The Strategy and Tactics of Information Warfare

MATT BISHOP and EMILY O. GOLDMAN

Over the last decade, information technology has been championed by policymakers, activists, international bureaucrats, business leaders and intellectuals as a catalyst for social transformation – generating economic growth and development, peace and global cosmopolitanism, personal freedom and individual empowerment. Like the industrial revolution before it, the information technology revolution appears to be creating a new ruling class, a new economy and a new society. It should come as no surprise that strategic thinkers and security experts have become enamoured with the ways that information technology can transform military operations and warfare. Information technology, military leaders and intellectuals argue, can supplant the Clausewitzian industrial-era model of destructive war with an information-era model promising greater efficiency and flexibility, and fewer risks of casualties through the use of more highly skilled troops and 'smart' technologies. Just as the nuclear age elevated the logic of deterrence over destruction, in the information age, the logic of disruption has the potential to rival the logic of destruction. For these reasons, the information age in warfare represents a significant disjuncture with the past.

Information technology, however, has always been central to warfare and crucial for enhancing military effectiveness. The establishment of a telegraph network considerably influenced the conduct of military operations and enhanced the effectiveness of military forces during the American Civil War and Wars of German Unification.[1] The introduction of wireless around the turn of the twentieth century represented an important aspect of the naval revolution that many associated with the development of the all-big gun battleships powered by turbine engines, and the development of extended-range submarines and torpedoes. The wireless was also a means of providing greatly enhanced strategic warning. During the interwar period, the rapid

growth in the application of radio and, later, the advent of radar, had an enormous influence on military operations. The German Army's development of *Blitzkrieg* depended as much on the ability of radio to coordinate large, fast-moving, highly dispersed forces as it did on mechanization and aviation.[2] Great Britain's integrated air defence network was also heavily reliant upon – indeed, held together by – a radio and radar infrastructure.[3] The continuity between these historical examples and the present are evident in efforts by the US military to employ emerging information systems, like space-based GPS, to inform terrestrial manoeuvre and precision targeting.

Information as 'content', as distinct from information as 'conduit', has also always been a critical dimension of strategy in combat and competition, whether due to its absence or presence.[4] It was Carl von Clausewitz's scepticism about the reliability of information and intelligence at the tactical and operational levels that led him to emphasize, in *On War*, the need to maximize and concentrate one's troops, maintain reserves, and ensure that leaders possessed intuition and experience. For Sun Tzu, on the other hand in *Art of War*, deception, disinformation and knowledge of the enemy's innermost thoughts and plans are the keys to surprise and victory, perhaps even a bloodless victory.

What makes the information age unique is the fact that information *as* warfare has become as important as information *in* warfare. Information is not just a means to boost the effectiveness of lethal technologies as has occurred often in the past, but opens up the possibility of non-lethal attacks that can incapacitate, defeat, deter or coerce an adversary. By expanding the tools and techniques of information attack, the information age has enlarged the domains of IW and its purveyors. Warfare now occurs on the battlefield, in the marketplace, and against the infrastructure of modern society. Attackers include individuals and private groups in addition to professional militaries, making warfare an activity no longer the exclusive province of the state.

Yet even though the repertoire of tools, domains and purveyors of war have changed in important ways, the logic of warfare remains the same. Warfare involves sequencing and coordinating attacks to achieve lower order technical or 'cyber' goals, that are part of a broader campaign to achieve higher order political, material and/or symbolic goals. Understanding how different types of technical goals can

contribute to the achievement of higher order strategic goals requires bridging the worlds of the strategist and computer scientist. Only then can the techniques of information attack be effectively used in the service of strategy, and can strategic concepts like deterrence, escalation, retaliation and linkage, adapt to embrace the new contingencies presented by information warfare.

This essay examines the strategy and tactics of information warfare by showing how the tools of cyberwar present novel ways of achieving traditional political, material and symbolic objectives. We discuss how information capabilities have altered the current conflict environment: the nature of vulnerabilities and threats. We provide an overview of how to think about information warfare and discuss the underlying logic and technical prerequisites of various types of information attacks. We conclude by discussing some of the most important continuities and discontinuities between the past and present regarding the strategy and tactics of information warfare.

THE CONFLICT ENVIRONMENT

With the recent explosion of information technologies, the growing reliance of advanced societies on them, and the burgeoning of capabilities to manipulate information and disrupt its flow, the role of information warfare has become central to nearly every discussion of adversarial relations, military and commercial. Conventional wisdom says that we have entered an age where information is not only an adjunct to conventional military and business operations, but has become a key arena of conflict and competition.

In important ways, information warfare continues trends that were already underway in the evolution of combat. Like strategic bombing and counter-value nuclear targeting, efforts to deter or defeat an adversary by bypassing destruction of his armed forces and directly attacking his society predate the information technology age. Techniques of information warfare simply provide attackers with a broader array of tools and an ability to target more precisely and by non-lethal means the lifelines upon which advanced societies rely: power grids, phone systems, transportation networks, and aeroplane guidance systems. IT can also make conventional combat more accurate, thereby improving the efficiency of high explosive attacks. Here again, IT continues trends in warfare that have improved the lethality of military force over time.

In other ways, information technology has altered the environment of conflict. It has changed the way we think about vulnerability. Control of information and knowledge is a central engine driving human activity, evident in the incredible growth of computing power, the increasing reliance on information technology for business transactions (credit cards, electronic banking), the rise of consumer electronics, and most of all, the increasing reliance on the internet. The distribution of a computer virus that can be activated on command, the electronic theft of funds from a credit card company, the spread of disinformation via the internet or the media, or tampering with e-mail present contemporary society with new points of vulnerability.

Paradoxically, IT has made the most advanced and powerful societies, by traditional indices, the most vulnerable to these types of attack. A distinguishing hallmark of the information age is the 'network', which exploits the accessibility and availability of information, and computational and communicative speed, to organize and disseminate knowledge cheaply and efficiently.[5] The strength of the network lies in the degree of connectivity. Connectivity can increase prosperity and military effectiveness, but it also creates vulnerabilities. Information-intensive military organizations are more vulnerable to information warfare simply because they are more information-dependent, while an adversary need not be information-dependent to disrupt the information lifeline of high-tech forces. Information-dependent societies are also more vulnerable to the infiltration of computer networks, databases and the media, and to attacks on the very linkages upon which modern societies rely to function: communication, financial transaction, transportation and energy resource networks. From a competitive perspective, it would be foolish for a well-financed and motivated group not to attack the technical infrastructure of an adversary.

IT has also changed the way we think about threats. The information revolution has empowered traditionally weaker actors by diffusing and redistributing power. Information warfare is not confined to interstate interactions. Individuals and non-state actors, be they corporations, interest groups, criminal organizations, or terrorist groups, can acquire the means to wage some level of information warfare. The US GAO estimates that 120 groups or countries have or are developing offensive information warfare capabilities. It is not necessary to be a high-tech networked society to have access to information warfare capabilities

because of their relative cheapness, accessibility and commercial origins. Relatively low entry costs mean that the diffusion of information technologies is likely to accelerate far more quickly than did nuclear or aerospace weapons.

