains, logistics, command and control networks, intelligence, surveillance and reconnaissance capability, and most platform management, sensor and weapon systems. All these digital systems form part of cyberspace.

1.17. **Layers of cyberspace.** Cyberspace can be thought of as comprising six interdependent layers: social; people; persona; information; network and geographic. These layers can be placed within three effect dimensions, as shown in Figure 1.1.



Cognitive

Encompasses all forms of interaction and thoughts, beliefs, interests and perception of individuals and groups.

Virtual

Consists of intangible activity in cyberspace such as the connections between network nodes transmitting data and information, and the electronic representation of information and narratives.

Physical

Consists of individuals, objects, infrastructure, digital systems, networks (which may be electromagnetic spectrum-dependent) and their associated geography.

Figure 1.1 – Layers of cyberspace and their relationship with the three effect dimensions

1.18. **Social, people and persona layers.** The social, people and persona layers consist of the details that connect people to cyberspace, the virtual communities they occupy and the people and organisations who interact with and operate digital systems and networks. Together, these three layers represent the cognitive dimension. Unique addresses or titles (for example, a user login or email address) are matched to virtual addresses in the information layer which, in turn, map to computer addresses in the network layer and devices in the geographic layer. A single person may have multiple personas in cyberspace, for example, many social media accounts accessed through different applications, computers or mobile devices. Equally, multiple people can share a single persona such as a multi-user email account. Personas can be deliberately complicated to obscure identity, with elements in many virtual locations and not linked to a single physical location or territory. Linking human, organisational or state responsibility for any action or event (known as attribution) is therefore difficult in cyberspace. This complexity implies that well-resourced intelligence collection and analysis capabilities are required to gain sufficient insight to enable evidenced attribution, or effective targeting.

1.19. **Information layer.** The only layer in the virtual dimension, the information layer consists of software, data and the virtual connections that exist between network nodes. A node is a physical device connected to a network, such as a computer, smartphone, robot or other digital device. The information layer includes:

- user applications and the data that people store online;
- data, applications and protocols which govern transfers between nodes and interaction across the geographic layer;
- individual network configuration details;
- information assurance processes, security status and management information;
- details of communication service providers and Internet domain names; and
- ownership data.

1.20. **Network layer.** The network layer is electronic, electromagnetic or electro-optic rather than virtual or binary; it can be measured but not touched. It includes the logical constructs within hardware that manipulate electrons and photons to connect nodes reliably and enable data transfer in the information layer; it provides the foundation stones of security and integrity (for example, through network layer cryptography). The network layer is increasingly software-defined rather than hardwired into electronic components. This layer can often (but not exclusively) be the target for: signals intelligence; intelligence, surveillance and reconnaissance; and measurement and signature intelligence.

1.21. **Geographic layer.** The geographic aspect relates to the location of tangible elements of a system or network. The tangibility relates to the fact that it can be seen and touched, components of it are made of matter and are physically present, such as computer hardware and network infrastructure, cabling and radio masts. It is important to note that the transmission medium, including air and some liquids, of electromagnetic waves form part of the physical layer. The geographic layer, together with the network layer, forms the physical dimension of cyberspace.

The cyber and electromagnetic operational domain

operational domain
A specified sphere of capabilities and activities that can be applied within an engagement space. (NATOTerm)[10]

cyber and electromagnetic domain
A domain comprising of capabilities which enable activities that maintain freedom of action by creating effects in and through cyberspace and the electromagnetic spectrum. (JDP 0-50, 2nd Edition draft)

1.22. UK Defence has chosen to consider capabilities and activities relating to cyberspace and the electromagnetic environment together, as a single operational domain. The rationale is logical because the two environments overlap, albeit partially, and some capabilities and activities are inextricably both 'electromagnetic' and 'cyber'. Figure 1.2 shows the cyber and electromagnetic domain and its relationship to the other operational domains.

[10] An operational domain is an artificial construct intended to aid understanding and reflects Defence perceptions on how things should be organised. The five operational domains are: maritime, land, air, space, and cyber and electromagnetic.

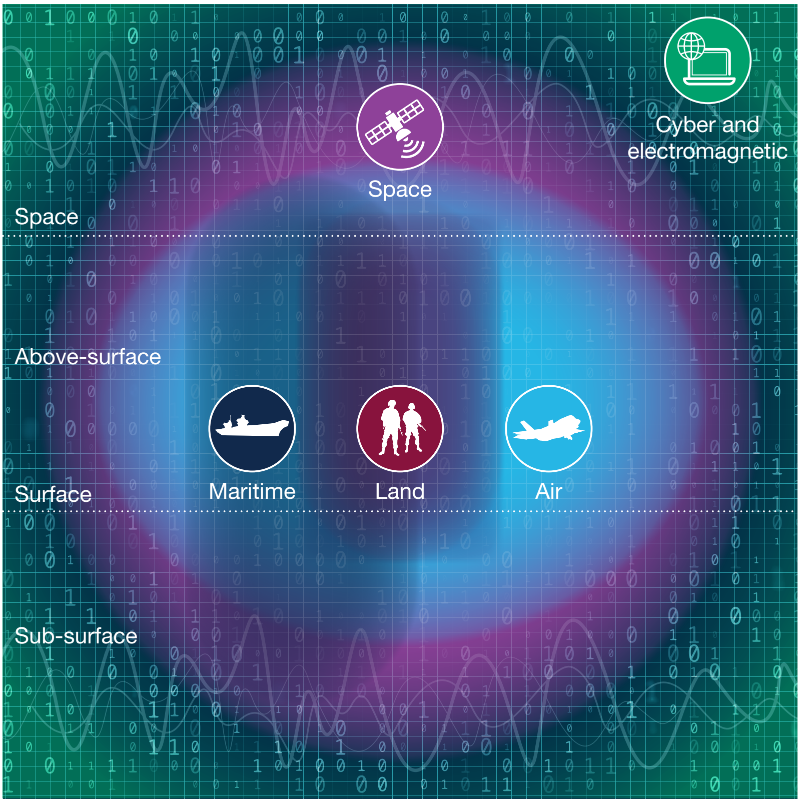


Figure 1.2 – The all-encompassing nature of the cyber and electromagnetic domain

1.23. Cyberspace is continuously contested – not just in a Defence context but commercially, nationally and internationally. Although there is no standalone treaty governing its use, there is a plethora of international and domestic law that applies to the use of cyberspace, both above and below the threshold of armed conflict. The UK has adopted a proactive attitude to this challenge and is a world leader in confirming that existing law applies to cyberspace.

1.24. This continuous competition within cyberspace represents one of the most persistent arenas for sub-threshold activity in an era of systemic competition.[11] A range of threat actors are constantly probing UK-owned networks and systems seeking vulnerabilities, intelligence collection opportunities or military and commercial advantage; some do it to raise money or awareness of their cause and some simply for fun. More insidiously,

[11] The United States and NATO refer to this as ‘strategic competition’. See Allied Joint Publication-01, *Allied Joint Doctrine* for further detail.

the manipulation of social media platforms and their algorithms is a routine influence activity conducted by certain states and groups to destabilise Western democracies and reduce our social cohesion.

1.25. Internet protectionism is increasing. Deviation from international technical standards and segregation of 'national cyberspace' is common among authoritarian states. Some seek to influence developing nations to adopt proprietary versions of Internet technology and digital platforms to gain economic and diplomatic leverage in the future. The World Wide Web may not be 'worldwide' for much longer.

1.26. Defence is not responsible for defending all of UK cyberspace or countering all these potential threats. It is a whole of society effort as made clear by the *National Cyber Strategy 2022*.

1.27. Building on an understanding of cyberspace as an environment, there are a number of themes which emerge when we consider a cyber and electromagnetic operational domain for military use. Some of these are described below.

a. Cyberspace is pervasive and global, offering opportunities for strategic reach, persistence and direct influence without deploying physical forces, but access is not assured.

b. Cyber operations require substantial intelligence collection and understanding to be successful. They are not a quick or cheap fix, despite their portrayal in popular culture.

c. Cyber operations and the effects they create are often target specific. Precision is a key attribute for cyber but unlike other capabilities switching targets often requires additional resources, time and supporting intelligence.

d. Cyberspace is highly changeable; investment in a particular cyber capability can be rendered worthless by the application of a software or hardware change elsewhere in cyberspace. Equally, this changeability means that new opportunities (vulnerabilities and technology that could be exploited) emerge all the time.

e. The cyber and electromagnetic domain is relied on by the other operational domains. Cyber activity must be planned and integrated from the outset with joint or multi-domain operations to be effective. All physical deployments of forces must treat cyber activity as a critical dependency and potential risk vector.

f. Military digital infrastructures, whether national, coalition or international, coexist and overlap with civil infrastructure. This poses organisational problems for defining, defending and managing Defence's equities in cyberspace.

g. Cyber resilience is more valuable than applying cybersecurity measures alone. The ability to recover quickly and effectively from a cyberattack or a technical issue is a vital factor which Defence must train for and invest in.

h. Defence does not have sole or unilateral use of all its capabilities for cyber operations. Activity must be conducted in conjunction with other government organisations.

Mainstreaming cyber confidence and understanding

1.28. Increasing awareness and an understanding of the threats, as well as the opportunities of digitisation, is vital for all Defence personnel. In the Information Age, 'cyber' must be normalised and can no longer be regarded as a 'specialist activity'.

1.29. All Defence personnel are expected to operate effectively and securely in cyberspace, using and exploiting information and information systems and working to counter potential threats. The pervasive and ubiquitous nature of cyberspace means Defence must consider the full range of cyber capabilities and requirements across the Defence lines of development. This requires awareness, education,[12] individual and collective training, exercises and, for all leaders, an understanding of risk management in cyberspace.

1.30. Defence personnel must be mindful that their personal activity within cyberspace may form a pattern that allows a profile to be generated and a link to be established with their professional role. This can be achieved by an actor correlating the multiple cyber personas (social media, email, website data) using open-source intelligence techniques.

[12] For example, Protecting Personal Data, Records Management, and Information and Knowledge Awareness mandatory training courses and the Information Matters and Cyber Awareness e-learning modules aimed at all personnel.

All Defence personnel are expected to operate effectively and securely in cyberspace

1.31. Improving cybersecurity across Defence has implications beyond education and training, including timeliness of system updates and a focus on the 'basics' of managing our growing digital capability responsibly. Every individual user of information technology and digital capabilities is a potential cyber sensor and defender, or a potential vulnerability.

Law applicable to cyber

1.32. UK and international law is applicable to cyber activities. Within the UK, comprehensive legislation is in place to provide guidance on the safe and legal use of computers and information technology including the data stored, transmitted and processed. Such legislation includes the Computer Misuse Act 1990, Data Protection Act 2018 and the Fraud Act 2006. Further details of these Acts, together with links to additional relevant legislation and joint Service publications (JSPs) can be found via the Defence Digital policy rules and guidance portal.

1.33. Legal support to military operations must include an operational understanding of potential cyber activities, including intended effects and possible unintended consequences. The law of armed conflict, also known as international humanitarian law, will apply in an armed conflict, whether international or non-international.[13] In peacetime (below the threshold of an

[13] JSP 383, *Joint Service Manual of the Law of Armed Conflict*.

armed conflict) the UK conducts cyber operations in accordance with a well-established domestic legal framework, which includes the Intelligence Services Act 1994, the Regulation of Investigatory Powers Act 2000 and the Investigatory Powers Act 2016. Legal advice should be provided at an early stage on the planned deployment and use of any cyber and electromagnetic capabilities against an adversary or competitor.

International engagement

1.34. Cyber presents a fundamentally international set of challenges and opportunities. Collaboration with international partners is important to develop Defence's cyber capabilities. International engagement is prioritised and directed by the Ministry of Defence's Cyber Policy team, who have close links across wider government.

1.35. While broader Defence bilateral partnership objectives are a key factor, cyber engagement is principally driven by existing and anticipated military requirements. As a leading member of the North Atlantic Treaty Organization (NATO), the UK contributes to a collective approach, ensuring that it secures its own networks and working with other partners to develop their own cyber capabilities.

1.36. With regard to doctrine, the UK implements the North Atlantic Council and Military Committee NATO Standardization Policy by using NATO doctrine wherever possible. Where this is not possible, efforts are made to ensure UK doctrine is coherent with NATO doctrine, thereby underpinning interoperability.

