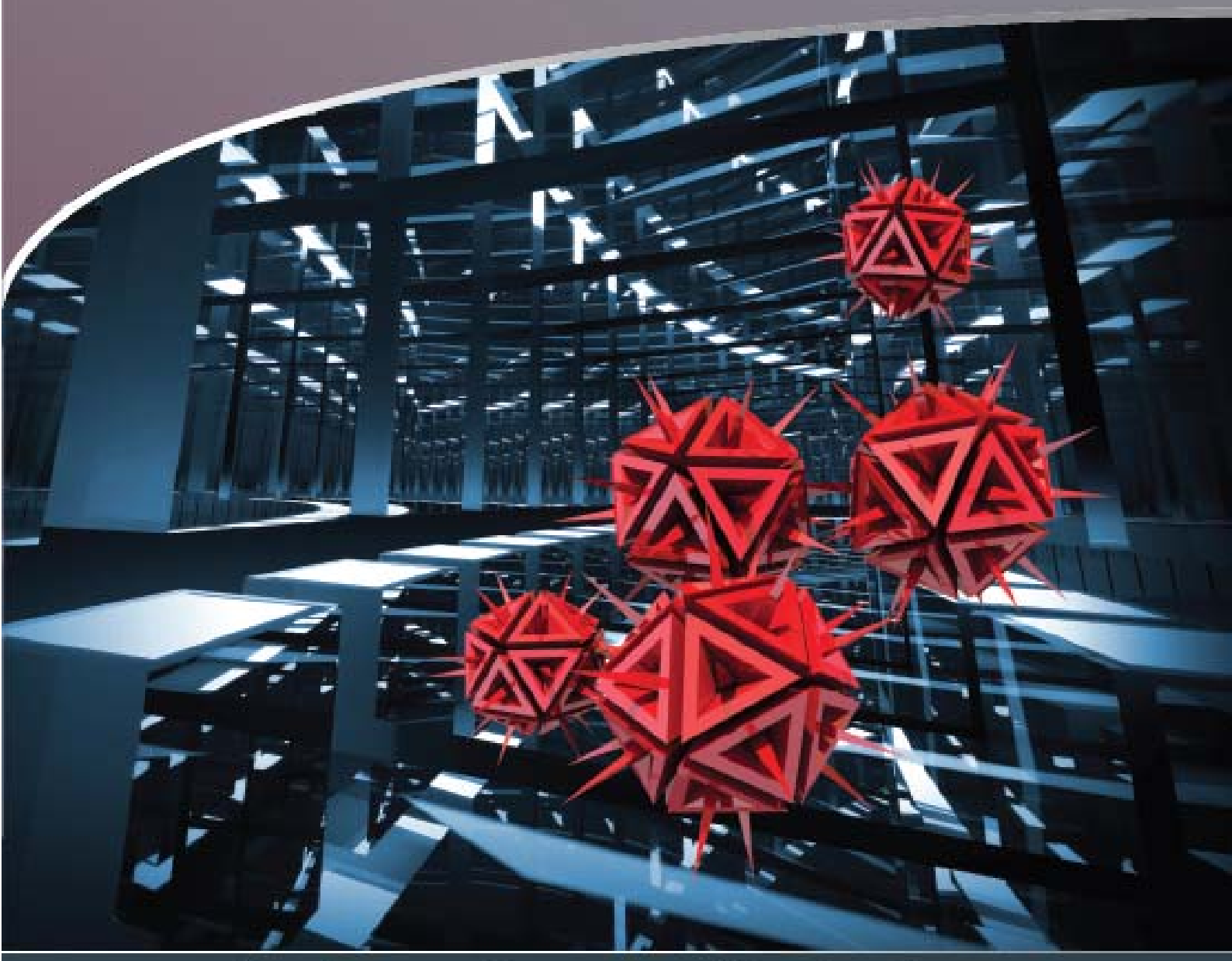
Ministry of Defence

Cyber Primer



Development, Concepts and Doctrine Centre

Cyber Primer

The *Cyber Primer*, dated December 2013,
is promulgated
as directed by the Joint Force Commander and Chiefs of Staff

Head of Doctrine, Air and Space

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 doctrine 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

Email: DCDC-DocEds@mod.uk

Distribution

Distributing our publications is managed by the Forms and Publications Section, LCSLS Headquarters and Operations Centre, C16 Site, Ploughley Road, Arncott, Bicester, OX25 1LP. All of our publications, including a regularly updated DCDC Publications CD, can also be demanded from the LCSLS Operations Centre.

LCSLS Help Desk: 01869 256197
Military Network: 94240 2197

Our publications (including drafts) 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/development-concepts-and-doctrine-centre

Foreword

> ‘People think of military as land, sea and air. We long ago recognised a fourth – space. Now there’s a fifth – cyber.
>
> Cyber is the new frontier of defence. For years, we have been building a defensive capability to protect ourselves against these cyber attacks. That is no longer enough.
>
> You deter people by having an offensive capability. We will build in Britain a cyber strike capability so we can strike back in cyberspace against enemies who attack us, putting cyber alongside land, sea, air and space as a mainstream military activity. Our commanders can use cyber weapons alongside conventional weapons in future conflicts.’
>
> Rt Hon Phillip Hammond MP
> Secretary of State for Defence
> 29 September 2013[1]

We live in a world that is interconnected as never before. The proliferation of information technology and digital communications has revolutionised the way we lead our lives in almost every way – housing, transport, communications, entertainment, travel, and even sport all now depend to some degree on this technology. The character of conflict in our time has already been shaped by cyberspace. It has delivered many opportunities in the way we build capability and conduct operations, extending from the weapons and equipment in the hands of one man right up to the most highly complex intelligence, surveillance and reconnaissance capability. Cyberspace is fundamental to the exercise of command and control.

There are as many vulnerabilities as opportunities. The downside of the capability we possess is the potential exposure to our adversaries of our critical capabilities and processes. We have to see this as an intrinsic part of modern military operations and deal with it. The risk extends beyond military

[1] Media interview, 29 September 2013. http://www.bbc.co.uk/news/uk-24321717.

capability. The safety, security and prosperity of our country is at risk from the interference of others unless it is protected by a unified national effort.

All this means that every part of UK Defence must see that cyberspace is part of their responsibilities. There are highly specialist elements such as the Joint Force Cyber Group who will provide the cutting edge of MOD capability, but the contemporary operating environment now requires commanders at every level to understand the vulnerabilities that they have to cyber attack and how to build the necessary defences into capability, plans, tactics and procedures. Military cyber operations will be vital, complex activities and subject (like any other operations) to ministerial oversight. Such operations must also be conducted in accordance with domestic and international law.

The purpose of this primer is to provide baseline awareness of cyber for the entire Defence audience. It will underpin the mainstreaming of cyber into all forms of Defence activity and highlight the scale and importance of cyberspace to all our people. We all need to know about the threat, the importance of adopting sound cyber security practices and how to think about exploiting the potential weaknesses of opponents. In short, whatever you do in Defence, unless you know enough about cyber you will never be good enough at your job.

General Sir Richard Barrons KCB CBE ADC Gen
Commander Joint Forces Command
December 2013

Preface

This *Cyber Primer* introduces you to the subject, particularly in a Defence context, but also in your life at work and home. It is also a good precursor to reading doctrine on the subject.

The primer is divided into two distinct parts. Part 1 is structured around the fundamentals of cyber and its relevance for Defence. The Primer explores the boundaries of cyber and cyberspace, and introduces you to the terms and definitions used. The threats from cyberspace, their characteristics and the tools and techniques used are described. The primer also raises awareness of key UK government organisations involved in cyber, how they cooperate and where they fit into the national picture. Specifically addressing the question of mainstreaming cyber in Defence, the primer looks at cyberspace as an operating environment and how we operate within it. It looks at the intelligence support to cyber operations and the cyber skills and competences required of generalists and specialists.

Cyber and cyberspace are full of opportunities for improving the way we work and live, but this also introduces new hazards of which you need to be aware. Part 2 of the primer references several examples from media reports of actors, ranging from individuals and extremist groups to foreign military, allegedly using cyber to their advantage. No MOD comment is offered on the validity or otherwise of this open source reporting. A brief lexicon of cyber terms are listed along with useful links to resource documents for greater awareness in the subject.

Finally, a short guide to protecting yourself in cyberspace is included on the back cover.

Contents

Part 1

Control of this domain and with it the ability to defend and attack in order to seize and maintain the initiative will be a prerequisite for successful operations.

General Sir Peter Wall, Chief of the General Staff

Cyber and Defence

This section provides some essential definitions related to cyberspace and highlights cyber's role in Defence and the wider context.

What is cyber?

1. There is no universally accepted definition for cyber, but for the purpose of this primer, UK Defence uses the Concise Oxford English Dictionary (COED) definition for cyber: relating to information technology, the Internet and virtual reality. There are other related terms that have already been defined in Defence doctrine: Joint Doctrine Note (JDN) 3/13, *Cyber Operations: the Defence Contribution*, defines cyberspace and cyber operations as shown below.

