Ministry
of Defence

Cyber Primer

Second Edition

Development, Concepts and Doctrine Centre

Ministry of Defence's cyber good practice guide to protecting yourself in cyberspace

1. We are all personally responsible for protecting Defence assets, and information is one of our key assets.
   Report any concerns immediately.

2. If you think an email is suspicious, forward it as an attachment to SPOC-Spam and delete from your inbox using Shift-Del. If you think you have opened something by mistake, then report it at once.
   Never reply to spam email.

3. If unsure, don't click on any links or open attachments.
   Use Favourites for websites you visit often.

4. Be alert to potential targeting by social engineers and report any concerns immediately.

5. Think before you share online – including posting on social media sites – are you giving away information which could impact on personal or operational security, or could be used by a social engineer?

6. Never give sensitive information unless you are sure the recipient is who they say they are and has a valid need to know.

7. Protect passwords – never share them or leave them where they can be found. Don't make them easily guessable, or use the same password for different applications.

8. Don't plug anything into the USB ports of military IT systems including DII, not even to charge them, except for officially – procured MOD USB devices. If you find any unaccounted for USB devices in your workplace you should hand them to your Security Officer.

9. Keep your anti-virus up to date at home so that it can help reduce the risk of downloading malware.

**Remember that however well protected you are,
nothing can guard against every threat – so be vigilant.**

Cyber Primer

The Cyber Primer (2nd Edition), dated July 2016, 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 send them to:

The Development, Concepts and Doctrine Centre
Ministry of Defence Shrivenham
SWINDON,
Wiltshire, SN6 8RF

Telephone:	01793 31 4216/4217/4220
Military network:	96161 4216/4217/4220
E-mail:	DCDC-DocEds@mod.uk

Distribution

The distribution of the Cyber Primer (2nd Edition) is managed by the Forms and Publications Section, LCSLS Headquarters and Operations Centre, C16 Site, Ploughley Road, Arncott, Bicester, OX25 1LP. All of our other publications, including a regularly updated DCDC Publications Disk, can also be demanded from the LCSLS Operations Centre.

LCSLS Help Desk:	01869 256197
Military Network:	94240 2197

Our publications are available to view and download on the Defence Intranet (RLI) at: http://defenceintranet.diif.r.mil.uk/Organisations/Orgs/JFC/Organisations/Orgs/DCDC

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

Preface

> 'The Government will ensure that our Armed Forces have strong cyber defences, and that in the event of a significant cyber incident in the UK, they are ready to provide assistance. We will provide the Armed Forces with advanced offensive cyber capabilities, drawing on the National Offensive Cyber Programme which is run in partnership between the MOD and GCHQ. We will continue to help NATO and other allies to protect their networks using our intelligence and technical insights, and we will use our advanced capabilities to enable the success of coalition operations.'

National Security Strategy and
Strategic Defence and Security Review 2015

This *Cyber Primer* introduces you to the subject of cyber, particularly in a Defence context, but also in your life at work and home. It is also a good foundation to reading the UK's cyber doctrine.

The primer is divided into four chapters. The first chapter is structured around the fundamentals of cyber and its relevance for Defence. We explore the boundaries of cyber and cyberspace, introduce you to the essential terms and definitions used and look at the important role Defence personnel play in cyber. The second chapter covers threats from cyber; their characteristics; threat actors; the characteristics of a cyber attack; and a description of the tools and techniques used. The third chapter of the primer looks at the four cyber operations roles: defensive cyber operations; cyber intelligence, surveillance and reconnaissance; offensive cyber operations; and cyber operational preparation of the environment. Finally, the fourth chapter looks at how cyber is integrated, synchronised into military operations and provides some detail concerning cyber command and control.

Cyber and cyberspace are full of opportunities for improving the way we work and live, but they also introduce new hazards of which you need to be aware. A brief lexicon of cyber terms can be found at the back of this publication, along with useful links to resource documents which will give you greater awareness of the subject.

Finally, the Ministry of Defence's (MOD's) cyber good practice guide to protecting yourself in cyberspace is included inside the front cover and on the back cover.

Note

The examples and case studies included in this primer contain reports selected from various external sources. All of this information is publicly available online and provided for situational awareness and understanding only. The views and opinions expressed do not reflect those of the 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.

Contents

Chapter 1

“In the information age almost all acts of physical violence come with an on-line component, exploiting social networks to manipulate opinion and perception. The tactics employed by Russia in Ukraine, Estonia and Georgia for example, include combinations of information warfare, cyber activity, counter-intelligence, espionage, economic warfare and the sponsorship of proxies.”

Chief of the Defence Staff
RUSI, December 2015

Chapter 1 – Fundamentals of cyber

This chapter discusses cyberspace as an operating environment and includes information on the legal aspects for military operations in cyberspace.[1]

Cyber is vital to our national security, playing an integral role in protecting the UK against external and internal threats and acting as a deterrence. Cyber cannot be dealt with by one government department or agency alone, each will have their own experiences and expertise. Cyber security is also vital to Defence as our Armed Forces depend on 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.

The impact of cyber activities on military activity requires all personnel to understand the depth of our dependence on it. This chapter provides some essential definitions related to cyberspace and highlights the nature of cyber and its role in Defence.

Cyber definitions

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

cyber
To operate and project power in and from cyberspace to influence the behaviour of people or the course of events.

cyberspace
An operating environment consisting of the interdependent network of digital technology infrastructures (including platforms, the Internet, telecommunications networks, computer systems, as well as embedded processors and controllers), and the data therein spanning the physical, virtual and cognitive domains.

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

National context

1.2. In November 2015 the UK's *National Security Strategy and Strategic Defence and Security Review 2015*[2] identified three core strategic objectives. These are to:

- protect our people – at home, in our Overseas Territories and abroad, and to protect our territory, economic security, infrastructure and way of life;

- project our global influence – reducing the likelihood of threats materialising and affecting the UK, our interests, and those of our allies and partners; and

- promote our prosperity – seizing opportunities, working innovatively and supporting UK industry.

1.3. The UK's cyber capability supports these three strategic objectives through three core functions. These are:

- preventing conflict and threats materialising;

- protecting the UK and its Overseas Territories from attack, particularly (but not exclusively) in, and through, cyberspace; and

- projecting influence and power rapidly and responsively, either directly from the UK or as part of an expeditionary operation.

Defence supports these three strategic objectives by ensuring that our UK Armed Forces:

- have strong cyber defences;

- are able to project power in cyberspace (just as they do in the other operating environments);

[2] *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*, November 2015.

- are ready to assist the wider UK in the event of a significant cyber incident; and

- can respond to a cyber attack as they would respond to any other attack – using whichever capability is most appropriate.

1.4. Defence's ability to conduct protective operations in cyberspace is mission critical, demands resilience and enables information superiority. Our adversaries will contest our freedom of manoeuvre in cyberspace, so we need to have agile capabilities that can anticipate, deter, prevent, detect, assess, protect, respond to and recover from attacks against our networks.

1.5. Cyber can also act as an information source in its own right. Information gained from cyber can be used to strengthen our own cyber defences, but can also form the basis of intelligence analysis.

1.6. Defence's activities in cyberspace are constantly being transformed. To defend itself, Defence needs to ensure existing security policies are enforced and, where risk is held, the full impact of that risk is completely understood. The basics of network defence go a long way in protecting Defence's data, but there will always be vulnerabilities.

1.7. Cyber is recognised as a capability that must be integrated with all areas of military planning, preparation activities and budgeting across the new *Defence Operating Model*.[3] A range of support and implementation is required, covering:

- research and development;

- training;

- procurement and through-life cost management of capabilities;

- fielding deployment of those capabilities; and

- eventual disposal.

[3] *How Defence Works: The Defence Operating Model*, December 2015.

Cyberspace

1.8. Cyberspace is a complex and dynamic environment, interdependent with the electromagnetic spectrum, and is key to all military operations on land, sea, and in air and space. It is far more than just the Internet. Cyberspace is a pervasive and all-encompassing operating environment, incorporating, for example, aircraft flight control systems, medical life-support systems, physical device controllers[4] and national electricity distribution systems. Cyberspace can also be less geographically constrained than other environments.[5] So, distance and reach must be viewed differently to traditional environments when considering cyberspace operations.

1.9. Access to cyberspace is possible via many means, most often through computer terminals, laptops, tablets and mobile phones. Connectivity may be achieved via wireless connections or physical cables. Cyberspace is dependent upon physical assets – power sources, cables, networks, data-centres, as well as the people who operate and manage them.

1.10. The technologies and systems that define and make up cyberspace have evolved from being enablers of modern life into being fundamental and critical to how we live. All aspects of modern society are influenced by information flows, making cyberspace an integral part of today's global environment. We now live in a digital world and have become familiar with smartphones, office and home computers, social media applications and email.

1.11. Most electronic control systems have cyber vulnerabilities, although not all are readily exploitable.[6] We would consider a short-term loss of the Internet or connectivity in our homes as an irritant; but someone hacking into our email account and stealing our personal information is more serious. A cyber attack leading to a prolonged loss of the electricity grid or Defence

[4] A device controller is a part of a computer system that makes sense of the signals going to, and coming from the central processing unit (CPU).

[5] Non-Internet facing devices and systems, for example, air-gapped adversary networks, distinct complex devices (remotely-piloted air systems, aircraft, closed networks) may have far greater geographical constraints.

[6] Such exploitation is normally via technical means, but it could equally be undertaken by human interference.

cyber and cyberspace-dependent capabilities,[7] on the other hand, could have severe consequences, including loss of life and could equate to a kinetic attack.

1.12. **Layers of cyberspace.** Cyberspace can be thought of as comprising of six interdependent layers: social; people; persona; information; network; persona; and real, as shown in Figure 1.1.

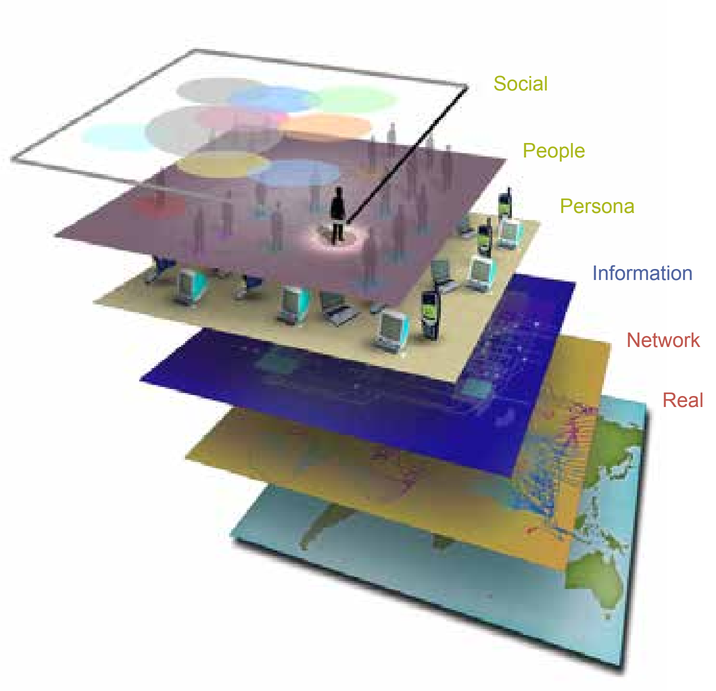


Figure 1.1 – The six layers of cyberspace

1.13. **Social, people and persona layers.** The social, people and persona layers consist of the details that connect people to cyberspace and the people and groups who interact with and operate the networks. Unique addresses or titles are matched to virtual addresses which, in turn, map to the real and network layers. A single person may have multiple personas; for example, a person may have different social media accounts accessed through different computers and mobile devices. Equally, multiple people

[7] Defence cyber capabilities can be a combination of hardware, firmware, software and operator action.

can share a single persona; for example, a multi-user single email account. Attributing responsibility and targeting in cyberspace is difficult; personas can be complex, with elements in many virtual locations and not linked to a single physical location or form. Significant intelligence collection and analysis capabilities are required to gain sufficient insight and situational awareness to enable effective targeting and to create the desired effect. The social, people and persona layers can be further analysed through four sub-areas: social networking; operating and maintenance procedures; people; and security.

a. Social networking. Social networking covers information regarding human interactions and may include details on culture, interests, how and with whom people communicate, and their persona or personas.

b. Operating and maintenance procedures. Operating procedures across the breadth of cyber operations include network monitoring, information assurance, disaster recovery, contingency and backup plans. Maintenance includes the skill levels of the personnel maintaining the network and the frequency of maintenance activity.

c. People. This refers to all individuals involved; including those developing and operating the various systems.

d. Security. Security includes the security posture of the network and levels of awareness of the network users, managers and maintainers.

