Chapter 4

Targeting Information Infrastructures

Ian Dudgeon

Introduction

The national, defence and global information infrastructures underpin and enable today's information society. They play a critical role in how we and others live, and they shape and influence our decision cycle, i.e. what we see, think, decide and how we act. In defence terms, these infrastructures largely determine the functional efficiency of a country's Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance and Electronic Warfare (C4ISREW) and net-warfare capability. And in both defence and broader national security terms, they provide a pathway to psychological operations. Foreign information infrastructures can be targeted to weaken the military capability and national morale of an adversary, and strengthen those of allies and friends. In certain non-war circumstances, foreign infrastructures may also be targeted to project national power, and shape events to national advantage. The ability to target foreign infrastructures for military advantage in combat operations, and to influence the morale and decision-making of friends and foes alike, is recognised as an essential inclusion in the twenty-first century inventory of national capabilities. Australia must develop this capability to protect and project its national interests.

The information society

The advent of the Information Age, now into its second decade, has brought about very fundamental changes in the way that all societies now function.

The information society, including the various information-based environments within, is now a reality. The exponential growth in Information Technology (IT), the accompanying seamless and virtually instant access to vastly disparate information resources, and the flexibility to positively exploit that technology and information across government, business and society generally, is unprecedented.

In all modern functioning nations, which include Australia and all developed and most developing countries, access to and the benefits derived from the information society are taken for granted.

At the personal or micro level, the expectation and ability to instantly communicate and access comprehensive information resources, including domestic and international media broadcasts, iPod downloads, chat rooms or the like, on a 24/7 basis, by such now-basic means as mobile phones,[1] the Internet, and Personal Digital Assistants (PDAs), is the norm.

At the macro level, the provision of reliable information and information technology-dependent services across government and the private sector, is also assumed. Examples include key industries and groupings which are essential to the efficient functionality of the state, such as communications; banking and finance; transportation and distribution services; energy including electricity, oil and gas; water supply; education; the media and other information services; and other essential government services including defence, and emergency services. It is these industries and groupings that enable such activities as share market trading; domestic and international banking; salary and social security payments; electricity distribution; robotics in manufacturing; integrated logistic systems; suburban and interstate train services; air traffic control; all telephone and Internet services; supermarket checkout transactions; and functional C4ISREW in support of the Defence forces.

In less-developed countries, including, for example, some nations in the Asia-Pacific region, the availability of many of the above services across society generally may be limited, because of less infrastructure-related investment or the skills to maintain a reliable service. However, they do exist and generally work well where the local government and key private sector organisations want them to; for instance, for political, defence and other security reasons, and for commercial profitability.

The benefits enjoyed by the information society identifiably include access to better services, enhanced government and private sector capabilities generally and other lifestyle improvements. But the information now available, and the sophistication of supporting technology, impacts across society both quantitatively and qualitatively, and with an intensity, never before experienced. This impact affects not only how we live, but also shapes and influences our decision cycle (what we see, hear, think, decide, and how we act).[2]

For this combination of reasons, information and its supporting technology would—indeed must—routinely be included on the targeting list of any nation at war, especially any nation that includes Information Operations (IO)[3] as a core capability of its warfighting inventory. Furthermore, they would also be included on the list of potential targets of a nation, non-state organisation or individual who seeks to shape or influence specific physical events, or decision-making, across any part of the public, private or general sectors of the information society, in non-war circumstances.

Information Infrastructures: the NII, GII and DII

What is being targeted, by us or by others? The answer is three mostly interconnected and interdependent information infrastructures. The first is the National Information Infrastructure (NII), this being the key network element within a country that enables its information society to function, and determines the efficiency of its functionality. The second is the Global Information Infrastructure (GII), which provides the international connectivity to the NII. The third is the Defence Information Infrastructure (DII), which, as the name implies, serves a country's Defence organisation, both military and civilian.

Definitions of the above vary between authorities, authors and so on within and between countries, but all boil down to the same essential characteristics. ADF definitions have been used below as the primary definitions for the NII and DII because of the ADF's lead role in Australia for targeting any foreign infrastructures. Another definition of the NII, drawn from Defence sources, has also been cited because of its simplicity. Interestingly, the ADF has no definition of the GII.

The National Information Infrastructure

The NII is defined in Australian Defence Doctrine Publication (ADDP) 3-13—*Information Operations* (2006), as

> compris[ing] the nation wide telecommunications networks, computers, databases and electronic systems; it includes the Internet, the public switched networks, public and private networks, cable and wireless, and satellite telecommunications. The NII includes the information resident in networks and systems, the applications and software that allows users to manipulate, organise and digest the information; the value added services; network standards and protocols; encryption processes; and importantly the people who create information, develop applications and services, conduct facilities, and train others to utilise its potential.[4]

The above is more a statement of the composition of the NII than a typical definition, but is very useful in that regard. A shorter definition initially used by Australia's Defence Signals Directorate (DSD) in 1997, in Australia's first national study of the threats to and vulnerabilities of the NII, reads:

> [The NII] comprises those components that make up the network within and over which information is stored, processed and transported. It includes those people who manage and serve the infrastructure, and the information itself. This information may take the form of electronic voice, facsimile or data.[5]

The Global Information Infrastructure

Although there is presently no ADF definition of the GII, the current US Department of Defense definition is

> the worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The global information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact discs, video and audio tape, cable, wire, satellites, fibre optic-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure. Also known as the GII.[6]

This definition is essentially the same as the US definition for the NII, the only difference being the substitution of the words 'the worldwide interconnection' with 'the nationwide interconnection' as the lead.[7] As for the ADF definition of the NII, the US NII and GII definitions contain a useful description of the composition of components within these infrastructures.

Alternatively, the GII may be defined simplistically as comprising *a global network of NIIs as well as other dedicated international information networks*.

However, the GII, as defined, is not identical with the Internet. The Internet is the global network of networks; other dedicated networks that are stand-alone and not networked, are not part of the Internet.

The Defence Information Infrastructure

The DII is defined in ADDP 3-13 as

> the shared or interconnected system of telecommunications networks, computers, data bases and electronic systems serving the Defence Department's national and global information needs. It is a subset of and comprises the NII, and includes the people who manage and serve the infrastructure, and the information itself. It includes information infrastructure which is not owned, controlled, managed or administered by Defence.[8]

The issue of ownership, control and management applies to the NII and GII as well as the DII, and is discussed further below.