Cyberspace
In Defence, cyberspace is the interdependent network of information technology infrastructures, (including the Internet, telecommunications networks, computer systems, as well as embedded processors and controllers), and the data therein within the information environment. (JDN 3/13)

Cyber operations
The employment of capabilities where the primary purpose is to achieve effects in, or through, cyberspace. (JDN 3/13)

Cyberspace

2. Cyberspace is a complex and dynamic environment, interdependent with the electromagnetic spectrum, and is key to all military operations on land, sea, air and space. It is far more than just the Internet. Cyberspace is pervasive, incorporating for example aircraft flight control systems, medical life-support systems and national electricity distribution systems. Cyberspace is also geographically less constrained than other environments. So, distance and reach must be viewed differently.

3. 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.

4. 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 element of today's global environment. We now live in the digital world and have become familiar with smart phones, office and home computers, social media applications and email.

5. Most electronic control systems have cyber vulnerabilities, although not all are readily exploitable. 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 identity is more serious. A cyber attack leading to the temporary loss of the electricity grid, on the other hand, could rapidly bring a country to a standstill with severe consequences.

National strategy

6. In October 2010, the National Security Council placed hostile attacks upon UK cyberspace by other states and large scale cyber crime as one of the four Tier 1 threats[2], together with international terrorism, a major accident or natural disaster and international military crisis. This was followed by the Strategic Defence and Security Review (SDSR) 2010 stating that a UK Defence cyber capability would be established as part of the transformative cross-government approach. The review tasked the MOD to, 'provide a cadre of experts to support our own and allied cyber operations to secure our vital networks and to guide the development of new cyber capabilities'.[3]

7. The 2011 Cyber Security Strategy further described the risk of this rapidly evolving environment and stated that the MOD, through Joint Forces

[2] The National Security Strategy, *A Strong Britain in an Age of Uncertainty*, October 2010.
[3] The Strategic Defence and Security Review, *Securing Britain in an Age of Uncertainty*, October 2010.

Command, will take the lead in developing and integrating cyber capabilities. It also states that a Joint Cyber Unit at Corsham will act as a focus for cyber defence for our armed forces and another unit (hosted by GCHQ) would be established whose role will be to, 'develop new tactics, techniques and plans to deliver military effects, including enhanced security, through operations in cyberspace'.[4]

Defence context

8. Defence communications and operations are reliant on cyberspace. It is as much about the people as it is about the hardware and software that support the flow and management of information. The MOD manages its networks to:

- assure information flows that underpin daily business and operations;
- assure integrity and confidentially of information; and
- achieve and maintain information superiority.[5]

9. This contributes to our freedom of manoeuvre in cyberspace while existing cyber defence techniques deter a range of potential adversaries. The ability to maintain situational awareness through detection and understanding the nature of these attacks is key to countering such attacks.

10. As early as 1998 the emerging reliance of Defence on civilian infrastructure, such as utilities and commercial suppliers, was seen to pose serious problems. The majority of today's Defence communications are reliant on civilian-owned and operated networks and use commercial off-the-shelf hardware and software. Consequently, such companies may not use the same levels of integrity on their systems or networks.

11. Recognising that national infrastructure, government and businesses depend on information, communications and technology (ICT) a comprehensive outlook on critical information infrastructure protection (CIIP)

[4] The Telegraph, *Britain prepares cyber attacks on rogue states*, 26 November 2011, http://www.telegraph.co.uk/news/uknews/defence/8916960/Britain-prepares-cyber-attacks-on-rogue-states.html.
[5] Joint Doctrine Note 2/13, *Information Superiority*.

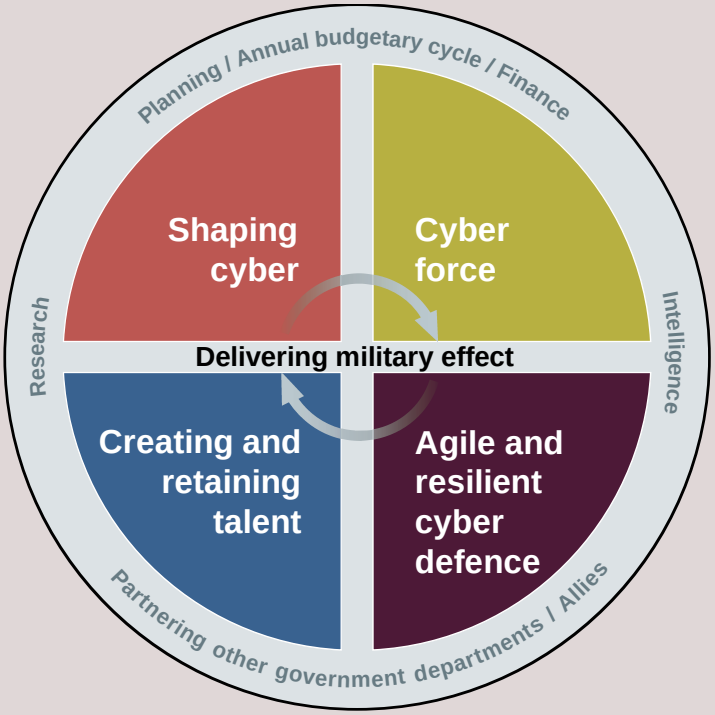
began to evolve. The essential structure of any critical information infrastructure (CII) is unlikely to change over time, although the ICT associated with many of the components will evolve, or even become radically different. UK critical information infrastructure protection policies and procedures identify the Defence critical information infrastructure as a part of the complex critical national infrastructure (CNI).

12. Globally, governments and militaries have an increasing dependence on cyber and this provides our adversaries with new and more exploitable opportunities. This complex environment and its interdependencies enable adversaries' cyber activities to have a local effect while being conducted globally. This new and challenging global environment has forced changes in technology and tempo on defence and security operations. The UK government and the MOD have maintained their operational agility by implementing new forms of governance, command and delegation of authority.

Defence cyber security programme

13. During the past three years the Defence Cyber Security Programme (DCSP) has been the MOD's vehicle for mainstreaming cyber. It ensures resilience of our vital networks and, by continuing to place cyber at the heart of Defence operations, our doctrine and training. Figure 1 shows the four themes of this approach:

- shapi ng cyber;
- cyber force;
- agile and resilient cyber defence; and
- creating and retaining talent.



Shaping cyber. Cyber is being integrated into Defence, building on a solid policy and doctrinal base and becoming part of our normal daily business planning and conducting operations. The DCSP is improving our ability to meet national security objectives by providing commanders with access to national capabilities, reinforced by collaboration with international partners.

Cyber force. Initial cyber force elements are being equipped, manned and trained with supporting infrastructure which allows them to be rapidly deployed and integrated into operations. The DCSP has developed, tested, evaluated and validated pilot cyber capabilities, including initial expeditionary assets as a complement to other military capabilities. Commanders and their supporting staffs now routinely consider the cyber environment when planning operations.

Agile and resilient cyber defence. The DCSP provides the capability for effective situational awareness of our networks (and wider cyberspace) drawing on national intelligence assets to enable effective and timely decision-making.

Creating and retaining talent. The MOD recognised the need for cyber specialist career management. It has developed skills and competence frameworks for both civilian and military (including Reserves) specialist manpower and is promoting a wider understanding of cyber across Defence.

Figure 1 – Defence Cyber Security Programme

14. As we near finishing the Programme, much of the defensive work will continue under the guise of the Defence Cyber Programme (DCP) which will deliver coherent defensive workstreams within the MOD. Preparations are now underway for a new offensive cyber programme to develop and mainstream cyber effects, which will then be available to complement existing military capabilities.

15. 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*.[6] A spectrum of support and implementation is required across the Defence Lines of Development, covering:

- research and development;
- procurement and through-life cost management of capabilities;
- fielding deployment of those capabilities; and
- eventual disposal.

[6] *The New Operating Model – How Defence Works* can be found at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/69149/216820130108_new_operating_model_v3_final_u.pdf.

Cyber threats

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

16. The growing role of cyberspace in society has opened up new threats, as well as new opportunities. We have 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. National threat assessments, including those for cyberspace, are provided by the Government. An overview of the cyber threats is presented in the National Cyber Security Strategy.

17. The risk to national security and economic well-being includes the threat to public and private sector 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
- damaging industrial control systems (also known as supervisory control and data acquisition systems (SCADA)).

18. These attacks can appear in many guises and without inflicting visible or tangible material damage. Cyber attacks are more easily deniable by the perpetrator. All of this significantly increases the likelihood that an adversary may use attacks in 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. Cyber is a ‘new means to old ends’.

Threat actors

19. The term *threat actor* is used to identify those who pose a threat. Threats to security and information 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. 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);
- make money (either through legitimate company or through crime);
- improve personal technical skills; or
- support political ideals (hacktivisim).