1.37. Cyber brings additional complexities to the structures and processes of NATO through the need to include national organisations, such as computer emergency response teams (CERTs), and national and international legal requirements. Some key organisations are listed here.

a. NATO Cyberspace Operations Centre. The NATO Cyberspace Operations Centre supports military commanders with situational awareness to inform the Alliance's operations and missions. It also coordinates NATO's operational activity in cyberspace, ensuring freedom to act in this environment and making operations more resilient to cyber threats. The Cyberspace Operations Centre can also facilitate the integration of cyber activity provided on a voluntary basis by member states under a process known as Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA). Should SCEPVA be used, command and control of the providing forces will remain with the contributing nation.[14]

b. **NATO Communications and Information Agency.** The NATO Communications and Information Agency manages those networks owned by NATO. The Agency also has a coordinating role across individual NATO and NATO-nation CERTs.[15]

c. **NATO Cooperative Cyber Defence Centre of Excellence.** Although not under unified NATO command, the Cooperative Cyber Defence Centre of Excellence's mission is to enhance capability, cooperation and information sharing among NATO, its member states and partners in cyber defence by virtue of education, research and development, lessons-learned and consultation. The Centre of Excellence is funded by 18 nations, including the UK, who, with NATO, can task it.[16]

d. **The NATO Industry Cyber Partnership.** NATO and its Allies are working to reinforce their relationships with industry. This partnership includes NATO entities, national CERTs and NATO member states' industry representatives.[17]

1.38. Individual NATO nations have their own cyber command structures. In many cases, UK Defence has other liaison arrangements with allies. Examples of this are found in the long-standing Five Eyes intelligence sharing community of Australia, Canada, New Zealand, the UK and the United States, which can include cyber intelligence. Strategic Command cooperation with the United States Cyber Command, and the UK–France relationship are examples of where formalised bilateral arrangements exist.[18] Further bilateral relationships are under development with close allies.

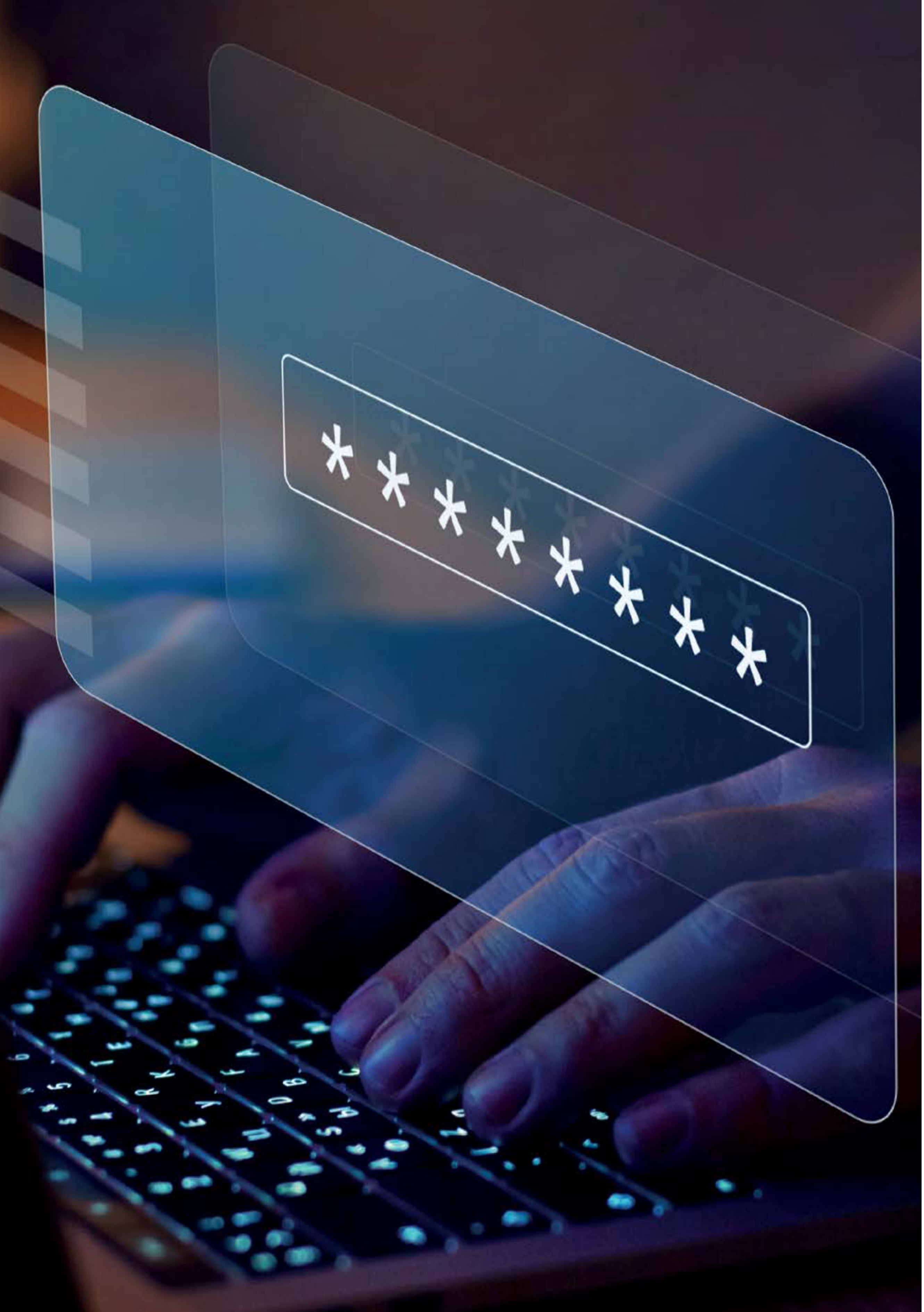
[14] See NATO's article, 'Cyber defence', 23 March 2022.

[15] See NATO's article, 'NATO Communications and Information Agency', 4 April 2022.

[16] See NATO's Cooperative Cyber Defence Centre of Excellence website.

[17] See the NATO Industry Cyber Partnership website.

[18] Underpinned by the Combined Joint Expeditionary Force and the Lancaster House Treaty of 2010.



Chapter 2

Cyber threats

Chapter 2 outlines: the threats from cyberspace; the range of threat actors; the characteristics of a cyberattack and the different tools and techniques used; and cyber threat mitigation. The chapter concludes with Annex 2A detailing seven case studies.

2.1. The growing role of cyberspace in society has opened up new threats, as well as new opportunities. For this reason, the UK's *Integrated Review*[19] published in 2021 identifies cyber resilience as one of the UK's highest priorities for action, a concept expanded in the *National Cyber Strategy 2022*.[20] Defence has no choice but to find ways to confront and overcome cyber threats if the UK is to prosper in an increasingly competitive and globalised world. An overview of the cyber threats to the UK can be found in the *Government Cyber Security Strategy 2022–2030*.[21]

2.2. The risk to national security and economic well-being includes the threat to public and private sector information systems, critical national infrastructure and the underpinning of international cyber infrastructure. Attacks in or through cyberspace can have serious consequences on government, military, industrial and economic well-being. Cyberspace is permanently contested by our competitors and potential adversaries, who conduct attacks such as:

- stealing sensitive information, including intellectual property theft from Defence contractors and our wider industrial and scientific base;

- identity theft, stealing information technology credentials and masquerading as legitimate Defence or government personnel online to extract information about operations, the Armed Forces and our personnel;

[19] HM Government, *Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy*, 2021.
[20] HM Government, *National Cyber Strategy 2022*.
[21] HM Government, *Government Cyber Security Strategy 2022–2030*.

© Song_about_summer / Shutterstock.com

- reconnaissance of our information systems and services to gain intelligence for future cyberattacks;
- shutting down or interrupting telecommunications services or email, blocking access to databases and websites;
- extorting funds through ransomware;
- damaging our digital systems and critical national infrastructure through attacks on industrial control systems; and
- undermining social cohesion and our system of democratic government through malign use of online tools, including social media, to spread propaganda and sow mistrust.

2.3. The range of opportunities and types of attack is growing and evolving as our use of cyberspace becomes ever more deeply embedded in day-to-day life and military operations. Cyberattacks can appear in many guises, without necessarily inflicting visible or tangible material damage and so are easily deniable by the perpetrator. All of this significantly increases the likelihood that an adversary will seek to create effects through cyberspace.

2.4. Evidence of cyber activity and an actor's will to use it against the UK can be challenging to find and difficult to attribute. Cyber threats emanate from state, state-sponsored proxies and criminal groups with personnel and capabilities moving seamlessly between them. Attribution is difficult not only due to the disparate and anonymous nature of cyberspace (as described in Chapter 1) but because it is not solely a technical problem. The attribution challenge spans technical/tactical (how), operational (what) and strategic levels (why). Ultimately public attribution to a particular adversary will demand substantial evidence and may be considered a political act. Therefore, attribution of alleged state cyberattacks is often coordinated with allies and will rarely be a Defence lead.

2.5. As with other operational domains, cyber and electromagnetic domain activity is often leveraged as part of a wider, coordinated and integrated attack. Espionage undertaken using a cyber vector can and will be used as part of wider influence and propaganda campaigns, as well as in support of physical hostile activity up to and including conventional warfare.

2.6. Assessing the level of threat from and through cyberspace can be achieved by understanding the sum of three factors. These are described below.

a. **Intent.** Intent is the most critical component as it provides 'intelligence in depth' or context as to why an adversary may act. An adversary's intent can either be **declared**, **demonstrated** or a **combination of both**. In some cases, intent may be unknown so understanding will be based on observed activity.

b. **Capability.** Intelligence analysis focuses primarily on understanding the adversary's strengths and their ability to generate and sustain them. However, whilst a capability may exist, there may be no intent or opportunity to use it. It should be noted that holding a capability at readiness will consume resources to maintain the necessary access for effective deployment.

c. **Opportunity.** Opportunity is the key variable in assessing threat, which can present itself in many guises. An adversary may seek to generate opportunity through influencing or shaping activities, or the opportunity may become available through changes in the cyberspace environment, providing potential advantage to the adversary.

2.7. Cyberattacks currently have a lower political and public perception of aggression when compared with more traditional and visibly damaging kinetic attacks where lives or property are obviously and physically threatened.[22] This is largely based on the fact that there have been no large-scale losses of life that have been positively attributed to a cyberattack.[23] Should such an event happen, this would likely change the public's perception to the potential 'aggressive' nature of cyberattacks; it is the effect that is important not the means of delivery.

[22] Many cyberattacks are actually criminal acts.

[23] German authorities linked the death of a hospital patient to a cyberattack in 2020 and Israel in 2020 suffered a cyberattack that changed chlorine levels in a water processing plant.

Threat actors

2.8. The term 'threat actor' is used to identify those who pose a threat. Threats to security in and through cyberspace include state-sponsored attacks, ideological and political extremism, serious organised crime, lower-level individual crime, cyber protest, cyber espionage and cyber terrorism. Threat actors exploit cyberspace's characteristics through innovative approaches that often have a low-entry cost and they are helped by the ease of access often presented to them. Such malevolent actors may seek to create uncertainty and mistrust through:

- direct access to people and systems;
- attacking and exploiting our national and economic infrastructures;
- attacking military capabilities including command and control systems, logistical support and personnel; and
- manipulation of data and information.

2.9. Threat actors fall into several broad categories. These are: nation states; advanced persistent threats (APTs); terrorists; criminals; patriotic hackers; hacktivists; and insiders.

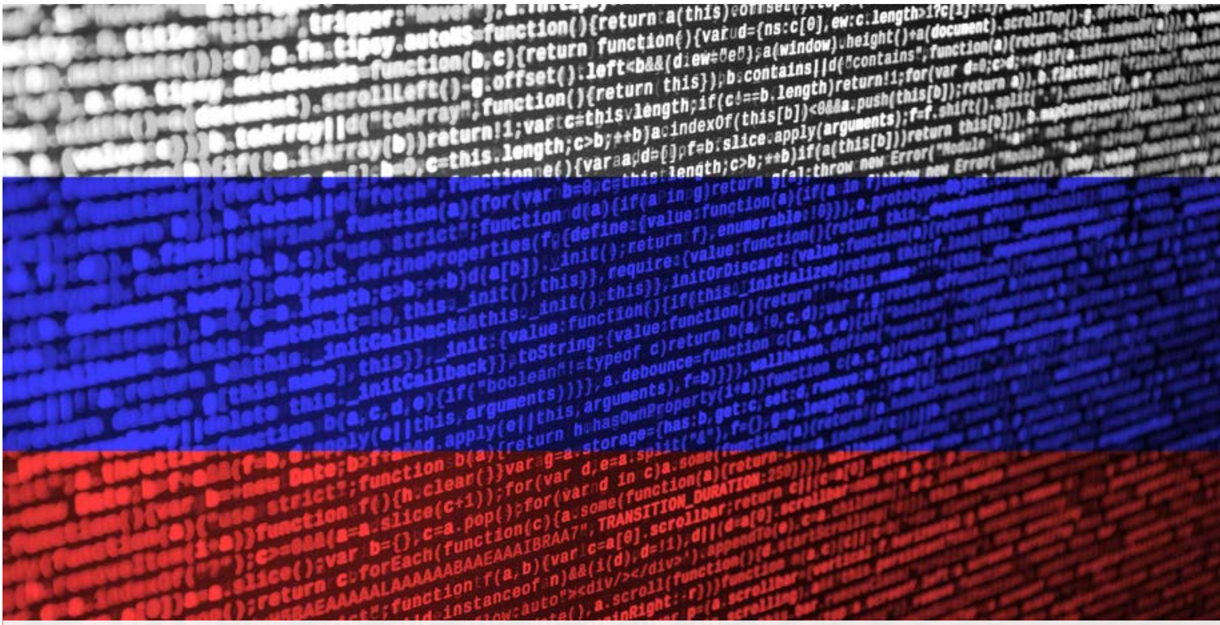
2.10. **Nation states.** The most sophisticated threat is likely to come from established, capable states (or their proxies) who exploit cyberspace to gather intelligence on government, military, industrial and economic targets. Examples of such activity are provided in Case studies 1, 3 and 5 in Annex 2A. Defence is particularly concerned when states:

- seek intelligence about UK military plans;
- steal intellectual property and intelligence on UK military capabilities;
- exploit UK military capabilities using their military and intelligence services with knowledge of the vulnerabilities of our capabilities;
- disrupt or deny the UK use of cyberspace, particularly systems supporting command and control, communications systems, military platforms and weapons systems;
- conduct subversive activities using their intelligence services; and
- use proxies or large numbers of synchronised and coordinated partisans to cover the true origin of their activities within cyberspace.