For all these reasons, information has become one of the most valuable commodities and strategic assets. A nation's (or corporation's) ability to produce and utilize information and to protect its information assets has become synonymous with protecting its national (or corporate) security and ensuring its citizens' (or shareholders') prosperity. Information systems will be a key arena of operations and a primary means for conducting offensive operations, and information warfare a key element in any 'strategy' of conflict or competition.

HOW TO THINK ABOUT INFORMATION WARFARE

Information warfare conjures up all sorts of definitions, taxonomies and images. We find it useful to think in terms of the conceptual categories laid out in Figure 1. The four domains of attack capture many of the prevailing taxonomies of information warfare.

We start from the assumption that the means of attack and the targets of attack can be classified as predominantly physical or cyber. We do not find it useful to focus on the target of attack as do many other taxonomies. Schwartau distinguishes personal IW which targets

FIGURE 1
DOMAINS OF ATTACK

	Target of attack	
Means of attack	*Physical*	*Cyber*
Physical (hurling mass and/or energy)	***I – Traditional War and Cyber-enhanced Physical Attack*** Bombing military or civilian facilities; conventional warfare or terrorism	***II – Blast-based Information War*** Physical strikes on information infrastructure (e.g., 9-11 impacted cell phone switching area); EMP from directed-energy weapons that destroy or disrupt digital services
Cyber (hurling information)	***III – Cyber-enabled Physical Attack*** Attacks on aircraft navigation system; spoofing air traffic control system; attacks on specialized digital devices that control electrical power and dam floodgates	***IV – Non-lethal Information War*** Denial-of-service attacks, worms, logic bombs inserted into information systems

individuals, corporate IW targets which targets business, commercial and economic interests, and global IW which targets assets associated with the national interest.[6] A more common way of distinguishing targets is to separate the domains of 'strategic' and 'battlefield' IW. The former comprises targets in the societal realm, the latter in the military realm. Information war is frequently associated with new military targets (e.g., enemy air defences; radar facilities) for conventional and cyber forces.[7] It is also frequently used to refer to new civilian targets for cyber forces, such as denial of service attacks on the nation's critical national infrastructure.[8] These distinctions, however, obscure the fact that what is really new is the widening ability, due to both the changing nature of the capabilities of state and non-state actors and the increasing vulnerabilities of advanced society, to disrupt the information and networks that support crucial day-to-day workings of civilian, commercial and military systems alike. The civilian–military distinction is even less useful in a world where military systems increasingly use and rely on civilian information infrastructures, and where there are important commonalities in the vulnerabilities of military and civilian information systems.[9]

Despite the characterization of this era as the information age, attacks will surely continue to combine physical and cyber capabilities, as, for example, when IT is used in combined-arms operations to improve the efficiency of high explosive attacks. The means of attack in this case remains predominantly physical. Information simply improves the efficiency and accuracy of physical attack. In the near future, national militaries in particular are unlikely to adopt purely non-physical strategies of conflict.[10] Physical destruction will remain a compelling proximate goal and cyber-attacks are likely to be used in support of lethal operations on the battlefield and against the adversary's homeland. Cell I of Figure 1 captures these characteristics of traditional warfare and cyber-enhanced physical attack. Information technologies augment conventional attack, as enablers of existing technologies by boosting the ability to find targets, direct fire to targets, as well as facilitating planning and communication among one's own forces. In several post-Cold War military engagements including the Persian Gulf War, Kosovo and Afghanistan, information technologies have been used quite effectively in battle to support and enhance traditional destructive warfare.

Cell II captures the idea that the information systems that undergird the operations of modern day societies and military organizations can be

directly targeted through physical attack. Blast-based information war targets information systems with firepower, be it mass or energy. Physical attacks with conventional munitions on command and control targets, as well as on civilian critical infrastructure, such as electrical power generation and transmission systems, have been hallmarks of recent Western military campaigns. These attacks can have consequences far beyond the physical assets directly destroyed as the impact of losing services ripples throughout society. In recent years, attention has turned toward a new category of firepower – directed-energy weapons – which use high-power microwaves to disable electronic targets, in contrast to traditional jamming equipment that blocks communications devices from functioning but does not physically damage them. The new generation of directed-energy weapons 'is meant to emulate the sort of damage that nuclear EMP [electro-magnetic pulse] can inflict upon electronics but at far less range, with more control of the damage and without all the ancillary physical destruction and radioactivity'.[11]

Our analysis focuses in detail on cyber attacks directed against physical and cyber targets. Cell III, cyber-enabled physical attack, captures the destruction of physical targets by means of attacks on underlying technical systems. These attacks may be lethal, destroying lives and property, although only indirectly so. Recent attention has been directed toward the potential for terrorists to use the internet to target specialized digital devices, namely the distributed control systems (DCS) and supervisory control and data acquisition systems (SCADA) that throw railway switches and adjust valves in pipes that carry water, oil and gas. Increasingly, these digital control devices are connected to the internet and lack rudimentary security. Moreover, utilities worldwide allow technicians to remotely manipulate digital controls, and information on how to do this is widely available.[12]

Information warfare has been used to refer to combat waged solely within the domain of information and information systems. Cell IV captures this pure form of information warfare, or what we call non-lethal warfare. The tools are 'digital' and the targets include enemy population beliefs, enemy leadership beliefs, and the economic and political information systems upon which society relies to function.

Arguably the most distinctive quality of conflict in the information age is the capacity to coerce and deter adversaries, and influence and shape the strategic environment in non-lethal ways. Information technologies used in a non-destructive mode can serve a variety of

preventive conflict goals. They could enhance transparency, build confidence and possibly prevent conflict if used in support of arms control verification regimes or peace operations. The increased abilities of sensors to detect military build-ups and disseminate that intelligence could reduce strategic surprise and deter conflict. Information technologies could be used to combat terrorism and international crime through the creation of global databases that track the movements and activities of these transnational actors. Information technologies could possibly prevent genocide and ethnic clashes *before* they start by ensuring accurate information supplants inflammatory nationalist rhetoric.[13]

Information technology, we argue, will also be used increasingly in a non-lethal mode during conflict, as a substitute for high explosive attacks via cyber operations that target an adversary's coordination capacity (military or societal) rather than their physical assets, that disrupt rather than directly destroy. The ultimate end goals of competition will remain the same: they may be political, material or symbolic. Those goals may be pursued by states, organizations, or personal actors. The weapons, however, will be cyber rather than physical, hurling information rather than mass or energy. The targets, whether military or civilian, will be the digital systems or coordinating capacity that undergirds physical capabilities rather than the physical capabilities themselves. The proximate or technical means of attack may in fact be destruction of information and information systems but more often than not given limited resources and system vulnerabilities, it will be the disruption of those systems.