Information Infrastructures: Some key characteristics

A number of key characteristics of information infrastructures flow from the above definitions that are important to targeting considerations. These include

components, *connectivity*, *bandwidth*, *functional interdependence*, and *ownership and control*.

Components

The NII, DII and GII comprise five distinct interdependent components. The first four are explicit in the definitions above; the fifth is more implicit:

- the *hardware*, e.g. the computers; sensors; physical transmission components such as cable; radio/wireless; satellites, and transmission towers;
- the *software* applications, e.g. processes; protocols; encryption; and firewalls;
- the *information* itself, e.g. the databases; and information in transmission including voice, facsimile, text messages, imagery, or information in other forms;
- the *people* who operate and maintain the infrastructure; and
- *power supply*, without which hardware and software cannot function and information cannot be transmitted or accessed. While integrated backup power supply (e.g. uninterrupted power systems (UPS)) could be considered a part of the hardware component, mains supply is not. Most UPS have only a limited capability in terms of both duration and capacity, and mains supply remains critical for full and enduring functionality.

Connectivity

The very broad, virtually instantaneous and seamless connectivity and reach across the various domestic and international information domains of the NII/GII/DII networks is a characteristic that also contributes significantly to infrastructure functional efficiency. Users of these infrastructures have adjusted business or other practices accordingly. Real-time communications are now critical in many areas of business and government. The domestic and global marketplace, which includes stock exchange and credit card transactions, are such examples.[9] This real-time dependence also applies to many emergency services and especially to Defence functions across the whole C4ISREW spectrum, including sensor to weapon configurations, during combat operations. Disruption to connectivity, even for relatively brief periods of time, could have a major impact on outcomes.

Bandwidth

Bandwidth across all three infrastructures is constantly increasing, particularly over data networks, in parallel with technology improvements. Client demand has not only kept pace with bandwidth availability, but has outstripped it. Broad bandwidth allows access to vast quantities of information in a very short space of time. In a Defence context in particular, it is an important feature of real-time delivery of surveillance and reconnaissance imagery, and the immediate 'pull-down' accessibility of deployed combat forces to their headquarters'

intelligence databases. It is also important in emergency services scenarios, for example in real-time or near real-time monitoring of bushfires or other natural disasters where lives are at risk and the timely delivery of humanitarian aid is critical.

Functional interdependence

Functional interdependence between information and its supporting systems, and between the supporting systems themselves, is a major factor related to the functional efficiency and security of any information infrastructure. And the more complex the system or network, the greater that interdependence. Failure, in whole or by a part of any component of an interdependent system, can impact on the functionality of another part or, potentially, on the whole system. Depending on the type of system affected (for example, its size or complexity) and the scale of the failure, the cascade effect can have significant implications for specific or general services and capabilities, and ultimately affect how people live and behave. In military terms especially, this cascade of 'knock-on' effects fits the classic mould of targeting outcomes in 'effects-based' operations.[10]

The principle of related 'effects-based' considerations also applies to any compromise of the five key criteria of Information Assurance (IA), which is discussed in more detail later in this chapter.

Ownership and control

Ownership of the networks that make up the NII, DII (and thus GII) varies between the government and private sector, depending on the country, and what part of the network within that country, is involved. In most countries today, the major telecommunications service providers are privately owned. And in the world of globalisation, those services may be owned, or part owned by foreign private corporations, the exceptions being where the major telecommunications service providers are state-owned enterprises, like, for example, in North Korea.

In addition, the majority of software systems, especially commercial off-the-shelf (COTS) operating systems, are sourced from foreign corporations, as are many specialist hardware components used within those systems.[11]

Furthermore, the people who develop and maintain and administer particular systems within networks, or the networks themselves, will usually be from the private sector, and indeed may be foreigners.

The up-side of the above is that globalisation or selective global marketing enables access, potentially, to the best hardware, software and people services that are available to deliver and maintain key parts of a country's NII and DII.

The down-side is that a country (i.e. its people and government as both shareholders and stakeholders) may not own or, in reality, fully control or

manage these vital national services. Potentially at least, systems and networks could be vulnerable (in the production, operating and administrative phases) to a hostile person (local or foreign), acting on behalf of others or alone, who accesses, manipulates (or establishes the means to access and manipulate) the functionality of the systems and networks at a future date. There are many ways how this might be done, within and without the target country, but could include covertly inserting trap-doors and 'Trojan horses' in its operating software, causing the malfunction of key hardware and software components at a critical time, or enabling other hostiles to access exploitable parts of the system. In normal circumstances this situation might not pose a significant risk, but it could become a national security issue in a time of crisis or war.

The percentage of the DII that is made up of and dependent on the NII, and GII, varies from country to country, but it is generally assessed in most technically advanced countries as about 90 per cent or more. Thus, only 10 per cent or less of the DII in these countries falls into the category of being owned, controlled, managed or administered by their Defence organisation. And, generally, the infrastructure that they do own, control and manage exists primarily at the tactical level only. Few countries can afford to have their own fully independent strategic and/or operational broadband communications systems. The United States is one such country, but that resource is nevertheless limited relative to the total size and operational commitments of the US armed forces. This limitation necessitates the majority of communications being transmitted over leased or other non-Defence owned networks.

One important conclusion is, therefore, that a significant proportion of any Defence organisation's C4ISREW capability, its Network Centric Warfare (NCW) 'information superiority' capability, and any potential information-based Asymmetric Warfare capability, is outside its total control, and may well be foreign owned and under actual or de facto foreign control.

It also means that maintaining and protecting a functional and efficient NII (inclusive of DII components) and its GII connectivity is a critical *Defence-specific security requirement*, as much as a broader *national security requirement*.

The Importance of Information Assurance

IA is another key consideration of NII/DII and GII targeting. Effective IA is a critical element in the information society, and underpins both the functionality and efficiency of all information infrastructures.

IA comprises five essential criteria for the protection of information and friendly systems against unauthorised access: *availability*, *integrity*, *confidentiality*, *authentication* and *non-repudiation*:

- *availability* applies to the information itself, its supporting technology and the people who operate and serve the infrastructure;
- *integrity* refers to the trustworthiness of information and system/process reliability;
- *confidentiality* is about denying access to the information and sensitive aspects of supporting technology, to those persons without authorisation;
- *authentication* refers to assuring that those who do access the information or supporting systems have the requisite authorisation; and
- *non-repudiation* is linked to authentication and, effectively, is the digital signature.