20. Threat actors exploit cyberspace's characteristics of innovative approaches, low-entry cost and frequent ease of access. Such malevolent actors may seek to create uncertainty and mistrust through:

- accessing people and systems;
- attacking and exploiting our national and economic infrastructures; and
- military capabilities including command and control systems and personnel.

21. Malicious cyber events can occur before an attack is detected and even then may be very difficult, or impossible, to attribute. The range of threat actors includes: nation states; criminals; hackers; hacktivists; terrorists; insiders; or proxies. We look at each actor in more detail below.

22. **Nation states.** The most sophisticated threat is likely to come from established, capable States who exploit cyberspace to gather intelligence on government, military, industrial and economic targets. The MOD is particularly concerned when States:

- seek intelligence about UK military plans and capabilities;

- steal intellectual property and intelligence on UK military warfighting capabilities;
- exploit UK military capabilities using their militaries and intelligence services with knowledge of the vulnerabilities of our capabilities;
- deny our use of social media applications and other communications channels;
- conduct subversive activities using their intelligence services; and
- use proxies or large numbers of synchronised and coordinated partisans to mask the true origin of their activities within cyberspace, (proxies collaborate and deliver effect by reaching across interconnected and complex physical and virtual networks, using internet connectivity, or by exploiting individuals with network and system access).

23. **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.

24. **Hackers.** Hackers use their skills to adapt and exploit computer software and systems for purposes unintended by the original creators. Some malicious hackers use their skills for illegally bypassing security systems or writing and distributing malicious software (malware).

25. **Hacktivists.** Hacktivists and politically-motivated activist groups, are facilitated by hacker skills. They may also be state-sponsored, comprising computer hackers supporting a specific political, social or ideological cause (for example, stopping military activities). They aim to:

- cause disruption, reputational and financial damage (for example, through releasing sensitive information); and
- gain publicity by attacking public and private sector websites and online services.

Hacktivists will exploit social media to further their cause.

26. **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.

27. **Insiders.** Disgruntled or subverted employees may seek to exploit cyberspace to cause harm to their employer in a number ways.[7] Three examples of insiders causing harm are shown in Example 12 in Part 2.

Characteristics of cyber attack

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

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; or getting local access to the system used by the target.

b. **Payload.** Payload is a computer code that will impact the target system through exploiting vulnerabilities, enabling adversary access and/or impact on 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 evidence of their activities once the attack is complete.

d. **Effect.** Effects may vary depending upon the attacker's intent and nature of the payload. Effects may include:

[7] Insiders are more likely to be the cause of accidental, rather than malicious damage, resulting in denial of service.

- direct action on the target system – for example denial of service (DoS);
- exfiltration 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 (such as, financial, logistics, or personnel data) to provide false readings; or
- 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 valuable information.

Five properties that differentiate cyber threats from conventional threats

28. Adversarial cyber operations provide more vectors for traditional **espionage**, **subversion**, and **sabotage**.

a. **Reach.** The pervasive and borderless nature of cyber activities allows both global and local operations. It has targets from the tactical to the strategic.

b. **Asymmetric effect.** Cyberspace is able to reach many organisations and specific individuals. An individual, or relatively small organisation with appropriate motivation, resourcing and technical capability could conduct an attack with strategic and/or large scale effect (for example, disrupting communications channels).

c. **Anonymity.** Cyber activity is notoriously difficult to trace and, despite technological developments, many cyber incidents are likely to be deniable and some untraceable. Non-attributable attacks increase uncertainty and potentially reduce political risk and opportunities for retaliation.

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

- 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.
- The effects of cyber activity can be instant, 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 collateral damage and thus make cyber attack more politically and socially acceptable.

Forms and techniques of cyber attack

29. 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. The cyber toolbox includes (but is not limited to): social engineering; malware; local physical access; and supply chain corruption. We look at these in more detail below.

Social engineering

30. Social engineering is manipulating individuals to carry out specific actions, or to divulge information. The information gained is frequently used as an enabler of cyber attacks. As the adversaries' 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 (OPSEC) is particularly susceptible to social engineering tools and techniques as these exploit knowledge at the personal level, such as service 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.

31. Social engineering is commonly used to deliver 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 which build the victim's confidence, making the victim more likely to comply with any requests. Some of the most commonly used techniques are outlined below.

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.
Fake emails	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. Often emails appear to come from individuals or organisations the victim would expect to receive them from, or relate to a subject the victim is interested in or works on. This technique is known as spear-phishing.
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.

Social engineering techniques (continued)	
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.

32. 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.

Malware

33. 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) attack on your own 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);
- 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 smart phones, tablets, laptops and similar devices; and
- exploiting social networks.

34. Malware has traditionally been designed to infect computers and computer networks. However, the rapidly increasing popularity of smart phones, 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 below.

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.

Malware types (continued)	
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 will 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 PCs, 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.

35. **Local physical access.** Entry to premises can be gained in a number of ways, for example, by posing as public officials or couriers delivering a package, or by tailgating employees. Once in the premises, there may be opportunities for intruders to interfere with ICT by installing software, such as keystroke loggers and remote access hardware to gain data from, or future access to, systems.

36. **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/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.

Cyber governance

This section identifies key UK government organisations including MOD which are involved with cyber activities nationally and internationally.

National cyber activities

37. The National Cyber Security Strategy provides the strategic framework for all 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, and providing advice to the public and industry, is a matter for other government departments and agencies. Key UK government organisations are identified below.

38. **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.

39. **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 MOD, Foreign and Commonwealth Office and law enforcement agencies.

40. **CESG** (a part of GCHQ) is the national technical authority for information assurance, with the lead responsibility within government for providing information assurance advice to public sector organisations.

41. The **National Crime Agency** aims to prevent cyber crime and make the UK a safer place to do business. Legacy organisations incorporated are the National Cyber Crime Unit, Police e-Crime Unit and the Serious Organised Crime Agency.

42. **Centre for the Protection of National Infrastructure** (CPNI) is the government organisation that provides physical, personnel and information

security advice to business 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.

43. **Centre for Cyber Assessments**, due late 2013, will be multi-agency, enabling better understanding of attacks against UK networks and users; and will provide advice and information about the risks to business and the public.

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

45. **Cyber Security Operations Centre** (CSOC) provides an understanding of attacks against UK networks and users, improving analysis, decision-making and incident response. This centre is likely to be stood down once the CERT UK and Centre for Cyber Assessments are established.

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

MOD cyber command and control

47. Cyber cannot be dealt with by one business, government department or agency alone. Each has their own specific responsibilities and expertise. The MOD's main aim is to protect its own systems and networks so that our Armed Forces can continue to carry out their mission wherever.

48. Cyber underpins so many aspects of Defence business that cyber command and control for Defence is complex. Joint Doctrine Note 3/13, describes the MOD'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.

49. Through mainstreaming cyber, the MOD is developing command and control and force structures to deliver and sustain cyber capabilities as part of its future force. The evolving MOD 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, from cyber.

50. Our military cyber operations will 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. We must recognise 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.

51. An adversary will be likely to conduct cyber activity against all the elements of national power.[8] 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.

International engagement

52. Collaboration with international partners is important to developing MOD cyber activity. Managing the international engagement programme is delegated by Commander Joint Forces Command to the MOD Cyber Policy Team. Our policy is linked with the FCO's International Cyber Policy Unit.

[8] Elements of national power include: diplomatic; military; and economic.

53. While broader MOD 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 lead nation in NATO on cyber, working to ensure that it secures its own networks and encouraging all partners to develop their own cyber capabilities.

54. NATO, our Allies and the European Union structures and processes are complex, a complexity aggravated by the need to include national organisations, such as computer emergency response teams (CERTs), and national and international legal requirements. Key organisations are below.

a. **NATO Communications and Information Agency.** The NATO Communications and Information (NCI) Agency manages those networks actually owned by NATO. Formed on 1 July 2012, this organisation absorbed the former NC3A (The NATO Command, Control and Communications Agency). The NCI Agency also has a coordinating role across individual NATO and NATO-nation CERTs.

b. **Cooperative Cyber Defence Centre of Excellence.** Their mission is to enhance capability, cooperation and information sharing across NATO, and its nations and partners in cyber defence through education, research & development, lessons-learned and consultation.

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

55. Individual NATO nations have their own cyber command structures. In many cases, the UK MOD has direct liaison with these.

Computer Emergency Response Teams

56. Most governments, many universities and industries run CERTs.[9] 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).

[9] 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.

Cyberspace as an operating environment

This section discusses cyberspace as an operating environment and how we integrate cyber activities in Defence. It includes information on the legal framework for military operations in cyberspace.

57. Defence's ability to conduct protective operations in cyberspace is mission critical, demands resilience and enables information superiority. Freedom of manoeuvre in cyberspace will be contested by our adversaries and requires agile capabilities that can anticipate, deter, prevent, detect, assess, protect, respond and recover from attacks on our networks.

58. The MOD's activities in cyberspace are constantly in transformation. To defend itself, the MOD 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 data, but there will always be vulnerabilities.