1.14. Information layer. The information layer consists of the connections that exist between network nodes. A node is a physical device connected to a network, such as a computer, smartphone or other mobile device. It also includes:

- individual network configuration;

- data, applications and protocols which govern interaction across the physical layer;

- information assurance processes;

- details of communication service providers;
- transfer protocols;
- Internet domain names; and
- ownership data.

1.15. **Network layer.** The network layer uses logical constructs as the primary method of security (for example, information assurance) and integrity. This layer can often (but not exclusively) be the target for: signals intelligence; cyber intelligence, surveillance and reconnaissance; and measurement and signature intelligence.

1.16. **Real layer.** The real layer consists of a geographic aspect and a physical aspect. The geographic aspect relates to the location of elements of a network, such as under the sea or ground, or in a building. The physical aspect concerns what components are present – such as hardware, systems software and infrastructure.

The cyber operating environment

1.17. As a relatively new operating environment, Defence continues to develop the means by which to exploit cyberspace and the cyber operating environment to its best advantage. Cyberspace is even contested in peacetime – threat actors are constantly probing our networks seeking vulnerabilities, intelligence or military and commercial advantage.

1.18. The concept of **near**, **mid** and **far** operating spaces help explain the cyber environment and how it might affect operations.

a. **Near.** The near comprises networks and systems that are controlled and assured by the commander, or controlled and assured on their behalf by Defence.

b. **Mid.** The mid comprises networks and systems that are critical to the operation or campaign, but are not controlled and assured by the commander. They may be controlled and assured on their behalf by a third party – for example, a commercial company or other government department.

c. **Far.** The far comprises networks and systems that, if influenced, will prove critical to the operation or campaign. Such systems will be predominately outside friendly forces control or assurance and are likely to be owned by third parties.[8]

1.19. There are a number of themes which emerge when we consider the cyber environment. Some of these include the following.

a. The cyber operating environment is largely global, but vulnerable.

b. Civilian and military information infrastructures, whether national, coalition or international, co-exist and overlap, posing problems for managing security within a network-enabled Defence capability.

c. A high baseline for cyber security is required which has implications for education and training, timeliness of system maintenance and intelligence (cyber situational awareness).

d. The threat in, and through, cyberspace is largely, but not exclusively, against the exploitation, manipulation and theft of information held across the Defence enterprise (this includes close collaborative defence of its civilian procurement, logistics and other support contractors[9]).

[8] Systems owned by third parties are more vulnerable as they could be influenced by our adversaries.

[9] The likely interdependencies of critical information infrastructures mean that successful attacks may not only come from unexpected quarters, but also have unexpected impacts.

Mainstreaming, competencies, understanding and skills

1.20. **Mainstreaming.** 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. Cyber's pervasive and ubiquitous nature means Defence must consider the full range of cyber capabilities and requirements across the Defence Lines of Development. This requires awareness, education,[10] individual and collective training, exercises and an understanding of risk management in cyberspace.

1.21. **Competencies.** Cyber operations require well-educated and trained professionals with relevant capability and capacity, as well as specialist technical and tactical expertise for success. Additionally, personnel who understand human factors will have an important role. The Ministry of Defence's (MOD's) *Cyber Skills Functional Competence Framework* addresses these needs through the operational and planning/policy competencies relevant to military cyber operations. Competency is the combination of knowledge, skills and experience. The competency levels are:

- awareness;
- practitioner;
- senior practitioner; and
- expert.

1.22. **Understanding.** Defence cyber operations staff need a sound understanding of the commander's intent and must be able to rapidly assess the impact of their decisions or recommendations. They should, however, be aware that:

- decisions may often need to be made without the opportunity for referral upwards for guidance; and

[10] For example, the Defence Information Management Passport – information matters and the cyber awareness e-learning modules aimed at all personnel and the cyber operational awareness programme, which includes the cyber operations awareness core course (COACC) and the cyber operations enhanced course (COAEC) aimed at personnel in operational planning roles and key staff appointments.

- independent decisions may need to be made when it is necessary to maintain operational tempo and, where appropriate, authority for action has been delegated by the commander.

1.23. Skills. More generally, skills relevant to the cyber environment are articulated in the *Institute of Information Security Functional Skills Framework* and the MOD Information Assurance Portal provides additional reference material on information assurance and cyber related subjects.

Law applicable to cyber

1.24. There are a number of bodies of law which may be applicable to cyber activity. The applicable laws will depend on whether the activity is supporting military operations during peacetime (including training and testing) or an armed conflict. There are no international treaties specifically addressing cyber activity, but existing international law is applicable. UK cyber activities must follow international and domestic law. Legal support to military operations must include an operational understanding of the cyber activities, including intended effects and possible unintended consequences. More details on international law applicable to cyber activity can be found at Annex 1A.

International engagement

1.25. Collaboration with international partners is important to develop Defence's cyber capabilities. International engagement is managed by MOD's Cyber and Space Policy, which has close links with the Foreign and Commonwealth Office's International Cyber Policy Unit.

1.26. While broader Defence bilateral partnership objectives are a key factor, cyber engagement is principally driven by existing and anticipated military requirements, hence there is a strong allied relationship. The UK is a leading nation in North Atlantic Treaty Organization (NATO) on cyber, working to ensure that it secures its own networks and encouraging all partners to develop their own cyber capabilities.

1.27. Cyber brings additional complexities to the structures and processes of NATO, our allies and the European Union[11] through the need to include national organisations, such as computer emergency response teams (CERTs), and national and international legal requirements. Key organisations are listed below.

a. NATO Communications and Information Agency. The NATO Communications and Information (NCI) Agency manages those networks owned by NATO.[12] The NCI Agency also has a coordinating role across individual NATO and NATO-nation CERTs.

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

c. European Network Information Security Agency. This agency is the European Union focus for technical assistance with the security aspects of cyberspace.

Individual NATO nations have their own cyber command structures. In many cases, Defence has direct liaison with these. An example of this is the UK-France relationship where a formal bilateral arrangement exists.[13]

[11] Despite the UK's referendum on membership of the European Union, it still maintains obligations under the European Union until its formal exit.

[12] On 1 July 2012, the NATO Communications and Information Agency absorbed the NATO Command, Control and Communications Agency (NC3A).

[13] Underpinned by the UK-France 2* chaired Military Cyber Coordination Group.

Annex 1A – International law aspects

1A.1. **Unlawful intervention.** The customary international law principle of non-intervention prohibits states from intervening or interfering in the affairs of another state. The principle prohibits conduct that is coercive in character against affairs that a state should be permitted to decide freely, including the choice of political, economic, social and cultural systems and the formulation of foreign policy. A cyber operation which does not constitute a use of force or armed attack may nevertheless contravene the principle of non-intervention.

1A.2. **Countermeasures.** An internationally wrongful act committed by a state entitles the injured state to take proportionate countermeasures. Countermeasures are actions:

- in light of a refusal to remedy the wrongful act;
- directed against the other state to induce compliance with its obligations; and
- which are proportionate.

1A.3. **Principle of state responsibility.** The principle of state responsibility applies equally to cyber operations. If one state assists another state, the assisting state must consider the lawfulness of the other state's activity; if the assisting state would consider the act to be internationally unlawful, that state could be responsible in international law for that act.

1A.4. **Prohibition on the threat or use of force.** Article 2(4) of the United Nations Charter (which reflects customary international law) prohibits the threat or use of force. A cyber operation may constitute a use of force if it causes the same or similar effects as a kinetic attack.[14]

[14] Such as a sustained attack against the UK banking system, which could cause severe financial damage to the state leading to a worsening economic security situation for the population.

1A.5. **Armed attack.** Armed attack is not defined in international law, but it is generally accepted that it must be an act of armed force of sufficient gravity, having regard to its scale and effects. A cyber operation may constitute an armed attack if its method, gravity and intensity of force is such that its effects are equivalent to those achieved by a kinetic attack which would reach the level of an armed attack.

1A.6. **Self-defence.** The inherent right of individual and collective self-defence is customary international law and is also recognised by Article 51 of the United Nations Charter. An armed attack or imminent armed attack triggers the right of self-defence or anticipatory self-defence. Any response under self-defence must be necessary and proportionate; it must be necessary to use force to deal with the threat. Military action should only be used as a last resort and the force used must be proportionate to the threat and limited to what is necessary to deal with the threat. There may be practical challenges in the application of self-defence to cyber, for example:

- in attributing a cyber attack;

- the speed with which an attack can be conducted, which greatly reduces the ability to respond to an imminent attack;

- the use of spoofing and deception by an actor that implicates another; and

- the difficulty of determining the original intent of the perpetrator, even if actions are provable and actors identifiable.

1A.7. **Law of Armed Conflict.** Cyber operations conducted during an armed conflict to which the UK is a party, and which are related to that conflict, are governed by the existing rules of the Law of Armed Conflict (LOAC) including the prohibition on perfidy (inviting the confidence of an adversary as to protection under the LOAC) and principles of neutrality. Cyber operations that constitute a use of force during an armed conflict are subject to compliance with the following principles.

a. **Military necessity.** A state can only use that degree and kind of force, not otherwise prohibited by the LOAC, that is required to achieve the complete or partial submission of the enemy at the earliest possible moment with the minimum expenditure of life and resources.

b. Distinction. Attacks must only be directed against military objectives; civilians and civilian objects must not be attacked. Military objectives are those objects that by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage.[15]

c. Proportionality. An action is proportionate when it does not cause incidental civilian harm which is excessive in relation to the concrete and direct military advantage anticipated.

d. Humanity. The infliction of superfluous injury or unnecessary suffering is prohibited.

1A.8. Methods of war and protections. The laws governing means and methods of war and protections apply equally to cyber activity, as they would traditional methods of warfare. Two examples are listed below but they are not intended to be definitive of the applicable rules.

a. Acts or threats of violence with a primary purpose to spread terror among the civilian population are prohibited.

b. Attacks against installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations are prohibited if attacks may cause the release of dangerous forces and consequent severe losses among the civilian population. Other military objectives located at, or in the vicinity of, these works or installations shall not be made the object of attack if such an attack may cause the release of dangerous forces.

[15] Targeting can be challenging in cyber operations due to the potential dual use nature of some targets, such as infrastructure.

Notes

Chapter 2

> "We reserve the right to respond to a cyber attack in any way that we choose. And we are ensuring that we have at our disposal the tools and capabilities we need to respond as we need to protect this nation, in cyberspace just as in the physical realm. We are building our own offensive cyber capability – a dedicated ability to counter-attack in cyberspace."

Chancellor's speech to GCHQ
17 November 2015

Chapter 2 – Cyber threats

This chapter outlines the threats from cyberspace, including the range of threat actors, the characteristics of a cyber attack and the different tools and techniques used.

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 *National Security Strategy and Strategic Defence and Security Review 2015*[16] identifies cyber attacks on the UK as a 'Tier 1' threat – one of the UK's highest priorities for action.[17] Defence has no choice but to find ways to confront and overcome these threats if the UK is to flourish in an increasingly competitive and globalised world. An overview of the cyber threats to the UK can be found in *The UK Cyber Security Strategy*.[18]

2.2. The risk to national security and economic well-being includes the threat to public and private sector information communication technology (ICT). The digital architecture on which we now rely was built to be efficient and interoperable – security was given less consideration. Information theft or system disruption could have serious consequences on government, military, industrial and economic well-being. Cyberspace is permanently contested by our adversaries, who exploit areas such as:

- corrupting and stealing sensitive information;
- denying services on telecommunications, commercial databases and websites; and

[16] *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*, November 2015.
[17] Cyber attacks can be simple criminal activity on a large or small scale or the use of force equivalent to a kinetic attack.
[18] *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*. Due to be updated in 2016.

- damaging industrial control systems (ICS) such as supervisory control and data acquisition systems (SCADA); distributed control systems (DCS) and programmable logic controls (PLC).[19]

2.3. Evidence of cyber activity and an actor's will to use it against the UK can be challenging to source and even harder to attribute. Attribution is difficult not only due to the disparate and anonymous nature of cyberspace, but because it is not solely a technical problem – the problem spans technical/tactical (how), operational (what) and strategic levels (why).

2.4. Assessing the level of threat from and through cyberspace can be achieved by understanding the sum of the following three factors.