2.11. **Advanced persistent threat.** An APT is a threat actor with sophisticated (advanced) capability and significant resources. The aim of an APT will typically be to gain access to a target network with the intention of establishing an undetected long-term (persistent) presence. Once established, the APT will conduct activities such as network reconnaissance, information gathering, data extraction and specialist espionage-related tasks. Some APTs are widely assumed to be state-level actors or state-sponsored groups.

2.12. **Terrorists.** Terrorists, their supporters and sympathisers use cyberspace to spread propaganda, radicalise potential supporters, raise funds, communicate and coordinate plans. Such groups may also use cyberspace to facilitate or mount attacks against our critical national infrastructure.

2.13. **Criminals.** Criminals target the information on Defence and industries' computer networks and online services for commercial and financial gain (for example, contractual intelligence or intellectual property theft). They also target civilian and military personnel for fraud, blackmail or identity theft. As government services and businesses transfer more of their operations online, the scope for potential targets and criminal revenue will continue to grow. Annex 2A, Case study 2 provides an example of criminal activity conducted against British Airways.



© Mehaniq / Shutterstock.com

The most sophisticated threat is likely to come from established, capable states

2.14. **Patriotic hackers.** Patriotic hackers (who can also be described as state proxies) act on a state's behalf, particularly during times of increased tension. They aim to:

- spread disinformation;
- attempt to perpetrate attacks on, or block attacks by, perceived enemies of the state; and
- disrupt critical services.

An example of patriotic hacking, described in Annex 2A, Case study 3, is the spread of false information by Russian-aligned hackers against American political targets.

2.15. **Hacktivists.** Hacktivists are groups or individuals who seek to gain unauthorised access to computers, data or networks to further their cause, usually for social or political ends. They aim to:

- cause disruption, reputational, political and financial damage (for example, through releasing sensitive government information);
- gain publicity by attacking public and private sector websites and online services; and
- exploit social media to further their cause.

2.16. **Insider threat.** Disgruntled or subverted employees may seek to deliberately exploit cyberspace to cause harm to their employer in a number of ways. Additionally, all personnel, regardless of their role or seniority, are on the front line in cyberspace and can, accidentally, give an adversary the 'in' they need into Defence systems by ignoring or circumventing cybersecurity advice and procedures. Several examples of insider threats are provided in Annex 2A, Case study 4.

Non-targeted threats

2.17. Although this chapter concentrates on targeted threats, there are numerous threats in cyberspace that are not specifically aimed at any one individual that could cause Defence harm. An example of a non-targeted threat is the Wannacry ransomware attack that impacted the UK's National

Health Service (NHS), described in Annex 2A Case study 6. Additionally, malware used for a targeted attack, may spread beyond its original target with widespread impact. One of the most notable incidents of this nature is probably the NotPetya attack, which is described in Annex 2A, Case study 7.

Characteristics of cyberattacks

2.18. There are a number of cyber exploitation, attack tools and techniques freely available on the Internet. Adversaries traditionally employ four elements in an attack – vector, payload, behaviour and effect – all underpinned by intelligence.

a. **Vector.** This describes the method and route an adversary uses to form initial contact with the target in cyberspace. This could be through an email, a link on a web page, removable media, wireless connection or getting local access to the system used by the target.

b. **Payload.** Payload is computer code that will impact the target system through exploiting vulnerabilities, enabling the adversary to establish access and/or interact with the target. Often the vector and payload are combined in the form of malware.

c. **Behaviour.** Behaviour describes the actions taken by an adversary to ensure the initial and enduring success of the vector and payload in their attack. Actions may include concealing adversarial activity, for example, being undetected in both system log audits and by antivirus software. Adversaries will often delete or disguise evidence of their activities once the attack is complete.

d. **Effect.** The outcomes of cyber operations may be physical, but the majority of outcomes are virtual and cognitive effects. Effects may vary depending on the actor's intent and nature of the payload. Effects may include the following.

(1) Accessing a system, which not only gives the actor access to the information held on that system, but may also provide the means to investigate and gain further onward connections to other, more protected and sensitive, systems.[24]

[24] Access to a system will depend on the system configuration and administrative privileges acquired by the attacker.

(2) Theft of data – for example, password theft, data theft for creating reputational impact or loss of intellectual property and therefore undermining capability development and operational advantage in the other operational domains.

(3) Changing and undermining the integrity of information (such as radar signatures, geographic mapping, financial, logistics or personnel data) to provide false readings to impact other computer-aided processes such as fire control, targeting and support to operations.

(4) Changing decisions based on the addition and presentation of false data. Or, simply undermining faith in the accuracy of information so that timely decisions are deferred or cannot be made.

(5) Providing 'alternative facts' or a counter-narrative to undermine or support influence activity and information operations.

(6) Altering artificial intelligence and machine learning algorithms to change the rules by which computers make recommendations.

(7) Changing software functionality – for example, changing permissions, controlling hardware (such as webcams or entry systems) or implanting malicious programmes for use later. Functionality changes may also allow onward connectivity to other, potentially more interesting and valuable, information.

(8) Direct action on the target system – for example, render equipment useless or simply create a denial of service where an attacker aims to make a service or network unavailable to its users by overloading it with repeated requests for information or messages.[25]

[25] An extension of a denial of service is a distributed denial of service which uses multiple computers to attack the system, which can increase the duration and severity of the disruption.

The relatively pervasive and borderless nature of cyber activities enables both global and local operations

© ioat / Shutterstock.com

Properties of cyber threats

2.19. Cyberspace offers additional ways for an adversary to conduct traditional operations in support of espionage, subversion and sabotage. Reach, asymmetric effect, anonymity/attribution, timing and versatility are the main properties that differentiate cyber threats and attacks from conventional ones.

a. **Reach.** Compared to the other environments, the relatively pervasive and borderless nature of cyber activities enables both global and local operations.[26] It enables access to targets spanning the tactical to strategic level of operations.

b. **Asymmetric effect.** Cyberspace is open to almost all. An individual, or relatively small organisation with appropriate motivation, limited resources and high technical capability could conduct an attack with strategic and/or large-scale effect.

c. **Anonymity/attribution/deniability.** The process of attribution identifies the actor who conducted or sponsored a cyber action against another state, organisation or individual and the intent behind it.

[26] It must be noted that not all digital devices are interconnected and some communities still have limited or no cyberspace presence. They are therefore difficult or impossible to affect with cyber capabilities; however, such isolation is steadily reducing.

Non-attributable attacks increase uncertainty and potentially reduce political risk and the opportunity for retaliation. The process of attribution can be difficult, which can make an actor's use of cyberattacks more easily deniable.

d. **Timing.** There are two aspects to timing for cyber activity which we should consider.

(1) The preparation time for an adversary can be short where access, anonymity, collateral damage or target complexity are not concerns; equally, the time can be long where these are important considerations. Sophisticated attacks can take years to prepare and mount.

(2) The effects of cyber activity can be instant, triggered or purposely delayed. This provides a potentially very high operational tempo and a constant state of change. From a defender's perspective, nearly every cyberattack will be a surprise attack.

e. **Versatility.** The impacts of some cyberattacks are potentially reversible or tailored, and this can determine the degree to which services are affected. For example, an attack that prevents power from reaching a factory could be stopped, allowing the factory to resume working. Such reversible effects could reduce the amount of temporary collateral damage and therefore make a cyberattack more politically and socially acceptable. A good example is the extent to which many commercial companies now view ransomware attacks as inevitable and simply a business cost to be paid.

Forms and techniques of a cyberattack

2.20. There are a number of forms of cyberattack which make up a 'cyber toolbox'. A common feature is that the technical aspects of individual attacks frequently mutate daily.[27] The cyber toolbox includes (but is not limited to) malware, social engineering, supply chain corruption and local physical access.

[27] Mutations may be planned or unplanned; whether planned or not, some mutations may be controllable and others may not be.

2.21. **Malware.** Malicious software, known as malware, is an overarching term for software that is designed to infiltrate or damage a computer. Malware's purpose can include:

- keystroke logging – this uses code that logs a user's keystrokes as they type, compromising sensitive data, for example, passwords and credit card details;
- monitoring online activity, eavesdropping (voice and video) and geolocation of smartphones, tablets, laptops and similar personal electronic devices;
- exploiting social networking applications to support social engineering attacks;
- privilege escalation, where access is gained to a system and information technology security permissions are escalated to increase the attacker's level of control, eventually to include the accumulation of administrator (or 'root') privileges;
- denial of service intended to overload a system; and
- recruiting the target system as part of a botnet (also known as becoming a zombie), which can result in launching a distributed denial of service on everyone/everything a computer is connected to (for example, connecting to others using a user's contacts or email address book).

2.22. **Malware types.** Malware has traditionally been designed to infect computers and computer networks. However, the rapidly increasing popularity and sophistication of smartphones, tablets and other Internet-enabled technology, even relatively simple devices in the Internet of things, provide new and appealing targets for malware developers. Some malware combines attributes into 'blended threats' that are difficult to detect and remove. Some of the more common types of malware available are described in Table 2.1.

Malware types	
Virus	A virus is malicious computer code that can replicate itself and spread between computers. Once it has infected a machine, it spreads from one file to another, typically corrupting it or deleting it. Viruses are normally spread by human interactions, inserting USB sticks or opening emails.
Worm	A worm is closely related to a virus but differs in that it can replicate itself without having to infect files on the host machine. Worms spread over networks from one computer to another without human intervention. Once a worm is running on a computer, it can inflict similar damage to a virus.
Spyware	Spyware is software that collects information on a computer without a user's permission or knowledge and sends it back to the originator. This can be for malicious commercial purposes. Some online advertising resembles spyware.
Trojan horse	A trojan horse (also referred to as a 'trojan') contains malicious code masquerading as a legitimate and benign application. It will entice a user to launch it, which initiates the payload to take its effect. Trojans do not replicate, instead they rely on deceiving users into downloading and running them, frequently installing a rootkit.
Ransomware	Ransomware secures and encrypts a victim's data within an information technology system, only releasing it once a suitable passcode is entered. The passcode is available to the victim after a ransom has been paid. The ransom is typically substantial and demanded in untraceable crypto-currency.

Table 2.1 – Malware types

2.23. **Social engineering.** Social engineering is generally the manipulation of individuals to carry out specific actions, or to divulge information; it is commonly used to deliver malicious software onto target systems. Specifically, the information gained is frequently used as an enabler of cyberattacks. As an adversary's understanding of an individual's social use of the Internet deepens, there is a greater threat to that individual through their online interactions.

2.24. **Techniques.** In many cases the threat actor using these methods will have carried out extensive research on the target to maximise their chances of success. They will try to find organisation charts, telephone details and email addresses, and will use social media to refine their knowledge about the intended victim. This enables the attacker to use personal references that build the victim's confidence, making them more likely to comply with any requests. Some of the most commonly used techniques are outlined in Table 2.2.

Social engineering techniques	
Phishing	Phishing is a way of attempting to acquire information such as usernames, passwords and credit card details by masquerading as a trustworthy entity online. It typically involves falsely identified (spoofed) emails and/or directing users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing also occurs via social media posts, short message service (SMS) messages and instant messaging services.
Spear phishing	Spear phishing builds on phishing but is narrowly targeted against a specific individual, organisation or business. Emails will often contain reassuring details or appear to originate from individuals or organisations the target recognises to enhance their authenticity. Spear phishing attempts are not typically acts of random hackers but are conducted for financial gain or espionage.
Whaling	Whaling is a specific kind of malicious hacking within the more general category of phishing. It involves hunting for data that can be used by the hacker to specifically target phishing attacks against senior executives and other high-profile targets within businesses.
Baiting	The attacker simply places removable media, such as USB memory sticks or DVDs, in a target premises. The media may be labelled in such a way as to provoke interest, or simply left unmarked. This technique relies on employees within the target organisation picking up the media and loading it out of curiosity. Once running on a computer, the payload on the media (for example, malware allowing remote access of the computer) will usually run automatically. It is a surprisingly successful technique.
Telephone	The victim is telephoned by an individual posing as a figure of authority to persuade the victim to perform a task. Common scams involve criminals masquerading as an employee of the victim's Internet service provider or Microsoft to warn the victim of a fictitious problem on their computer. The victim can be persuaded to: carry out alterations to their computer to weaken its defences; navigate to a website that allows remote access; navigate to a website to download malware (on the pretext of fixing a supposed problem or downloading protection from viruses); or hand over personal or financial details.