The principle that applies to functionally-interdependent systems, whereby the failure of one component can impact on the functionality of one or more other components, also applies to IA. Thus, if any of the above IA criteria are compromised for any reason, at least some element of information and/or functionality and efficiency of related information infrastructures is also likely to be compromised. The more significant the compromise, particularly in key areas or system choke-points or nodes, the more significant the impact will be on functionally and efficiency. Identifying existing vulnerabilities, or creating vulnerabilities that will enable IA to be compromised, is an important part of the targeting process.

The effective implementation of IA involves a wide range of security processes and procedures, as well as physical measures. One important measure is redundancy and diversity, which is intended to counteract the effects of any failure within, or compromise of, a system, or at least to minimise those effects. However, the high-end functionality and efficiency of many of the processes, systems, services and capabilities we rely on and take for granted is dependent, or largely dependent, on current-generation hardware and software. For high-tech systems in particular, the rapid changes in technology resulting in increasingly more powerful hardware and software, means that planned redundancy and diversity to provide effective backup and continuity, must also largely keep pace technologically with primary-use hardware and software.

In Australia and other developed and many developing countries, redundancy and diversity across critical infrastructure has been significantly hardened since the 11 September 2001 terrorist attacks on the United States, but at a cost. However, even high-quality redundancy and diversity might struggle to provide a full service if challenged to do so. But where that quality of investment is not made, or made in depth, technologically-dated backup systems may simply be incapable of maintaining even a basic level of services over a short period to meet national or sector needs, if put to the test.

Redundancy and diversity, however robust, must be recognised as part of the IA equation. They must therefore be factored into targeting considerations.

Targeting Information Infrastructures: who and why?

As indicated earlier above, there are three broad groups of people who, potentially, might target information infrastructures: a nation-state or country for national security reasons; a non-state organisation such as a terrorist, criminal, or political or other Issue Motivated Group (IMG) in pursuit of group objectives; or an individual in pursuit of personal objectives.

Motivation, be it for the short, medium or long term and whether for tactical, operational, strategic or other reasons, is important as it will indicate potential targets, irrespective of whether that targeting process and plan is highly sophisticated and focused or, apparently, more simple, random and opportunistic.[12]

Nation-state targeting

Nation-state targeting may occur during war or non-war situations.

War: targeting the adversary

At the national level, the most obvious scenario for one or more countries to target the NII, DII and GII connectivity of another country or countries is when those countries are at war. The overriding political objective in this scenario would be to win the war by destroying the military warfighting capability and the military and civilian logistic and other support capacity of the adversary or adversaries to wage war; and by changing the will of their military, politicians and civilian population from pursuing the war to seeking peace.

Post-war objectives, ideally shaped during the conflict itself, concerning the future profile of the enemy nation or nations, would include the restoration of a politically viable and economically functional state, sympathetic (in the case of Australia) to Australia's national interests.

Operations and activities undertaken during war against an adversary to achieve the above objectives would, of necessity, be directed at both military and civilian targets, and be both overt and covert.[13] In addition, activities across the adversary's NII, DII and relevant GII linkages, that are undertaken to shape and influence outcomes, would employ destruction and degradation of those infrastructures. Deception and psychological measures would also exploit the adversary's information infrastructures, and those in other countries where these also could contribute to denigrating the adversary's capability and will.

In sum, the measures undertaken would encompass the full spectrum of IO including computer network attack, deception and psychological operations.

War: targeting allies, friends and neutrals

Other activities undertaken during war would target allies and friendly countries to boost their morale and commitment to the war effort and post-war objectives. Such activities would be primarily psychological in nature.

Neutrals would also be targeted, in an effort to persuade them to commit to the allied cause, or at least counter any enemy propaganda aimed at persuading them to commit to the axis cause. Such activities would focus primarily on psychological measures. In certain circumstances, however, where a neutral country or business enterprise within is supplying important military or military-support matériel to the adversary, the information infrastructure within the neutral country that is linked to the production or delivery of that matériel, could be targeted to cease or disrupt supply.

Non-war situations or circumstances short of war

In these situations and circumstances a range of scenarios exist that may politically justify targeting another country's information infrastructures. Scenarios include, but are not limited to:

- Intelligence gathering directed at obtaining information from the NII, DII or GII linkages of the targeted country or countries, through activities as communications intercept, computer network exploitation (CNE)[14] and/or human intelligence (HUMINT) operations. Depending on the country, these operations could be enduring and undertaken to meet specific national intelligence requirements, whether political, strategic, military, economic, societal or any combination of these. The intelligence product would feed the national assessment and policy process of the collector, enabling that collector to plan and undertake action to maximise that country's advantage, or minimise any disadvantage, relevant to the target.
- Assisting friendly opposition elements in a target country that is hostile or opposed to our key national security interests, but does not pose the threat of war, to assist the opposition to bring about a change to that government's policy, or indeed change the government itself. Assistance in this scenario would be mostly covert and generally limited to psychological measures and possibly deception, but would not include destruction or degradation of the NII/DII.
- Pre-emptive action against a country with which we are not at war, but where that country poses an imminent threat to us of war or aggression. As in the previous scenario, activities could be directed at assisting opposition elements in the target country to bring about change to that government's policy or of the government itself. Opposition elements in this scenario could include any armed resistance groups, and assistance could incorporate

psychological measures and covert attacks directed at destroying or degrading the NII/DII and GII linkages, and deception.

- Pre-emptive action as above, but where the threat of war or aggression is to allies or friendly governments.

- Activities against hostile occupation forces in an allied or friendly country, where those invasion and occupation forces involved a country with whom we are not at war. Activities would be directed at undermining the capability and morale of occupation forces, while boosting the capability and morale of resistance forces, in order to force the ultimate withdrawal or capitulation of the aggressor. Activities would include psychological measures, deception and the destruction and degradation of the aggressor's DII and relevant parts of the occupied country's NII and GII linkages. Activities generally would be covert, but the veneer of deniability may be thin. In these circumstances, psychological and other appropriate activities would also be undertaken against the targeted aggressor within their country and appropriate third countries in support of these objectives.