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.

c. Opportunity. Opportunity is the key variable in assessing threat as the opportunity to act can present itself in many guises and at any time. An adversary may also actively seek to generate their own opportunity to act, through a variety of influencing or shaping activities. Opportunities will be available through changes or variances in the environment, providing potential advantage to the adversary. An adversary could also drive friendly forces along a specific operational path resulting in potentially higher, repeatable risk. There may also be opportunities provided by friendly force activity more widely – their vulnerabilities provide avenues that threat actors can exploit to achieve their aims.

[19] Similar functionality to that of dedicated industrial control systems (ICS) can be provided through the use of embedded controllers or control software.

2.5. Cyber attacks can appear in many guises, without necessarily inflicting visible or tangible material damage and are more easily deniable by the perpetrator. All of this significantly increases the likelihood that an adversary may seek to create effects through cyberspace. Cyber attacks currently have a lower political and public perception of aggression when compared with more traditional and visibly damaging attacks where lives or property are obviously and physically threatened.[20] This is largely based on the fact that there have been no publicised, large-scale events (including the loss of life) that have been positively attributed to a cyber attack. Should such an event happen, this would likely change the public's perception to the potential 'aggressive' nature of cyber attacks; it is the effect that is important not the means of delivery.

Threat actors

2.6. 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 fall into six broad categories: nation states; terrorists; criminals; patriotic hackers; hacktivists; and insiders.[21] To some degree each category of threat actor is supported by the actions of hackers, who use their skills to adapt and exploit computer software and systems for purposes unintended by the original creators.[22] Each group's membership can vary greatly in terms of sophistication, scale and motive and may pose differing types of threat. At all levels, the actor's motivation is key, whether it is to:

- support national goals (either on behalf of, or directly for, a governmental body);
- generate income (either legitimately or through crime);
- improve personal technical skills; or
- support political ideals (hacktivisim).

[20] The majority of cyber 'attacks' are actually criminal acts.
[21] More information on these categories can be found from paragraph 2.8 onwards.
[22] Some hackers, such as the notorious hacker Kevin Mitnick, claim they are motivated by the challenge of hacking alone and do not seek financial gain or ideological advancement from their activities.

2.7. 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; and
- attacking military capabilities including command and control systems, logistical support and personnel.

2.8. 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. 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;
- deny the UK use of its cyberspace communications channels;
- 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.

The theft of personal data from the United States Office of Personnel Management shows the alleged use of cyber operations by a state.[23]

[23] Details on this case study can be found at Annex 2A on pages 36-37.

2.9. **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.

2.10. **Criminals.** Criminals target the information on Defence and industries' computer networks and online services for commercial gain (for example, contractual intelligence or intellectual property theft). They also target civilian and military personnel for fraud or identity theft. As government services and businesses transfer more of their operations online, the scope for potential targets will continue to grow. The impact that a cyber attack can have on e-commerce is illustrated by the drop in the Dow Jones Stock Exchange following false information concerning the President of the United States being posted in social media.[24]

2.11. **Patriotic hackers.** Patriotic hackers act upon states' behalf. 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.

The cyber attack against Estonia in 2007 shows the disruption that patriotic hackers can cause.[25]

2.12. **Hacktivists.** Hacktivists are groups or individuals who seek to gain unauthorised access to computer files or networks to further social or political ends.[26] They aim to:

- cause disruption, reputational, political and financial damage (for example, through releasing sensitive government information);

[24] More details on this case study can be found at Annex 2A on pages 38-39.
[25] More details on this case study can be found at Annex 2A on pages 40-41.
[26] Hacktivists, as with other threat actors, employ the skills of hackers.

- gain publicity by attacking public and private sector websites and online services; and
- exploit social media to further their cause.

The attacks against Georgian and Western websites on the outbreak of the Russian military incursion into Georgia is a good example of the damage that can be inflicted against a state by hacktivists.[27]

2.13. **Insiders.** 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 to Defence systems by ignoring or circumventing cyber security advice and procedures. The Bradley Manning, Edward Snowden and Jeffrey Paul Delisle cases show the threat posed by insiders.[28]

2.14. **Non-targeted threats.** 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 Conficker virus, which caused significant disruption to the Ministry of Defence's (MOD's) information and communication technology (ICT) system.[29]

Characteristics of cyber attacks

2.15. 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 media or getting local access to the system used by the target.

[27] More details on this example can be found at Annex 2A on pages 42-43.
[28] More details on these examples can be found at Annex 2A on page 44.
[29] More details on this example can be found at Annex 2A on pages 46-47.

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 anti-virus software. Adversaries will often delete or disguise evidence of their activities once the attack is complete.

d. **Effect.** The outcomes of a cyber attack may be physical, but the majority are created through the virtual and cognitive domains. Effects may vary depending upon the attacker's intent and nature of the payload. Effects may include the following.

i. Direct action on the target system – for example, a denial of service (DoS) where an attacker aims to make a service or network unavailable to its users by overloading it with repeated requests for information or messages.[30]

ii. Accessing a system, which not only gives the actor access to the information held by that system, but may also provide the means to investigate and exploit further onward connections.[31]

iii. Accessing a system that may enable an adversary to render equipment useless, thus denying Defence the capabilities it relies upon to accomplish its missions.

iv. Theft of data and/or altering of data – for example, password theft, data theft for reputational impact or loss of intellectual property and changing the integrity of databases

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

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

(such as financial, logistics, or personnel data) to provide false readings.

v. Changing the system's functionality – for example, changing permissions, controlling hardware (such as webcams) or implanting malicious programmes. Functionality changes may also allow onward connectivity to other, potentially more interesting and valuable, information.

Properties of cyber threats

2.16. Cyber offers additional vectors 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.[32] It enables access to targets spanning the tactical to strategic.

b. Asymmetric effect. Cyberspace is able to reach many organisations and specific individuals. 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 (for example, disrupting communication channels).

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. Non-attributable attacks increase uncertainty and potentially reduce political risk and the opportunity for retaliation.

[32] Cyber cannot truly be pervasive or borderless as not all devices are interconnected; some countries and geographical locations have limited to no cyber presence and are therefore difficult or impossible to effect with cyber capabilities.

The process of attribution can be difficult, which can make an actor's use of cyber attacks more easily deniable.

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

i. 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.

ii. 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.

e. **Versatility.** The impacts of some cyber attacks 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 cyber attack more politically and socially acceptable.

2.17. **Encryption.** The increasing and widespread use of complex encryption across multiple applications in cyberspace is one of the most concerning issues for intelligence and law enforcements agencies today. Once the preserve of states, 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 that enable activities such as command and control and financial transactions. The issue of the United States Federal Bureau of Investigation's attempts to force Apple to gain access to data held on Syed Rizwan Farook's (one of the San Bernardino shooters) iPhone is a good example of the increasing impact of encryption.[33]

[33] More detail on this case study can be found at Annex 2A on page 45.

Forms and techniques of a cyber attack

2.18. There are a number of forms of cyber attack which make up a cyber toolbox. A common feature is that the technical aspects of individual attacks frequently mutate on a daily basis.[34] The cyber toolbox includes (but is not limited to) social engineering, malware, local physical access and supply chain corruption.

2.19. Social engineering. Social engineering is the manipulation of individuals to carry out specific actions, or to divulge information. The information gained is frequently used as an enabler of cyber attacks. As the 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. Operations security is particularly susceptible to social engineering tools and techniques as these exploit knowledge at the personal level, such as personnel using Facebook while on operations, giving details of where they are and what they have been doing. This may mean our adversaries become aware of our activities, dispositions, intentions, capabilities and vulnerabilities. An example of social engineering would be the targeting of friends of Admiral James Stavridis (Commander United States European Command and Supreme Allied Commander Europe) via social media to collect personality information.[35]

2.20. Techniques. Social engineering is commonly used to enable the delivery of malicious software onto target systems. 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 the victim more likely to comply with any requests. Some of the most commonly used techniques are outlined on page 31.

[34] Mutations may be planned or unplanned; whether planned or not, some mutations may be controllable and others may not be.
[35] More details on this case study can be found at Annex 2A on pages 48-49.

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 in an email. It typically involves spoofing emails and/or directing users to enter details at a fake website whose look and feel are almost identical to the legitimate one.
Spear phishing	Spear phishing builds upon phishing but is targeted against an individual, organisation or business. Emails will often contain specific details or appear to originate from individuals or organisations that the target recognises to enhance their authenticity. Spear phishing attempts are not typically acts by random hackers, but 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.
Fake email	The victim is sent an email containing an attachment or an embedded link which they are persuaded to open. This in turn deploys malware or directs the victim to a bogus website. The more plausible the email, the more likely the victim will open the attachments or links.
Baiting	The attacker simply places removable media, such as CD-ROMs or USB memory sticks, in a target premises. The media may be labelled in such a way as to provoke interest, or 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.
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 credit card details.
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 web 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.

2.21. **Social media.** Significant data can be gathered and analysed from links made from social media applications. Technical collection of computer traffic patterns by third parties using commercially available software can provide information on location, strengths, movements of individuals and units, as well as morale and intentions.

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

- denial of service (DoS) intended to overload a system;
- 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 (DDoS) on everyone/everything you're connected to (for example, connecting to others using your address book);
- privilege escalation, where access is gained to a system and escalated to include the addition of admin/root privileges;
- keystroke logging – this uses a virus or physical device that logs a user's keystrokes as they type, compromising data, passwords and credit card numbers;
- geo-location of smartphones, tablets, laptops and similar devices; and
- exploiting social networks.

2.23. **Malware types.** Malware has traditionally been designed to infect computers and computer networks. However, the rapidly increasing popularity of smartphones, tablets and other Internet-enabled technology provides new and appealing targets for malware developers. Some malware combines attributes into so-called 'blended threats' that are becoming difficult to detect and remove. Some of the types of malware available are described on page 33.

Malware types	
Viruses	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. Viruses are normally spread by human interactions, inserting USB sticks or opening emails.
Worms	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 or commercial purposes.
Rootkits	A rootkit is a technique, or 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.
Botnets	Botnets (robotic network applications) are the most common form of malware. They are a collection of distributed malware-infected devices (bots), often home computers, used collectively under the command and control of an individual or group as an attack platform. Botnets use attack vectors such as spam and DDoS.
Trojan horse	A trojan horse (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.

2.24. **Access.** Access is crucial to the success of any cyber attack and can be obtained 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 ICT by installing software, such as keystroke loggers and remote access hardware to gain data from, or future access to, systems.

b. **Close access** is the ability to access to a computer or network from deployed platforms, people and equipment operating within the area of that network but do not have physical access. Typically this could be through use of the electromagnetic spectrum, such as connecting via Wi-Fi. Alternatively, close access can be achieved by an adversary through 'baiting'.[36]

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.

If we can reduce the opportunities of an adversary to access to our cyberspace, then we can mitigate the success of potential attacks.

2.25. **Advanced persistent threat.** An advanced persistent threat (APT) is a network attack in which an unauthorised person gains access to a network and stays there undetected for a long period of time. The intention of an advanced persistent threat attack is to steal data rather than to cause damage to the network or organisation.

2.26. **Supply chain corruption.** 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,

[36] For more information, see social engineering techniques described on page 31.

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.

Annex 2A – Threat actor case studies

Case study 1 – Cyber used for personal data theft

Theft of personal data – United States Office of Personnel Management	
Who	There has been no official attribution of those responsible, although General (Retired) James Clapper, the United States National Director for Intelligence, has been quoted as saying China remains the 'lead suspect'. According to the Wall Street Journal, United States government officials suspect that Chinese hackers perpetrated the breach. The Washington Post has also reported that the attack originated in China, citing unnamed government officials.
What	In 2015, the United States Office of Personnel Management (OPM) announced that it had been the target of two separate, but related, cyber security breaches. In the first event records of as many as four million people may have been compromised with personally identifiable information such as Social Security numbers, as well as names, dates and places of birth, and addresses being targeted. The data breach was noticed by the OPM in April 2015 and is believed to have started in March 2014, but may started even earlier. In the second event, identified in June 2015, OPM discovered that the background investigation records of current, former and prospective Federal employees and contractors had been stolen. The OPM and the interagency incident response concluded with high confidence that sensitive information, including the Social Security numbers of 21.5 million individuals, was stolen from the background investigation databases. This included 19.7 million individuals that applied for a background investigation, and 1.8 million non-applicants, primarily spouses or co-habitants of applicants. Some records also included findings from interviews conducted by background investigators and approximately 5.6 million include fingerprints and the usernames and passwords that background investigation applicants used to fill out their background investigation forms. The theft was more significant as this was the first event where physical data was stolen in the form of the 5.6 million sets of fingerprints. These breaches were described by Federal officials as among the largest breach of government data in the history of the United States.