Social engineering techniques	
Social networking	Social networking provides a number of opportunities for social engineering. Some social media users have been targeted with messages pretending to be from a friend who is stranded abroad needing emergency funds, while others have been contacted by convincing spoof accounts which tell a tale of hardship. These both divert to criminal website pages requesting personal information. Criminals exploit other social media to discover a victim's interests. This knowledge is then used to target messages or tweets containing embedded links to malware. Also, target emails or tweets offering a way to get more followers often divert victims to websites that download malware. Useful intelligence can be gathered and analysed from links and responses made in social media applications. Technical collection of such computer traffic patterns by third parties using commercially available software can be aggregated to provide information on location, force strength, movements of individuals and units, as well as morale, intentions and sentiments of whole groups of people. Armed with such data an adversary can craft plausible and damaging information operations.

Table 2.2 – Social engineering techniques

2.25. **Supply chain attack.** Every effort should be made to verify the trusted supply of all components, including hardware and software, for Defence capabilities. However, unscrupulous and/or malicious suppliers may interfere with the supply chain resulting in untrusted or unaccredited equipment being delivered, which may not function properly, safely and/or securely. Such interference can result in malware or maliciously modified hardware – such as a 'backdoor' – being embedded in newly delivered or recently repaired electronic equipment. Equally the supplier may be an innocent medium in a supply chain attack that is designed by a third-party attacker to attack end users of the supplier's software or equipment, who are the actual intended target.

2.26. **Access.** Access to the target is crucial to the success of any cyber operation. If the opportunities for the adversary to gain access are reduced, then a greater degree of protection can be achieved. Access can typically be gained in three ways: physical, close and remote.

a. **Physical access** is the ability to gain direct access to a computer or network, such as by connecting a USB device directly to a computer. Access can be gained in a number of ways, for example, posing as public officials or couriers delivering a package, or by tailgating staff. Once in the premises, intruders can interfere with information and communications technology by installing software, such as keystroke loggers and remote access hardware to gain data from, or allow future access to, systems.

b. **Close access** is the ability to access a computer or network from deployed platforms, people and equipment operating within the area of that network. Typically, this would be through use of the electromagnetic spectrum, such as connecting via Wi-Fi, Bluetooth or third, fourth and fifth generation networks. Alternatively, close access can be achieved by an adversary through 'baiting'.

c. **Remote access** is the ability to get access to a computer or a network from external locations (physical and virtual) that may be considered outside of that network. Typically, this is conducted via the Internet.

© TarikVision / Shutterstock.com

Portable electronic devices are an attractive target for threat actors

2.27. **Encryption challenges.** Once the preserve of governments, encryption protocols are now available to those engaged in more nefarious activities, whether state or non-state sponsored. These protocols can be used across a range of commercial and personal applications, particularly messaging applications that enable activities such as command and control and financial transactions. The widespread use of complex encryption across multiple applications in cyberspace presents increasing difficulty for intelligence and law enforcement agencies investigating nefarious activities.

2.28. **Exploitation of portable electronic devices.** The term portable electronic devices (PEDs) encompass a wide range of small electronic devices including laptop computers, tablets and smartphones amongst others. Their popularity, size, connectivity and relatively basic security standards imply that PEDs are an attractive target for threat actors, either for the data they hold or as a vector for gaining wider network access through direct or indirect means; they are one of the most common means by which individuals are likely to encounter social engineering techniques. Mobile phones, or other PEDs, can be compromised by a knowledgeable and determined attacker. They could:

- look at, take copies of, or delete information stored on the device;
- locate the position of the device to an accuracy measured in metres;
- track your movements using your locational information;
- remotely activate the camera and microphone without you knowing;
- log every button press/keystroke;
- remotely manipulate the security levels;
- infect systems that are connected to the device, especially if connected via a USB; and
- remotely turn the device on when it is switched off.

Mitigation of cyber threats

2.29. Considerable effort is made to protect Defence's people and infrastructure from cyber threats. A key component of this is the *Cyber Resilience Strategy for Defence,*[28] which identifies the following strategic priorities.

a. **Secure by design.** Defence's capabilities are inherently protected from the outset throughout their life cycle, built to be resilient against cyberattacks with pre-planned recovery measures in place.

b. **Governance, risk and compliance.** Defence's risk management approach provides good governance that drives change and achieves compliance.

c. **Rapidly detect and respond.** Defence's integrated cyber defences cover the critical functions providing the ability to detect and respond to cyberattack.

d. **People and culture.** The people in Defence are cyber aware, exhibiting the appropriate behaviours that form a positive culture and embeds cyber resilience across Defence's outputs.

e. **Industry.** Defence's relationship with industry is enhanced, allowing us to achieve improved supply chain security and resilience.

f. **Secure foundations.** Defence's entire digital enterprise incorporates security controls, supported by people and processes, that make it resilient to cyberattack.

g. **Experimentation, research and innovation.** Our approach seizes on experimentation, research and innovation opportunities to ensure we can stay ahead of the developing cyber threat.

[28] Ministry of Defence, *Cyber Resilience Strategy for Defence*, 2022.

Individual responsibility

2.30. Whilst comprehensive measures are in place to mitigate cyber threats, one of the most effective forms of defence remains personal awareness and responsibility. This includes the willingness to take appropriate action to deter an attack in the first place by applying and maintaining good practices and having the ability to respond quickly and correctly when problems do arise. Good baseline cyber and information management skills are essential to the modern operating environment.

2.31. Good operational security procedures are essential. Electronic devices, particularly PEDs, are likely to be a target for both foreign intelligence services and criminals. Messages, be they voice or data sent via such systems, are liable to intercept. Care must be taken not to inadvertently disclose operational data, or data that can compromise individual security when using information technology, particularly when deployed.

2.32. Initiatives such as the 'Cyber Confident' campaign are helping to raise and maintain this awareness. Personnel should also know where to seek additional advice and assistance relevant to their specific role and location. In most cases, the local information technology security officer is a good start, as is the Defence Single Point of Contact (SPOC).

2.33. Advice on personal cybersecurity, including PEDs is available from sources such as the National Cyber Security Centre (NCSC). As a bare minimum, individuals should ensure that simple actions such as keeping operating systems updated, using strong passwords and a virtual private network (VPN),[29] as well as the use of security functions when using social media are observed. Joint Service Publication 440, *The Defence Manual of Security* provides further comprehensive guidance on the subject. If in doubt, ask.

[29] A virtual private network is an encrypted network often created to allow secure connections for remote users, for example, in an organisation with offices in multiple locations. NCSC Glossary.

Annex 2A

Threat case studies

Case study 1 – State versus state offensive cyber operations

Cyberattacks used to harness scientific advantage	
Who	APT29 is the name given to an APT actor attributed to, and almost certainly a part of, the Russian Foreign Intelligence Service. They are linked with multiple other groups such as 'Cozy Bear', 'Dark Halo' and 'The Dukes'. They have been in operation since at least 2008 and target the North Atlantic Treaty Organization (NATO), European countries and other organisations of interest to Russia including research institutes. They are a persistent, highly sophisticated and patient threat actor and that represents a potent challenge to the UK and allies (military and commercial).
What	Throughout 2020, APT29 targeted various organisations involved in COVID-19 vaccine development.
How	The attacker used custom malware known as 'WellMess' and 'WellMail' as well as several publicly known vulnerabilities in software such as virtual private networks. Combined with spear phishing, the groups have attempted to gather login details from Internet facing nodes of targeted organisations. Having gained access, the perpetrators were then able to inject the malware designed to execute commands, upload and download files.
Target	Various organisations involved in COVID-19 vaccine development in Canada, the United States (US) and the UK.
Why	It is highly likely that the attacker's intention was the stealing of information and intellectual property relating to the development and testing of COVID-19 vaccines. This would have been used to either accelerate domestic vaccine research or to discredit Western efforts to produce vaccines.
When	2020 to 2021.
Impact	Significant disruption to UK COVID vaccine development and the risk of loss of intellectual property rights from UK Sovereign and commercially sensitive COVID vaccine research and development leading to reputational damage, loss of revenue earning potential and compromise of vaccine efficacy.
More information	https://www.wired.co.uk/article/russia-hack-coronavirus-vaccine

Case study 2 – Cyber used for data theft

Theft of personal data – British Airways	
Who	There has been no official attribution of those responsible, although RiskIQ, a Microsoft cybersecurity company, have linked the Magecart cybercrime syndicate.
What	On 6 September 2018, British Airways announced that it had suffered a data breach and that customer data had been stolen, affecting some 380,000 customers. The data included personal and payment information.
How	The attackers injected code designed to steal sensitive data entered by customers in online payment forms. Magecart is also the name of the JavaScript code that the groups inject. Both the British Airways website and mobile application were affected. Customers using either portal had their data submitted to an external site once they clicked the 'submit' button to confirm their transaction.
Target	British Airways customers. Magecart mainly targets e-commerce websites.
Why	To obtain victim's payment card information and then resell this information to other criminals.
When	August 2018.
Impact	As well as the theft of the data and the loss of confidence in the British Airways payments system, the company was also fined £183 million by the Information Commissioner's Office, this was later reduced to £20 million.
More information	https://www.riskiq.com/blog/external-threat-management/magecart-british-airways-breach/

Case study 3 – Patriotic hackers

Cyberattacks interfering with United States elections	
Who	Russian President Vladimir Putin said in 2017 that Russian hackers supportive of Russian Government aims may have staged cyberattacks against countries that had strained relations with Moscow of their own accord.[30] This remark was in response to a question about election interference but not specifically about the US.
What	An information campaign sharing false information about the election candidates and leaking sensitive party information.
How	Starting with a phishing campaign, the attackers were able to gain access to the information technology network of the Democratic Congressional Campaign Committee and then used this to spread deeper and wider into the Democratic National Party network. The information harvested was the basis of some of the WikiLeaks releases. Social media was also used to spread propaganda, using bots to promote pro Donald Trump messages.
Target	The Democratic Party and Hilary Clinton's election campaign.
Why	To damage the Clinton campaign, boost Trump's chances of being elected and to reduce confidence in the electoral system.
When	At least between January 2015 and August 2017.
Impact	It is difficult to quantify the impact of the attacks but electorates increasingly rely on social media and it is likely to have had some negative impact on the Clinton campaign. The scale was large: 50,258 Twitter accounts were linked to Russian bots that were responsible for 3.8 million tweets, about 19% of the 2016 US presidential election from just one social media platform.[31]
More information	The Mueller report sums up the findings of an investigation into the 2016 election. https://www.justice.gov/archives/sco/file/1373816/download

[30] Reuters, 'Patriotic Russians may have staged cyberattacks on own initiative: Putin', 1 June 2017.

[31] The Conversation, 'Fact check US: What is the impact of Russian interference in the US presidential election?', 29 September 2020.

Case study 4 – Insider threats

Insider threat examples	
National Health Service	NHS data leak – March to May 2020 Data from the NHS COVID-19 contact tracing application was hosted on Google Drive and was inadvertently left open for viewing by anyone with a link.
Bupa	Bupa data sold for financial gain – January to March 2017 A Bupa employee obtained the personal information of 547,000 Bupa customers. This information was sent to the employee's personal email account. The data was later offered for sale on the dark web.[32]
Tesla	Tesla engineer steals proprietary technology code – 2017 to 2019 Dr Guangzhi Cao, an employee of Tesla, stole source code for their proprietary driver-assistance software. Dr Cao subsequently took a job with Tesla's competitor XMotors, Tesla sued Dr Cao in response. He admitted to having taken the data but denied using it for his new employer.[33]

[32] Digital Health, 'Bupa fined by ICO after employee stole customer information', 2 October 2018.

[33] Steptoe, 'Hazards of the Digital Age: A Case Study of Tesla v. Cao on Handling Confidential Material', 14 May 2021.

