The Strategic Value of Information in Effects-Based Operations

Gary Waters

Introduction

The attraction of effects-based operations (EBO) is the prospect of improved efficiency in the planning and conduct of operations. Put simply, EBO can be seen as a coordinated set of actions that are directed at shaping the behaviour of friends, foes and neutrals in peace, crisis and war.[1] In shaping nation states, we would focus on politics, which drives the various dimensions of national power. In shaping the behaviour of non-state actors, the focus would be on ideology.

But what brought us to this culminating point that presents EBO as an attractive option? Ed Smith has suggested that the combination of three technology revolutions – sensor, information and weapons – combined with the promise of network-centric thinking within an effects-based approach herald enormous promise for improved efficiency as well as effectiveness. [2]

Sensor technology, which essentially provides situational awareness, offers the promise of comprehensive, near-real-time surveillance over vast areas and facilitates the move toward smaller, cheaper, more numerous sensors that can be networked to detect, locate, identify, and track targets. It's not the sensor technology itself that is important to EBO; rather, it's the information that the sensors provide.

Information technology, which essentially provides the network backbone, offers the potential to expand the capability of the sensors both by better integrating the data collected and by allowing the sensors to interactively build on one another's efforts. Furthermore, the scope and scale of the data provided by the sensor revolution is likely to be of such a quantity that it would be unmanageable if it were not for an information revolution that will bring the geometric increase in computing power necessary to process, collate, and analyse the resulting quantity of sensor data. Again, it's not the

---

[1] I am indebted to Ed Smith for this working-level definition.
[2] E Smith, *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War*, Command and Control Research Program (CCRP) Publication Series, July 2003.

information technology itself that is important to EBO; rather, it's what that allows – the flow of information.

Finally, weapons technology offers better streams of targeting data that can permit a 'dumbing down' of expensive guidance packages and thus reduce costs. Moreover, new designs, better electronics, 'lean manufacturing', and mass production of significantly larger numbers of weapons can decrease the cost for a given level of accuracy and capability.

Smith notes that first order improvements accrue from synergies associated with the three technology revolutions in that better sensors and information could create better situational awareness and thus reduce fratricide and enable forces to detect enemy moves as they occur, and that better targeting data would mean that fewer weapons would be required for a given mission. Second order improvements arise through networking as NCW allows forces to explore new ways of carrying out existing missions more effectively and efficiently and allows them to explore how they might undertake new missions that have not previously been attempted. NCW is characterised by an increased speed of command, improved shared situation awareness, and the ability for self-synchronisation. Finally, Smith argues that third order improvements can be realised through EBO by foreshortening the combat itself by breaking an enemy's will to resist, even though they may retain the forces and capabilities to continue do so.[3]

The changes offered by these new technologies and NCW actually allow defence forces to do more than just improve the efficiency of their attrition. Indeed, network-centric operations enable one to 'get inside the enemy's OODA loop',[4] and to use the increased pace of friendly operations to overwhelm the enemy and lock him out of an effective response. While we should expect that success would continue to be measured in terms of targets destroyed and attrition of enemy forces and capabilities, the promise of foreshortened combat by breaking an enemy's will to resist, even though they may retain the forces and capabilities to continue to fight is worth pursuing.

In a linear view of battle, we might argue that by getting inside the enemy's OODA loop, we would be able to destroy his force and that because the enemy would not be able to respond effectively, we would be able to destroy his infrastructure with relative impunity. Yet, the real efficiency that we seek with our new technologies and network-centric thinking is more in keeping with Sun Tzu's exhortation to avoid combat and subdue the enemy without

---

[3] *Ibid*, pp. 66-97.
[4] The Observe-Orient-Decide-Act (OODA) loop was first presented by Colonel John Boyd (USAF) in August 1987 at a briefing at Maxwell Air Force Base. The briefing was entitled 'A Discourse on Winning and Losing'. The concept is described further in G E Orr, *Combat Operations C3I: Fundamentals and Introductions*, Air University Press, Maxwell AFB, AL, p.198.

fighting.[5] Thus, the proponents of EBO do need to explore how we break our enemies' wills rather than grind down their means of waging war and how the new technologies and concepts of network-centric operations apply to the use of military power short of destroying the opposing forces and capabilities.

It is not just about battle and traditional war fighting scenarios. Indeed, national security is being broadened to include a plethora of government agencies and other organisations at federal, state and local levels. To support this multi-dimensionality, large quantities of information are flowing along with calls for better quality information, and connectivity. All of this leads to an increase in the strategic value of information and focuses attention on the challenges from potential information overload and underlying vulnerabilities.

The importance of acquiring, processing and disseminating information has been recognised since the beginning of time across all of mankind's endeavours. Through time, the basic principles have endured, but the means have changed quite dramatically, using technology to speed up the entire process and to allow increasing volumes of information to be moved around. We may well have reached a point in time where the strategic value of information is such that it has, itself, become a strategic target.