Theft of personal data – United States Office of Personnel Management	
How	The United States Department of Homeland Security official Andy Ozment testified that the attackers had gained valid user credentials to the systems they were attacking, likely through social engineering. The breach also consisted of a malware package which installed itself within the OPM's network and established a backdoor. From there, attackers escalated their privileges to gain access to a wide range of OPM networks.
Against whom	The United States Office of Personnel Management.
Why	It is not clear what the motive behind the data theft was; however, although the ability to misuse fingerprint data is limited at this moment the possibility could change over time as technology evolves. China is widely suspected of being behind the breaches, perhaps as part of a move to build a massive database on United States nationals.
When	March 2014 – June 2015.
Impact	Breaches involving biometric data like fingerprints are particularly concerning to privacy experts because of their permanence: unlike passwords and even Social Security numbers, fingerprints cannot be changed.
More information	Numerous media outlets and cyber security forums carried news of the theft. A brief summary of the incident can be found on the OPM and Department of Defense websites: https://www.opm.gov/cybersecurity/cybersecurity-incidents/ and http://www.dodea.edu/opm-cybersecurity.cfm

© Shutterstock

Theodore Roosevelt Building
1900
E Street, NW
U.S. Office of Personnel Management

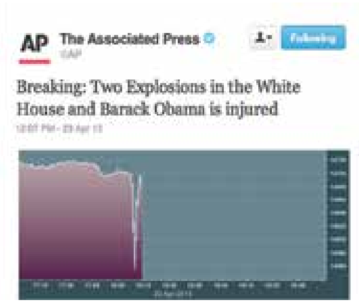
© Shutterstock

Case study 2 – Manipulation of e-commerce

The use of social media as a trusted source of 24-hour news was abused with a view to disrupting stock market activities globally through inserting false news feeds concerning the safety of the President of the United States.

Syria and US – conflict involving social media

Associated Press tweeted, 'breaking: two explosions in the White House and Barack Obama is injured'. The Dow Jones Stock Exchange dropped 70 points, although quickly recovered when the message was proved false. The Syrian Electronic Army hacktivist supporters of President Assad, claimed responsibility.



Breaking: Two Explosions in the White House and Barack Obama is injured

12:07 PM - 23 Apr 13

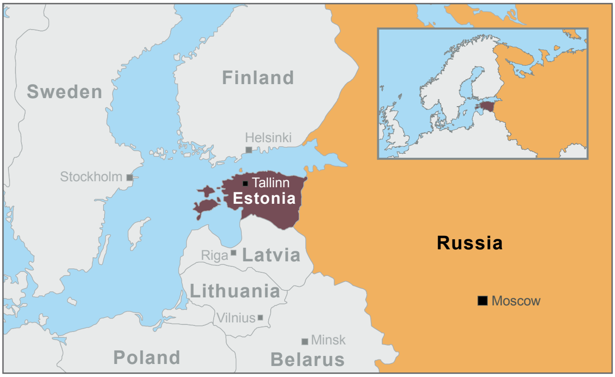
Syrian Electronic Army

Dow Jones movements

Using Twitter to manipulate politics and e-commerce	
Who	It appears to have been an alleged state-encouraged Syrian attack directed through Twitter at the United States political and economic stability. The Syrian Electronic Army have also reportedly attacked the al Jazeera news agency, Reuters and the BBC. Their most recent high profile attack (5 June 2015) was against the United States Army's public website.
What	Using fake Twitter accounts with a web-based interface, where the real Associated Press Twitter account uses the SociaFlow application.
How	Media reports that the fake account was initially taken as genuine by those who did not read or understand the process used by the Associated Press to broadcast news on Twitter.
Against whom	Main attack was against the Associated Press, causing reputational damage.
Why	The aim appears to have been to discredit the Associated Press and other news agencies which picked up the story as correct, without adequate authentication.
When	23 April 2013; previous attacks had occurred since April 2012.
Impact	Allegedly low impact to the Associated Press but high publicity value to Syrian Electronic Army and it disrupted the stock market. According to media reports, later attacks led to a degree of cooperation between the Syrian Electronic Army and Anonymous (a loosely associated international network of activists and hacktivists), although each has also reportedly attacked the other's websites. This attack emphasises the unreliability of uncorroborated stories broadcast on the Internet and the viability of news organisations as targets for hacktivists.
More information	A commentary on this specific attack is at: http://www.slashgear.com/twitter-and-syrian-electronic-army-go-to-battle-23278926/

Case study 3 – Cyber attack conducted by patriotic hackers

These attacks will often be carried out by hackers who believe they are supporting their government or culture. Such attacks may also be coordinated or directed by the state and the perpetrators may receive support on intelligence, information or technical tools and techniques from the state.



Estonia – a former member of the Union of Soviet Socialist Republics

The bronze soldier of Tallinn, Estonia – the perceived cause of the cyber attack

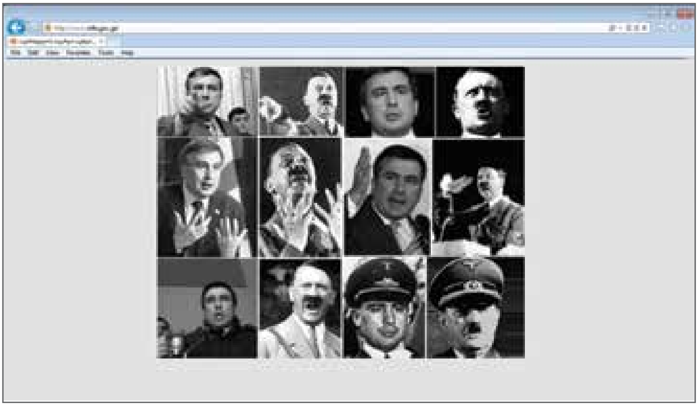
Cyber attacks against Estonian state infrastructure	
Who	Allegedly Russian patriotic hackers, although much broader groups including hackers and script kiddies (a person who uses existing computer scripts or codes to hack into computers, lacking the expertise to write their own) may have contributed.
What	Series of cyber attacks sustained over a three-week period, targeting websites of Estonian organisations.
How	Multiple denial of service and distributed denial of service against Estonian utilities, telecommunications and government facilities and their websites leaving them unworkable.
Against whom	Principally against Estonian electronic services but also impacted many European telecommunications providers and United States universities.
Why	The Estonian authorities relocated a Soviet-era war memorial from the centre of Tallinn to a war graves cemetery on the city outskirts. According to media reporting, Russia saw the war memorial relocation as an insult. Alleged Russian hacktivists then launched an economic cyber attack to attempt to coerce the Estonian government to return the memorial to the city centre.
When	It began on 27 April 2007 and lasted for three weeks. Media reports suggest that this could have resulted in fatalities if it had been conducted in the harsh Estonian winter.
Impact	Significant financial and social disruption in Estonia; but the biggest consequence was to put state-level cyber attacks on the NATO agenda. Over a three week period, confusion reigned in Estonia, NATO and the European Union over what the reaction should be to these attacks. Who was to blame? Could the perpetrators be firmly identified? How should attribution take place? Was retaliation a reality?
More information	Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia: https://www.ccdcoe.org/

Case study 4 – State-on-state cyber operations during periods of tension

These attacks have allegedly been used as a component of conventional military operations. In no cases have they been acknowledged as state actions but their use along with conventional operations, would strongly suggest that they are, or could be, a component of state military activity.

Russia
Black Sea
Georgia
Tbilisi
Kazakhstan
Caspian Sea
Azerbaijan
Armenia
Yerevan
Baku
Turkey
Iran

Georgia



Replacing the Georgian President's image on a website, comparing him with Hitler

State use of cyber operations during periods of tension – Georgia	
Who	Alleged Russian Business Network (group of Russian hacktivists) and the South Ossetia Hack Crew, thought by some media to be sponsored by Russia.
What	Cyber campaign attacked a total of 38 Georgian and Western websites upon the outbreak of the Russian military incursion, including defacing those of the Georgian President, the Ministry of Foreign Affairs, the National Bank, the Parliament, the Supreme Court, and the United States and UK embassies in Georgia. Most other attacks were distributed denial of service with website defacement and communications re-routing.
How	Replacing the president's image and comparison with Hitler. Redirection of communications from Georgia to the outside world.
Against whom	Georgian Government and President, communications providers from Georgia and selected Western embassies.
Why	Media reports this was to support the Russian military incursion to South Ossetia, aimed at disrupting Georgian communications and undermining the Georgian government.
When	05:15 hours, 8 August 2008 till 12:45 hours on 12 August 2008, covering a phase of the Russian military ground incursion.
Impact	Attacks on Georgia were perceived by the media as part of the military intervention by Russia (although Russia denies the cyber component). They inflicted economic and social damage – and allegedly caused confusion across the Georgian government through communications denial both internally and to the outside world. Website defacements offered a focal point for supporters of Russia's military incursion to South Ossetia. Georgia countered by using Western websites for hosting, including that of the Polish President, and by expanding its blogosphere using Western providers.
More information	Background to the conflict is at: http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL34618_08132008.pdf and http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1069.pdf. *Cyber Attacks Against Georgia: Legal Lessons Identified* (November 2008). CCDCOE document at: http://www.ccdcoe.org/

Case study 5 – Insider threats

Disgruntled or subverted employees may seek to exploit cyberspace to cause harm to their employers, organisations or nation in a number of ways.

US Army Private Bradley Manning

November 2010: Wikileaks published 251,000 State Department diplomatic correspondence, obtained by Bradley Manning, a US Army private stationed at Baghdad in 2009. Manning was sentenced to 35 years imprisonment.

Canadian Navy Officer Jeffrey Paul Delisle

January 2012: Royal Canadian Naval Officer Jeffrey Paul Delisle, working at Her Majesty's Canadian Ship Trinity in Halifax, disclosed large amounts of highly classified intelligence to his Russian handler. Delisle was sentenced to 20 years imprisonment.

National Security Agency contractor Edward Snowden

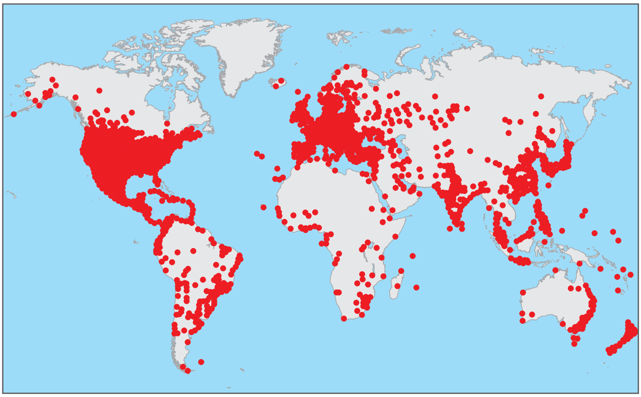
May 2013: release of classified United States National Security Agency material through disclosures leaked to *The Guardian* and *Washington Post* newspapers, while employed by contractor – Booz Allen Hamilton. A series of exposés revealed details on programmes such as the interception of United States and European telephone data, and the PRISM, XKeyscore, and Tempora Internet surveillance programmes. Snowden is currently residing in Russia.