- Disruption activities against an aggressor or hostile non-government organisation or individual in a third country or countries (e.g. targeting a terrorist organisation, IMG, criminal group or particular individual who might pose a specific but serious security risk), in order to destroy, disrupt or neutralise that group or individual's actions. Depending on the circumstances, activities could include the destruction or degradation of NII and GII linkages, deception, and psychological measures. Activities could be overt and covert, or a combination of both.

In the case of a terrorist organisation, the breadth and intensity of activities could match aspects of those undertaken in wartime.

In all circumstances in an Australian context, the above activities would have the endorsement of government at the highest level, and be coordinated with other activities that would or may be undertaken by government via other agencies of government, including its Defence forces, on a unilateral, bilateral or multilateral basis. Where appropriate, they would also be coordinated with similar concurrent activities undertaken by allies or friends.

Targeting by non-state organisations

Some targeting considerations applicable to three non-state organisations are reviewed briefly below. They are *terrorist organisations*, *criminals*, and *IMGs*.

Terrorist organisations

The targeting of information infrastructures by terrorists is normally aimed at the dissemination of propaganda that promotes the terrorist's political objectives. Objectives include justifying and proselytising their own cause and

actions, disseminating propaganda that emphasises the evils, corruption, injustices or misguided thinking of their opponents or enemies (usually, but not exclusively, ideologies, governments, and individuals within government), winning over converts to their cause, and recruiting new activists. Most terrorist organisations are very adept in the use of psychological measures across media outlets or the Internet, and know how to focus their messages to play on the emotions of their target group. And unlike the Western media or Internet sources which will often censor graphic descriptions or images of tragic scenes, including atrocities committed by terrorists, the terrorists themselves will play up graphically any tragic situation caused by, or which they attribute to, the 'enemy' in order to instil high levels of fear and/or hatred of that 'enemy'. Typical examples are images of 'collateral damage' by their 'enemy', involving graphic pictures of bodies of innocent women and children. Other examples of graphic releases have been 'justifiable acts of revenge' or 'justice' in the form of a video of the execution of an 'enemy' agent.[15]

Other forms of the use of information infrastructures by terrorists are illegal activities to finance their operations, counterfeiting, and money laundering. Examples of the former include drug trafficking and credit card fraud. Tamara Makarenko, an international specialist on criminal affairs, claims that these activities are widespread amongst some terrorist groups.[16] Interestingly, an autobiography published in 2004 and written by Imam Samudra, one of the Indonesians involved in the Bali bombings in 2002, includes a chapter entitled 'Hacking. Why Not?' In this chapter Samudra urges fellow Muslim radicals to take the holy war into cyber-space by attacking US computers specifically for the purpose of credit card fraud. Samudra apparently tried, unsuccessfully, to finance the Bali bombings by attempting such fraud himself.[17] Counterfeiting has been used for the production of false identity documents for the use of terrorist members, while money laundering has been used to hide the sources and quantities of any funds.

Most terrorist organisations are well aware of the vulnerability of their members' communications being intercepted when using telephones (mobile or land line) or the Internet, and have adopted procedures to minimise the risk. These include maximising the use of 'clean' phones by the frequent replacement of the phone and Subscriber Identity Module (SIM) card. One technique for clandestine communication over the Internet is the use of 'steganography', whereby secret messages are concealed beneath overt messages—a sort of electronic microdot. Encryption is also used.

The modus operandi of terrorist organisations can vary significantly depending on their objectives and the sophistication of their training. For example, in the Philippines many terrorist activities have involved the destruction of physical infrastructure by explosives or arson, particularly that

owned by companies who refuse to bow to extortion and meet terrorist demands for payment of 'revolutionary taxes'. Targets have included information infrastructure hardware, and/or supporting infrastructure, such as communications towers, electricity transmission towers, and electricity sub-stations. They have been selected not because of any focus on information infrastructure as such, but simply because such targets are accessible and incur less risk to the attackers than optional targets. In this sense, they can be described as opportunistic. But information infrastructure can also be deliberately targeted where this fits with terrorist objectives.

Publicly available information indicates that while there is evidence that a number of terrorists use sophisticated computer skills to conduct activities such as identity theft and credit card fraud, there is no evidence of them having, or at least using, hacking or other skills to conduct large-scale theft or extortion. There is, however, no reason to assume terrorists will not learn these skills and target information infrastructures accordingly, when or if it serves their purpose to do so.

Criminals

Criminals target information and supporting infrastructure mostly for reasons of extortion, theft and fraud. Targeting takes two general forms: targeting the computers themselves to illegally obtain the information within; and using computers as the implement of, or to facilitate, the crime.[18]

Targeting in order to access the computers themselves includes such techniques as hacking, the use of malware to obtain passwords by reading keystrokes, or insider help to obtain passwords. It also includes theft of the information within the computer system itself, such as identity information (e.g. credit card or bank account details of individuals, corporations and government).

The use of computers for criminal purposes has grown in parallel with the growth of computer availability and the information society generally. Related criminal activity includes the theft of intellectual property or other forms of commercial or industrial espionage, the misappropriation of money, money laundering, scams to solicit money using fraudulent investment schemes, and embezzlement. Activity also includes the distribution of illegal material such as child pornography, forgery including breaches of copyright (e.g. production of pirated compact discs and software), and extortion in its many forms. Types of extortion include the threat of destroying a corporation's key databases or disclosing confidential information within those databases. Implicit in the blackmail is the willingness to carry out the threat if the corporation fails to meets the extortionist's monetary demands.

Part of the criminal modus operandi has been the use of various skills or methodologies to obtain the necessary personal or other data to access targeted

sites. For example they might use hacking, spyware or phishing to obtain passwords or personal information, including bank account or credit card details, for later exploitation. Or they might use a combination of cyber and non-cyber methods to attack a target, for instance using an 'insider' to provide passwords or other operational data necessary to then plan and mount a cyber-attack. The skills and methodologies used, at least by some criminals, are very sophisticated. The use of state-of-the-art software, in operations involving theft and fraud, may take some time to detect and counter. While the above comprises a diverse range of criminal activities using cyber-crime, the general categories of crime are not new: it is, instead, the technology and circumstances involved that are new.

Like terrorists, criminals also communicate across information infrastructures using techniques to avoid detection and interception. Such methods also include steganography, encryption and cut-outs. Indeed, because of the overlap of systems, it is probable that many of the techniques used by terrorists were initially sourced from criminals.