Case study 5 – Impact of malware on military capability

	Impact of malware on military operations – SolarWinds
Who	Russian intelligence agencies exploiting a zero-day vulnerability on SolarWinds Orion, an industry-leading and widely used computer network management software tool.
What	The attackers compromised a software update to include a backdoor from the legitimate update server. This was installed by users in their normal update process.
How	Once users had downloaded the seemingly genuine update from the SolarWinds' website this gave attackers the ability to transfer files, execute applications, profile the system, reboot the machine and disable system services remotely. The nature of pervasive commercial management software such as SolarWinds Orion is that it requires administrative access across many network layers to operate, so any vulnerability which allows unauthorised management access is an extremely powerful and potentially destructive development.
Target	The first agency to identify this exploit was the well-respected US cyber threat management company FireEye, as their own systems had fallen victim to it. However, SolarWinds is such a popular tool across Western commerce, governments and military that the initial target was irrelevant; so widespread was the potential access across government systems that it was likely aimed at the US public sector.
Why	Anything which can provide system administration level access to a network is of considerable value to adversaries. There is speculation that the focus of the attack were US government agencies and that the perpetrators were Russian intelligence agencies.
When	September 2019 to December 2020. However, many networks may still not be patched due to reluctance to introduce downtime to critical systems.
Impact	Significant downtime for military and government network management systems and widespread disruption for staff and organisations over Christmas period 2020, there is no open-source evidence of data exfiltration via this route.
More information	https://www.wired.com/story/solarwinds-hack-supply-chain-threats-improvements/

Case study 6 – Impact of a cyberattack against a state's critical national infrastructure

Cyber collateral damage against UK critical national infrastructure	
Who	The NHS suffered its largest ever information technology outage due to the infection of WannaCry ransomware which encrypted the hard drives of over 230,000 computers globally in May 2017, this was eventually attributed to North Korean state hackers.
What	Wannacry was a worldwide ransomware attack that demanded repayments in the Bitcoin crypto-currency.
How	The WannaCry ransomware exploited a known vulnerability in server software which Microsoft had already released a patch for at the time of the attack. The NHS has a vast estate of users and computers, estimated in excess of a million devices with relatively few 'global' services such as NHSmail and the national NHS network backbone. This has led to unsupported operating systems such as Windows XP still being in use, and delays in critical patching, and the provision of unmanaged computers attached to proprietary equipment such as scanners and sequencers. This implied that the elements of the NHS were vulnerable to WannaCry.
Target	Although the NHS was the most publicly affected victim, it is not considered the prime target of this attack. The attack was opportunistic in nature with the malware being released on the Internet. Specifically, it did not require any user interaction, such as opening an email or clicking on a link, to spread.
Why	The exact motivation remains unknown, but financial gain is plausible. Each WannaCry instance demanded a relatively small amount of ransom so it is considered that its virulence would have ensured that even if only a small proportion of victims responded with the ransom, the profit for the perpetrators would have been enormous.
When	12 May 2017.
Impact	The Department of Health indicated that no NHS trusts paid any ransom. The attack caused disruption in at least 34% of the trusts in England. Sky News reporting during the day indicated 'general practitioners being forced to use pen and paper' and 'patients being told to attend accident and emergency only in an emergency'. Many operations and non-critical activities were cancelled. This incident remains the NCSC's only Tier 2 cyberattack. There have been no Tier 1 cyberattacks since the NCSC's founding in 2016.
More information	https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/

Case study 7 – Disruption of e-commerce

Manipulation of e-commerce by a nation state	
Who	NATO's Cooperative Cyber Defense Centre of Excellence attributed the NotPetya attack to a state actor. The UK's NCSC and Five Eyes partner cybersecurity organisations went further and assessed that the Russian military were ultimately responsible.
What	The NotPetya attack impacted businesses with strong trade links with Ukraine across multiple sectors including the UK's health and hygiene product maker Reckitt Benckiser, the US food and drink manufacturer Mondelez, the Dutch delivery firm TNT and notably the Danish international shipping organisation Maersk. NotPetya ultimately spread to over 60 countries in Europe, the US and beyond.
How	The M.E.Doc tax software, used to interact with Ukrainian tax systems by most Ukrainian businesses and tax filers was identified by multiple companies and experts, including Cisco and Microsoft, as the source of the infection. The software's legitimate automatic update mechanism was repurposed to deliver the malware to users. Infected computers displayed messages commonly used by ransomware, however, it was assessed that the malware was not created to ever allow for successful decryption and the true purpose was to act as a destructive piece of code called a wiper.
Target	Ukraine's financial, energy and government institutions were most impacted, with the Internet security company ESET estimating that over 80% of infections occurred within the country. However, infections spread further to businesses in Europe, the US and Russia.
Why	The attack was highly likely to have been politically motivated, with the intention of the perpetrators to destabilise the government in Ukraine, leading to financial and social disruption.
When	27 June 2017.
Impact	A White House assessment stated that the total damages as a result of the attack amounted to more than US $10 billion and labelled it the 'most destructive and costliest [cyberattack] in history'. NotPetya is an example where a cyberattack may have had unintended consequences far beyond the original target of the attackers.
More information	https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack

Chapter 3

Cyber functions

Chapter 3 looks at four military cyber operations roles – influence, defend, enable and inform – which are delivered by cyber capabilities through offensive and defensive cyber operations, cybersecurity and cyber threat intelligence. It also examines information management and finally looks at the relationship between cyber and other closely linked military functions.

Cyber operations

3.1. Cyber operations concern the planning and synchronisation of activities in and through cyberspace to enable freedom of manoeuvre and to achieve military objectives.[34] Cyber operations can be broadly categorised into four distinct roles: influence, defend, enable, and inform. These roles are rarely discrete. They are interdependent and interacting, providing support to, being supported by and placing constraints on each other.

3.2. Defence does not deliver all cyber operations; it provides its part within a complicated tapestry of UK national cyber capability. It must be remembered that for the UK, ‘cyber’ is a whole of society endeavour. Military cyber activity must therefore be integrated with key partners, including the following:

- the Cabinet Office, including the Government Cyber Coordination Centre for widespread or critical national infrastructure related cyber incident response;
- the National Cyber Security Centre (NCSC), which is a division of the Government Communications Headquarters (GCHQ);
- the National Cyber Force which is a joint organisation co-owned and co-staffed by the Ministry of Defence (MOD) and the UK Intelligence Community, including GCHQ;

[34] The North Atlantic Treaty Organization (NATO) defines cyberspace operations as: actions in or through cyberspace intended to preserve friendly freedom of action in cyberspace and/or to create effects to achieve military objectives. NATOTerm.

- other government departments, particularly the Foreign, Commonwealth and Development Office and the Home Office;
- industry;
- academia; and
- international partners and allies.

3.3. From a Defence perspective, a Cyber Security Operating Capability has been created to conduct defensive cyber operations. This federated capability is staffed by a military, civilian and industry workforce, including Reservists, and is explained in more detail in Chapter 4. The investment in a Cyber Security Operating Capability underlines the importance Defence places on cyber defence and resilience.

Influence

3.4. The influence role enables cyber and electromagnetic capabilities to shape (defeat, deceive, degrade and deny) adversaries capabilities, which allows Defence to mould the behaviour of audiences and the course of events. The missions which make a particular contribution to influence activities are: offensive cyber operations, cyber information operations, counter cyber and electromagnetic attack. Offensive cyber operations are defined as: activities that project power to achieve military objectives in or through cyberspace.[35] They may transcend the virtual dimension (for example, websites and social media feeds) into effects in the physical dimension (for example, causing computer hardware destruction) and, most importantly, directly influence the cognitive dimension of thoughts, beliefs, interests and perceptions of individuals and groups.

3.5. Offensive cyber activity can be used to inflict permanent or temporary effects, thus reducing an adversary's confidence in their networks, information or other capabilities for a specific period. Offensive cyber operations may be used in isolation, or in conjunction with other capabilities to create effect. Such action can support deterrence by communicating intent or threats. The link to influence activity is strong and at the operational/tactical level of operations there is a need to coordinate offensive cyber operations and information operations.

[35] Joint Doctrine Publication (JDP) 0-01.1, *UK Terminology Supplement to NATOTerm*.

3.6. Offensive cyber activity is commonly broken into seven phases, known as the cyberattack chain. The phases are not discrete events, instead they interact and overlap with each other and may vary in duration. They are equally applicable to the actions of a state or criminal. They are also dependent on an attacker's intent and availability of offensive cyber and intelligence capabilities. A representative cyberattack chain is shown at Figure 3.1.[36]

1 – Understanding. Information and intelligence gained by the adversary on a target's cyber environment and the identification of specific targets.

2 – Payload development. Development of an exploit that will create the desired effect by using the identified vulnerabilities of the target system.

3 – Delivery. Transmission of the payload to the target system using vectors like email attachments, websites and removable media (for example, USBs).

4 – Exploitation. After the payload is delivered to the target system, exploitation triggers the payload – exploiting a vulnerability.

5 – Installation. Installation of a remote access or backdoor on the target system allowing the adversary to maintain a presence/persistence inside the target system.

6 – Command and control. The adversary establishes communication channels to facilitate the transmission of commands.

7 – Desired effects created. After progressing through the first six phases, the adversary can take actions to create the desired effects.

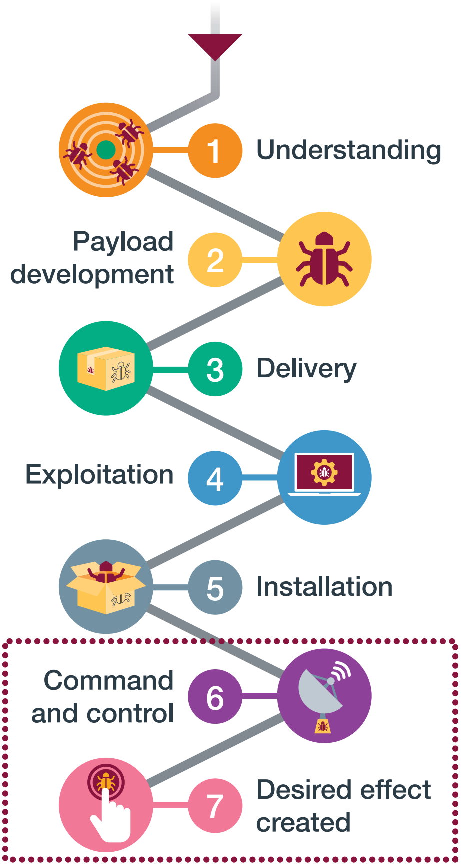


Figure 3.1 – Cyberattack chain

[36] Developed from Lockheed Martin's cyber kill chain framework.

Defend

3.7. Defensive cyber operations are defined as: active and passive measures taken to prevent, nullify or reduce the effectiveness of adversary actions to preserve our freedom of action in or through cyberspace.[37] They may be discrete, episodic or enduring but are focused activity that is designed to secure our access to, and freedom of action in, cyberspace. They may be undertaken against a specific threat or bounded in scope, for example, when in support of a named military operation or as part of a mission assurance[38] approach.

3.8. At the strategic level, defensive cyber operations assure freedom of action by protecting digital infrastructure and strategic capabilities from adversarial offensive cyber activity. At the operational and tactical levels, they protect critical computer and communication networks and systems that reside in the sea, land, air and space environments. Defensive cyber operations are likely to be localised in terms of time and space and will be at least partly reliant on the quality of information assurance controls and cyber risk management that has been conducted previously. The need to conduct defensive cyber operations is enduring and non-discretionary.

3.9. **Cybersecurity in relation to defensive cyber operations.** Cybersecurity, both individual and collective, is a foundational requirement of all Defence activity, including: the business of managing our people; capability acquisition; protecting sensitive information; and planning and conducting military operations. Any lapse in cybersecurity can affect our resilience or success and destroy the trust of our partners. The link with operations security is critical as actions in cyberspace may take place over a prolonged period and any compromise could undermine years of effort. Within the cyber environment, everyone must apply judgement, take responsibility for their actions, understand regulations and respond to possible incidents in a timely fashion. Defence has a comprehensive programme, ‘Cyber Confident’, designed to improve everyone’s understanding of risks and their personal ability to act responsibly in cyberspace.

3.10. **Resilience.** Dependence on the cyber environment dictates that Defence, commercial entities/contractors and our partners must withstand or recover rapidly from disruption. Defence must also deliver those capabilities and actions that are essential to operations.

[37] JDP 0-50, *UK Defence Cyber and Electromagnetic Doctrine*, 2nd Edition draft.

[38] Mission assurance is defined as: a process to protect or ensure the continued function and resilience of capabilities and assets, critical to the execution of mission-essential functions in any operating environment or condition. NATOTerm.

Defence must also deliver those capabilities and actions that are essential to operations

3.11. **Cyber resilience.** Cyber resilience is described as the ability of an organisation or platform to withstand and/or recover from malicious events in cyberspace. Simply put, this means that people and organisations can continue to operate even if their access to cyberspace, or ability to use digital tools, computers and communications, has been disrupted by a cyber incident. Business continuity plans must consider cyberattack alongside other risks or disruptive events such as a bomb threat or fire. In 2022 Defence published its *Cyber Resilience Strategy for Defence,*[39] which takes thinking beyond simple cybersecurity and toward genuine resilience.

3.12. **The National Institute of Standards and Technology Cybersecurity Framework.** The National Institute of Standards and Technology (NIST) is a United States government organisation that has contributed significantly to international thinking on cybersecurity. Specifically, it produced an updated Framework in 2018 to aid organisations conduct cyber defence, which has been widely adopted and is colloquially known as the NIST Cybersecurity Framework. The Framework comprises five core functions and is shown in Figure 3.2. The Framework and the sound principles it espouses underpin much of the work of the Cyber Security Operating Capability and the NCSC, although terminology may differ.