Case study 6 – The impact of encryption

Increasing complexity of encryption on Apple mobile devices	
Who	The United States Federal Bureau of Investigation (FBI) *versus* Apple.
What	On 16 February 2016, United States Magistrate Judge Sheri Pym for the Central District of California ordered Apple to disable an iPhone's auto-erase function, a feature that deletes a smartphone's data after ten failed passcode attempts. The FBI had brought the case in an attempt to gain access into San Bernardino shooter Syed Rizwan Farook's phone to see who he was in contact with, and confirm any ties to ISIS. (Note: the case was suspended following the FBI's employment of a third party to gain access to the phone's data, and subsequent reporting indicates nothing useful to the FBI's case was found on the iPhone.)
How	Due to the security features built into the software of Farook's iPhone, the FBI was unable to unlock the phone and access its data using a brute-force password-guessing technique. This method involves entering different passcodes repeatedly until the correct one is guessed, without running the risk that the device will permanently lock them out.
Against whom	Essentially, the FBI wanted the courts to impose an order on Apple to create a new software tool to enable law enforcement agencies to eliminate specific security protections the company built into its phone software to protect customer data, and unlock Apple devices such as iPhones themselves. The enhanced security is due to Apple being one of the few companies that designs its own software and hardware, including chips, thus enabling the iPhone to exclusively accept software signed with Apple's own encryption key.
Why	Apple does not have the means to disable the auto-erase function, which it introduced along with other security measures in iOS 8 (Apple 's operating system) following Edward Snowden's leak on the National Security Agency's capabilities.
When	16 February 2016.
Impact	Apple argues that once created, the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks – from restaurants and banks to stores and homes. This case is unique to Apple, due to it being one of the few companies that designs its own software and hardware, including chips. This enabled Apple to introduce the extra-strength encryption that lies at the heart of the issue of individual security *versus* state security. This issue is likely to endure.
More information	Background to the issue can be found at: http://www.huffingtonpost.com/sam-corey/stupid-is-as-stupid-votes_b_9287370.html

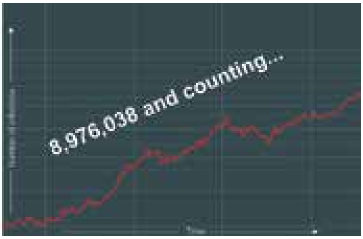
Case study 7 – Impact of malware on military capability

Malware may not necessarily be targeted towards military operations to have significant impact.



The Conficker virus in 2008 infected many systems globally. A number of these belong to Defence ministries; in some cases it impacted operations.

© Shutterstock



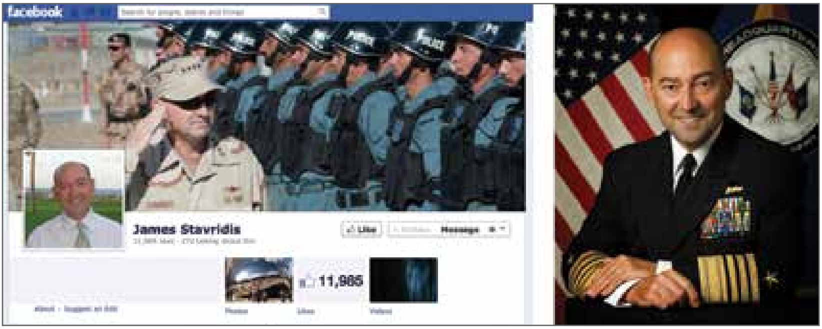
Conficker virus infecting systems

Increasing rate of Conficker virus infections

Impact of malware on military operations – Conficker	
Who	Unidentified. However, Ukrainian Internet protocol (IP) addresses are reported to be immune to Conficker, as are keyboards with Ukrainian layouts. On 13 February 2009, Microsoft offered a US $250,000 reward leading to the arrest and conviction of the perpetrators.
What	Conficker is a worm targeting Windows servers, opening random ports and downloading copies of itself, additional files and resetting system restore points.
How	This malware resets lock-out polices, congests networks, breaks administration passwords and generally creates a denial of service attack on infected machines.
Against whom	Any information communication technology running Windows server services. This includes, but was not targeted specifically against, military hardware where infection was transmitted both over networks and by misusing USB memory sticks.
Why	Unknown.
When	The 'A' variant of Conficker first surfaced on 21 November 2008; Conficker-related malware continues to dominate malware used by cyber criminals to date.
Impact	Within the UK, Royal Navy Navystar/N desktops, Defence's administrative systems and critical national infrastructure systems including the House of Commons were infected. Globally, up to 15 million computers in over 200 countries were infected. 1.7 million computers were infected within just the fourth quarter of 2011 and outbreaks of infections related to Conficker continue to date.
More information	Information on Conficker continues to emerge from individual anti-virus vendors. The Conficker working group reports intermittently at www.confickerworkinggroup.org

Case study 8 – Social engineering for the purpose of espionage

These actions frequently take the form of phishing attacks or identity theft and are often aimed at social engineering, fraud or embarrassing the individual.



US Admiral James Stavridis and his Facebook profile webpage

Facebook helps you connect and share with the people in your life.

© Shutterstock

Social media application Facebook

Social engineering against an individual's Facebook site	
Who	Allegedly state-sponsored individuals from China.
What	Social engineering attack, reportedly originating from China, harvested the details of those who accepted requests from a fake account.
How	Fake Facebook account created and used to send invitations from a fake profile to colleagues in the victim's address book.
Against whom	Commander, United States European Command and NATO Supreme Allied Commander Europe, Admiral James Stavridis and those to whom the invitations were sent.
Why	The aim appears to have been to use social engineering to collect personality information on Admiral Stavridis. This information could later be processed to provide intelligence on his personality profile and exploit his contacts network.
When	Early 2012.
Impact	The wealth of personal information on Admiral Stavridis and potentially his contact network would be invaluable for personality profiling by an adversary. 'Senior British military officers and Ministry of Defence officials are understood to have been among those who accepted "friend requests" from the bogus account for American Admiral James Stavridis. They thought they had become genuine friends of NATO's Supreme Allied Commander – but instead every personal detail on Facebook, including private email addresses, phone numbers and pictures were able to be harvested.' *The Sunday Telegraph* newspaper, 10 March 2012.
More information	More information can be found at: http://www.telegraph.co.uk/technology/9136029/How-spies-used-Facebook-to-steal-Nato-chiefs-details.html

Chapter 3

> “Today’s remotely-piloted air systems depend on over 100 commercial and military network connections, miles of fibre-optic cable and millions of lines of code. All of this is potentially vulnerable to cyber disruption.”

Chief of the Air Staff
DSEI 2015

Chapter 3 – Cyber functions

This chapter looks at the four military cyber operations roles: defensive cyber operations; cyber intelligence, surveillance and reconnaissance; offensive cyber operations; and cyber operational preparation of the environment. It also examines information management and finally looks at the relationship between cyber and other closely-linked military functions.

Cyber operations

cyber operations
The planning and synchronisation of activities in and through cyberspace to enable freedom of manoeuvre and to achieve military objectives.

3.1. Cyber operations can be categorised into four distinct roles:

- defensive cyber operations;
- offensive cyber operations;
- cyber intelligence, surveillance and reconnaissance; and
- cyber operational preparation of the environment.

These roles are rarely discrete. They are interdependent and interacting, providing support to, being supported by and placing constraints on each other. However, defensive cyber operations have primacy to protect our capabilities and enable our freedom of manoeuvre.

3.2. Defence does not deliver the full spectrum of cyber operations. Military cyber activity must be coordinated with key partners, such as:

- the Office of Cyber Security and Information Assurance (OCSIA);
- Government Communications Headquarters (GCHQ);

- Government Computer Emergency Response Team (GovCERT);
- Centre for the Protection of National Infrastructure;
- Computer Emergency Response Team (CERT) UK;
- other government departments;
- industry;
- academia; and
- international partners.

3.3. The *National Security Strategy and Strategic Defence and Security Review 2015*[37] confirmed a plan to create a National Cyber Security Centre that will provide the UK with a unified platform to handle incidents and will create a single point of contact in Government for the private sector. From a Defence perspective, the decision to create a Cyber Security Operations Centre staffed by experts underlines the importance placed on cyber and cyberspace.

Defensive cyber operations

3.4. Defensive cyber operations secure the freedom of manoeuvre in cyberspace and are normally undertaken within an information assurance framework.

defensive cyber operations
(DCO)
Active and passive measures to preserve the ability to use cyberspace.

active defence
Activities that target hostile offensive cyber operations in order to preserve our freedom of manoeuvre within cyberspace.

passive defence
Threat specific defensive measures to reduce the effectiveness of cyber activity.

3.5. At the strategic level, defensive cyber operations assure the freedom of action by protecting infrastructure and deployed sovereign capabilities from adversarial offensive cyber activity. At the operational and tactical

[37] *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*, November 2015.

levels, they protect critical networks and systems that reside in the sea, land, air and space environments. Such control is likely to be localised in terms of time and space, and will be reliant on the quality of information assurance. Control of equity in cyberspace depends on available resources and the level of risk that can be tolerated. Defensive cyber operations are enduring and non-discretionary.

3.6. Security. The *National Security Strategy and Strategic Defence and Security Review 2015* makes it clear that the opportunities presented by cyberspace have also introduced new vulnerabilities. Security, both individual and collective, is therefore an overarching principle in cyber operations. A lapse in security can affect our resilience, awareness 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 breaches in a timely fashion. The scale of damage that even one person can cause is illustrated by the Edward Snowden case.[38]

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

resilience

The ability of the community, services or infrastructure to withstand the consequences of an incident.

(JDP 02, *Operations in the UK: The Defence Contribution to Resilience*, 2nd Edition)

cyber resilience

The ability of an organisation or platform to withstand and/or recover from malicious events in cyberspace.

[38] More detail of which can be found at Annex 2A on page 44.

3.8. **Computer Emergency Response Teams.** Most governments, many universities and industries run CERTs.[39] In the main, these teams collaborate internationally on a voluntary basis to manage security aspects of cyberspace in near-real time. Most teams are members of the Forum for Incident Response and Security Teams (FIRST). Within Defence, cyber protection teams (CPTs) protect mission-critical assets including networks, data, information and systems.

Offensive cyber operations

3.9. Offensive cyber operations include activities that project force to create, deny, disrupt, degrade and destroy effects in and through cyberspace. These operations may transcend the virtual domain into effects in the physical and cognitive domains.

offensive cyber operations
(OCO)
Activities that project power to achieve military objectives in, or through, cyberspace.

3.10. Offensive cyber activity can be used to inflict temporary or permanent effects, thus reducing an adversary's confidence in networks or capabilities. Such action can support deterrence by communicating intent or threats. At the operational/tactical level there is a need to coordinate between offensive cyber operations and information operations/activities.

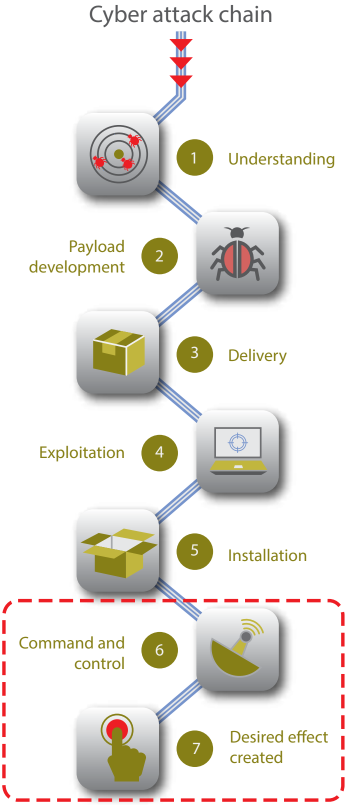
3.11. Offensive cyber activity can be simply categorised into seven phases, known as the cyber attack chain. These are commonly identified as:

- understanding;
- payload development;
- delivery;
- exploitation;
- installation;

[39] Computer Emergency Response Team is now a registered service mark of Carnegie Mellon University that is licensed to other teams around the world. www.cert.org.

- command and control; and
- effect achieved.

3.12. 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 upon an attacker's intent and availability of offensive cyber and intelligence capabilities. A representative cyber attack chain is depicted at Figure 3.1 below.[40]



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

2 Payload development: Development of computer code (for example malware) that will create the desired effect by exploiting 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 an application or operating system 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: Adversary establishes communication channels to facilitate the transmission of commands.

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

Figure 3.1 – Cyber attack chain

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

Cyber intelligence, surveillance and reconnaissance

3.13. Cyber intelligence, surveillance and reconnaissance (cyber ISR) comprises activities in cyberspace to gather active intelligence from target and adversary systems required to support military operations. The cyber ISR mission for Defence can be supported from national and/or single-Service capabilities.

cyber intelligence, surveillance and reconnaissance
(cyber ISR)
Intelligence, surveillance and reconnaissance activities in, and through, friendly, neutral and adversary cyberspace to build understanding.

3.14. Situational awareness is defined as: the knowledge of the elements in the battlespace necessary to make well-informed decisions.[41] 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 which can be exploited and assessed for intelligence and situational awareness.

3.15. A recognised cyber operational picture, within a common operating picture, will provide commanders with enhanced situational awareness, improved understanding, decision support and enable decision-making. Producing a recognised cyber operating picture is challenging, the reason for which could be:

- lack of a traditional joint operations area;
- speed at which events occur in cyberspace;
- volume of activity that occurs in cyberspace;
- difficulty in proving attribution;
- difficulty in recognising network faults opposed to cyber attacks; and
- locations in the physical and virtual cyber layers might vary.

[41] Allied Administrative Publication (AAP)-06, *NATO Glossary of Terms and Definitions*.