The reasons for this are two-fold. First, the IT revolution has begun to alter expectations about conflict. In democratic nations today, there is a decline in the legitimacy accorded to lethality as well as a redefinition of innocents to include non-military members of an enemy's society.[14] Together, these make anything other than extremely accurate killing increasingly unacceptable in Western societies. The speed and accuracy of information warfare capabilities, coupled with the intolerance of democratic publics for casualties, indiscriminate destruction, and attacks on innocents has raised the attractiveness of this type of information warfare.

Second, because the United States dominates the global battlefield in conventional weapons, foreign governments and non-state actors are likely to resort to asymmetric strategies, of which information warfare is one. Attacking computer network systems is one way to balance the odds

against a conventionally superior opponent. For weaker actors that cannot marshal the physical capability necessary to harm or influence more powerful adversaries, cyber attacks on information assets may become the strategy of choice. Particularly given an adversary with a highly informatized society and military, it makes logical sense to target the information systems of the adversary that provide intelligence about the opponents' tactics and strategy, that exercise command and control over, and direction of, capabilities and assets, and that undergird the functioning of the adversary's society and economy.

Information warfare of this disruptive variant is particularly challenging for our understanding of conflict because it blurs the peace–war boundary. Given the technological potential for intrusion, the temptation to pre-emptively disrupt in order to 'prepare the battlefield' before conventional hostilities or a crisis begins, or to incapacitate an adversary's war-making system by causing a complete or partial loss of function, is strong. A pre-battle information suppression operation might shatter an enemy's will to fight but does this first strike constitute a use of force?[15] The peace–war boundary may become virtually meaningless. Moreover, it is no longer self-evident what the battlefield is in an IW context, whether warfare is really occurring if there is no loss of life, and whether an actor would expend other types of personnel and equipment if attacked solely by electronic means.

The ultimate objective of information warfare – the use of information assets in the service of strategy – is to make the war or competition more costly for the adversary such that the adversary submits to one's will or never engages in the conflict or enters the competition/market at all. The proximate objective toward this end is always to compromise the adversary's information security. Information security rests on three pillars: confidentiality, integrity and availability (see Figure 2).[16] Confidentiality involves keeping secrets a secret. Integrity involves evaluating and maintaining the trustworthiness of data. Availability involves ensuring data and systems are available for use. Every IW attack compromises one or more of these three pillars.

Generically, all IW attacks are an assault on the security of information–the information itself and/or the systems that collect, process and disseminate the information. The targets are the enemy's beliefs, knowledge and information gathering, processing and disseminating capabilities. In the military realm, information attacks aim to send enough messages to convince the enemy to stop fighting or to

FIGURE 2

ASSAULTS ON INFORMATION SECURITY

Information Security Pillar	Goal of Attack	Technical Objective
Confidentiality	Exploit adversary's information systems	Theft or unauthorized use of valuable data
Integrity	Distribute misinformation or disinformation	Corrupt or modify adversary's information or information systems
Availability	Deny, destroy, or cripple adversary's information systems	Destroy key information; paralyze adversary's information systems

refrain from fighting, or to disrupt or destroy the communication channels to affect the adversary's implementation of strategy and ability to fight or resist. Messages may be direct – aimed at civilian and military leaders and their armed forces – or indirect – aimed at the public whose support may be necessary to wage a war. In the commercial realm, the goal is to influence the behaviour of actors in the marketplace – competitors, customers, suppliers, the public – to achieve business objectives.

Beyond this generic description, however, there is a vast array of modes of attack. Most discussions of IW focus on the dichotomy between destruction and disruption. But there are important differences between disrupting, disabling, crippling, corrupting and delaying such that the techniques short of destruction provide attackers with the ability to finely calibrate their assault. Moreover, destruction may be physical or logical. Finally, advances in IT have dramatically expanded the modes of diversion, distraction, distortion, monitoring and controlling.

The rest of this paper discusses the underlying logic and technical prerequisites of various types of information attacks focusing chiefly on Cell IV of Figure 1, non-lethal warfare. It is useful to think in terms of technical or cyber goals, and higher order political, material or symbolic goals. We first discuss the technical goals of attack, such as the use of cyber resources to cripple systems. Our discussion of these cyber goals applies equally to strategic information warfare – or attacks on the homeland directly – and to battlefield information warfare. Cyber goals however do not speak directly to the larger impact on society; rather, they characterize the effects upon the systems and infrastructure involved. The distinction between cyber goals and higher order goals is

important. Cyber goals are primitives, in the sense that they cannot be broken down further. Higher order goals result from an attacker achieving cyber goals in such a way that the effect of achieving those goals also achieves a more general political, material or symbolic goal. Any particular campaign is likely to be comprised of several different cyber goals (See Figure 3).

In what follows, we discuss each goal individually. However, different cyber goals, and hence different types of attack, can and probably will be combined to achieve the attacker's end purpose. Obtaining a desired result may require intermediate results. For example, suppose an attacker wishes to monitor or control an adversary. In order to do this effectively, the attacker may need to distract the enemy so the attacker can tamper with the system to be monitored. Hence two sets of attacks are launched. The first involves much activity that is likely to be detected but will require some set of defences to be created. This diverts the enemy from noticing the second, subtler set of attacks that tamper with the system (for example, by adding a kernel loadable module) to insert keystroke recorders in appropriate places, thus achieving the desired goal. The reader is encouraged to construct multi-level attacks in which the ancillary efforts aid in achieving the desired goal.

CYBER GOALS

Destruction requires disabling a system in such a way that it cannot be recovered. It must be rebuilt or recreated. Destruction may occur in either the virtual realm or the physical one, but the key point is that something in the virtual realm triggers the destruction.

Clausewitz championed the principle of destruction as the most expedient way to achieve one's political objectives, as the shortest and surest way to defeat the enemy and impose one's will. Destruction has typically required the maximum concentration of physical force at the decisive point to irreparably damage the adversary's armed forces, or 'centre of gravity'. Destruction is the most decisive method for achieving one's political objectives, the most costly if it succeeds and the most damaging if it fails. Though Clausewitz's 'principle of destruction' is usually equated with physical destruction, Handel notes that 'by destruction, Clausewitz does not necessarily mean physical eradication or devastation of the enemy; he is also referring to destruction of the enemy's will to go on fighting'.[17] Destruction, in other words, encompasses both the physical and moral destruction of the enemy's forces.