- Identify – gain visibility and control of digital assets, systems and identities.

- Protect – implement cybersecurity measures and cyber resilience measures.

[39] Ministry of Defence, *Cyber Resilience Strategy for Defence*, 2022.

- Detect – monitor, analyse and hunt for harmful activity.
- Respond – manage events and incidents when they occur.
- Recover – re-establish trusted access to cyberspace.

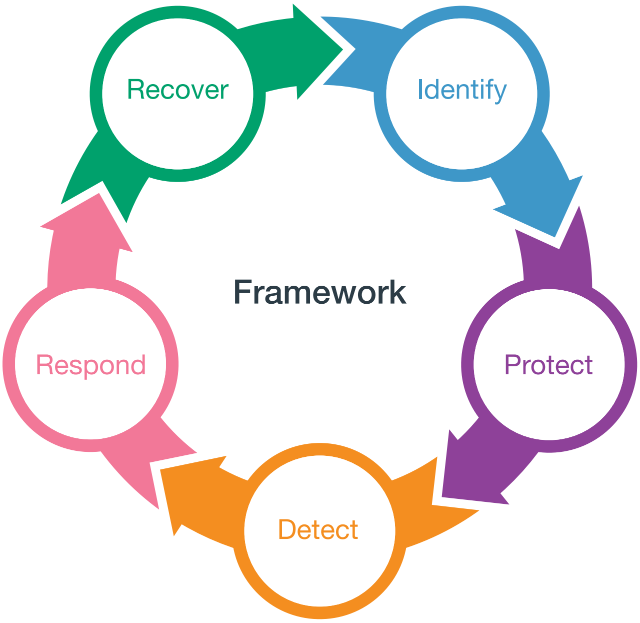


Figure 3.2 – The National Institute of Standards and Technology Cybersecurity Framework

Enable

3.13. The third role in cyber operations – enable – is a vital function; it harnesses, manages and operates the communication and information systems infrastructure controlled by Defence, and in support of our allies. Cyberspace is an artificial environment and must be deliberately created, maintained and assured for all other cyber activity to be possible. Enable is a foundational role.

3.14. Defence Digital is primarily responsible for the enable role in UK Defence and operates many information services as well as providing the assured information paths between fixed Defence networks and deployed forces. These information paths can either use the electromagnetic spectrum to enable global communications (for example, high frequency radio and satellite communications) or use fixed global communications links of which a key component is undersea cables that traverse international waters. Other enable activities include electromagnetic spectrum management, digital service integration and management, network operations and information assurance.

Inform

3.15. The inform role underpins all the other roles as it secures freedom of action to engage with the cyber and electromagnetic domain. This is achieved through the development of appropriate knowledge and understanding.

3.16. Intelligence preparation of the environment (IPE) is essential to gain a detailed holistic understanding of all elements, including cyberspace, relevant to a specific mission or task and to provide the commander with situational awareness; it has a place in both the enable and inform roles. The cyber element of IPE is a complex undertaking and may require considerable time to achieve the levels of detail required. To gain holistic appreciation of the cyber environment, it is necessary to link cyber IPE with the wider J2 intelligence function.

3.17. Situational awareness is defined as: the knowledge of the elements in the battlespace necessary to make well-informed decisions.[40] Accurate, detailed and timely intelligence is critical to military operations. Intelligence (including indicators and warnings) focuses on developing sound situational awareness and understanding by identifying trends and scanning for emerging threats, hazards or opportunities as well as understanding the consequences of any action. Cyberspace contains huge amounts of data that can be exploited and assessed for intelligence and situational awareness.

3.18. A recognised cyber operating picture, within a common operating picture, could provide commanders with enhanced situational awareness, improved understanding, decision support and enable decision-making. However, producing a recognised cyber operating picture is challenging, reasons for which could be:

- the high speed at which events can occur in cyberspace;
- the volume of activity, especially non-military, that occurs in cyberspace;
- difficulty in proving or judging attribution;

[40] NATOTerm.

- difficulty in recognising and categorising routine faults rather than cyberattacks;
- deception is commonplace and easy to achieve; and
- locations in the physical and virtual cyber layers might not align.[41]

3.19. Indicators and warnings for Defence are often sourced through commercial entities (for example, cybersecurity intelligence vendors, antivirus vendors or industry security operating centres) and from the intelligence agencies. Defence Digital has access to all these sources and assumes lead responsibility for disseminating cyber indicators and warnings across Defence's networks.

Information management

3.20. Acquiring, sharing, processing and protecting data and information is a vital supporting function to the four roles of cyber operations. All information has value, whether created and shared for the business of administering Defence or for the prosecution of military operations. Acquiring and sharing information to other people, multiple groups or collective locations should be timely, but must also maintain data integrity. Data covering personnel or other sensitive matters, for example, intelligence and operational plans, must be protected under the UK government security classification system.[42]

Data covering personnel or other sensitive matters must be protected

© deepadesigns / Shutterstock.com

[41] A factor that has become increasingly problematic with cloud computing.

[42] Cabinet Office, *Government Security Classifications*, May 2018.

3.21. The care and protection of information is also subject to multiple legal requirements, for example, the General Data Protection Regulation (GDPR)[43] and the Data Protection Act 2018. Compliance with these laws is mandated for all Defence personnel and the MOD is regulated by the Information Commissioner – conformance is non-discretionary. In the event of a suspected data breach, for example, sending a sensitive email to the wrong person or across the public Internet, it must be reported without delay.

3.22. Information assurance provides personnel and commanders with the confidence that their computer networks and communications and digital systems will protect the information they handle to meet the information management requirements applicable to the information being processed. It also assures that systems function as they need to, when they need to and under the control of legitimate users.

3.23. An effective approach to information sharing and interoperability of cyber activity requires information and intelligence to be shared. A balance must be struck between the 'need to protect' for security and the 'need to share' for mission success. Operations security is critical for effective cyber operations and must never be compromised.

Cyber and electromagnetic operations in context

3.24. Cyber and electromagnetic operations comprise of a series of interrelated disciplines. A short synopsis of each is provided below.

a. **Cyber operations.** Cyber operations concern planning and synchronising activities in and through cyberspace to enable freedom of manoeuvre and to achieve military objectives.

b. **Information operations.** Information operations are closely associated with cyber capability and there is a large degree of subject matter overlap. Whilst cyber operations take place in and through cyberspace, information operations can also use any of the operating environments to pursue its aims.

c. **Electromagnetic operations.** Electromagnetic operations are defined as: all operations that shape or exploit the electromagnetic environment, or use it for attack or defence including the use of

[43] Information Commissioners Office, 'Guide to the UK General Data Protection Regulation (UK GDPR)'.

the electromagnetic environment to support operations in all other operational environments.[44] Note: Electromagnetic operations include (but are not limited to) electromagnetic warfare, signals intelligence, intelligence, surveillance, target acquisition and reconnaissance, navigation warfare, battlespace spectrum management.

d. **Signals intelligence.** Signals intelligence is defined as: intelligence derived from electromagnetic signals or emissions.[45] Note: the main subcategories of signals intelligence are communications intelligence and electromagnetic intelligence. Cyber and signals intelligence are, to an extent, reliant on similar infrastructures, organisations, accesses, personnel training and skill sets.

e. **Communication and information systems.** Communication and information systems are essential to facilitate the enable role of cyber operations.

3.25. The relationship between the various operations disciplines within the cyber and electromagnetic domain is close, with a significant degree of overlap and mutual dependence. This is illustrated in Figure 3.3.

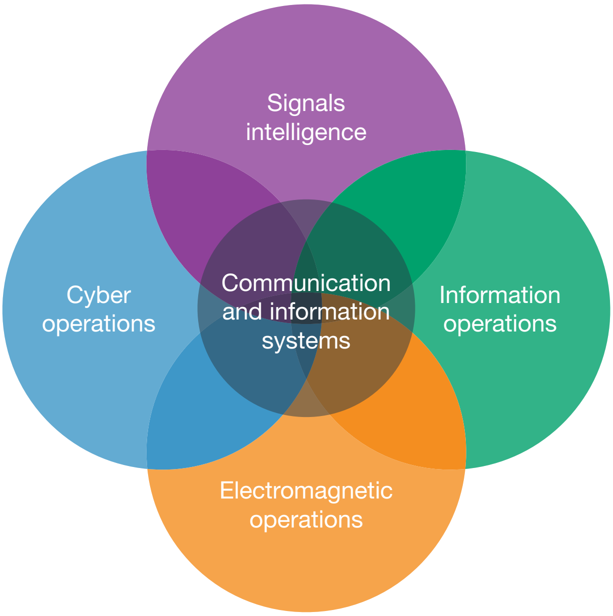

Signals intelligence
Cyber operations
Communication and information systems
Information operations
Electromagnetic operations

Figure 3.3 – Cyber and electromagnetic operating context

[44] NATOTerm.
[45] NATOTerm. An example is radar.

Notes

Chapter 4

Cyber operations

Chapter 4 looks at how cyber capability is currently organised and integrated with military operations and provides some detail concerning cyber command and control.

Integrating cyber-enabled effects

4.1. Cyber-based activities are vital to our national security, playing an integral role in protecting the UK against external and internal threats. For this reason, it is essential that cyber activities are considered an integral aspect of military operations. Military cyber and electromagnetic operations must be coordinated, synchronised and integrated across the strategic, operational and tactical levels of operations with all other military capabilities. These activities are part of Defence's approach to full spectrum targeting processes. It recognises that other nations or actors, both friendly and adversary, may use cyber capabilities to enhance their own ability to achieve a degree of local, regional and/or international influence, which may otherwise be limited through other means.

4.2. **Strategic effects.** Cyberspace is not affected by physical geography in the same way as other conventionally derived effects and may offer options to hold strategic target sets at risk that otherwise would be unreachable. The Stuxnet attack against the Iranian nuclear programme is an example of cyber-enabling operations for strategic effect.[46] However, cyber operations do not have to cause physical destruction. We can potentially create a variety of effects in terms of complexity and severity, and at a tuneable scale. One advantage of cyber effects is that they can be used to influence adversary decision-makers at the strategic level while being coordinated and conducted from afar. Arguably, as detailed in Case study 3 in Chapter 2, the alleged Russian manipulation of social media channels during the 2016 United States Presidential elections is a better example than Stuxnet of how cyber operations can create strategic effect. Furthermore, serious ransomware attacks may

[46] First uncovered in 2010, but in development and deployed prior to this date.

also cause strategic economic effects for a country without any military activity being conducted.

4.3. **Operational effects.** Incorporating cyber capability into operational-level planning is an evolving process but is critical for successful integrated action. A high degree of integration and cooperation between units and organisations, both in the cyber field and conventional forces, is required to successfully orchestrate cyber effects leading to desired outcomes within a campaign. It is entirely possible that cyber operations will have been taking place for some time, possibly years, before conventional forces are deployed.

4.4. **Integrated action.** As these operations may be dependent on non-attributable infrastructure and networks associated with, or even located within, physical target sets, de-confliction and understanding of intelligence gain/loss and avoidance of fratricide are key considerations. It may be possible to create a cyber effect using ‘low equity’ or open-source tools that can provide more agile and flexible response options than exquisitely crafted so called ‘zero-day’ exploits. Integrating cyber into operational planning is achieved through integrated action,[47] which is a framework for considering the integration, coordination and synchronisation of all military and non-military activity within the battlespace to influence the attitude and behaviour of selected audiences necessary to achieve successful outcomes.

4.5. **Tactical effects.** At the tactical level, the time required to develop access and invest in capability may mean that creating high-end cyber effects is reserved for early or important actions that have a high pay-off. However, lower-level attacks (such as locally interfering with a single building’s network access and subsequently employing a low-end common payload) may increasingly be seen on operations. The Israeli integration of cyber operations into the conventional bombing of a Syrian nuclear research institute is a good example of the operational/tactical use of cyber. This example also neatly highlights the synergy between cyber methods and electromagnetic warfare in tactical scenarios.[48]

[47] Ministry of Defence, *The Orchestration of Military Strategic Effects*, 2020, page 5.
[48] The Cyber Law Toolkit, ‘Operation Orchard/Outside the Box’, 2007.

4.6. **Time.** Cyber accesses often take years to develop. Knowledge of specific accesses and capabilities will be tightly controlled and held at the highest classification levels. Conversely, while this preparatory phase can take years, the execution phase may only take seconds. Similarly, in defensive terms, it may take far more people, time and resource to successfully protect and defend our own networks than for an adversary to launch a credible attack against them.

Command and control, authorities and responsibilities

4.7. Cyber underpins so many aspects of Defence's business that cyber command and control for Defence is complicated. Joint Doctrine Publication (JDP) 0-01, *UK Defence Doctrine* describes Defence's approach to command and control more generally. The span of military, multi-agency and multinational partners conducting cyber activities means simple supported/supporting relationships are more complex in reality. Instead, the commander and specialist staff must understand and manage multiple relationships, each of which is governed by particular freedoms and constraints. Government and industry must adopt a cautious but trusted partnered approach to cyber activity, orchestrated across strategic to tactical levels of command. This also applies to allies and coalition partners.