Who the criminals are, and the level of their sophistication, will determine their target selection. International computer crime statistics have shown a steady annual increase in the frequency of cyber-crime, and reports have surfaced occasionally about some allegedly highly sophisticated acts of extortion, theft and fraud involving very significant sums of money.[19] The incidence of computer crime (or cyber-crime) can be expected to increase in proportion to the growing awareness of and exposure to potential opportunities, assisted by increasingly higher levels of computer literacy generally, and accessibility to sophisticated hacking techniques.[20]

The simple conclusion that can be drawn from this situation is that where money (or other gain) is involved, the threat of criminal targeting is inevitable. And the larger the amount of money involved, the more probable the threat.

Issue Motivated Groups

IMGs, including politically motivated groups, most often target information infrastructures to exploit their reach so as to promote issues to their advantage. Such promotion may be information that explains or supports their position, or denigrates that of their opponents. The Internet is frequently used for this purpose and includes the hosting of websites, and the use of other means such as YouTube and chat rooms. Issues can be enduring, such as those supporting a Palestinian homeland or opposing the war in Iraq; more recent issues include promoting protection of the global environment (which is expected to become an enduring issue), and current issues include opposition to Japanese whaling.

However, some IMGs actively seek to hack into websites and access information which they are not authorised to receive, and particularly

information which, if leaked, would damage their opponent's position and thus support their cause. Forged documents or other fabricated information that advantages an IMG's position is not that uncommon, and is indeed often used to keep alive or inflame an issue.

Other forms of action by IMGs can include 'electronic vandalism' as a protest against a specific organisation, by defacing a web page or closing down a website by the use of Denial of Service (DS) attacks. However, while some IMGs are a threat to the confidentiality of information that can be exploited to advance their cause, and do target the functionality of specific infrastructure targets by electronic vandalism, in general they are not a threat to the broader functionality of the infrastructure itself.

Individuals

Individuals are a 'wild card'. They vary from the benign to the highly dangerous. The former include gifted hackers, some of whom break into restricted computer systems simply to prove to themselves or their colleagues that they can do it, but take no further action. They are sometimes referred to as 'joyriders'. However, as indicated above, other hackers are highly destructive. They include writers of malicious software programs, or malware, such as viruses and worms that can rapidly replicate themselves across computers and networks and cause significant damage through the destruction or corruption of operating systems and databases. This group of hackers also includes individuals who deliberately destroy or degrade hardware and software, or steal, disclose or enable the disclosure of confidential information from within. They include revenge seekers such as disgruntled employees, clients or customers.

Threats from individuals are a reality, but the specifics of who, what and when remain largely unpredictable.[21]

Targeting: objectives

Having painted the broader background canvas of targeting information infrastructures, this chapter now reviews the issues of *objectives*, *targets*, *capabilities required*, *vulnerability*, *accessibility* and *intelligence*. The context is Defence related, specifically a country at war, but considerations may be scaled down for application to limited war, crisis or other non-war situations.

The starting point for any plan of action is the end-state or objectives to be achieved. As earlier stated, the overriding objective of a country at war would be victory by destroying the military capability and military and civilian support capacity of the adversary to wage war, and to change the will of their military, politicians and civilian population from pursuing the war to seeking peace. Post-war objectives concerning the future profile of the enemy, shaped during the conflict itself, would include a politically and economically viable and

functional society sympathetic (in the case of Australia) to Australia's interests. Other objectives included boosting the morale and commitment of allies and friends, and countering efforts by the enemy to win over the sympathy or support of neutrals.

Targets were seen as psychological or cognitive, and 'physical' in terms of destroying, degrading or manipulating hardware, software, information, and power supply. People who operated or maintained the infrastructure could be targeted both psychologically and physically. Activities undertaken also could be overt and covert.

Both psychological and physical targets impact on the decision cycle. While perhaps self evident in the case of psychological operations, anything that can impact on an enemy's collection or 'observe' capability[22] (e.g. reconnaissance and surveillance) or their analysis or 'orient' capability (e.g. access to intelligence databases) will affect decisions and actions. And, often, incorrect or impaired decisions and actions can generate their own psychological effects which may adversely impact on morale and commitment, and on subsequent decision-making.

The above overarching objectives are strategic; objectives would also be set at the operational and tactical level, in all cases in support of and coordinated with achieving the higher aim.

Some examples follow. A basic military capability objective at the strategic/operational/tactical level would be to hide or disguise friendly-force manoeuvre from enemy observation, to achieve surprise. Targeting in this scenario would include the destruction or disruption of critical enemy satellite ground stations in order to neutralise headquarters-controlled imagery, reconnaissance and surveillance resources at that time. This action would also be supported by electronic deception activities.

Another basic objective would be the disruption to an enemy's logistic supply capability that provided critical support to the enemy's combat capability needs. Information systems on which such logistic supply depends could be targeted at the strategic, operational and tactical level. Besides the direct impact of logistic disruption to the enemy's warfighting capability, this impact would also affect enemy morale. Negative morale could be further exploited by appropriately tailored psychological operations (psyops).

A further objective using psyops to reach a broad multinational audience would be targeting the morale of the enemy, the morale and commitment of their supporters, the commitment of our allies and friends, and attitudes of neutrals, by the dissemination of adverse publicity, or propaganda, about any enemy illegal, unethical, immoral, or otherwise culturally insensitive activities. Issues exploited could include those affecting the treatment or welfare of

non-combatants in occupied areas, particular religious or ethnic groups, or political or military prisoners.[23]

Methods of delivering intended messages or publicity across information infrastructures could include all forms of domestic and international media (radio, television and newspapers), the Internet, and the use of phones, especially mobile phones (via oral or Short Message Service (SMS)), in enemy country or countries, and appropriate third countries. Methods chosen may need to circumvent severe censorship in enemy and enemy-occupied countries. Scope also exists for the focused use of disinformation. However, while disinformation can be an effective tool, especially for short-term gain, it is a double-edged sword. User credibility can be compromised if it is blatantly exposed or excessively used by the same source.