3.16. Indicators and warnings for Defence are often sourced through commerce (for example, anti-virus vendors or security operating centres) and the intelligence agencies. The Ministry of Defence's (MOD's) own CERT has prime responsibility for disseminating cyber indicators and warnings across Defence's networks.

Cyber operational preparation of the environment

3.17. The fourth role in cyber operations – cyber operational preparation of the environment (cyber OPE) – is a vital enabling function which significantly enhances the effectiveness of other cyber operations. The role is split into passive operational preparation of the environment tasks (which include maintenance and integrity of connections, networks and software) and the more covert active 'infrastructure' activities.

cyber operational preparation of the environment
(cyber OPE)
All activities conducted to prepare and enable cyber intelligence, surveillance and reconnaissance, defensive and offensive operations.

Information management

3.18. Acquiring, sharing, processing and protecting information is a vital supporting function to the four roles of cyber operations. Acquiring and sharing information through covert and open sources to multiple or collective locations should be timely, but must also maintain data integrity. These activities are non-discretionary.

3.19. Information assurance activities should provide commanders with the confidence that their networks and systems will protect the information they handle and function as they need to, when they need to and under the control of legitimate users.

a. The MOD Computer Emergency Response Team (MODCERT) is responsible for the information assurance of fixed and deployed networks.

b. Defence Assurance and Information Security (DAIS) is the Defence lead for information assurance. The Joint Information Assurance Coordination Cell (JIACC) coordinates all non-accreditation activity.

c. The Joint Security Coordination Centre (JSyCC) is part of DAIS, they conduct and coordinate all MOD information security incident management and related risk analysis activity.

3.20. 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 littorals

3.21. Much of the early and continuing cyber capability development is a result of innovation from communities within other areas of traditional war fighting. These other capabilities (where data is understood and manipulated in other ways) can be referred to as cyber littorals. The nature of cyberspace is such that it is closely integrated with the maritime, land, and air and space environments (as shown in Figure 3.2) and has symbiotic relationships with other military capabilities. These include:

- information operations (Info Ops) and information activities;[42]
- electromagnetic activities (EMA);[43]
- signals intelligence (SIGINT); and
- communication and information systems (CIS).

3.22. These capabilities use different approaches where data is both manipulated and understood. Such capabilities will need to be managed to achieve success on military operations.

[42] Such as psychological operations, deception and operations security.

[43] For the context of this Primer, electromagnetic activities is limited to electromagnetic spectrum operations and electromagnetic warfare.

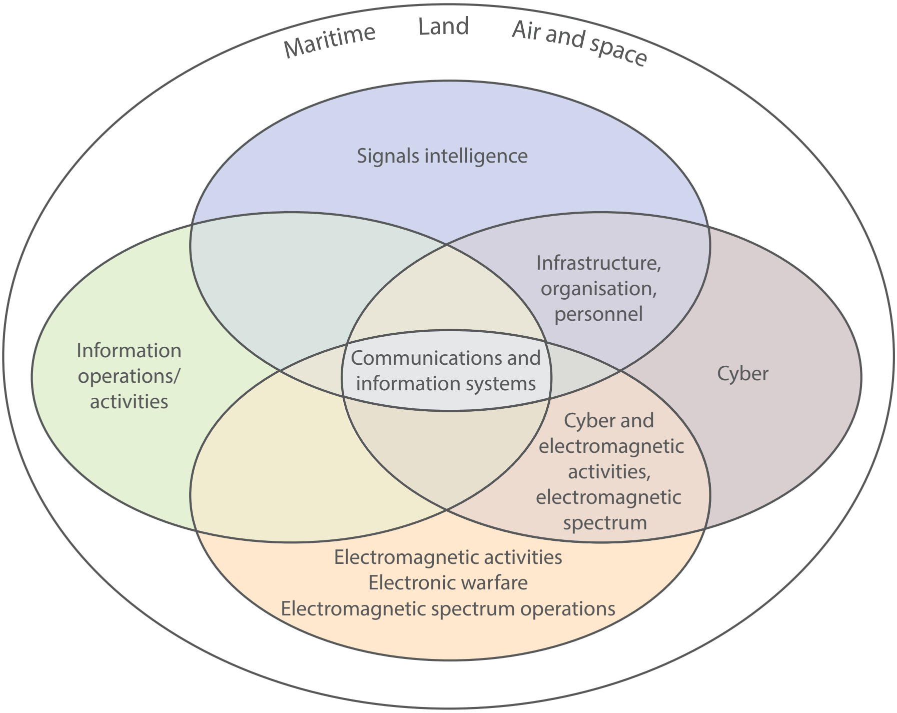

Maritime
Land
Air and space
Signals intelligence
Infrastructure, organisation, personnel
Information operations/ activities
Communications and information systems
Cyber
Cyber and electromagnetic activities, electromagnetic spectrum
Electromagnetic activities
Electronic warfare
Electromagnetic spectrum operations

Figure 3.2 – Cyber littorals in context of the operating environment

3.23. **Information operations and information activities.** The first 'cyber littoral' area is that of information operations and information activities. Information operations and activities are closely associated with cyber capability and there is a large degree of subject matter overlap. The key distinguishing feature between the two areas is the scope of the operating environment. Whilst cyber operations take place in and through cyberspace, information operations can also use any of the operating environments to pursue its aims. We can use cyber and cyberspace to enable information operations and activities in a symmetric or asymmetric manner.

3.24. Signals intelligence. Cyber's second symbiotic relationship is with SIGINT, which is defined as: the generic term used to describe communications intelligence and electronic intelligence when there is no requirement to differentiate between these two types of intelligence, or to represent fusion of the two.[44] Cyber operations and SIGINT are, to an extent, reliant on the same infrastructures, organisations, accesses and personnel training and skill-sets.

3.25. Signals intelligence and cyber. The key difference between cyber and SIGINT comes in the intent and resultant effect of the two. The output of SIGINT primarily resides in the cognitive domain and is one of increased knowledge. Cyber effects will primarily be in the virtual or physical domain, although some may also be in the cognitive domain, as we seek to deny, disrupt, degrade or destroy. As with information operations/information activities and cyber, SIGINT and cyber co-exist, overlap and may even compete for resources – but they must be seen as complementary, not competing, capabilities.

3.26. Electromagnetic activities. For the context of this Primer, EMA is limited to electromagnetic spectrum (EMS) operations and electronic warfare.

a. Electromagnetic spectrum. The EMS covers different types of electronic radiation from radio waves through visible light to gamma rays. From a military perspective, the EMS can be used indirectly, as a bearer for information, or directly as a means of creating an effect. It is in the former that the EMS and cyber have their relationship as electromagnetic energy enables the linking of computer networks and infrastructure.

b. Electronic warfare. Electronic warfare comprises electronic attack, electronic protection and electronic surveillance and is defined by NATO as: military action that exploits electromagnetic energy to provide situational awareness and create offensive and defensive effects.[45]

[44] AAP-06, *NATO Glossary of Terms and Definitions*.

[45] *Ibid*.

3.27. **Electromagnetic activities and cyber.** The relationship between cyber and EMA should be seen as one of resilience and complementary in nature rather than as one of competition. Cyber and electromagnetic activities (CEMA) will, therefore, need to be delivered in an increasingly coordinated manner within Defence. Intelligently applying CEMA can create outcomes greater than the sum of their parts. For example, electronic attack could be used to herd an adversary's communications onto a network already under surveillance. To improve the coordination between electromagnetic activities and cyber, Defence has created the Joint CEMA Group (JCG). A shared characteristic of EMA and cyber is the pace of development.

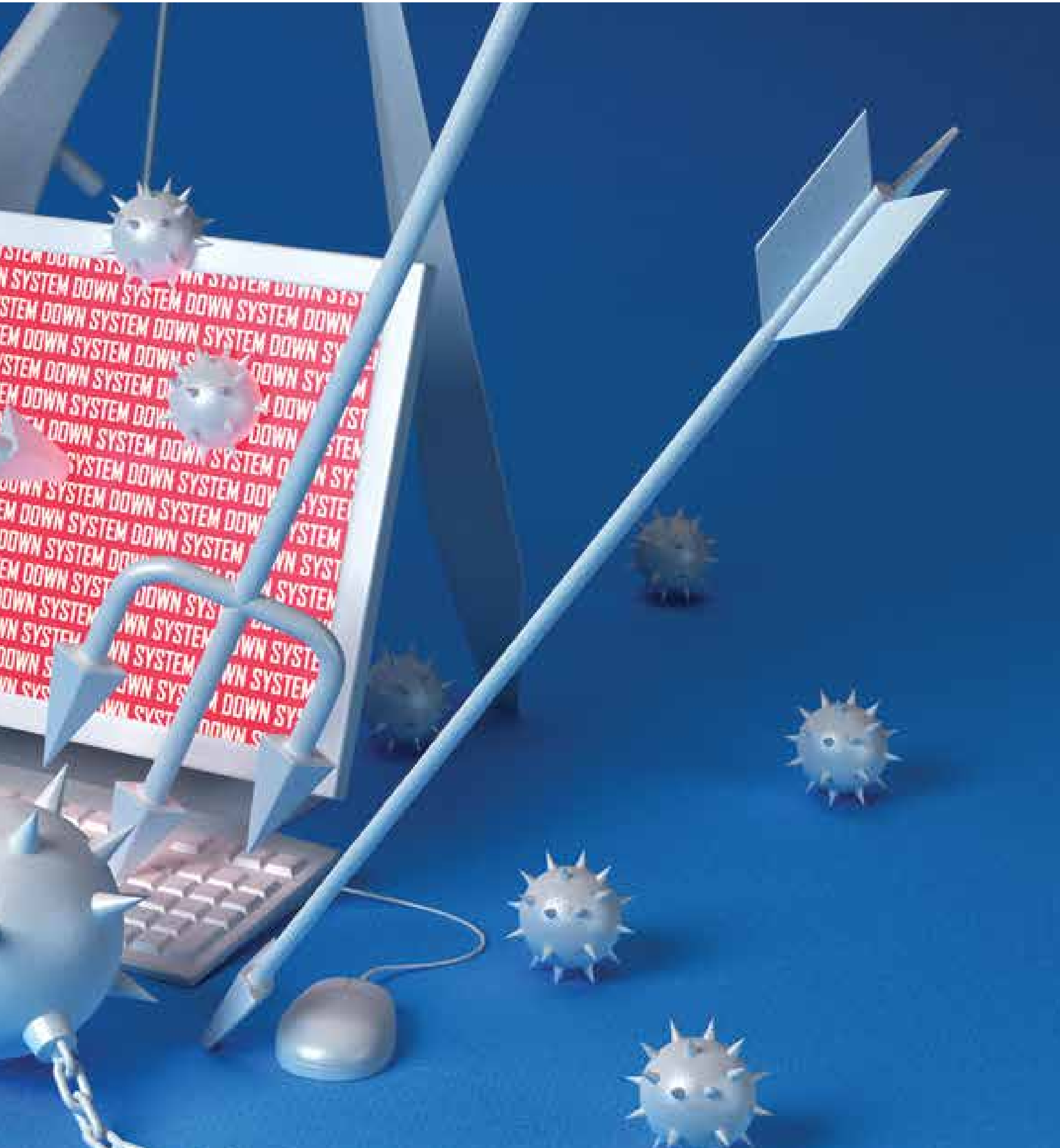
Communication and information systems

3.28. The final littoral relationship is with communication and information systems. With the advent of the information age, a large, but not exclusive, proportion of communication and information systems are computer based. Responsibilities within this function include security and resilience and this is where the overlap with cyber is greatest. Defensive cyber operations are an integral and non-discretionary component of network and security resilience.

Chapter 4

“It is important to really integrate cyber into our military capabilities. This means our militaries have to develop a ‘cyberinstinct’.”

General Sir Richard Barrons
Commander Joint Forces Command
visit to NATO Cooperative Cyber Defence Centre of Excellence,
April 2015



Chapter 4 – Integrating cyber operations

Cyber is 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 is considered an integral aspect of military operations. This chapter also provides details on cyber command and control and how it is coordinated, synchronised and integrated within Defence and across government.

Integrating cyber effects

4.1. Military cyber 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.** Cyber's virtual and flexible properties mean that we can potentially create a variety of effects in terms of complexity and severity, and at a tuneable scale. Cyber 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 2008 Stuxnet attack against the Iranian nuclear programme is a good example of cyber enabling operations for strategic effect.[46]

4.3. **Operational effects.** Integrating cyber capability into operational level planning is a new and evolving process. We need a high degree of integration and cooperation with units and organisations that routinely operate at the strategic level to successfully create cyber effects 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.