The span of military, multi-agency and multinational partners conducting cyber activities means simple supported/supporting relationships are more complex in reality

4.8. Defence is developing command and control and force structures to deliver and sustain cyber capabilities as part of its future force.[49] The evolving Defence structure emphasises the complexity of conducting operations in cyberspace and a need to ensure actions are coordinated while retaining the flexibility and agility to manage the threats, and opportunities, arising from cyber activities. An agile and resilient command and control approach will better survive and respond to the demands of hostile activities. The characteristics of the cyberspace environment infer some particular challenges for traditional models of command and control.

4.9. An adversary may conduct cyberattacks against all the elements of national power.[50] Command and control structures must not only support cross-government and industry working, but they must also be integrated into the UK's whole of society approach to cyber.

4.10. The UK's *National Cyber Strategy 2022*[51] sets out our intention to secure advantage in cyberspace by exploiting opportunities to gather intelligence and intervening as necessary against adversaries. Commanders should consider cyberspace to be an area for intelligence collection and analysis in its own right, particularly open-source intelligence.

4.11. Cyber activity cannot be dealt with by Defence, or any one government department, business or agency alone. Each has their own specific responsibilities and expertise. Defence's first responsibility is to protect its own digital systems and networks so that it can continue to deliver its outputs. An equally important responsibility is to interoperate our cyber capabilities with those of other government departments, particularly the National Cyber Security Centre (NCSC) and the National Cyber Force (NCF). Only in this way will Defence make an integrated strategic contribution to national security objectives.

4.12. **Government cyber activities.** The *National Cyber Strategy 2022* provides the strategic framework for all UK government activity on cybersecurity and makes it clear that this will be a whole of society endeavour. Government, business, the public and international partners all have a part to play because a broad approach to cyber activity is required. Unlike in maritime, land, air and space operational domains, the Ministry of Defence (MOD) does not lead the defence of 'UK cyberspace'. Protecting UK and other

[49] Joint Concept Note 2/17, *Future of Command and Control*.
[50] The instruments of national power are diplomatic, information, military and economic.
[51] HM Government, *National Cyber Strategy 2022*.

states' critical national infrastructure, as well as providing advice to the public and industry, is a matter for other government departments and agencies. Important wider UK government organisations are identified below.

a. **Cabinet Office.** The Cabinet Office is the central coordinating organisation for UK government cyber activity. It is the home to the Government Cyber Coordination Centre, a command and control hub for major, and critical national infrastructure related, cyber incident management. The Government Cyber Coordination Centre is a joint venture between the Government Security Group, the Central Digital and Data Office and the NCSC.

b. **Government Communications Headquarters.** Government Communications Headquarters (GCHQ) works in partnership with other government departments to protect UK national interests. Director GCHQ reports to the Secretary of State for Foreign, Commonwealth and Development Affairs. GCHQ's primary customers are the MOD, the Foreign, Commonwealth and Development Office and law enforcement agencies.

© ABCDstock / Shutterstock.com

Critical national infrastructure related cyber incidents are managed by the Cabinet Office's Government Cyber Coordination Centre

c. **National Cyber Security Centre.** The NCSC was formed in 2016 and subsumed previously established organisations including CESG, the Centre for Cyber Assessment, CERT-UK and the Centre for Protection of National Infrastructure. The NCSC is a division of GCHQ which gives it powerful access to indicators and warnings of potential cyber incidents. The NCSC provides a single point of contact for business, public sector organisations and the general public. The NCSC provides best practice guidance, alerts and warns of, responds to and manages cybersecurity incidents. It helps to develop the UK's cybersecurity profession and industry capability, and secures some public and private sector networks. The NCSC also provides a technical lead in key areas such as cryptography.

d. **National Crime Agency.** The National Crime Agency aims to prevent cybercrime and make the UK a safer place to do business. Legacy organisations which have been incorporated into the National Crime Agency are the National Cyber Crime Unit, Police e-Crime Unit and the Serious Organised Crime Agency. The National Crime Agency's National Cyber Crime Unit provides national leadership and coordination of the response to cybercrime, supported by a network of dedicated Regional Cyber Crime Units in each of England and Wales' nine police regions, in partnership with their counterparts in Police Scotland and Police Service of Northern Ireland, as well as the Metropolitan Police Service's Cyber Crime Unit.

e. **UK Cyber Security Council.** The UK Cyber Security Council launched in March 2021 and is a world first for the cybersecurity profession. Its mission is to be the voice of the profession, bringing clarity and structure to the growing cyber workforce and the range of qualifications, certifications and degrees that exist across the field.

4.13. **Industry.** The UK Cyber Security Information Sharing Partnership (CiSP)[52] has been developed to exchange cyber threat information in real time, in a secure, confidential and dynamic environment. CiSP is a joint industry and government initiative set up to increase situational awareness and reduce impacts on UK business. The Defence Cyber Protection Partnership will raise awareness and improve understanding of the cybersecurity risks with Defence's supply chain partners. These partnerships highlight the need for protective measures to increase the security of the wider Defence supply chain and enforce an approach to implement minimum cybersecurity standards.

[52] NCSC, 'Cybersecurity Information Sharing Partnership'.

4.14. **Military cyber activity.** Strategic Command (UKStratCom) has the Defence lead for cyber activity and capability development. Within the 4* UKStratCom Headquarters are a series of small teams that lead and cohere domain development activities, for example, within the command force development, human resources and the capability areas. However, operational cyber activity is conducted through subordinate commands within UKStratCom, partners across government and the single Services.

a. **National Cyber Force.** The NCF is a joint venture between Defence, and the UK intelligence community and brings together uniformed and civilian personnel. The NCF's mission is to keep the country safe and to protect and promote the UK's interests at home and abroad. It is responsible for operating in and through cyberspace to counter, disrupt, degrade and contest those who would do harm to the UK or its allies (activity commonly referred to as offensive cyber operations). NCF operations are conducted in line with well-established legal frameworks. The UK has made it clear that it develops and deploys cyber capabilities in accordance with international law, including the law of armed conflict where applicable. NCF activities are subject to ministerial approval, judicial oversight and parliamentary review, making the UK's governance regime for cyber operations one of the strongest in the world.

b. **Defence Digital.** Defence Digital, led by the 3* Chief Information Officer, has the responsibility for cybersecurity, resilience and defensive cyber operations across Defence. Defence Digital works closely with defence industry partners to secure and protect Defence's digital systems, corporate information technology and military communication and information systems. Defensive cyber operations are led by the 2* Defence Digital Operations Headquarters at Corsham and are conducted by the Cyber Security Operating Capability (CSOC), a federation of cyber defence teams spread across the front line commands and Reserve forces. Defence Digital works with the NCSC and the Cabinet Office to provide support across government and routinely cooperates with allied cyber organisations.

c. **MOD Computer Emergency Response Team.** The MOD Computer Emergency Response Team (CERT) is responsible for warning and reporting on cyber vulnerabilities and incidents on both fixed and deployed networks. It is a subordinate organisation within the Cyber Security Operating Capability.

d. **Defence Intelligence.** Defence Intelligence provides timely intelligence products, assessments and advice to: guide decisions on policy and the commitment and employment of our Armed Forces; inform Defence research and equipment programmes; and support military operations. The 2* Director Cyber, Intelligence, Information and Integration (DCI3) is responsible for cyber and intelligence. DCI3 is the 3* Chief of Defence Intelligence's (CDI's) lead for cyber and provides routine engagement and oversight of the NCF on behalf of CDI, and the Cyber Joint User. Defence Intelligence also includes the Joint Cyber and Electromagnetic Activities Group that has a coordination, facilitation and support role.

e. **Joint User Intelligence and Cyber.** The 1* Joint User Intelligence and Cyber is responsible for the unified authority that sets the requirement, assures delivery and prioritises the deployment of joint intelligence and cyber capabilities across Defence. This ranges from setting strategic intelligence and cyber policy for MOD, to the delivery of operationally focused joint intelligence and cyber capabilities to the single Services and the Permanent Joint Headquarters.

f. **Single Services.** The Royal Navy, British Army and Royal Air Force operate cyber information security operations centres which provide a range of defensive capabilities to their respective areas of responsibility. Additionally, the single Services also operate their own cyber protection teams who have responsibility for protecting mission critical assets.

Personnel integration

4.15. **Headquarters staff.** At every level of headquarters, military operational planners and those responsible for targeting must become cyber-literate and understand Defence's cyber capabilities, limitations and have access to legal advice. They may well need continuous access to subject matter experts; these may be provided on a similar basis to legal advisers and policy adviser roles either through permanent staff posts or liaison officers from the key organisations described in the previous paragraph.

4.16. **Cyber operators.** Cyber operators need current, expert knowledge of a range of computing technologies, including operating systems and applications. Many will therefore have some background in computing or information systems management trades and branches of the Armed Forces, but it is not essential. Cyber aptitude exists across the Armed Forces and Civil

Service; anyone can take the cyber aptitude test, which may lead to a place on the Defence cyber training pathway.

4.17. **Deep specialists.** Defence's deep specialist cyber resources are centrally managed by UKStratCom under the Unified Career Management (UCM) model, irrespective of their parent Service. This affords opportunity for career progression and the award of retention benefits within the cyber trade or profession. UCM(Cyber) is managed in consultation with the single Services and civilian agencies.

4.18. **Resourcing.** Cyber skills are in great demand across government and the private sector. A flexible approach to workforce resourcing is essential to deliver the necessary capacity and depth of skills Defence needs. Teams of cyber specialists will operate at different levels, have varying skill sets and be in geographically dispersed units. People may be sourced from:

- the Armed Forces and MOD Civil Service (internal transfers or through external recruitment);
- externally trained and experienced personnel (for example, in the Joint Cyber Reserves);
- secondments from relevant civilian companies; and
- through service level agreements with specialist contractors.

© Mathias Kniepeiss / Getty Images

A flexible approach to workforce resourcing is essential

Operating in cyberspace

4.19. **Defensive preparedness.** All personnel working with information communication technology need to have the confidence to recognise, respond to and recover from cyberattacks. Policies and practices in accordance with Joint Service Publication 440, *The Defence Manual of Security* need to be developed and rehearsed to manage our activities.

a. **Systems security.** Using appropriate warning systems, up-to-date antivirus software and continuous 'patching' (updating) of operating systems/applications is the most common and effective form of preparedness. Similarly, educating and training operators will ensure they are aware of, and prepared for, the latest forms of attack. All personnel should be continuously asking themselves what their alternatives are if their computer systems fail. We all must, therefore, understand and practise system recovery and business continuity plans. It is crucial that when planning against cyberattacks a wider, systems view is taken of potential problems and their solutions. For example, there is little value in protecting a critical computer controlling the fuel pump to the ship's engines if the logistics systems are attacked to provide false fuel states. The entire system needs to be protected.

b. **Security personnel.** Operators of a computer system may not be best placed to apply cybersecurity to that system. Key security personnel (identified in advance) should be on a readiness rota. They should maintain links to the appropriate security procedures and teams (for example, CERTs and the warning advice and reporting points). It is not uncommon to need to contact manufacturers or suppliers of a computer system when a cyberattack occurs. Contact lists should be maintained and the process tested. Again, business continuity plans must be maintained and practised.

c. **Recovering from malware attacks.** Malware is notorious for remaining in a system even though it appears to have been removed. Thorough cleansing is often a matter of opinion of the operators rather than a proven fact. Maintaining and installing verifiably clean backups, held off-site in a secure location, should be practised as part of normal operations and exercising. Attacks, and suspected attacks, should always be reported through the local chain of command.

4.20. **Exercising the capability.** Cyber activity needs to be exercised in the mainstream along with other capabilities so that users can develop understanding and resilience. Frequent, detailed and well-rehearsed actions in response to cyberattack will be exercised within the Defence Exercise Plan, managed by UKStratCom. Appropriate scenarios and practises for each level of command will differ and may change rapidly in line with the threat. Cyber response activity will need to be undertaken at all levels of training (individual, collective and joint). There will also be education as well as training aspects to this requirement. Cyber-related scenarios and injects are already being incorporated into joint exercises as well as those of the North Atlantic Treaty Organization and allies. In addition, specialist cyber units are involved in exercises with partner nations and allies, for example, Exercise Locked Shields and Exercise Cyber Flag.

4.21. **Business continuity.** Business continuity means being resilient and maintaining outputs or services through any given kind of cyber incident – malicious or otherwise. By developing a plan based on risk, resilience, impact and interdependency assessments, the effects of any loss of service can be mitigated. Operators need to be made aware of which systems and, more importantly, what information/data is critical at which times during operations. When considering business continuity plans, the following questions should be considered.

- Where does the priority lie in maintaining system availability?
- What is the impact of system loss?
- Who do I need to notify if I intend to close a system – or continue running it with known or even unknown faults?
- How is risk measured and managed and at what levels of command do various responsibilities lie?
- What is the recovery plan?
- Is it frequently exercised using only backup hardware, applications and data?