Cyber, information operations and electronic warfare

59. The nature of cyberspace is such that it is closely integrated with the maritime, land, air and space environments (as shown in Figure 2) and with military capabilities. These include:

- information operations (Info Ops);
- electroni c warfare (EW);
- signals intelligence (SIGINT);
- measurement and signature intelligence (MASINT); and
- human intelligence (HUMINT).[10]

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

[10] Fuller definitions of these terms can be found in the lexicon.

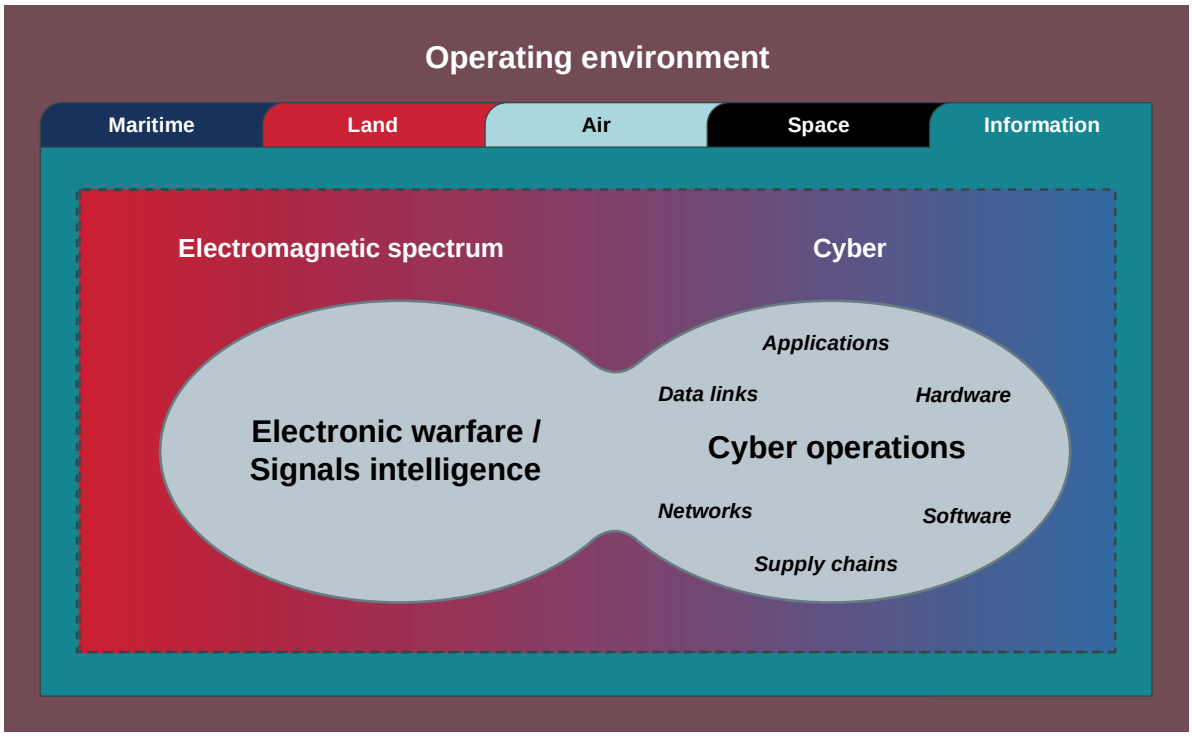


Figure 2 – Cyber operations in context of the operating environment

Operating environment

61. Cyberspace is a pervasive and all-encompassing operating environment. As a relatively new operating environment, MOD is still learning how to exploit cyberspace to its best advantage. Cyberspace is contested even in peacetime – threat actors are constantly probing our networks seeking vulnerabilities, intelligence or military and commercial advantage.

62. We use the concept of *near, mid* and *far* operating spaces to help us understand the cyberspace environment and how it effects our operations.

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

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 his 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 party or adversarial forces.

63. Themes which emerge are:

- the cyber operating space is global, but vulnerable;
- civilian and military information infrastructures, whether national, coalition or international, co-exist and overlap, posing problems for managing security in a network-enabled Defence capability;
- a high baseline for cyber security is required which has implications for education and training, timeliness of system maintenance and intelligence (cyber situational awareness); and
- the threat in, and through, cyberspace is against information which can be held across the Defence enterprise (this includes close collaborative defence of MOD's civilian procurement, logistics and other support contractors[11]).

Legal framework

'Top of the list of the UK principles on activity in cyberspace is the need for governments to act proportionately and in accordance with national and international law. These principles should apply in the civilian and military sphere alike.'

Rt Hon Nick Harvey MP
Minister of State for the Armed Forces[12]

64. While there are no international treaties specifically governing cyber activity, cyber operations must be conducted in accordance with existing domestic law. The international law that applies to military cyber operations will depend on whether an armed conflict is in existence, be it an international armed conflict or a non-international armed conflict. Where there is no armed

[11] The likely interdependencies of critical information infrastructures mean that successful attacks may not only come from unexpected quarters, but also have unexpected impacts.
[12] *Responding to Cyber War*, 1 June 2011. https://www.gov.uk/government/news/armed-forces-minister-responding-to-cyber-war.

conflict, military cyber activities are governed by domestic and international law applicable in peacetime.

65. The law that applies will depend on circumstances such as: the nature and location of activities; who is conducting them; who they are conducted against; and whether or not they are within a peacetime context or part of an armed conflict.

66. Legal support to military operations must include an operational understanding of the cyber activities, including intended effects and possible unintended consequences.

67. **Law of Armed Conflict.** Any military response to conflict is governed by the existing rules of the Law of Armed Conflict (LOAC). Cyber operations conducted during an armed conflict to which the UK is a party, and which are related to that conflict, are governed by LOAC including the prohibition on perfidy (inviting the confidence of an adversary as to protection under LOAC) and principles of neutrality. If the UK is the subject of an imminent or actual cyber attack that crosses the threshold so as to be an 'armed attack' as recognised by Article 51 of the UN Charter, the UK would be entitled to use force in national self-defence in accordance with Article 51. Any response under self-defence must be necessary and proportionate. There is no consensus as to what degree of force constitutes an armed attack, other than that it must be an act/acts of armed force of sufficient gravity, having regard to its/their scale and effects.

68. **Legal implications for cyber.** The implications of the law of self-defence turn on three practical issues:

- attribution;
- the speed with which an attack can be conducted, which greatly reduces the ability to respond to an imminent attack; and
- the difficulty of determining intent, even if actions are provable and actors identifiable.

Other difficulties posed by cyber events include deciding what is a lawful response to a (potentially hostile) cyber incident that may or may not cross the armed attack threshold.

Intelligence support to cyber operations

Cyberspace is a data-rich environment with many layers from the physical, virtual to the cognitive. Intelligence and situational awareness are critical elements.

69. The National Cyber Security Strategy seeks to secure the advantage in cyberspace by exploiting opportunities to gather intelligence and intervening as necessary against adversaries. Commanders should 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 MOD networks. It is not different to the intelligence support function on traditional operations – the outputs will include providing timely of indicators and warnings.

Intelligence and situational awareness

70. Situational awareness is defined as: the ability to identify trends and linkages over time, and to relate these to what is happening and not happening.[13] 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.

71. When observing changes in cyberspace, timescales vary from days or months to milliseconds. Individuals and groups operating in cyberspace leave digital trails but these can be disguised, thus making accurate identification, geo-location and attribution difficult.

72. Exploiting this data-rich environment requires thorough intelligence preparation of the battlespace (IPB). Cyberspace has three interdependent

[13] Joint Doctrine Publication 04, *Understanding*.

layers which align with, and span, the physical, virtual and cognitive domains as shown in Figure 3.