FIGURE 3
GOALS AND TACTICS OF INFORMATION ATTACKS

Goal of Attack	Information Security Pillar Compromised	Tactics	Type of Goal
Destroy	Availability	Insert information that causes destruction of system; messing with refresh rate on some early monitors	Cyber
Disable, cripple, disrupt	Availability	Targets conduit; denial-of-service; swamp system (distributed denial of service attack); ping of death (sending a special packet that causes system to freeze, effectively disabling it); some worms and viruses	Cyber
Delay	Availability Integrity (e.g., trustworthiness of information degrades over time)	Prevent timely delivery of messages (e.g., that authorize payment on contract or delivery of critical supplies to different military theater); increase traffic on some segments of network to increase time to delivery; increase load on routers or servers	Cyber
Divert and distract	Availability	Divert target's attention and resources; hide other attacks or delay their discovery; script kiddie attacks while others are working much more subtly	Cyber
Distort	Confidentiality Integrity	Targets content vs conduit; perception management; psychological operations	Cyber
Monitor and control	Confidentiality Integrity	Code breaking; feeding misinformation (mimicking known signal so well that receiver cannot distinguish phony signal from real signal); mirror image sites; use of various techniques to mask identity of penetrating party into network or system	Cyber
Swagger	Confidentiality Integrity Availability	Demonstrations of one's abilities by attacking high value targets, highly protected systems, or by launching simultaneous attacks	Symbolic
Punish	Availability	Attacks on electrical, water, and medical infrastructure to maximize societal pain and suffering	Political
Deter	Availability	Impressive simulations and exercises; prebattlefield information attacks against command and control networks or leadership to shatter will to fight	Political
Coerce	Integrity Availability	Limited attacks that demonstrate power to hurt and inflict calibrated pain and damage to induce compliance	Political
Undermine confidence and legitimacy	Integrity	Infiltrate bank's computer system; alter critical files on system to allow unauthorized users entry to alter/delete user files unexpectedly; Trojan horses	Symbolic
Market manipulation	Confidentiality Integrity	Industrial espionage; information denial; break in and copy files; plant backdoors to allow reentry; plant sniffing programs to obtain user keystrokes and other actions	Material
Personal gain	Confidentiality Integrity Availability	Infiltrate bank's computer system to transfer money into or out of account; infiltrate registrar's computer to change semester grades; extortion; blocking access to a competitor's service	Material

Destruction has always required knowledge of how the system interacts with external entities, and this is true in the virtual world as well as the physical world. Physical destruction in particular requires knowledge of the environment of the system, such as characteristics of its hardware or its location. Two examples are changing the refresh rate

of some older monitors (which causes them to burn out), and modifying the programming of avionics systems that control aeroplanes (which could cause the aeroplane to crash). The refresh rate is a function of the monitor's hardware. The avionics computer is in a precarious location, and its well-being depends upon its programming (and inputs) being correct. In both cases, the attack is designed to override any constraints intended to ensure the system functions within acceptable parameters, causing destruction.

Logical destruction, in which the hardware of the system is left alone but the logic or data of the system is rendered unintelligible and unrecoverable, typically requires physical destruction of backup information. If no backup information is present, deleting the software or data suffices for the attack to succeed. This requires either inserting code to delete the information (using a buffer overflow attack, for example), triggering resident code (such as resides in some servers), or acquiring privileges (for example, by compromising a privileged server). In order to determine which of these approaches is feasible, the attackers will probe the system to determine first, what servers are active and second, whether any of the active servers have these capabilities. The probes may request identifying information or characteristics of the server or simply send command sequences to the servers to determine how they react.[18]

The attacker needs information about the system to identify the most effective way to destroy it. Thus, an attack with the goal of destruction will begin with some type of analysis of the target's relationship to its environment. This phase again may be logical, in which case the attacker will probe the target, or physical, in which case the attacker will acquire instruction manuals and descriptions of the target system and its uses. In this case, probing the target will establish the characteristics that enable an attacker to discover the needed information to launch the attack, but the information will be obtained from manuals. Hence the level of probing may be much less.

Thus, the precursors to an attack intended to destroy the target system will require identifying the ways in which the system interacts with its environment. This in turn requires identifying the target system type, and its function. Probing network servers and the network protocol stack will help establish this information. Further, the attacks will target specific functions and features of the target.

Disabling renders equipment inoperable but repairable (e.g., by reboot). With *crippling*, equipment continues to operate but some key

functions, those that are central to the goal or purpose of the system, fail. For example, a mail server may no longer be able to process mail but will respond to other requests. With *disruption*, equipment continues to function with intermittent failures, or a message changes unexpectedly as it moves from one point to another. A key tactic to achieve these results is denial of service. In principle, denial of service is nothing new in warfare, given that bombing a target takes it out of service. However, cyber attacks allow one to disable, cripple and disrupt non-lethally, and to pre-emptively disrupt in order to prepare the battlefield before conventional hostilities begin. In the military domain, the object of a denial of service attack would be to make the enemy blind and deaf, to cut off his ability to see and deny him access to information necessary to fight the war and command his troops. Though computer software operators disrupting other computers are not likely to be seen as dangerous, let alone as acts of war, disruption can be as great a security threat as destruction.

Disabling, crippling and disrupting are all goals that require that the system be overwhelmed in some fashion. In this context, 'overwhelmed' means that all resources of a particular type are serving an attacker, and none can be deallocated to be reassigned to a legitimate user. An example is the distributed denial of service attack. This attack simply swamps the target system (or its gateway), preventing network connections from users who wish to use the system. The requests for network connections from the attackers absorb all available space in the connection queue, and whenever a connection is terminated (by a time-out, for example), the deallocated resource is immediately reallocated to the attacker. If network connections unrelated to the distributed denial of service attack occur, they are highly unlikely to succeed.

A variant is to block the use of resources, as in the ping of death. An attacker sends a ping packet of maximum size, with the offset also set to maximum size. This causes the receiver to freeze, or lock its resources so they are unavailable to other senders. This achieves the same effect as overwhelming the system, except that the attacker need not send requests continuously. One request is enough.

In this case, the attack will either exploit known characteristics of the target or simply overwhelm resources. This suggests two characteristics. Either the attack uses specific inputs to block the resources, or the attack uses resources repeatedly. The first of these is difficult to characterize a priori, because the inputs that will cause the system to freeze are not

known. However, an attacker will likely try inputs that are known to block some systems in the hope that one will succeed with the target. The second is characterized by an anomalous increase in the amount of traffic, the goal being to prevent the target from having resources free to assign to the non-attacking users.

An interesting insight into the nature of this attack is that the system recovers when the attack ends, or when the system managers reallocate resources to avoid the attacker being given any. This distinguishes it from destruction, in which the system managers must take specific steps to make it recover. Once a destructive attack is launched, the attacker cannot restore the system.

With *delay*, equipment continues to function as before but more slowly; or a message takes an unexpectedly long time to go from one point to another. The goal of delay is to disrupt the timely delivery of messages. The attack may either disrupt the network components of the sender or receiver, or of the path that the message will take. Two approaches are possible. Either the sending or receiving machine will be attacked, or a network component will be attacked. In both cases, the attack is similar to that of disabling, crippling and corrupting, except that the attack aims at overwhelming the target system intermittently rather than until the next reboot.