Notes

Lexicon

Section 1 – Acronyms and abbreviations

AJP	Allied joint publication
APT	advanced persistent threat
CDI	Chief of Defence Intelligence
CERT	computer emergency response team
CiSP	Cyber Security Information Sharing Partnership
CNI	critical national infrastructure
COED	Concise Oxford English Dictionary
CSOC	Cyber Security Operations Centre
DCDC	Development, Concepts and Doctrine Centre
DCI3	Director Cyber, Intelligence, Information and Integration
DVD	digital versatile disc
GCHQ	Government Communications Headquarters
GDPR	General Data Protection Regulation
HM	His Majesty
IPE	intelligence preparation of the environment
JDP	joint doctrine publication
JSP	joint Service publication
malware	malicious software
MC	Military Committee
MOD	Ministry of Defence
NATO	North Atlantic Treaty Organization
NCF	National Cyber Force
NCSC	National Cyber Security Centre
NHS	National Health Service
NIST	National Institute of Standards and Technology

PED	portable electronic device
SCEPVA	Sovereign Cyber Effects Provided Voluntarily by Allies
SMS	short message service
SPOC	Single Point Of Contact
SSL	secure socket layer
UCM	Unified Career Management
UK	United Kingdom
UKStratCom	Strategic Command
US	United States
USB	universal serial bus
VPN	virtual private network

Section 2 – Terms and definitions

This section includes endorsed doctrinal definitions along with other terms readers of this publication may find useful.

backdoor
A backdoor is a tool installed after a compromise to give an attacker easier access to the compromised system around any security mechanisms that are in place. (SANS Institute)

botnet
A network of private computers infected with malicious software and controlled as a group without the owners' knowledge. (COED)

cyber
Relating to information technology, the Internet and virtual reality.
(*Concise Oxford English Dictionary*, 12th Edition, 2011)

cyber and electromagnetic domain
A domain comprising of capabilities which enable activities that maintain freedom of action by creating effects in and through cyberspace and the electromagnetic spectrum. (JDP 0-50, 2nd Edition draft)

cyberspace
The global environment consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data. (JDP 0-50, 2nd Edition draft)

defensive cyber operations
Active and passive measures taken to prevent, nullify or reduce the effectiveness of adversary actions to preserve our freedom of action in or through cyberspace. (JDP 0-50, 2nd Edition draft)

distributed denial of service attack
Distributed denial of service attack seeks to overload a service, usually web-based, by repeatedly sending requests for information or messages many times a second. These attacks prevent legitimate users from accessing the service. Distributed denial of service attack uses multiple PCs to launch the attack, which increases the disruption, and attackers usually make use of a botnet. (CSOC)

electromagnetic operations
All operations that shape or exploit the electromagnetic environment, or use it for attack or defence including the use of the electromagnetic environment to support operations in all other operational environments. (NATOterm) Note: Electromagnetic operations include (but are not limited to) electromagnetic warfare, signals intelligence, intelligence, surveillance, target acquisition and reconnaissance, navigation warfare, battlespace spectrum management.

electromagnetic spectrum
The entire and orderly distribution of electromagnetic waves according to their frequency or wavelength.
Note: the electromagnetic spectrum includes radio waves, microwaves, heat radiation, visible light, ultraviolet radiation, x-rays, electromagnetic cosmic rays and gamma rays. (NATOTerm)

electromagnetic warfare
Military action that exploits electromagnetic energy to provide situational awareness and create offensive and defensive effects. (NATOTerm)

firewall
A part of a computer system or network which is designed to block unauthorised access while permitting outward communication. (COED)

information operations
A staff function to analyze, plan, assess and integrate information activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and audiences in support of mission objectives. (NATOTerm)

measurement and signature intelligence
Intelligence derived from the scientific and technical analysis of data obtained from sensing instruments for the purpose of identifying any distinctive features associated with the source, emitter or sender, to facilitate the latter's measurement and identification. (NATOTerm)

mission assurance
A process to protect or ensure the continued function and resilience of capabilities and assets, critical to the execution of mission-essential functions in any operating environment or condition. (NATOTerm)

offensive cyber operations
Activities that project power to achieve military objectives in or through cyberspace. (JDP 0-01.1)

operational domain
A specified sphere of capabilities and activities that can be applied within an engagement space. (NATOTerm)

operations security
All measures taken to give a military operation or exercise appropriate security, using passive or active means, to deny an adversary knowledge of the essential elements of friendly information or indicators thereof. (NATOTerm)

rootkit
A rootkit is a collection of tools used to hide the presence of malware or obtain privileged access to a computer, sometimes using a 'backdoor' (covert means of access). The computer's operating system may show no sign of the rootkit and it can go undetected for long periods – even indefinitely. Perpetrators can use their privileged access to conduct other malicious activity, extract data or attack other machines. (Description for this Cyber Primer)

signals intelligence
Intelligence derived from electromagnetic signals or emissions. (NATOTerm)
Notes: The main subcategories of signals intelligence are communications intelligence and electromagnetic intelligence.

situational awareness
The knowledge of the elements in the battlespace necessary to make well-informed decisions. (NATOTerm)

spear phishing
Spear phishing is a form of phishing that is aimed at a specific target audience and worded in such a way as to appeal to that audience. Although this requires more effort and knowledge about who is being targeted, spear phishing is more likely to be successful and users find it harder to detect. (Description taken from MOD e-learning for this *Cyber Primer*)

zero-day
Recently discovered vulnerabilities (or bugs), not yet known to vendors or antivirus companies, that hackers can exploit. (NCSC)

Resources

HM Government, *Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy*, 2022
This policy describes how, in a competitive age, we need the structures in place so we can react quickly and effectively to new and evolving threats to our security.

HM Government, *National Cyber Strategy 2022*
This strategy seeks to secure national advantage in cyberspace by exploiting opportunities across the whole of society as well as to gather intelligence and intervene against adversaries.

HM Government, *Government Cyber Security Strategy 2022–2030*
This strategy sets out the government's approach to building a cyber resilient public sector.

Ministry of Defence, *Cyber Resilience Strategy for Defence*
This provides a focused approach to cyber, ensuring the resilience of the MOD's vital networks and placing cyber at the heart of Defence operations, doctrine and training.

JSP 440, *The Defence Manual of Security*
This publication contains policy and guidance relating to communications and information communication technology security. (Not available externally)

AJP-3.20, *Allied Joint Doctrine for Cyberspace Operations,* Edition A Version 1
This is NATO's doctrine to plan, execute and assess cyberspace operations in the context of Allied joint operations.

JSP 383, *Joint Service Manual of the Law of Armed Conflict*
This publication is a reference for members of the UK Armed Forces and officials within the MOD and other government departments. It is intended to enable all concerned to apply the law of armed conflict when conducting operations and when training or planning for them.

Cyber Security Information Sharing Partnership

This is a joint, collaborative initiative between industry and UK government to share cyber threat and vulnerability information to increase overall situational awareness of the cyber threat and therefore identify the risks to reduce the impact on UK business.

Defence Cyber Protection Partnership

This partnership between Defence and industry aims to meet the emerging threat to the Defence supply chain by increasing awareness of cyber risks, sharing threat intelligence, and defining approaches to cybersecurity standards.

The CNI Hub

The CNI Hub provides advice, guidance and content aimed at those with an interest in securing UK critical national infrastructure.

Get Safe Online

Get Safe Online is the UK's leading internet safety website providing practical advice on how to protect yourself, your computers and mobiles device and your business against fraud, identity theft, viruses and many other problems encountered online. It contains guidance on many other related subjects too – including performing backups and how to avoid theft or loss of your computer, smartphone or tablet.

Cyber Aware

This is the government's campaign run by the NCSC to change the way people view online safety and provide the public and business with the skills and knowledge they need to take control of their cybersecurity.

Cyber First

Cyber First is a programme of opportunities helping young people explore their passion for technology by introducing them to the world of cybersecurity. It covers a broad range of activities: comprehensive undergraduate bursary and apprenticeship schemes; a girls only competition; and a series of summer and autumn development courses either online or at UK universities and colleges.

NIST Cybersecurity Framework

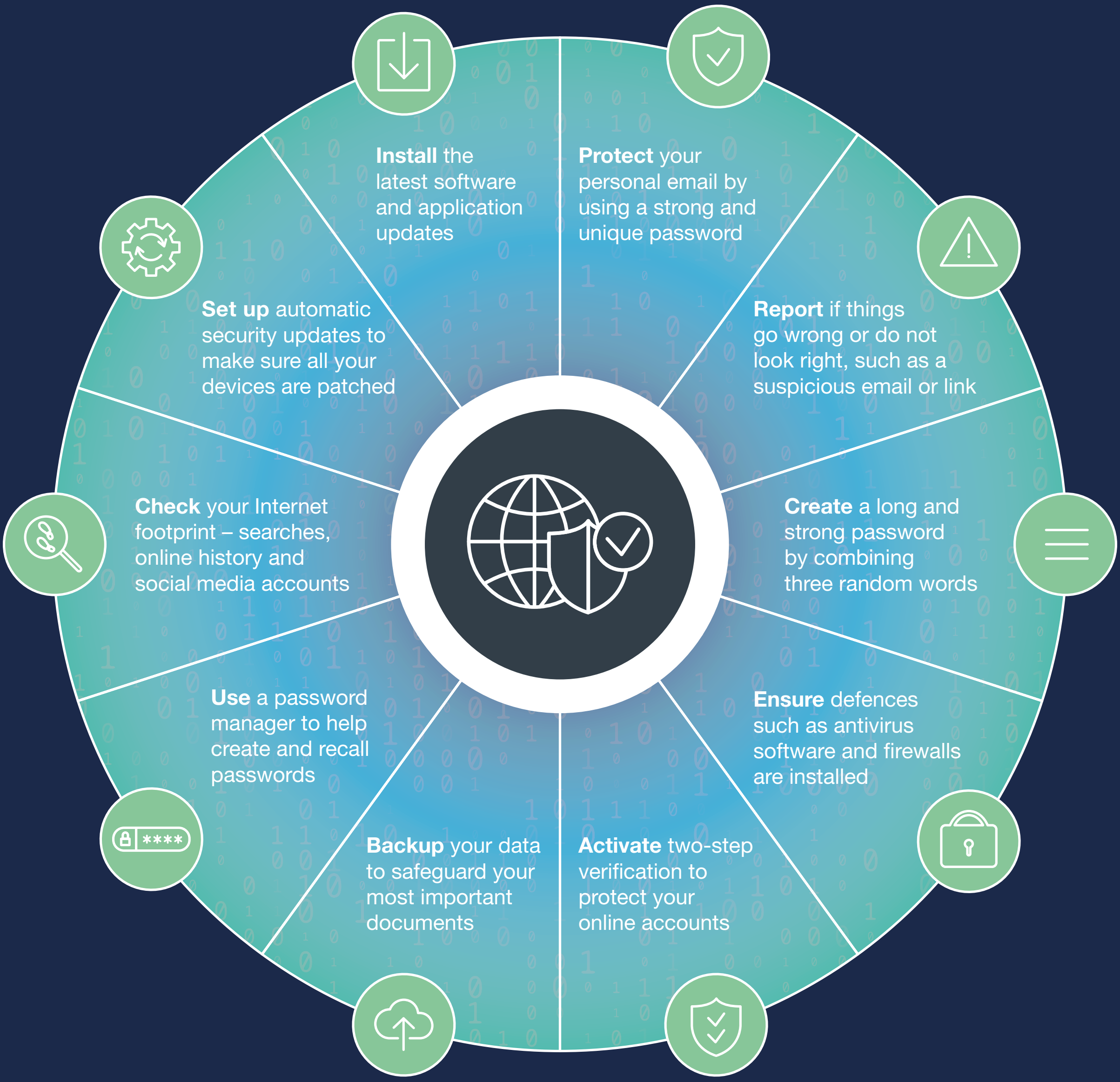
The United States Government National Institute for Standards and Technology has developed an influential framework for cybersecurity.

SANS Institute Centre for Internet Security Controls

This resource provides those with a formal remit to operate the MOD's networks, or connect to them, with security advice.

All personnel share the responsibility of protecting Defence's cybersecurity as well as protecting ourselves in cyberspace.

10 top tips for staying secure online



Install the latest software and application updates

Protect your personal email by using a strong and unique password

Report if things go wrong or do not look right, such as a suspicious email or link

Create a long and strong password by combining three random words

Ensure defences such as antivirus software and firewalls are installed

Activate two-step verification to protect your online accounts

Backup your data to safeguard your most important documents

Use a password manager to help create and recall passwords

Check your Internet footprint – searches, online history and social media accounts

Set up automatic security updates to make sure all your devices are patched

The above tips are based on advice and guidance published by the National Cyber Security Centre and the Cyber Confident Awareness Campaign.

Designed by the Development, Concepts and Doctrine Centre

Published by the Ministry of Defence
This publication is also available at www.gov.uk/mod/dcdc