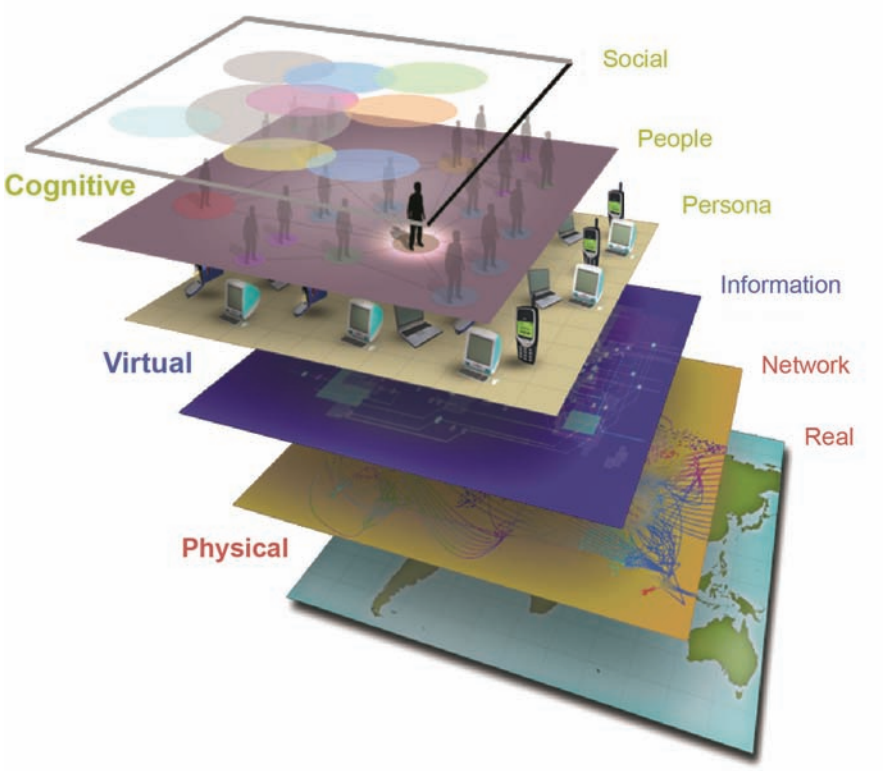


Figure 3 – The layers of cyberspace

a. **Physical layer.** The physical layer (*real*) consists of the physical network components and their associated geography.

b. **Virtual layer.** The virtual layer (*network, information*) consists of the software/applications and connections between network nodes.

c. **Cognitive layer.** The cognitive layer (*persona, people, social*) consists of the information that connects people to cyberspace and the people and groups who interact by using and operating the networks.

Indicators and warnings

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

Cyber skills and competencies

This section discusses the core skills and competencies which need to be developed prior to operating in cyberspace.

Mainstreaming

74. All MOD personnel are expected to operate securely in cyberspace, using and exploiting information and information systems and working effectively to counter potential threats. Cyber's pervasive and ubiquitous nature means we must consider the full range of MOD's cyber capabilities and requirements across the Defence Lines of Development. This requires awareness, education,[14] training, exercises and understanding of risk management in cyberspace.

Personnel

75. Cyber specialists are vital to the success of the Defence Cyber Security Programme which aims to fully integrate cyber operations into Defence. For those engaged in specific cyber specialist roles, a cyber functional competence framework has been created which addresses both the operational and planning/policy competences relevant to Defence. More generally, skills relevant to the cyber environment may be found in the information assurance and ICT functional competence frameworks:

- Institute of Information Security Professional Skills Framework
- Skills Framework for the Information Age

76. MOD cyber operations staff need a sound understanding of the commander's intent and must be able to rapidly assess the impact of their decisions. They should be aware that:

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

[14] For example, the Defence Information Management Passport – information matters and the cyber awareness e-learning modules.

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

77. **Operational planners.** Planners need to understand the MOD's cyber capabilities and limitations. They need to either be trained in computer-related and physical inter-dependencies of ICT or have access to subject matter experts.

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

79. **Specialist organisations.** Joint Forces Cyber Group within Joint Forces Command heralds the formation of specialist units in cyberspace for MOD, frequently using existing resources. These scarce cyber resources will now be centrally managed, in consultation with single-Services and civilian manning 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 regular and reserves personnel;
- secondments from civilian companies; and
- service level agreements with contractors.

Those already qualified as specialists in electronic warfare, telecommunications and engineering will be well placed to take up many of the new posts. Reserves will provide support to the Joint Forces Cyber Group.

Operating in cyberspace

80. **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, for example, current 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 practice 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.

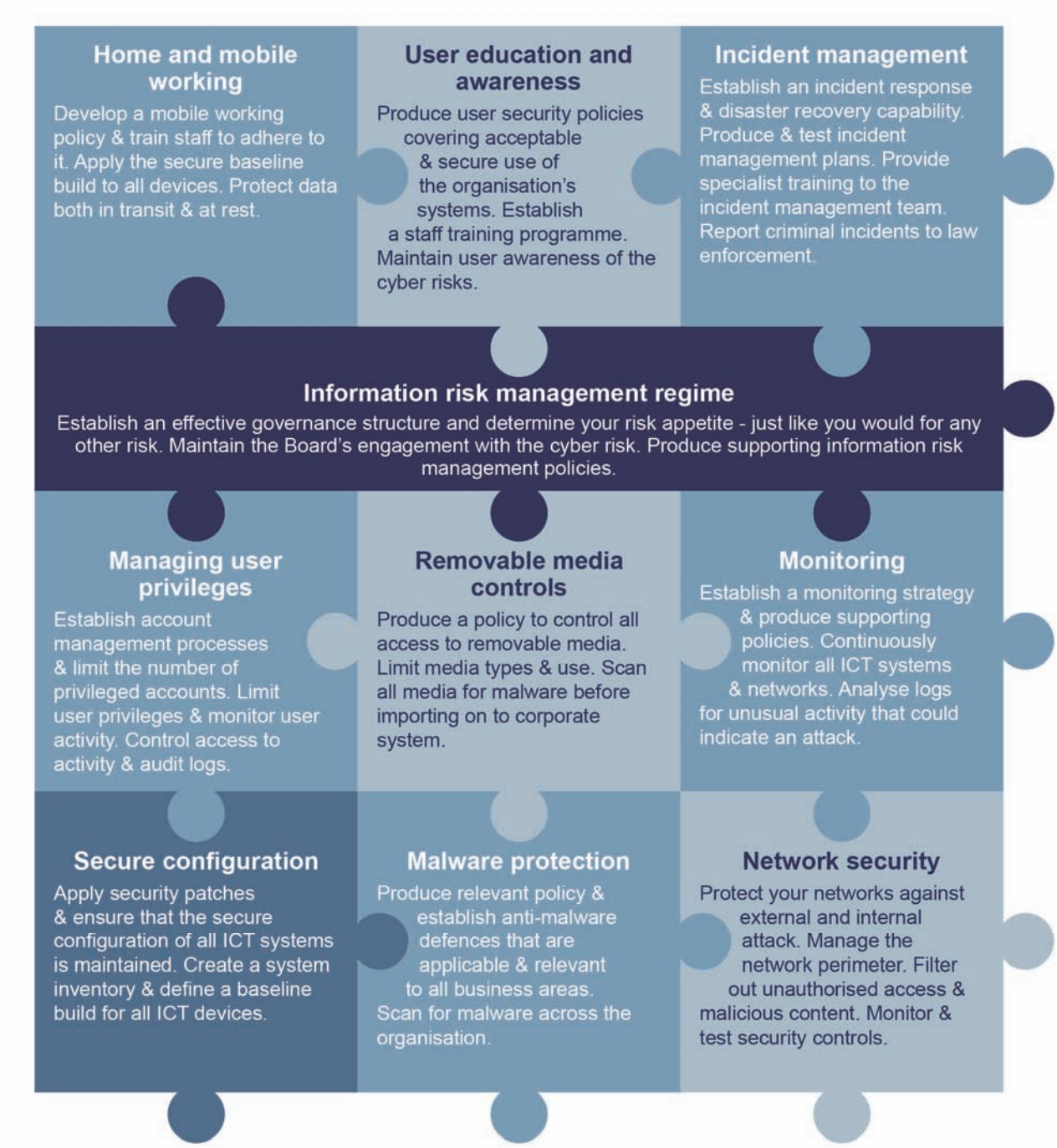
c. **Exercises.** Cyber needs to be exercised in the mainstream along with other capabilities so that users can develop understanding and reversionary modes. Frequent, detailed and well-rehearsed actions in response to cyber attack will be exercised within the Defence Exercise

Plan. Appropriate scenarios and practices for each level of command will differ and may change rapidly in line with the threat. Cyber response activity will be needed to be undertaken at all levels of training (individual and collective). There will also be education as well as training aspects to this requirement.

81. **Business continuity.** Business continuity means being resilient and maintaining service while under attack. By developing a plan based on risk, resilience, impact and interdependency assessments, the effects of such an attack 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 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?

82. **Recovering from malware attack.** 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. System logs for the period of the attack must be retained and ideally the system should be left in its failed state for the investigating officer.



Ten steps towards cyber security

Part 2

Cyberspace is contested every day, every hour, every minute, every second. I can vouch for that from the displays in our own operations centre of minute-by-minute cyber attempts to penetrate systems around the world.

Sir Iain Lobban, GCHQ Director

Examples of cyber attacks

This section illustrates a variety of targets which have been attacked or subjected to malicious activities in cyberspace.

83. We have seen that attacks that take place in cyberspace can take a number of different forms. Some attacks are very simple, while others are more complicated. Some were carried out by individuals, others (allegedly) with State sponsorship or encouragement. The examples chosen demonstrate the complexity and interdependency of cyberspace and some of the many attack tools and techniques available. Few of the attacks were on traditional military targets, illustrating the adversary's perspective on influencing their ultimate goal.