The boundary between delay and disruption lies in the fate of the messages. Disruption requires their destruction. Delay simply prevents them from arriving in a timely fashion. Hence a delaying attack will not disrupt all components of the communication path, but merely some. This type of attack is more localized than disruptive attacks. It is comparable to a 'surgical strike' that disables critical resources that can be replaced, but the time required to replace the resource causes delay. Thus, delaying attacks are characterized in the same way as those for disabling, crippling and corrupting, but are localized to particular elements of the path rather than attacking the entire path (by flooding) or discarding messages at the end points.

Diversion and *distortion* are forms of deception. The logic behind deception is to 'fabricate a pattern, albeit a bogus one, which will result in your adversary building up a false picture of reality. You hope that, as a result of his conclusion, he will either act incorrectly or fail to take advantage of a situation which, although he may not realize it, is favourable to him.'[19] *Diversion or distraction* is the simplest and most common form of deception. The mechanism employed is the

disposition of one's own forces, physical or cyber, to dilute the adversary's ability to concentrate resources and efforts at the decisive point to achieve swift victory.[20] According to Sun Tzu, victory depends on superiority at the decisive point of engagement but this goal is best achieved not by focusing only on concentrating one's own forces while ignoring the enemy. It requires a method to force the enemy to disperse his forces, resources, capabilities and attention. Deception through diversion becomes central.[21]

Distortion is a form of deception that targets the content of the population's information space. It is frequently referred to as 'perception management'.[22] In this respect, it differs from many other types of information warfare that target the conduit of information whether through destruction, disabling, crippling, disruption or delay. However, distortion requires that one exploit the conduit of the information, or the communications medium, whether it is face-to-face contact,[23] print, telecommunications, broadcast or computer networks.[24] The mechanism employed in distortion is the manipulation of the accuracy of information (through fabrication of information or falsification of existing information) in order to shape the adversary's perceptions, and by extension influence his reasoning, decision making and actions.[25]

While Clausewitz viewed destruction as the core principle of warfare, Sun Tzu accorded deception to that paramount position because successful deception may allow one to achieve surprise. If the deceiver can conceal his true objectives, the enemy may concentrate his forces in the wrong places, thereby weakening himself at the decisive point of engagement.[26]

Deception is intimately related to security. Dewar summarizes the purposes of security as preventing the enemy from deducing your location, capabilities, plan of attack, timing of attack, means of attack, and sources of intelligence.[27] Conversely, the purposes of deception are to persuade the enemy that you are elsewhere, your capabilities are different from what they are, your plan is to do something else, somewhere else, at a different time and in a different manner. The successful deception is difficult to achieve. It requires centralized control and coordination; thorough preparation; consistency with the pattern of events the enemy has come to expect; redundancy (e.g., false indicators presented to the enemy through as many intelligence or surveillance sources as possible); careful timing to allow the enemy

enough time to react to false information but insufficient time for analysis to uncover the deception; and maintenance of normal security precautions so as not to arouse the enemy's suspicions.[28] Dewar emphasizes that 'All deception has a limited and relatively short life span before it is exposed. The degree of sophistication required to make a ploy successful is directly related to the length of time over which it has to be sustained.'[29] Moreover, individuals, groups and populations will vary in their susceptibility to deception. In the information age, those who have come to rely heavily on electronic and digital sources of information and intelligence are likely to be the most susceptible to the manipulation and distortion of those sources of information.

Dewar contends that the battlefield has not always presented the same opportunities for deception. In the eighteenth century, the battlefield was completely visible; hence Clausewitz's scepticism about the chances for successful deception and surprise. In the nineteenth century, the battlefield became much larger and visibility declined. The Second World War was the apex of the 'Empty Battlefield' while reconnaissance and surveillance technologies in the post-1945 era have returned a much larger battlefield to near complete visibility. Yet today's digital technologies allow one to easily create and manipulate documents and digital images. While the physical battlefield may be more transparent, the digital battlefield provides unprecedented opportunities for deception.

The essence of diversion is to attract the enemy's attention. While the enemy is otherwise occupied, the attacker can launch the 'real' attack. This makes diversion and distraction uniquely suited to be a precursor to, or component of, other attacks. This suggests a simple characterization of such an attack: obviousness. If the attack cannot be detected, the enemy cannot respond. Hence the attack must be of a nature that the enemy can detect. Ideally, the enemy will be forced to divert resources to handle the attack as well. Thus, the attacker may use well-known attacks that require the enemy to take procedural steps to protect the enemy. The enemy must then focus on the attack, and may not notice the more subtle attack from which her attention is being diverted.

Diversionary attacks can be defensive, as in the classic diversionary response launched when some East German attackers broke into a computer at Lawrence Berkeley Laboratory in the mid-1980s. Cliff Stoll, a system administrator, was determined to trace the attackers, whom he realized were coming over a telephone line from somewhere in

Germany. But tracing an international call required time, and the attacker was never connected for long enough. So Stoll created a false document that contained information the attacker would desire. It would also take several hours to download over a telephone line. When the attacker found the document, he downloaded it – and that diverted the attacker's attention from the telephone trace, which located him.[30]

Distortion manages the enemy's perception of what is happening. The goal of distortion is to make the enemy believe something that the attacker wants the enemy to believe. For example, one can configure an electronic mail server to greet a client with a declaration that it is *sendmail* version 8.9, when in reality it is a *postfix* mailer. As different mail servers have different vulnerabilities, this leads to an attacker wasting resources on attacks that work on *sendmail* version 8.9 mail servers but not on *postfix* servers. In a parallel fashion US surveillance and reconnaissance aircraft not only can collect and jam enemy radar and radio emissions but also plant false targets in enemy radars and spoof enemy air defence systems.[31]

A characteristic of distortion attacks is control of resources. The attacker must control the enemy's access to information involved in the distortion. If the enemy can obtain information indicating inconsistencies, then the enemy may realize that the attack is under way. Thus, the attacker must identify all paths along which the enemy can obtain the information to be distorted. This requires a complete understanding of the enemy's relationship to the information involved in the distortion. This would require probing not only the enemy, but also intermediaries along the paths of information flow to determine if they can detect the distortion (and feed information back to the enemy).

While distortion and deception usually involve replacing information with a phoney signal, *monitoring* and *controlling* involve infiltration of the enemy's information space and hiding the signal in order to gather information. Infiltration for the purposes of monitoring creates opportunities for deception since the enemy presumably is unaware that his information resources have been compromised and will continue to trust them. Monitoring is a crucial foundation for deception. Good intelligence and penetration of the enemy's camp are the means to understand the enemy's thoughts, expectations, and plans.[32]

The distinction that is important is your ability to predict the resulting actions of the enemy. With distortion/deception, we are simply misleading the enemy, either in his information space or our space, by

feeding the enemy false or distorted information. With monitoring/controlling, we are attempting to see what the enemy is doing, and force her to specific actions or situations. For example, we may place false documents in our information space to mislead the enemy, but not know what the results will be. This is distortion/deception. Or we may concoct the documents to produce specific results or actions. This is controlling, of which deception is a part. Or, we may instrument the system to record who grabs the documents. This is monitoring.