[46] More details of this case study can be found at Annex 4A on pages 76-77.

As these operations may be dependent on infrastructure and networks associated with, or even located within, physical target sets, we need to de-conflict and thoroughly understand the gain/loss balance to avoid fratricide and the compromise of 'equity'. It may be possible to create the required effect using relatively low equity or open-source (or modified open-source) tools that can provide agile and flexible response options. Integrating cyber into operational planning is achieved through joint action[47] which is a framework for considering the integration, coordination and synchronisation of all military activity within the battlespace. Joint action is implemented through the orchestration of:

- information activities;
- fires;
- outreach; and
- manoeuvre.

4.4. **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.[48]

4.5. **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.

[47] Joint action is defined as: the deliberate use and orchestration of military capabilities and activities to affect an actor's will, understanding and capability, and the cohesion between them to achieve influence. Joint Doctrine Publication (JDP) 3-00, *Campaign Execution* (3rd Edition, Change 1).

[48] More details on this case study can be found at Annex 4A on pages 78-79.

Cyber command and control

4.6. Cyber underpins so many aspects of Defence's business that cyber command and control for Defence is complex. UK cyber doctrine describes Defence's cyber command and control. The span of military, multi-agency and multinational partners conducting cyber activities means simple supported/supporting relationships are inappropriate. 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.

4.7. By mainstreaming cyber, Defence is developing command and control and force structures to deliver and sustain cyber capabilities as part of its future force. The evolving Defence structure emphasises the complexity of conducting operations in cyberspace and our need to ensure actions are coordinated while retaining the flexibility and agility to manage the threats, and opportunities, arising from cyber.

4.8. An adversary may conduct cyber attacks against all the elements of national power.[49] An agile and resilient command and control approach will better survive and respond to the demands of such hostile activities. Command and control structures must also support cross-government and industry burden sharing. Further details of this will evolve as the UK Cyber Security Information Sharing Partnership (CISP) develops. The Defence Cyber Protection Partnership (DCPP) will raise awareness and improve understanding of the cyber security risks. These partnerships highlight the need for protective measures to increase the security of the wider Defence supply chain and define an approach to implement cyber security standards.

4.9. The *UK Cyber Security Strategy*[50] sets out our intention to secure the advantage in cyberspace by exploiting opportunities to gather intelligence and intervening as necessary against adversaries. Commanders should

[49] The three instruments of national power are diplomatic, economic and military, which are underpinned by information. An example of this can found at Annex 4A on pages 80-81.

[50] *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*. Due to be updated in 2016.

consider cyberspace to be an area of intelligence collection and analysis in its own right. Intelligence support to operations within cyberspace is essential to provide knowledge, reduce uncertainty, and support effective operational decision-making in defending Defence networks. It is not different to the intelligence support function on traditional operations – the outputs will include providing timely indicators and warnings.

4.10. Cyber cannot be dealt with by one business, government department or agency alone. Each has their own specific responsibilities and expertise. Defence's main aim is to protect its own systems and networks so that it can continue to carry out its missions.

4.11. **National cyber activities.** The *UK Cyber Security Strategy* provides the strategic framework for all UK Government activity on cyber security. Government, business, the public and international partners all have a part to play because a coherent approach to cyber security is required. Protecting our own and other states' critical national infrastructure, as well as providing advice to the public and industry, is a matter for other government departments and agencies. Key UK Government organisations are identified below.

a. **Office of Cyber Security and Information Assurance (OCSIA)** is a directorate in the Cabinet Office and provides strategic leadership across Government for UK cyber security issues. OCSIA works closely with the Government's Chief Information Officer in the Cabinet Office.

b. **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 and Commonwealth Affairs. Their primary customers are the Ministry of Defence (MOD), the Foreign and Commonwealth Office and law enforcement agencies.

c. **CESG**[51] (a part of GCHQ) is the national technical authority for information assurance within the UK. It has the lead responsibility within government for providing advice on information assurance

[51] CESG is an initialisation of Communications Electronics Security Group, but that title is no longer used and the organisation is simply known as CESG.

architecture and cyber security to the UK Government, critical national infrastructure, the wider public sector and suppliers to UK Government.

d. The National Crime Agency aims to prevent cyber crime 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.

e. Centre for the Protection of National Infrastructure (CPNI) is the government organisation that gives advice on physical, personnel and information security to businesses and organisations across the national infrastructure. It aims to reduce the vulnerability of organisations in the national infrastructure to terrorism and other threats, such as espionage, including those from cyberspace.

f. Computer Emergency Response Team UK (CERT UK) is the national-level organisation, established late 2013, which conducts cyber response and recovery across all government departments.

g. Government Computer Emergency Response Team (GovCERT), provides warnings, alerts and assistance to public sector organisations regarding computer security incidents and advice to reduce exposure.

h. The National Cyber Security Centre, announced in the UK's *National Security Strategy and Strategic Defence and Security Review 2015*,[52] will provide the UK with a unified platform to handle incidents and will create a single point of contact within the UK Government for the private sector.

4.12. Military cyber organisations.

a. Joint Cyber and Electromagnetic Activities Group. MOD established a new 1* Joint Cyber and Electromagnetic Activities

[52] *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*, November 2015.

Group (JCG) to coordinate activities in cyberspace and the electromagnetic environment to gain freedom of movement, operational advantage and create effect, whilst simultaneously exploiting, denying and degrading our adversary's use of the same.

b. **Joint Force Cyber Group.** The Joint Force Cyber Group delivers Defence's cyber capability; including the Joint Cyber Reserve. The Joint Force Cyber Group is subordinated to the Joint Cyber and Electromagnetic Activities Group.

c. **Defence Assurance and Information Security (DAIS).** DAIS is the Defence lead for information assurance. The Joint Information Assurance Coordination Cell (JIACC), within DAIS, coordinates all non-accreditation activity.

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. Director Cyber, Intelligence, Information and Integration (DCI3), a serving 2* military officer, is responsible for cyber.

e. **Joint Service Signals Organisation.** The Joint Service Signals Organisation (JSSO) is a tri-Service MOD organisation that provides specialist support to military operations. As part of its role the JSSO conducts research into new communications systems and techniques to provide operational support to static and deployed MOD units.

f. **MOD Computer Emergency Response Team.** The MOD Computer Emergency Response Team (MODCERT) is responsible for the information assurance of fixed and deployed networks.

Military staff integration

4.13. **Operational staff.** Operational planners and those responsible for targeting need to understand Defence's cyber capabilities, and have access to legal advice. They need to either be trained in computer-related and physical interdependencies of information communication technology (ICT) or have access to subject matter experts.

4.14. **Technical specialists.** Technical specialists need current, expert knowledge of a range of operating systems and applications. Civilian training is supplemented by specialist military, government and commercial courses.

4.15. **Specialist organisations.** Defence's cyber resources are centrally managed by the Joint Forces Cyber Group in consultation with the single Services and civilian agencies. Teams of cyber specialists will operate at different levels, have varying skill sets and be in geographically dispersed units. Manpower will be sourced from:

- in-house and external specialist trained personnel (regular and/or reserve);
- secondments from civilian companies; and
- service level agreements with contractors.

Operating in cyberspace

4.16. **Defensive preparedness.** All personnel working with ICT need to have the confidence to recognise, respond to and recover from cyber attacks. Policies and practices in accordance with Joint Service Publication (JSP) 440, *The Defence Manual of Security* and JSP 541, *MOD Information Security and Computer Network Defence Organisation and Reporting Procedures* need to be developed and rehearsed to manage our activities.

a. **Systems security.** Using appropriate warning systems, up-to-date anti-virus 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 business continuity plans. It is crucial that when planning against cyber attacks 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 cyber security 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 warning and reporting points (WARPs)). It is not uncommon to need to contact manufacturers or suppliers of a computer system when a cyber attack 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. Attacks, and suspected attacks, should always be reported through the local chain of command.

4.17. **Exercising the capability.** Cyber 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 cyber attack will be exercised within the Defence Exercise Plan, managed by Joint Forces Command. 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 such as the UK's Exercises JOINT HORIZON and JOINT VENTURE as well as those of

NATO and allies.[53] In addition, specialist cyber units are involved in exercises with partner nations and allies.

4.18. **Business continuity.** Business continuity means being resilient and maintaining service though 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.

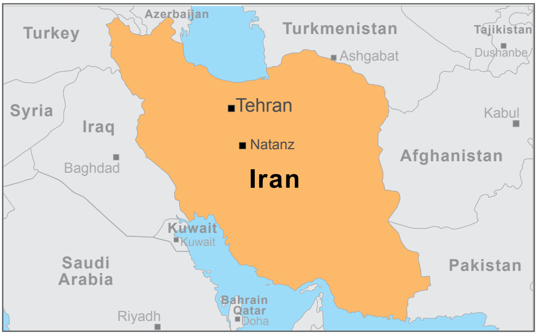
- Where does the priority lie in maintaining system availability?
- What is the impact of system loss?
- Who do I need to notify if I intend to close a system – or continue running it with known or even unknown faults?
- How is risk measured and managed and at what levels of command do various responsibilities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

[53] Such as the United State's joint cyberspace training exercise CYBER FLAG or the NATO Cooperative Cyber Defence Centre of Excellence's Exercise LOCKED SHIELDS.

Annex 4A – Case studies

Case study 1 – State *versus* state offensive cyber operations

These attacks have been used as part of covert operations to influence or undermine the political will of a third party to change their policies.

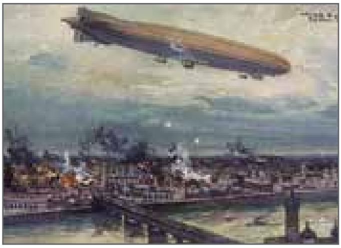


Alleged use of cyber to influence national policies

> ‘I can’t help but think that some watershed has been passed, that Stuxnet of September 2010 will be remembered rather in the way we do the aerial bombings of civilian centres by Zeppelin airships – not as particularly strategically significant at the time but as a harbinger of what is still to come.’

Dr David Betz, *Kings of War*, 28 September 2010

Centrifuge control room



Aerial bombings of civilian centres by Zeppelin airship

Cyber weapon used to realise physical effects	
Who	Unknown.
What	Intelligence collection, denial of service attack against Siemens SCADA (supervisory control and data acquisition) systems – Flame, Stuxnet and others.
How	Media reports that W32 Stuxnet is a highly sophisticated worm designed to exploit vulnerabilities in the Siemens WinCC SCADA systems. It was probably manually inserted in the original target local area network. It used zero day exploitation scripts and genuine Internet security certificates to avoid detection and only attacked specified Iranian targets.
Against whom	Iranian centrifuges at the Natanz uranium refinery plant. Several additional networks were also unintentionally infected.
Why	Reportedly an effort to delay Iranian production of nuclear weapons.
When	An original version of what became Stuxnet appeared on 20 November 2008, but the most sophisticated version used against Iran was first detected on 17 July 2010.
Impact	Media reports that approximately 100,000 hosts were infected globally (although most of these infections caused no damage) and that approximately 984 centrifuges were damaged at Natanz. Media also reports that Iran established the Cyber Passive Defence Organisation and developed a cyber defence programme, as a direct result of Stuxnet. Allegedly, Iranian hacktivists retaliated by attacking the United States banking structure and other targets.
More information	Symantec technical report is at: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Case study 2 – Cyber attacks in support of conventional operations

Turkey
Syria
Iran
Cyprus
Lebanon
Beirut
Damascus
Iraq
Baghdad
Mediterranean Sea
Israel
Jerusalem
Amman
Jordan
Cairo
Egypt
Saudi Arabia

Israel and Syria – cyber attacks in support of conventional operations

© Getty images (not insert)

Aerial view of the Syrian nuclear research institute at Dayr az-Zawr, allegedly attacked by Israeli military aircraft

Israeli cyber attack in support of conventional operations	
Who	Unconfirmed, but believed to have been Israeli intelligence agencies.
What	Media reports that a piece of malware was installed in the Syrian integrated air defence system and activated in the course of the attack, denying a recognised air picture to the Syrian defenders.
How	Counter-integrated air defence system seems to be a likely target for a blended attack comprising cyber and electronic warfare creating a safer passage for attacking aircraft and destroying the enemy's situational awareness.
Against whom	Syrian integrated air defence system.
Why	Blended use of cyber and electronic warfare provides good stand-off capability and timely activation with little or no warning.
When	6 September 2007.
Impact	This alleged use of cyber as a mainstream military component may well be an indicator to a future integrated force structure. The incident allegedly disrupted Syrian nuclear research. More importantly, it may have also served as a warning to other countries that appropriate means will be used to mitigate nuclear threats.
More information	A commentary on this specific attack is at: www.defensetech.org/2007/11/26/israels-cyber-shot-at-syria/