84. In the context of malicious activities, the Home Affairs Select Committee reported on 17 July 2013 that:

> 'A growing number of adversaries now use cyberspace to steal, compromise or destroy critical data. The scale of our dependence means that our prosperity, our key infrastructure, our places of work and our homes can all be affected.'[15]

Note. The following examples contain media reports selected from various external sources. All information contained is publicly available online and provided for situational awareness and understanding. The views and opinions expressed do not reflect those of the Ministry of Defence. Similarly, where alleged perpetrators are identified they have been done so through public sources and not through any investigations or conclusions conducted by the Ministry of Defence. The names of the operations associated with the examples have been assigned by the international cyber security community.

[15] http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/7004.htm.

Example 1 – Actions against individuals

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

Social media application Facebook™

Social engineering attack, reportedly originating from China, harvested the details of those who accepted requests from a fake account.

Social engineering to provide intelligence in peacetime – Facebook™	
Who	Allegedly Chinese hackers.
What	Social engineering.
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, US 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	10 March 2012.
Impact	The wealth of personal information on Admiral Stavridis and potentially his contact network would be invaluable for personality profiling by an adversary. **Embarrassment.** 'Allegedly senior British military officers and MOD officials are understood to have been among those who accepted 'friend' requests...(the information) is believed to include names, email addresses, current locations, pictures of friends and family, clues about home addresses as well as the insights gained about personalities from wall posts.' The Sunday Telegraph newspaper, 10 March 2012.
More information	A guide to keeping safe on Facebook is at: http://www.blogs.mod.uk/onlinesecurity/guidance.html

Example 2 – Hacktivists attacks used against States

These attacks will often be by hacktivists who see themselves supporting their government or culture. Such attacks may also be State coordinated, directed and receive intelligence, and technical tools and techniques support.

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

The bronze soldier of Tallinn (Tallinn Military Cemetery), Estonia

Cyber attacks used in context of State action – Estonia	
Who	Allegedly Russian patriotic hackers, although much broader groups including hackers and script kiddies may have contributed.
What	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?
How	Multiple DoS and DDoS against Estonian utilities, telecommunications and government facilities and their websites making them useless.
Against whom	Principally against Estonian electronic services but also impacted many European telecommunications providers and US 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 this was seen as an insult by Russia. 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.
More information	Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia: https://www.ccdcoe.org/.

Example 3 – Alleged State actions against commerce

Attacks will not normally be acknowledged by the responsible States and may not even be admitted to by the company. States may often claim that the attacks are mounted by patriots or as deception by their adversaries.

Iran and The Netherlands – alleged State action against commerce

Iranian Cyber Army

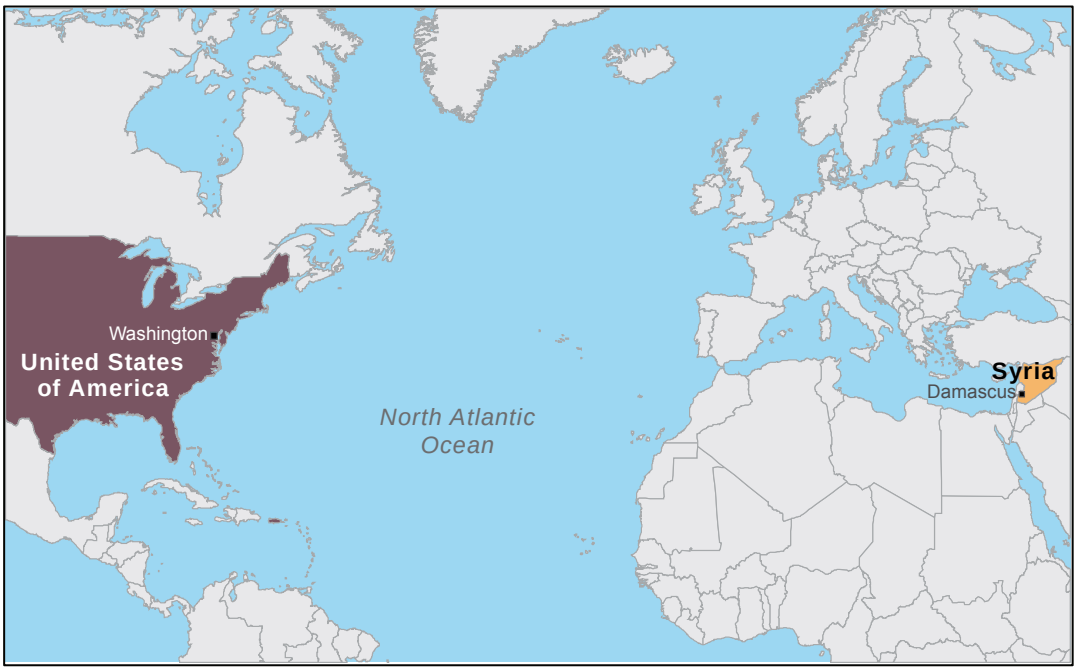
DigiNotar
Internet Trust Services

Dutch Internet company

Cyber undermining confidence in e-commerce – Operation Black Tulip	
Who	This appears to have been a deniable State-encouraged Iranian attack directed at Google, Skype, Yahoo!, Mozilla and others, to collect intelligence on Iranian opposition groups.
What	Issue of false internet security certificates leading to fraudulent ICT access.
How	Misuse of these certificates undermines almost all aspects of secure, remote computing.
Against whom	DigiNotar, now a defunct Dutch company which issued internet security certificates (SSL certificates) to major companies. DigiNotar was a key component of the Dutch government's cyber security policy.
Why	The fake SSL certificates, which authenticate https links for e-commerce and other secure transactions, enabled fraudulent, trusted access to otherwise secure systems including personal, e-commerce and intellectual property data. The aim was also to undermine the Dutch government's cyber security strategy.
When	From 10 July 2011 until approximately 9 September 2011 although some certificates remained valid until July 2013.
Impact	DigiNotar ceased trading and collapsed. DigiNotar did not report the breach when first uncovered, putting millions of transactions and personal details at risk. Trust in the Dutch government's public key infrastructure was undermined affecting identity management, tax, customs and aspects of global e-commerce. Google's Gmail service, amongst other services, was breached and compromised. This attack demonstrates the risks associated with current Internet trust structures.
More information	European Network Information Security Agency (ENISA) provide a detailed report at: http://www.enisa.europa.eu/media/news-items/operation-black-tulip/view

Example 4 – Attacks using social media in political and e-commerce manipulation

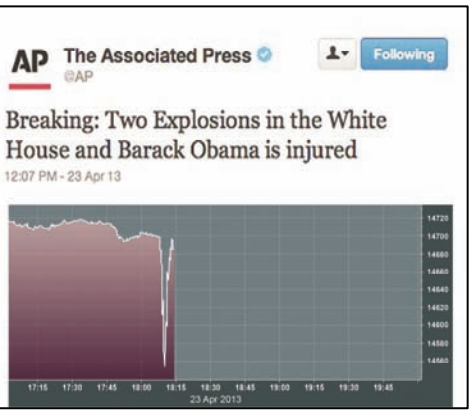
The use of social media as a trusted source of 24hr news was abused with a view to disrupting stock market activities globally through inserting false news feeds concerning the safety of the US president.



Syria and US – conflict involving social media

AP 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.

Syrian Electronic Army



Dow Jones movements

Cyber attacks using Twitter™ in political and e-commerce manipulation	
Who	It appears to have been an alleged State encouraged Syrian attack directed through Twitter at US political and economic stability. The Syrian Electronic Army have also reportedly attacked the Al Jazeera news agency, Reuters and the BBC. Their most recent alleged attack (5 June 2013) was against the Turkish Interior Ministry.
What	Using fake Twitter™ accounts with a web-based interface, where the real AP 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. Media reports that later attacks led to a degree of cooperation between the Syrian Electronic Army and Anonymous,[16] although each has also reportedly attacked the other's websites. This attack emphasises the unreliability of uncorroborated stories broadcast on the Internet, but 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/.

[16] A loosely associated international network of activists and hacktivists.

Example 5 – Cyber attacks used for espionage in peacetime

Operation Aurora is an example of advanced persistent threats used against Google, and Mandiant (an American cyber security firm). The hacker persona we call 'UglyGorilla' (UG) was first documented on 25 October 2004. In addition to his email address, he listed his 'real name' as 'JackWang'.