The difference between monitoring and controlling is that monitoring is passive, whereas controlling is active. Monitoring may require action to initiate the monitoring, but once the mechanisms for monitoring are in place, the attacker need take no further action. An example of monitoring is to record keystrokes. The attacker must insert appropriate code into the kernel (usually done via a kernel-loadable module), but after the insertion the mechanism simply records all keystrokes entered at the system. In some cases, the attacker need only persuade the enemy to take some action, such as downloading a file or executing a program. The Trojan horse is an example of this technique.[33]

Controlling is similar to distortion, except that the goal of control is to force the enemy to take specific actions or to enter specific states of operation. Distortion may be a component of control, as it was in Cheswick's manipulation of Berferd.[34] By distorting the environment that Berferd perceived, Cheswick made Berferd take specific actions which (he hoped) would identify Berferd. Contrast this to the use of honeypots,[35] in which the distortion fools the enemy into thinking they are on a system with sensitive information or desired resources. They then try to compromise the system. The attackers can monitor every action, and by changing the configuration of the system, trick the enemy into revealing their capabilities.

Controlling may be more direct. The NetBus[36] attack tool allowed the attacker to perform system administrative tasks, such as monitoring the other users of the system, inserting keystrokes, reading screens, and shutting the system down. This tool was placed into a computer game that was made publicly available. A number of sites downloaded and installed the game, giving the attackers complete control of their system.

Monitoring requires the ability to read traffic. This means that the attacker must have, or obtain, read access to some part of the communications channel. Similarly, controlling requires the ability to write or modify traffic, meaning that the attacker must have, or obtain, write

access to some part of the communications channel. Thus, a characteristic of these attacks is an analysis of the communications paths that the enemy uses, in order to obtain the needed access. A secondary characteristic is that the attacker must penetrate some component of the channel, such as the kernel (or sending or receiving process) of an endpoint, or an intermediate system such as a router. The attacker may compromise the component directly, through a penetration attack, or indirectly, through a Trojan horse that contains the compromise when it is executed.

HIGHER ORDER GOALS

Swaggering traditionally has involved the peaceful use of military force to display one's might. Typically, nations display their military prowess at military exercises, national demonstrations, or through the purchase or manufacture of prestigious weapons.[37] According to Art, 'the swagger use of force is the most egoistic: It aims to enhance the national pride of a people or to satisfy the personal ambitions of a ruler. A state or statesman swaggers in order to look and feel more powerful and important, or to be taken seriously by others in the councils of international decision making, to enhance the nation's image in the eyes of others.'[38] In the short run, swaggering serves no specific instrumental purpose. In the long run, it may enhance the state's offensive, defensive, and deterrent capabilities. Der Derian argued that impressive cyber demonstrations and exercises could serve the same purpose as nuclear testing. Through technological exhibitionism, swaggering one's cyber capabilities could render visible and plausible one's power, thereby acting as a cyber-deterrent.[39]

As swaggering is primarily a public activity, the attacker must create an effect that others can see. The attack, or its effects, must be obvious to all. The attacker who penetrated Stanford's network is a good example of swaggering, because he discussed with the Stanford administrators what he was doing as he did it.[40] The (possibly apocryphal) compromise of a sensitive Air Force system, in which a group of Air Force computer security experts were assured the system was impenetrable and promptly demonstrated the falsity of the claim by having the computer print a parody of the press release, is another example.

The characteristic of an attack with swaggering as its goal is visibility. The result need not be visible to all; it may only be visible to a select few (as in the above examples). But it must be visible to someone. Hence

these attacks tend to be obvious either in their execution or their results. This suggests the use of well-known techniques of attack for which adequate responses are not available, so the enemy can detect the attack, or publicly visible results, such as the recent spate of defacements of web pages. In this sense, swaggering attacks are similar to attacks used to divert and distract.

Punishing involves the use of force to inflict pain and suffering. Schelling distinguishes brute force, which seeks to overcome another's strength, from the threat of pain, which seeks to structure another's motives.[41] Punishment is a form of coercion designed to induce compliance. Successful use of the strategy of punishment requires knowing what an adversary treasures and fears. According to Schelling, the difference between brute force and coercion is less in the instrument than in the intent. Brute force seeks to eliminate a military obstacle while the coercive use of force seeks to convince an adversary to behave or to surrender by inflicting unacceptable anguish and pain. Punitive attacks on people can also be used in a broader military campaign to subdue short of a direct military engagement.

Historically, victory has resulted from defeat of an enemy's military forces rather than simply hurting people to make the conflict terrible beyond endurance. Terrorism, blockade and strategic bombing – all examples of violence against civilians intended primarily to coerce rather than weaken the enemy militarily – have rarely been effective in and of themselves to achieve victory. The major exception was probably the atomic bombs released on Japan, weapons of terror and shock whose value lay in inflicting pure pain as much as direct military destruction. Nuclear weapons have also made it possible to inflict unacceptable pain without first achieving military victory. Typically, such violence was reserved for the victors over the vanquished. Not only have nuclear weapons changed the amount of destruction that can be inflicted but also the role that destruction plays in the decision process.

Punishment is a strategy that not only blurs the distinction between combatants and non-combatants but also specifically targets non-combatants, either during or preceding war, in order to intimidate, coerce or deter governments.[42] Information attacks on critical infrastructure may not produce the same destructive impact as conventional bombing but they serve a similar purpose although the result may be to confuse more than to hurt.

Punishing through technical means requires targeting infrastructure systems that disrupt the use of the internet. As the internet is not yet a

necessary component of people's lives, the degree of disruption must affect the use of the internet to distribute products or services that are necessary for society to function. Hence attacks designed to punish would target the suppliers of services or the network infrastructure. The technical types of attacks involved could be drawn from any of the above set of technical goals. The specific technical goal that would create the greatest havoc would dictate the nature of the attack.

Deterrence seeks to make an attack unattractive so that an opponent does not initiate action. This goal may be achieved either through threats of retaliation and punishment as discussed above, or through denial of the attacker's likelihood of success. The problem with deterrence through retaliation is well-addressed by Harknett, who warns that deterrence is likely to fail if launched by a non-state actor that can retain its anonymity and that has no physical assets or population against which to retaliate. Deterrence through denial could involve improving one's own defences against attack, through robust computer security, or incapacitating the enemy's offensive capabilities through a pre-battle information suppression operation designed to dissuade the enemy from attacking. This would involve attacks that destroy, disable, corrupt or disrupt.