A final example relates to coordinated cyber-attack and psychological operations at the tactical level against enemy occupation forces in a third country. This scenario assumes our forces are deployed against the enemy in the combat zone, the existence of an armed and capable resistance behind enemy lines with whom we are in contact and can coordinate operations, and whose post-war political ambitions, together with those of the local population generally in enemy-occupied areas, are compatible with ours. The enemy's C4ISREW capability would be fully targeted, using all resources available to us, including the local resistance against related targets as directed by us. The result, especially at a time of proposed major combat operations aimed at inflicting serious losses on and, potentially, the withdrawal or capitulation of the local enemy forces, would be to severely disrupt the enemy's surveillance capability and thus knowledge of the battlefield, his decision-making and C2 capability generally, thereby giving us the significant combat advantage we need to win.

Concurrent psyops, and those mounted after the battle, would be directed at boosting the morale of the resistance and local population generally, and demoralising further the enemy. Psyops would not only target friend and foe in the immediate area of combat operations, but those in adjacent areas that will be the scene of future combat operations.

The above are indicative examples only, and specific objectives may involve highly complex plans necessitating the coordination of highly varied resources across many different countries. But the starting point is clearly identifying the objectives (primary and other), both physical and psychological, and then applying the requirements, assessment and planning methodology.

Targeting: capabilities required

Australia requires a comprehensive physical and psychological operations capability to effectively target, attack or exploit information infrastructures in support of its national and Defence interests. That capability is essential, not

just as a part of a twenty-first century warfighting capability, but also as an option for power projection across the whole spectrum of national interests in both war and non-war situations. Developing and maintaining such a capability would not be without challenge.

All significant national security and Defence capabilities cost money and resources, and this chapter does not attempt to cost all resource requirements. Four considerations do, however, apply:

- First, Australia has long recognised the need to develop and maintain a technological edge in its regional warfighting capability. That edge has been progressively eroded as neighbours develop and acquire new technology weapons and thus capabilities. IO is not only a new technology capability, but offers to many countries a significant asymmetrical warfare capability if properly used. All regional countries in East Asia are aware of this. In the case of technologically advanced countries such as China, Japan, South Korea, Taiwan and Singapore, the concept of IO has been accepted, and the capability is reportedly well developed. If Australia is to remain in the advanced-technology sphere, IO is a capability that must be acquired.
- Second, used in the right circumstances and the right way, the application of this holistic capability in some circumstances may well avoid the need to engage in combat operations. Or it might otherwise significantly reduce the scope of combat operations. Not only might this save a significant number of lives of Australian Service personnel, but it would be a significantly cheaper option than engaging in major combat operations. The cost of a comprehensive capability needs to be assessed against the totality of the national security budget, the cost of other warfighting capabilities, their effectiveness at the strategic, operational and tactical levels, and particularly the cost of major combat inventory items such as aircraft and ships that could be lost in combat operations.
- Third, acquiring the capability would not be a substitute for other existing or planned capabilities, but would supplement those capabilities. This new capability offers not only support to existing capabilities, but a greater reach of military and general national security options, and a greater flexibility of options.
- Fourth, the blocks on which to build a comprehensive capability are already in place. What is required is the identification and acquisition of the necessary additional equipment and skill sets, in a similar vein to any other priority national security requirement.

A comprehensive capability to target information infrastructures includes, but is not limited to the following:

Psychological operations

A basic psyops capability exists within Defence. The Department of Foreign Affairs and Trade (DFAT) does not have this specific capability; it has expertise in advocacy. Understanding and developing a capability that properly meets national IO requirements needs to be developed. Part of such a development will necessitate comprehensive databases within the Defence Intelligence Organisation (DIO) on the region's inhabitants (demographics, characteristics of race, culture, religion, relationships within and between ethnic and religious groups, national aspirations, and attitudes to Australia). Databases must also include comprehensive details on how these individuals communicate domestically and internationally (e.g. Internet, media, landline and mobile telephone, personal meetings) and the relative influence of the different methods of communications.

Much of this knowledge already exists within Australia, within various universities, Non-governmental Organisations (NGOs), and our immigrant population. But accurately interpreting this information, and knowing how to properly and effectively use it to meet specific objectives, requires a great deal of skill. It is essential that the people be profiled to accurately reflect who they really are and what attitudes and thinking they hold, rather than who we would like them to be and what we would like them to think.

'Wargaming' in psyops involving, as a minimum, Defence, DFAT, the Department of Prime Minister and Cabinet (DPM&C) and relevant Ministers is also essential. Key decision-makers and those responsible for policy implementation and practice must develop an informed understanding of the most appropriate use of psyops in different circumstances, including nation building and national cohesion.

Database management

A detailed knowledge and maintenance of current databases is required of the NII, DII and GII linkages in all relevant countries within our regional area of interest. Databases should include specific knowledge about operational aspects, vulnerabilities and accessibility relevant to the systems and networks that make up these structures. The DSD will have a lead role in assembling this knowledge.

Computer Network Operations (CNO)

Knowledge and experience is required in the full range of CNO skill sets, including destruction, degradation, manipulation, and intelligence extraction.[24] This must include the practical know-how of hacking into all relevant commercially available and other IT operating systems, and the development and placement of trap-doors, 'Trojan horses', viruses, worms and the like. Knowledge and expertise must also include cascade effects, and how to monitor

the effects of CNO. DSD and DIO will have the lead roles in developing this capability.

The potential application of CNO skill sets raises a number legally (and politically) sensitive issues such as hacking through the information infrastructures of neutral countries, and the ability to destroy or disrupt major commercial IT systems or equipment, including satellites, by different forms of electronic attack. These legal issues need to be addressed, and also considered in the Rules of Engagement (ROE) in any operational application.

Other weapons and methodologies

Other weapons and methodologies for attacking and destroying or degrading information systems must be developed. Weapons will include those that employ high-powered microwave, and directed energy, including laser beams. The Defence Science and Technology Organisation (DSTO) will have a lead role in the development of this capability.

Media

It will be necessary to acquire a radio and television capability that can beam broadcasts into target countries. In the event that these broadcasts are jammed by the target country, a capability to break into and override existing radio and television broadcasts within the target country is also required. Psyops specialists, in cooperation with other key contributors, will have a lead role in selecting which individuals should do the broadcasting, and the appropriate content of broadcasts.

HUMINT assets

HUMINT assets must be acquired and other specialist HUMINT assistance provided, in target and third countries, in support of all aspects of physical, psychological and deception operations. The Australian Secret Intelligence Service (ASIS) would have the lead role in providing these assets and assistance.

Additional capabilities

Any other capabilities which are required would build on those already in existence. These include conventional and other specialist intercept techniques, decryption and EW.