中国军网 www.chinamil.com.cn 国防社区

关心国防 就是关心我们的家园

User Profile

新飞行员

		User ID:	(O) 5681
		Gender:	Male
		City:	
		Personal home page:	
		Email:	uglygorilla@163.com
		Nickname:	Greenfield
On station Views:	14	Experience:	44 [new pilots]
Last arrival time:	2004-03-17 21:43:11.0	Published number of articles:	15
Real Name:	JackWang	Work units:	
MSN:		ICQ / OICQ / QQ:	
Tel:			

The china.mil profile for 'UglyGorilla', translated by Google

Mandiant report describing China's cyber espionage capability

Cyber attacks used for espionage in peacetime – Operation Aurora	
Who	Alleged attacks by China.
What	Advanced persistent threats (APT), typically spear phishing.
How	Placing rootkits on target ICT to steal intellectual property.
Against whom	Various defence contractors and other commercial entities. One example is Mandiant who published on China's alleged activity. One attack on Mandiant reads: *'Date: Wed, 18 Apr 2012 06:31:41 -0700* *From: Kevin Mandia <kevin.mandia@rocketmail.com>* *Subject: Internal Discussion on the Press Release* *Hello, Shall we schedule a time to meet next week? We need to finalize the press release. Details click here. Kevin Mandia'* At first glance, the email appeared to be from Mandiant's Chief Executive Officer, Kevin Mandia. Scrutiny shows the email was not sent from a Mandiant email account, but from 'kevin.mandia@rocketmail.com'. Rocketmail is a free webmail service. The account 'kevin.mandia@rocketmail.com' does not belong to Mr Mandia, rather an actor signed up for the account specifically for this spear phishing attack.
Why	This attack appeared to have been in retaliation for Mandiant's published report describing China's alleged cyber espionage capability.
When	APT attacks were first identified in 2004 and are ongoing.
Impact	Clicking '*click here'* the computer would have downloaded a malicious ZIP file. 'Internal_Discussion_Press_Release_In_Next_Week8.zip'. This file contains a malicious executable that installs a backdoor giving root access. This would have: compromised Mandiant's human and electronic sources; undermined data integrity; and given the APT advance notice of future publications.
More information	A full report is at the Mandiant website: http://intelreport.mandiant.com/Mandiant_APT1_report.pdf

Example 6 – Cyber attacks in support of conventional operations

Israel and Syria – Cyber attacks in support of conventional operations

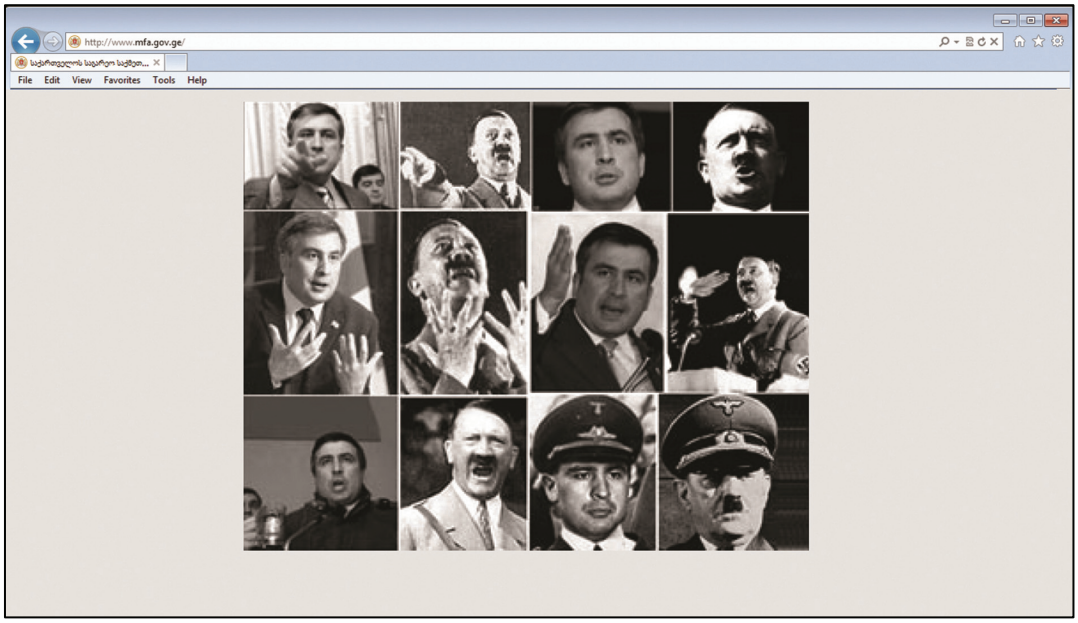
Aerial view of Syrian nuclear research institute at Dayr az-Zawr, allegedly attacked by Israeli military aircraft

Cyber attacks in support of conventional operations	
Who	Unconfirmed.
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/

Example 7 – Alleged State against State cyber actions

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.

Cyber attacks used in the context of State action – Georgia



Replacing Georgian President's image on website and comparing him with Hitler

Cyber attacks used in context of State action – Georgia	
Who	Alleged Russian Business Network (group of Russian hacktivists) and the South Ossetia Hack Crew, thought by 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 US and UK embassies in Georgia. Most other attacks were distributed denial of service with website defacement and communications re-routing.
How	Replacement of 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 hrs, 8 August 2008 till 12:45 hrs 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 sowed confusion in the government sphere 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* (Nov 08). CCDCOE document at http://www.ccdcoe.org/.

Example 8 – Alleged covert State against State cyber actions

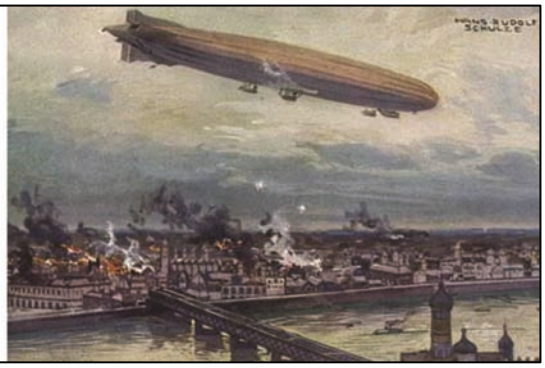
These attacks have been used as part of covert operations to influence or undermine the political will of a third party to change their policies.

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 attacks used for destruction	
Who	Unconfirmed.
What	Intelligence collection, denial of service attack against Siemens SCADA[17] 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 targets of opportunity were also incidentally infected overseas.
Why	Reportedly a 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 US banking structure and other targets (see Shamoon example).
More information	Symantec technical report is at: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[17] SCADA – supervisory control and data acquisition.

Example 9 – Cyber used for destructive attacks

Iran and Saudi Aramco – alleged retaliation for Stuxnet

Saudi Aramco restores network services

News

Latest news

2012

Saudi Aramco has restored all its main internal network services that were impacted on August 15, 2012, by a malicious virus.

Saudi Aramco has restored all its main internal network services that were impacted on August 15, 2012, by a malicious virus that originated from external sources and affected about 30,000 workstations. The workstations have since been cleaned and restored to service. As a precaution, remote internet access to online resources was restricted.

Saudi Aramco implying cyber attack had little significant business impact

Destructive cyber attacks – Shamoon	
Who	Attack allegedly to have been conducted by the Iranian hacking group 'Cutting Sword of Justice'.
What	Denial of service attack against oil and gas company networks, wiping hard disks. The sophistication of the malware, whilst effective, was relatively low.
How	Recognized as *W32.Disttrack*, a piece of wiper malware, the malware also changes the active partitions of an infected machine and wipes 'priority' files tagged with download, document, picture, music, video and desktop. Once the wiping 'death' date is read from a .pnf file and checks out, the wiper is activated.
Against whom	Principally Saudi Arabian and US oil and gas companies.
Why	Media reports that this was apparently in retaliation for Stuxnet and as a wider economic attack on Saudi Arabian, US and Allied assets.
When	September 2012.
Impact	Shamoon is linked to the malware outbreaks at Saudi Aramco and RasGas, Gulf-based oil and gas firms. Saudi Aramco lost its network for 10 days as a result of the attack, which affected 30,000 to 50,000 workstations. The outbreak was significant because Shamoon contains file-wiping functionality that made infected machines inoperable as well as destroying data.
More information	Media reports that the creators of Shamoon malware appear not to be high-profile programmers and the nature of their mistakes suggests that they are amateurs, albeit skillful, as they created a practicable piece of self-replicating, destructive malware. Kaspersky Labs have conducted detailed analysis - a brief summary can be found at: http://www.theregister.co.uk/2012/09/12/shamoon_analysis/

Example 10 – Cyber attacks used in State against State tension

Hactivists, allegedly encouraged and supported by States, are frequently used to publically conduct conflict in cyberspace as an alternative to conventional warfare.

North and South Korea in constant tension

This relatively low-tension form of conflict may be easier to manage than the uncertainties of kinetic actions. But it can inflame passions on the part of both participants as they see conflict brought to their doorstep in the form of denial of service of utilities and commerce.