While deterrence is aimed at dissuading an adversary from undertaking a damaging action, *coercion* is used to persuade an adversary to stop or reverse an action. Coercion can use threats of punishment if the adversary does not comply. Or, exemplary or symbolic uses of limited military force – mass, energy or information – could be employed to persuade the opponent to back down.[43] Exemplary actions must use just enough force to demonstrate resolve and lend credibility to further uses of force if deemed necessary. But as George notes, coercion does not require the use of force; it may be executed entirely through diplomacy and persuasion. If force is employed, it is used flexibly, as a 'refined psychological instrument' in contrast to a blunt instrument of destruction. A strategy of coercion with or without force necessarily includes appropriate communications to the opponent to signal intent and negotiate an acceptable compromise. IW attacks could be very useful in a coercive strategy because they can be finely calibrated to limit damage yet also demonstrate resolve. Like swaggering, coercive uses of information warfare must be visible and distortion must be minimized.

Undermining confidence and legitimacy involves attacks that reveal an enemy's weaknesses, or that distort others' perceptions of the enemy.

Revealing weaknesses may require attacks that destroy, disable, corrupt or disrupt. If availability and timeliness are services that the enemy provides, delay may also be a goal that will undermine confidence and legitimacy. Diversion and distraction undermine confidence in the enemy's ability to cope with attacks. Monitoring and controlling may reveal actions that the enemy wishes to keep secret, and publicizing them may achieve the social goal. Similarly, controlling an enemy allows the attacker to force them to take action inimical to their best interests, undermining confidence.

Distortion as a goal towards undermining confidence and legitimacy has two effects. The first is as a form of control, in which the enemy is presented with a distorted view of reality and takes discreditable action as a result. The second is to distort observers' perceptions of the enemy's actions, causing them to discredit the enemy. If the enemy is viewed as a 'black box', the first view arises from the attacker controlling the inputs upon which the enemy bases her decisions and actions. The second arises from the attacker controlling the conduits from the enemy to the observers, and distorting the outputs from the enemy. The difference dictates the response of the enemy: whether to gather inputs from other sources that the attacker cannot (or does not) control, or whether to find alternate channels of communications with the observer.

Market manipulation is a social goal that arises from the 'cyber' goals of monitoring and controlling. To acquire data, the attacker monitors the enemy. To manipulate the market, the attacker uses the data to determine what actions to take to achieve the desired result. *Personal gain* may require any of the 'cyber' goals to help the attacker achieve the desired result. Hence the characteristics and precursors of that 'cyber' goal will arise for this social goal.

CONCLUSION

Our approach to understanding the dynamics of information warfare is grounded in a belief that an 'attack-based' analysis has merits over an 'effects-based' analysis. It is important to understand the effects of attacks in order to recover. But defence against information warfare requires foremost an understanding of the likelihood of different types of attack, and all attacks are not equally likely, nor equally executable by all types of attackers. Nor are systems equally vulnerable to all types of attack. The choice of attack will vary in some systematic way based on

the type of attacker (e.g., state, non-state actor, or individual) because different types of actors are likely to have different motives, capabilities, adaptability and time horizons.

Accordingly, attack-based analysis has diagnostic potential. The type of attack launched should tell us about the motivations and capabilities of the attacker, and indicate the attacker's understanding of the vulnerabilities of the target. There should be similarities in the dynamics of warfare across the military and commercial domains that did not exist in the past because entrepreneurs and warriors have similar requirements for information systems – that those systems be resilient and can function correctly under uncertainty whether due to human error, system failure, or malicious attack. However, attackers working for a government are likely to launch different types of attacks than attackers working for a company because their goals and training may differ significantly.

From an attack-based perspective, we see that despite the levelling affect of information technology, states and state-sponsored groups will retain certain advantages in waging information warfare. A common belief holds that IT is levelling the field of attackers, making it possible for a lone individual to create the same havoc that was once the purview of states and organizations with large amounts of resources. Certainly, the attacks used may be the same; the repertoire of attacks may be available on the internet for both individual and state use. Certainly, the lone attacker may cause great damage. But equating a lone attacker with states and similar organizations overlooks three factors: organization, intelligence about the target, and sustainability.

First, the state-sponsored attack allows the attackers to be better organized. If the defenders resist the attack by, for example, adding more powerful routers to handle an increase in traffic (from a distributed denial of service attack), the state-sponsored attackers can quickly increase their delivery of packets to overwhelm the new router. An individual attacker, or a group of loosely organized attackers, would need to co-ordinate the response without having planned for that contingency. They would be unable to respond to the defence quickly or effectively. The state-sponsored attackers have the advantage of resources, more robust communication abilities, and support for planning that would allow them to anticipate defences and plan counters.

Second, while the attack tools provide the capabilities to launch attacks, they do not provide the knowledge to use the attacks effectively.

A lone attacker may be able to use some number of attack tools effectively, but an organized group that could draw upon team members with a wide variety of experience and knowledge would be able to determine which attack tools to use effectively, and how to use them to reach their goal swiftly. If the attackers had resources beyond the team members, so much the better; especially if they were able to learn about their target's organization and response capabilities. Further, in the technical realm, the attackers could practice against a duplicate of the enemy's systems, networks and organizational procedures, just as professional militaries have practised the art of war in training situations, so they could more quickly proceed to their goal. An individual attacker could not do this.

Third, the effectiveness of an attack is a function of the resources needed to sustain the attack. When an individual launches an attack, her resources are limited to those she has available. When a state supports the attack, the attackers have more resources (and more money) at their command. For example, a state-sponsored group could sustain the attack in the face of detection and interference, because they can simply move the origin of the attack to a new location. A lone attacker, once caught, could not do this.

The observations above hold true not just for state sponsored attacks, but for attacks that spring from a non-state entity with resources and the ability to organize. Attacking can be an individual activity or a group activity. But the basic requirements for sustaining a campaign in warfare that have existed in the past have not changed fundamentally. They have simply moved to a new arena.

NOTES

1. Geoffrey L. Herrera, 'Inventing the Railroad and Rifle Revolution: Information, Military Innovation and the Rise of Germany', paper prepared for The Center for Strategic and Budgetary Assessments workshop on 'Military Revolutions: The Role of Information Capabilities' (Washington DC, 4–5 March, 2002).
2. Robert Citino, 'Beyond Fire and Movement: Command, Control, and Information in the German *Blitzkrieg*', paper prepared for The Center for Strategic and Budgetary Assessments workshop on 'Military Revolutions: The Role of Information Capabilities' (Washington DC, 4–5 March, 2002).
3. David Zimmerman, 'Information and the Air Defense Revolution, 1917–1940', paper prepared for The Center for Strategic and Budgetary Assessments workshop on 'Military Revolutions: The Role of Information Capabilities' (Washington DC, 4–5 March, 2002).
4. Information as 'content' refers to a signal that contains meaningful content and can be transmitted, either in the form of intelligence or as messages between commanders and troops. Information as 'conduit' focuses on flow, or on the *communication* of signals rather than signal content. A view of information as conduit focuses one's analysis on information technologies

that permit one to transmit and receive messages.