Targeting: vulnerability and accessibility

Vulnerability and accessibility are also critical elements to the targeting process. There is an interdependence between both these elements and capability. Any potential vulnerability that is also accessible cannot be exploited unless the attacker has the requisite capability.

There is also an interdependence between vulnerability and accessibility. As for capability, any known or potential vulnerability cannot be exploited unless some relevant component is accessible.

Vulnerabilities

Vulnerabilities include:

- Identified weaknesses in a system due to inadequate security procedures or processes designed to prevent unauthorised access (e.g. passwords, level of encryption).
- Weaknesses due to the failure of a person or persons to follow proper security procedures to prevent unauthorised access (e.g. improper disclosure of passwords or security procedures, disclosure of classified information over open line telephones or the Internet, failure to secure buildings or security containers housing critical hardware or software).
- Physical access to parts of the infrastructure that are not protected by physical or electronic barriers of some kind (e.g. fibre-optic cable runs or radio/microwave transmission towers outside protected establishments).
- Nodes or physical choke points where different parts of an infrastructure are concentrated and which, therefore, offer a rich assembly of targets. Nodes can offer the benefits of economy and concentration of force, and the outcome, if attacked, of more significant damage and delays in restoring functionality than if an individual component only was attacked.
- Vulnerability may be a product of interdependence and complexity, i.e. the more interdependent and complex the infrastructure, the more vulnerable the information or systems if almost any part of the infrastructure is destroyed, disrupted or manipulated.
- Vulnerability may also be a product of the time required to repair the infrastructure or reinstate business continuity, e.g. the longer the time it takes to repair or replace hardware, software or human components to restore functionality, the more vulnerable the target. Critical components that significantly affect functionality and require extended time to repair or replace are the preferred targets.

Accessibility

Accessibility is multifaceted. It may seek to target one or more of the key criteria of IA, e.g. availability, integrity or authentication. It could also target any one component of hardware, software, information, the people who operate and maintain, or power supply, or it may be a combination of these. Targeting might be by direct access to the infrastructure, or indirect access in or from third countries.

Examples of direct access in order to destroy or disrupt key hardware could range from a missile strike, to sabotage by resistance forces or Special Forces. Direct access in order to intercept the enemy's communications may require 'tapping' into accessible fibre-optic cables. It might also include destroying an enemy's primary communications route that is inaccessible to tapping or other forms of intercept, in order to force the target to use an alternative communications route that is accessible. HUMINT assets, potentially, could assist directly in all the above situations.

Indirect access to degrade, corrupt or manipulate data within a critical enemy intelligence or logistic database could be achieved by hacking into that database through third countries. Important information about an enemy's intentions might also reside in, for example, their embassy or an axis partner's embassy in a third country. That information might be accessible in that country, but not elsewhere, through HUMINT, signals intelligence (SIGINT) or CNO operations mounted there.

A final example could be 'disruption' at a critical time to enemy communications across a foreign-owned satellite, through cooperation by the foreign owners/operators of the satellite service, or a HUMINT asset among those who operate or maintain that facility.

All information infrastructures are potentially vulnerable in some way. The issue is where and how. While an initial assessment might suggest a particular objective is impossible, it might actually prove to be possible with the application of lateral thinking. The issue then is whether the risk and resources are worth it.

Intelligence

The quality of intelligence input into the targeting of information infrastructures will largely determine the effectiveness of the targeting outcomes.

As previously mentioned, the intelligence applies to psychological requirements as much as to requirements related to all components of the infrastructures themselves. These requirements are comprehensive and need to be identified and fulfilled in advance of any crisis or conflict, not once they occur.

Many of the requirements may be met from open-source material or overt means. Examples are sociological and related information about the people, and details about the information infrastructures themselves, especially the NII and GII. Covert collection requirements will also apply, covering aspects of all components (hardware, software, and details about the information, people and power supply) across both the NII and particularly the DII.

High-quality analysis of the intelligence is also critical. This necessity applies across the board, but particularly in psyops related areas where judgements about the people in our region and their responses in various wartime situations and post-war aspirations may be a difficult and, at times, controversial call.

'Wargaming' that identifies intelligence gaps and challenges assessments (as well as developing skills and experience) will form an important part of the intelligence process.

Conclusion

The information society has seen the introduction of rapid technological change that has conditioned how we now live, think, decide and act. From a national perspective, harnessing this change to our national advantage is important, as is protecting our interests from its exploitation by others.

Defence, as for other key national security and wellbeing issues, is particularly important. Defence has acknowledged and embraced the offerings of the new technologies, and is now moving down the path of a networked force that will deliver efficiencies across the whole C4ISREW spectrum. This is also the case in countries within our region, and in other areas where the ADF could be operationally deployed.

In war, our objective would be to win by destroying an enemy's capability to fight as well as their will to fight. This objective entails political, strategic, military, economic, and societal elements and targets. The objectives are both psychological and physical.

A country's NII, DII and GII linkages enable the information society, including its Defence capability. The ability to target and attack the information infrastructures of an enemy in war, or to exploit those of allies, friends or neutrals, must be part of a Defence capability and a national capability. The requirement may also exist to target these infrastructures in non-war circumstances. Developing the capability to target foreign information infrastructures is not only a necessity, but a national priority.

ENDNOTES

1 An article entitled 'Half the world has a mobile phone', published in the January–February 2008 edition of *ITU News*, the newsletter of the International Telecommunications Union (ITU), stated that the number of mobile phone users was expected to reach 3.3 billion subscribers, or 50 per cent of the global population, in early 2008. This compared with mobile phone ownership by only 12 per cent of the global population in 2000. Developing countries were identified as rising the fastest, with Brazil, Russia, India and China accounting for more than 1 billion subscribers in 2007.

2 Colonel John Boyd, a US military strategist, devised a four-phase interactive process, known as the *OODA loop*, to simplistically describe the decision cycle. The four phases are: *observe* (what is seen, by whatever means), *orient* (analysis, assessment, knowledge), *decide* (the decision, based on knowledge options), and *act* (action taken or attempted). In addition to its widespread use in a military context, it has also been applied widely in non-military contexts.