Case study 3 – Alleged cyber attack against a state's critical national infrastructure

	Cyber attack against Ukrainian critical national infrastructure
Who	Although the United States' Department of Homeland Security, who conducted the analysis, did not name any group or nation as being responsible for causing the power cuts, independent analysts have linked the spear-phishing attack to Russia – iSight Partners, a United States security firm, said the probable culprit was the so-called 'Sandworm Team', a Russian hacking group it has been tracking for more than a year.
What	Cyber attack against three Ukrainian regional electric power distribution companies (Oblenergos) that cut power to 225,000 people in Ukraine. The attack is thought to be the first known successful cyber attack aimed at critical national infrastructure.
How	A report written by the cyber emergency response team in the Industrial Control Systems arm of the Department of Homeland Security said the attack had several stages and initially involved hackers installing malware on computer systems at power generation firms in Ukraine, probably facilitated by a spear-fishing email sent to an employee. The cyber attack was reportedly synchronised and coordinated across the three locations, probably following extensive reconnaissance of the target networks. According to company personnel, the cyber attacks at each company occurred within 30 minutes of each other and impacted multiple central and regional facilities. During the cyber attacks, malicious remote operation of the breakers was conducted by multiple external individuals using either existing remote administration tools at the operating system level or remote industrial control system (ICS) client software via virtual private network (VPN) connections. The companies believe that the actors acquired legitimate credentials prior to the cyber attack to facilitate remote access. While the power was cut, the attackers also bombarded customer service phone lines with fake calls to stop customers reporting the cut.

Cyber attack against Ukrainian critical national infrastructure	
How (continued)	The attack was more alarming than a simple malware infection that allowed remote access as the widespread disruption of services was caused by power outages at three different regional electric power distribution companies. Note: Details of the attack were based entirely on interviews with staff at Ukrainian organisations that dealt with the aftermath of the attack. The Department for Homeland Security Cyber-Response Team was unable to independently review technical evidence.
Against whom	Three Ukrainian regional electric power distribution companies (Oblenergos).
Why	Crimea, the region annexed from Ukraine by Russia, has suffered repeated power cuts since Russia seized the territory in March last year. Russia has blamed pro-Ukraine saboteurs for the outages and it is possible this was conducted in retaliation for the outages in the Crimea.
When	23 December 2015.
Impact	Disruption of electrical power to 225,000 customers. First assessed attack on critical national infrastructure.
More information	Background to the issue can be found at: US Dept of Homeland Security IR-ALERT-H-16-056-01 Cyber Attack Against Ukrainian Critical Infrastructure and http://www.bbc.co.uk/news/technology-35667989

© Shutterstock

Ukrainian electrical plant

Lexicon

Part 1 – Acronyms and abbreviations

AAP	Allied administrative publication
APT	advanced persistent threat
CERT	computer emergency response team
CIS	communication and information systems
CISP	Cyber Security Information Sharing Partnership
COED	Concise Oxford English Dictionary
CPNI	Centre for the Protection of National Infrastructure
CPT	cyber protection team
CPU	central processing unit
CSOC	Cyber Security Operations Centre
cyber ISR	cyber intelligence, surveillance and reconnaissance
cyber OPE	cyber operational preparation of the environment
DAIS	Defence Assurance and Information Security
DCDC	Development, Concepts and Doctrine Centre
DCO	defensive cyber operations
DCPP	Defence Cyber Protection Partnership
DCS	distributed control systems
DDoS	distributed denial of service (attack)
DoS	denial of service (attack)
EMA	electromagnetic activities
EMS	electromagnetic spectrum
FIRST	Forum for Incident Response and Security Teams
GCHQ	Government Communications Headquarters
GovCERT	Government Computer Emergency Response Team
GPS	global positioning system
https	hypertext transfer protocol secure

ICS	industrial control systems
ICT	information and communication technologies
Info Ops	information operations
IP	Internet protocol
JCG	Joint Cyber and Electromagnetic Activities (CEMA) Group
JDP	joint doctrine publication
JIACC	Joint Information Assurance Coordination Cell
JSSO	Joint Service Signals Organisation
JSyCC	Joint Security Coordination Centre
LOAC	Law of Armed Conflict
malware	malicious software
MC	Military Committee
MOD	Ministry of Defence
MODCERT	Minstry of Defence Computer Emergency Response Team
NATO	North Atlantic Treaty Organization
NCI	NATO Communications and Information Agency
NC3A	NATO Command, Control and Communications Agency
OCO	offensive cyber operations
OCSIA	Office of Cyber Security and Information Assurance
PLC	programmable logic controls
SCADA	supervisory control and data acquisition
SIGINT	signals intelligence
SSL	secure socket layer
UK	United Kingdom
USB	universal serial bus
WARPs	warning and reporting points

Part 2 – Additional terms and definitions

These additional terms and definitions are provided for general awareness.

advanced persistent threat
(APT)
An advanced persistent threat refers to a cyber attack launched by an attacker with substantial means, organisation and motivation to carry out a sustained assault against a target. (www.techopedia.com)

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[1])

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

chat rooms
An area on the Internet or other computer network where users can communicate, typically one dedicated to a particular topic. (COED)

clickjacking
Clickjacking is a malicious technique of tricking a user into clicking on something different to what the user perceives they are clicking on, thus potentially revealing sensitive information or losing control of their computer while clicking on seemingly innocuous web pages.
(Ministry of Defence (MOD) Information Management Passport – Cyber module)

[1] https://www.sans.org/security-resources/glossary-of-terms/

distributed denial of service attack

Distributed denial of service (DDoS) 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. (Cyber Security Operations Centre (CSOC))

electronic warfare

Military action that exploits electromagnetic energy to provide situational awareness and achieve offensive and defensive effects.
(Allied Administrative Publication (AAP)-06)

firewall

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

global positioning system

(GPS)

An accurate worldwide navigational and surveying facility based on the reception of signals from an array of orbiting satellites. (COED)

honeypots and honeynets

Programs that simulate one or more network services that you designate on your computer's ports. An attacker assumes you're running vulnerable services that can be used to break into the machine. A honeypot can be used to log access attempts to those ports including the attacker's keystrokes. This could give you advanced warning of a more concerted attack. (SANS)

human intelligence

A category of intelligence derived from information collected and provided by human sources. (AAP-06) information operations

Information operations is a staff function to analyse, plan, assess and integrate information activities to create desired effects on the will, understanding and capabilities of adversaries, potential adversaries and approved audiences in support of mission objectives.
(North Atlantic Treaty Organization (NATO) Military Committee (MC) policy, MC 422/4)

information security

The preservation, confidentiality, integrity and availability of information; other properties such as authenticity, accountability and non-repudiation may be involved. (Joint Service Publication (JSP) 440)

Internet service provider

(ISP)
An Internet service provider is a company that provides a service allowing business or personal users to access the internet.
(MOD Information Management Passport – Cyber module)

measurement and signature intelligence

Scientific and technical intelligence derived from the 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. (AAP-06)

operations security

The process which gives a military operation or exercise appropriate security, using passive or active means, to deny the enemy knowledge of the dispositions, capabilities and intentions of friendly forces. (AAP-06)

proxy

A human proxy is: a person authorised to act on behalf of another. (COED)
A computer proxy is a server acting as an intermediary between users and the World Wide Web. These terms taken together have come to mean a hacker group conducting cyber operations on behalf of a client (which may be a Nation State). (CSOC)

secure sockets layer

(SSL)

A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data out that's transferred over the SSL connection. (SANS)

signals intelligence

The generic term used to describe communications intelligence and electronic intelligence when there is no requirement to differentiate between these two types of intelligence, or to represent fusion of the two. (AAP-06)

spam

Irrelevant or unsolicited messages sent over the Internet, typically to large numbers of users. (COED)

SQL injection

SQL injection is a type of input validation attack specific to database-driven applications where SQL code is inserted into application queries to manipulate the database. (SANS)

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.
(MOD Information Management Passport – Cyber module)

spoofing

Spoofing is activity to make a transmission appear to come from a source other than the real source of the transmission. Spoofing is commonly seen in phishing emails, where the email address that the message appears to be from is not the real origin of the message.
(MOD Information Management Passport – Cyber module)

TEMPEST
TEMPEST refers to the unintentional radiation or conduction of compromising emanations from communications and information processing equipment.
(MOD Information Management Passport – Cyber module)

watering hole
A website that has been compromised with the intention to serve malicious content to specific and likely known IP addresses with the effect of compromising specific targets of interest. (CESG)

zero-day
A vulnerability that has been identified in software that has no available patch. (CESG)

Resources

The UK's ***National Security Strategy and Strategic Defence and Security Review*** describes how, in an age of uncertainty, we need the structures in place so we can react quickly and effectively to new and evolving threats to our security.

The UK Cyber Security Strategy seeks to secure advantage in cyberspace by exploiting opportunities to gather intelligence and intervene against adversaries.

The Ministry of Defence's (MOD's) **Defence Cyber Security Programme** provides a focussed approach to cyber, ensuring the resilience of the MOD's vital networks and placing cyber at the heart of Defence operations, doctrine and training.

Joint Service Publication 440, Part 8 – *The Defence Manual of Security* contains policy and guidance relating to communications and information communication technology security.

Joint Service Publication 541 – *MOD Information Security and Computer Network Defence Organisation and Reporting Procedures* provides the relevant policy, procedures and responsibilities regarding the reporting and handling of all MOD information security/computer network defence incidents and the alert, warning and response infrastructure.

Allied Joint Publication-3.10 – *Allied Joint Doctrine for Information Operations* provides understanding, information and guidance to all involved in the planning and execution of information operations on joint operations.

Joint Service Publication 383 – *The Manual of the Law of Armed Conflict* is a reference for members of our 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.

CESG 10 Steps to Cyber Security provides cyber security guidance for businesses. Produced by CESG, Business Innovation and Skills and the Centre for the Protection of National Infrastructure, it will help the private sector to minimise their risks to cyber vulnerabilities.

Cyber Security Information Sharing Partnership is a joint, collaborative initiative between industry and 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 upon UK business.

Cyber Streetwise is the Government's campaign aims 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 cyber security.

Defence Cyber Protection Partnership aims to meet the emerging threat to the Defence supply chain by increasing awareness of cyber risks, sharing threat intelligence, and defining approaches to cyber security standards.

SANS Top Twenty Criticality Controls provides those with a formal remit to operate the MOD's networks, or connect to them with security advice. This is a good guide to effective cyber defence.

Get Safe Online provides top tips to avoid personal fraud and identity theft. Their *Rough Guide to Staying Safe on Line* should be read by all.

Social media information card leaflet from the MOD briefly describes social media behaviours for military personnel and for commanders.

The Global Cyber Game report on the findings of the MOD Defence Academy cyber inquiry.

1. We are all personally responsible for protecting Defence assets, and information is one of our key assets.
Report any concerns immediately.

2. If you think an email is suspicious, forward it as an attachment to SPOC-Spam and delete from your inbox using Shift-Del. If you think you have opened something by mistake, then report it at once.
Never reply to spam email.

3. If unsure, don’t click on any links or open attachments.
Use Favourites for websites you visit often.

4. Be alert to potential targeting by social engineers and report any concerns immediately.

5. Think before you share online – including posting on social media sites – are you giving away information which could impact on personal or operational security, or could be used by a social engineer?

6. Never give sensitive information unless you are sure the recipient is who they say they are and has a valid need to know.

7. Protect passwords – never share them or leave them where they can be found. Don't make them easily guessable, or use the same password for different applications.

8. Don't plug anything into the USB ports of military IT systems including DII, not even to charge them, except for officially – procured MOD USB devices. If you find any unaccounted for USB devices in your workplace you should hand them to your Security Officer.

9. Keep your anti-virus up to date at home so that it can help reduce the risk of downloading malware.

**Remember that however well protected you are,
nothing can guard against every threat – so be vigilant.**

Designed by the Development, Concepts and Doctrine Centre
Crown copyright 7/16
Published by the Ministry of Defence
This publication is also available at www.gov.uk/mod/dcdc