5. See Richard J. Harknett, 'Integrated Security: A Strategic Response to Anonymity and the Problem of the Few', in this volume.
6. Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunder's Mouth Press, 1994).
7. Roger W. Barnett, 'Information Operations, Deterrence, and the Use of Force', *Naval War College Review*, Vol. 51, No.2, pp.7–19; T.L. Thomas, 'Deterring Information Warfare: A New Strategic Challenge', *Parameters* (Winter 1996–97), pp.81–91.
8. See Harknett in this volume; L. Sullivan, Jr., *Meeting the Challenges of Regional Security* (Carlisle, PA: US Army War College Strategic Studies Institute, 1994); G.F. Wheatley and R.E. Hayes, *Information Warfare and Deterrence* (Washington DC: National Defense University Press, 1996).
9. Berkowitz reports that approximately 95 per cent of all military communications are routed through commercial lines and that the US government buys most of the microchips used in military systems from commercial vendors. Bruce D. Berkowitz, 'Warfare in the Information Age', *Issues in Science and Technology* (Fall 1995), pp.59–66.
10. See Chris C. Demchak, 'War of Disruption: International Competition and Information Technology-Driven Military Organizations', in this volume for a discussion of why lethality will remain a defining characteristic of how states, particularly the United States, wages warfare in the information age.
11. Seth Schiesel, 'Taking Aim at an Enemy's Chips', *New York Times*, 20 Feb. 2003, pp.E1, E5.
12. Barton Gellman, 'The Cyber-Terror Threat', *Washington Post National Weekly Edition*, 1–4 July 2002, pp.6–7.
13. Joseph S. Nye, Jr. and William A. Owens, 'America's Information Edge', *Foreign Affairs*, Vol. 75, No.2 (March/April 1996), pp.20–36.
14. Chris C. Demchak, 'Watersheds in Perception and Knowledge: Twenty Years of Military Technology', draft manuscript (June 1999).
15. Thomas G. Mahnken, 'War in the Information Age', *Joint Force Quarterly* (Winter 1995–96), pp.39–43.
16. Schwartau, *Information Warfare*, p.265.
17. Michael I. Handel, *Masters of War* (third edn), (London: Frank Cass, 2001), p.150.
18. Fyodor, 'The Art of Port Scanning', <http://www.insecure.org/nmap/namp_doc.html>; D. Lee, J. Rowe, C. Ko and K. Levitt, 'Detecting and Defending Against Web-Server Fingerprinting', *18th Annual Computer Security Applications Conference*.
19. Michael Dewar, *The Art of Deception in Warfare* (Devon, England: David and Charles Publishers, 1989), p.19.
20. The classic example of deception through diversion was Operation FORTITUDE, the codename for the deception plan associated with Operation OVERLORD, the Allied invasion of Europe in 1944. The diversion focused German attention on the Pas de Calais and other parts of Europe. When the Allied invasion took place in Normandy, the Germans were not sure for nearly two months whether it was the main invasion or merely a feint to draw attention away from a subsequent invasion of the Pas de Calais. Ibid., p.11.
21. Handel, *Masters of War*, p.159.
22. Dorothy E. Denning, *Information Warfare and Security* (Boston: Addison-Wesley, 1999), pp.101–29 examines five areas of perception management: lies and distortions, denouncement, harassment, advertising and censorship.
23. Sun Tzu discussed the use of expendable agents who unknowingly would be given false information and sent into enemy territory, in the hopes that they would be captured and forced to reveal the false information.
24. Denning, *Information Warfare and Security*, p.101.
25. Ibid.
26. Handel, *Masters of War*, p.217.
27. Dewar, *The Art of Deception in Warfare*, pp.18–19.
28. Ibid., pp.14–15.
29. Ibid., p.10. Dewar provides a list of techniques of deception. The first is encouraging the enemy to believe that the most likely way of achieving the objective will in fact be adopted thereby diverting his attention from an alternative plan. The lure presents the enemy with what

appears to be sudden or ideal opportunity, which he would be wise to exploit whereas in fact he is being lured into a trap. The repetitive process lures the opponent into a false sense of security. The double bluff involves openly revealing the truth to the enemy – who has come to expect deception – in the conviction that he will not believe it. The unintentional mistake leads the enemy to believe that valuable information has come into his hands through a break of security or by negligence or inefficiency on the part of the enemy. The piece of bad luck encourages the enemy to think he has acquired information of vital importance by accident because of a train of circumstances over which his adversary has no control. Substitution encourages the enemy to recognize something as false and to continue in the belief that it is false even after it has been covertly replaced by the real – and vice versa. One can disguise one's own forces in enemy uniforms. Finally, Dewar notes that deception techniques can be categorized in terms of the senses. Camouflage and concealment involve visual deception. Sound can also be used to deceive.

30. C. Stoll, 'Stalking the Wily Hacker', *Communications of the ACM*, Vol. 31, No.5 (May 1988) pp.484–97.
31. Thom Shanker and Eric Schmitt, 'Firing Leaflets and Electrons, U.S. Wages Information War', *New York Times* (24 Feb. 24 2003), pp.A1, A7.
32. Handel, *Masters of War*, pp.217–8.
33. J. Anderson, 'Computer Security Technology Planning Study', Technical Report ESD-TR-73-51, Electronic Systems Division, Hanscom Air Force Base, Hanscom, MA (1974).
34. W. Cheswick, 'An Evening with Befrerd, in Which a Cracker is Lured, Endured, and Studied', *Proceedings of the 1992 Winter USENIX Conference* (Jan. 1992) pp.163–73.
35. L. Spitzner, *Honeypots: Tracking Hackers* (Boston, MA: Addison Wesley Professional, 2002).
36. Symantec, 'Information on Back Orifice and NetBus', <http://www.symantec.com/avcenter/warn/backorifice.html>.
37. Robert J. Art, 'The Four Functions of Force', reprinted in Robert J. Art and Robert Jervis, *International Politics* (fourth edn) (New York: Harper Collins, 1996), pp.159–60.
38. Ibid.
39. James Der Derian, 'Cyber-deterrent', *Wired*, Vol. 2, No.9, pp.116–22.
40. B. Reid, 'Reflections on some Widespread Computer Break-Ins', *Communications of the ACM*, Vol. 30, No.2 (Feb. 1987), pp.103–5.
41. Thomas C. Schelling, 'The Diplomacy of Violence', reprinted in Art and Jervis, *International Politics*, pp.169.
42. Ibid., p.178.
43. Alexander L. George, 'Coercive Diplomacy: Definition and Characteristics', in Alexander L. George and William E. Simons, ed., *The Limits of Coercive Diplomacy* (Boulder: Westview Press, 1994), p.10.