Cyber attacks on the Republic of Korea President's Office website

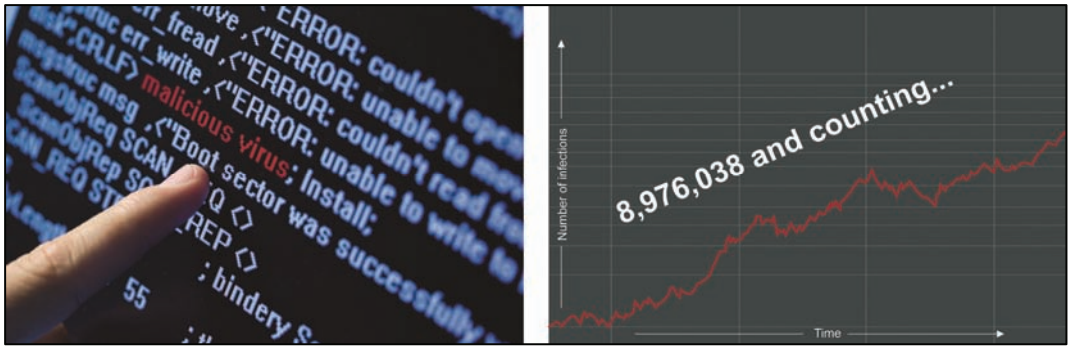
Republic of Korea (South Korea) Cyber Terror Response Center

Cyber attacks used in context of State against State tension	
Who	North Korea and South Korea are alleged to be in constant low-level cyber conflict attacking each other's government, media, commercial and banking websites. Both nations also blame Anonymous.
What	Attacks against critical national infrastructure using a very wide range of computer network attack tools and techniques.
How	Website hijacking, defacing and also significant GPS jamming against aircraft and shipping. Open-source information states that the servers used by both nations appear to be based in China.
Against whom	Each nation accuses the other, and Anonymous, of the attacks.
Why	To cause economic damage, provoke government responses and for nationalistic propaganda purposes. In these cases, cyber operations appear to be a proxy, maintaining tensions and the appearance of military superiority without the danger of widespread kinetic conflict.
When	These attacks have been constant since at least 2009 and appear to be continuing to date.
Impact	Low impact on ICT and navigation safety. Disrupts inter-government relations and loses confidence in South Korean utility provision and security of e-commerce. South Korea has established a national cyber alert system.
More information	Background to the on-going cyber conflict between North and South Korea and how this contributes to the levels of tension is expanded at: http://www.theregister.co.uk/2013/06/25/korean_war_anniversary_ddos_attacks http://www.guardian.co.uk/world/2013/jun/25/north-korea-south-websites-hacking-cyber-attack

Example 11 – Impact of malware on military operations

Malware may not necessarily be directed at 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.



Conficker virus infecting systems

Increasing rate of Conficker virus infections

Impact of malware on military operations – Conficker	
Who	Unidentified. On 13 February 2009, Microsoft offered a $250,000 reward leading to the arrest and conviction of the perpetrators. Ukrainian IP addresses are reported to be immune to Conficker as are keyboards with Ukrainian layouts.
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 admin passwords and generally creates a DoS attack on infected machines.
Against whom	Any ICT running Windows server services. This includes, but was not targeted specifically against, much military hardware where infection was transmitted both over networks and by misusing USB memory sticks.
Why	Unknown.
When	The 'A' variant of Conficker surfaced on 21 November 2008; the 'E' variant continues to date.
Impact	Within the UK, Royal Navy Navystar/N desktops, MOD 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 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

Example 12 – Threat from insiders

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 cables, 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 HMCS Trinity in Halifax, disclosed large amounts of highly classified intelligence to his Russian handler. Delise was sentenced to 20 years imprisonment.

Contractor Edward Snowden

May 2013: Release of classified NSA 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 US and European telephone data, and the PRISM, XKeyscore, and Tempora Internet surveillance programmes. Snowden is currently seeking refuge in Russia.

Lexicon

Part 1 – Acronyms and abbreviations

APT	advanced persistent threat
CERT	computer emergency response team
CERT UK	Computer Emergency Response Team UK
CII criti	cal information infrastructures
CIIP	critical information infrastructure protection
CISP	Cyber Security Information Sharing Partnership
CNI	critical national infrastructure
CPNI	Centre for the Protection of National Infrastructure
CSOC	Cyber Security Operations Centre
DCSP	Defence Cyber Security Programme
DCP Defence	Cyber Programme
DCPP	Defence Cyber Protection Partnership
DoS	denial of service (attack)
DDoS	distributed denial of service (attack)
DMC	Defence Media Communications (MOD)
EW electroni	c warfare
FIRST	Forum for Incident Response and Security Teams
GCHQ	Government Communications Headquarters
GPS global	positioning system
GovCERT	Government Computer Emergency Response Team
ICT	information and communication technologies
IP Internet	protocol
HTTPS	hypertext transfer protocol secure
HUMINT human	intelligence
LOAC	Law of Armed Conflict

Malware	malicious software
MASINT	measurement and signature intelligence
MOD	Ministry of Defence
NATO	North Atlantic Treaty Organization
NCI	NATO Communications and Information Agency
NC3A	NATO Command, Control and Communications Agency
OCSIA	Office of Cyber Security and Information Assurance
OPSEC	operations security
SCADA	supervisory control and data acquisition
SFIA	Skills Framework for the Information Age
SIGINT	signals intelligence
SSL	secure socket layer
USB	universal serial bus
WARPs	warning and reporting points

Part 2 – Additional terms and definitions

These additional terms and definitions are for educational awareness. Endorsed definitions are in purple, those which are not endorsed are in black.

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)[18]

botnet
A network of private computers infected with malicious software and controlled as a group without the owners knowledge.
(Concise Oxford English Dictionary (COED), 12th edition, 2011)

chat rooms
An area on the Internet or other computer network where users can communicate, typically one dedicated to a particular topic..
(COED, 12th edition, 2011)

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.
(MOD Information Management Passport – Cyber module)

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

[18] http://www.sans.org/security-resources/glossary-of-terms.

from accessing the service. Distributed denial of service attack uses multiple PCs to launch the attack, which increases the disruption, and attackers usually make use of a Botnet. (CSOC[19])

electronic warfare
Military action that exploits electromagnetic energy to provide situational awareness and achieve offensive and defensive effects. (Allied Administrative Publication (AAP)-06, 2013)

firewall
A part of a computer system or network which is designed to block unauthorized access while permitting outward communication.
(COED, 12th edition, 2011)

global positioning system (GPS)
An accurate worldwide navigational and surveying facility based on the reception of signals from an array of orbiting satellites.
(COED, 12th edition, 2011)

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 honey pot 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 provide by human sources. (AAP-06, 2013)

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. (NATO MC422/4)

[19] CSOC is the Cyber Security Operations Centre.

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 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 indentifying any distinctive features associated with the source, emitter or sender, to facilitate the latter's measurement and identification. (AAP-06, 2013)

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, 2013)

proxy
A human proxy is: a person authorised to act on behalf of another. (COED, 12th edition, 2011) 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, 2013)

spam
Irrelevant or unsolicited messages sent over the Internet, typically to large numbers of users. (COED, 12th edition, 2011)

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

UK National Security Strategy 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.

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

MOD Defence Cyber Security Programme provides a focussed approach to cyber, ensuring the resilience of MOD vital networks and placing cyber at the heart of defence operations, doctrine and training.

Joint Doctrine Note 3/13, Cyber Operations – The Defence Contribution describes cyber activities in the contemporary operating environment. This publication provides the doctrinal basis for operations, exercises, force development and experimentation.

Joint Service Publication 440, Part 8 – The Defence Manual of Security contains policy and guidance relating to Communications and ICT 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.

Joint Warfare Publication 3-80 – Information Operations provides understanding, information and guidance to all involved in the planning and execution of information operations on Joint and single Service operations.

Joint Service Publication 383 – The Manual of the Law of Armed Conflict is a reference for members of the UK's 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.

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 MOD's networks, or connect to them with security advice. These are 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.

Cyber bullying. This link is to the Army's advice on cyber bullying. Navy advice is here.

Social media information card leaflet from 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.

House of Commons Defence Committee, Defence and Cyber - Security: Government Sixth Report of Session 2012-13 focuses on the how MOD was adapting to cyber including the management and planning to overcome the threats emanating from it.

Tallinn Manual on International Law Applicable to Cyber Warfare examines how extant international law applies to this 'new' form of warfare. The manual is not an endorsed UK position.

10 top tips for protecting yourself and MOD

1. If in any doubt, don't open e-mails from strangers without running them past your IT security team first. Don't visit inappropriate websites.
2. Don't connect untrusted devices, especially USB sticks, mobile phones etc.
3. Don't attempt to change your system configuration – it is like that for a reason.
4. Keep security patches and anti-virus software updated – and switched on.
5. Don't be tempted to carry unencrypted data – you will lose it.
6. Be conscious of Social Engineering – if you've ever given away a business card or your contact details, you are vulnerable.
7. Don't work on MOD business on your home computer – it may be already compromised.
8. Don't be tempted to 'top and tail' documents just to lower the classification – contextual keyword and password searches will uncover your sins.
9. Be security conscious at all times. All ranks are targets; remember, Bradley Manning was a Private and compromised over 240,000 classified documents; James Stavridis is an Admiral and his identity was used to compromise senior NATO officers.
10. Read, understand and follow JSP 440 and associated security documentation.

Published by the Ministry of Defence UK
This document is also available at
www.gov.uk/development-concepts-and-doctrine-centre