3 Information Operations are described in Australian Defence Doctrine Publication (ADDP) 3-13—*Information Operations* (2006) Glossary of Terms as 'IO is the coordination of information effects to influence the decision-making and actions of a target audience and to protect and enhance our decision-making and actions in support of national interests'. By definition, IO has offensive and defensive aspects. The core purpose of *offensive IO* is to 'influence the decision-making and actions of a target audience'. All or some elements of offensive IO might apply in war or non-war circumstances, and targets include adversaries, neutrals or friends and allies. Targets also could be high-level political/strategic in character, and/or in support of military operations at the operational/tactical level.

4 ADDP 3-13—*Information Operations*, Glossary of Terms, Australian Defence Headquarters, 2006.

5 See Defence Signals Directorate (DSD—Australia), *Australia's National Information Infrastructure: Threats and Vulnerabilities*, February 1997. An unclassified version of this report is at Attachment A to a report to the Australian Government by the Attorney-General's Department dated December 1998 entitled 'Protecting Australia's National Information Infrastructure'. This report is available at <http://law.gov.au/publications/niirpt.ptl>.

6 US Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, 17 October 2007, available at <http://www.dtic.mil/doctrine/jel/doddict/data/g/02329.html>, accessed 28 February 2008.

7 US Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*.

8 ADDP 3-13—*Information Operations*, Glossary of Terms.

9 The *Blackberry* blackout in the United States and Canada in April 2007, lasting about 10 hours and due to a primary server fault, caused considerable confusion and disruption to many thousands of business and government users, especially those who did not have ready access to alternative communications during that period. According to press reports of the incident, many businesses lost considerable amounts of money because of their inability to close deals or exploit market opportunities within critical timeframes.

10 The concept of modern effects-based operations has largely been developed by Dr Edward A. Smith, Executive Strategist of Effects-Based Operations at the Boeing Corporation. His most recent book on this subject entitled *Complexity, Networking & Effects-Based Approaches to Operations*, Command and Control Research Program (CCRP), Department of Defense, July 2006, is available at <http://www.dodccrp.org/files/Smith_Complexity.pdf>, accessed 26 February 2008.

11 In today's global marketplace, a critical electronic system might be designed in the United States, comprise operating software written in India, and include physical components manufactured in such countries as China, Malaysia or South Korea.

12 Identifying who is a threat, knowing their aims and modus operandi, and thus likely targets, is a fundamental part of any associated protective risk assessment and risk management process.

13 For further details about covert intelligence techniques, see Ian Dudgeon, 'Intelligence Support to the Development and Implementation of Foreign Policies and Strategies', *Security Challenges*, vol. 2, no. 2, July 2006, pp. 61–80, available at <http://securitychallenges.org.au/SC%20Vol%202%20No%202/vol%202%20no%202%20Dudgeon.pdf>, accessed 26 February 2008.

14 CNE refers to software hacking operations aimed at extracting intelligence from databases within a computer network. CNE is normally a covert activity, and undertaken in such a way as to avoid detection for at least the duration of the intelligence requirements it serves. It differs from Computer Network Attack (CNA), which is hacking into software systems for the purpose of destruction, disruption or degradation of the software, information and/or hardware itself. Both are capabilities under the general heading of Computer Network Operations.

[15] The release on the Internet of a video of the execution and decapitation in February 2002 of Daniel Pearl, the *Wall Street Journal*'s Indian-based South Asia bureau chief, is one example of this. Pearl, a US citizen and Jew, was pursuing a terrorist-related story when he was kidnapped in Pakistan in January 2002. His kidnappers, a group calling itself The National Movement for the Restoration of Pakistani Sovereignty, claimed he was a spy for both the United States and Israel. Western analysts believe one of the reasons for Pearl's assassination was to motivate and recruit new members to the Islamic jihad cause.

[16] See Tamara Makarenko, 'The Crime-Terror Continuum: Tracing the Interplay Between Transnational Organised Crime and Terrorism', *Global Crime*, vol. 6, no.1, February 2004, pp. 129–145, available at <http://www.silkroadstudies.org/new/docs/publications/Makarenko_GlobalCrime.pdf>, accessed 26 February 2008. I am indebted to Professor Peter Grabosky for referring this reference to me. According to Makarenko, many terrorist organisations engage in illegal activity to raise finances. These include the al-Qaeda financial network in Europe, which was reported to be primarily dependent on credit card fraud for funding. However, the primary source of funding for many terrorist groups is the illegal drug trade. Makarenko also claims that since the collapse of the Soviet Union there has been a convergence of transnational organised crime and international networked terrorist groups. This has resulted in the cooperation between terrorist and crime groups where their interests intersect. One example cited was terrorist organisations using criminal organisations to transport and market illegal drugs grown and produced in areas under terrorist control. Another example was the acquisition of guns by criminals on behalf of terrorists.

[17] Alan Sipress, 'An Indonesian Prison Memoir Takes Holy War Into Cyberspace', *Washington Post*, 14 December 2004, p. A19.

[18] For a comprehensive overview of cyber-crime, see Peter Grabosky, *Electronic Crime*, Prentice Hall, Upper Saddle River, NJ, 2007.

[19] The word 'allegedly' has been used as financial institutions generally seek to avoid any publicity about the frequency and type of computer crime, and especially the extent of any major crime, because of the adverse effect it can have on investor or customer confidence. However, one example of a major case of proven fraud was the loss of $A1.6 billion by Barings Bank in Singapore in 1995 by Nick Leeson, their head trader. Leeson conducted rogue trading by falsifying accounts and various misrepresentations that were not detected by internal controls and audit systems.

[20] Sophisticated hacking software is readily available on the Internet, and has been for many years.

[21] An interesting profile of malware writers was in an article by Clive Thompson entitled 'The Virus Underground' published in the *New York Times* on 8 February 2004, available at <http://engineering.dartmouth.edu/courses/engs004/ virusarticle.html>, accessed 26 February 2008.

[22] Colonel John Boyd, *OODA loop* process (refer note 2 above).

[23] A vivid example was the severe anti-US publicity generated in 2004 in the world media in response to reports and photos of the abuse and torture of Iraqi prisoners by some US military police in the Abu Ghraib prison in Baghdad. Anti US and anti-war elements quickly exploited this 'windfall gain', which also gave rise to significant disinformation about other alleged adverse behaviour by US and Coalition partners in Iraq, and US and Western attitudes towards Islam generally.

[24] Dudgeon, 'Intelligence Support to the Development and Implementation of Foreign Policies and Strategies', *Security Challenges*, pp. 61–80.