Thinking about effects based planning and EBO brings with it vastly increasing information flows underpinned by increasing levels of connectivity. Indeed, the pervasiveness of information could see it become a new dimension of warfare such that it joins the existing physical dimensions of maritime, land, air and space to underpin EBO. As such, it possesses strategic value and hence demands we pay attention to the concept of strategic information warfare and its attendant vulnerabilities. In that respect, we need to look at the information infrastructure as something more than a technology issue that can be delegated to the chief technology officer or chief information officer. Indeed, it becomes a key enabler for effects based planning and effects based operations.

The Fifth Dimension – The Infosphere

National security is certainly being broadened – encompassing diplomatic, military, economic, information, societal and technical dimensions. To deal with this broadened security environment, we need more not less intelligence to underpin effects based planning activities.

---

[5] S B Griffith, *Sun Tzu: The Art of War*, Oxford University Press, London, 1963, p. 77.

Some would argue that we have ended up with too much information through an emphasis on quantity rather than quality, which came about through computerisation and automation. Over-compartmentalisation of vastly increased amounts of information has simply exacerbated the problem with high quality analysis often not finding the right person at the right time.

As Alvin and Heidi Toffler say 'the computer revolution, the multiplication of satellites, the spread of copying machines, VCRs, electronic networks, data bases, faxes, cable television, direct broadcast satellite, and dozens and scores of other information handling and distributing technologies have created many rivers of data, information and knowledge that now pour into a vast, constantly growing ocean of images, symbols, statistics, words and sounds'.[6]

As the increasing strategic value of information needs to be understood, so too do the tactical and technical implications of dealing with this enormous increase in information and connectivity. While we have traditionally viewed strategic power as emanating from the environments of land, sea and air, to which the fourth dimension – that of space – has more recently been added, we now need to embrace information as a fifth dimension. Some refer to this environment as the 'infosphere'.[7]

As touched on earlier, the DIMEST construct looked at through the lens of this infosphere leads us to conclude that each of the dimensions depends on the infosphere and it is through the infosphere that we can better understand the interactions and interdependencies across these various dimensions of national power.[8] The infosphere will increasingly underpin the effective functioning of society, as the Tofflers have argued, and it will increasingly underpin any national effects based planning approach that Australia may adopt in future.

The infosphere relies on the electromagnetic spectrum and a number of physical assets such as people, cables, computers and satellites. So there is an overlap between this fifth dimension and the physical world. And, as David Lonsdale argues, we are increasingly seeing ownership claims for information by businesses, states and individuals. All of this leads Lonsdale to conclude that we need to understand the nature of the infosphere and regard it as something that can be manipulated and used for strategic advantage.[9]

---

[6] A & H Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*, Little, Brown and Co, 1993, p. 160.
[7] This term is explained well in D J Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*, Frank Cass, London, New York, 2004, p. 181.
[8] DIMEST – diplomatic, information, military, economic, societal, and technical.
[9] Lonsdale, *The Nature of War in the Information Age*, p. 182.

In understanding the nature of the infosphere we first need to understand just what 'cyberspace' is. Martin Libicki offers a useful start point in defining cyberspace as 'the sum of the globe's communications links and computational nodes'.[10] Lonsdale argues that as such cyberspace is only part of the infosphere and that the developing salience of information also needs to be incorporated.[11]

Emergence of this concept of cyberspace and the continuing exploitation of the electromagnetic spectrum are allowing us to better appreciate the strategic value and power of information. If we accept that the value of information is its accessibility and flexibility, then we can argue that when information is used in a strategic sense, its strength lies in its accessibility and flexibility. Indeed, as Lonsdale suggests, as a consequence of this accessibility and flexibility, it is difficult to see how any actor can perform at the strategic level without understanding and taking account of the power of information.[12]

While clearly the power of information will enhance the potency of the conventional military power of nation states, and indeed overall national security power, the ubiquitous nature of information means it can also empower the smallest of actors, thus endowing non-state and sub-state actors with the ability to impact nation states. This leads us to conclude that in becoming ubiquitous, information has strategic value.

The Strategic Value of Information

Some of the challenges in trying to plan the strategic use and protection of information are that information is abstract; it has multiple and even simultaneous uses; it is inexhaustible, but its value can perish over time; and its value is complex and non-linear.[13] It exists as measurements and observations, which are referred to as data. It exists as data in context that is organised and indexed, which is referred to as information. It exists as information that is understood and explained, which is referred to as knowledge. Finally, it exists as knowledge that is effectively applied, which is referred to as wisdom.

Simplistically, we might view data as the basic elements, information as organised data, knowledge as contextualised information, and wisdom as applying knowledge to achieve an effect. The process flow through this hierarchy starts with collecting, tagging and moving observations. Waltz

---

[10] M C Libicki, 'The Emerging Primacy of Information', *Orbis*, vol. 40, no. 2, 1996, pp. 261-76.

[11] Lonsdale, *The Nature of War in the Information Age*, pp.183-4.

[12] *Ibid*, p. 196.

[13] E Waltz, *Information Warfare: Principles and Operations*, Artech House Publications, Boston and London, 1998, pp. 49-50.

refers to this as 'observation'.[14] Bridging the information and knowledge levels is the process of comprehending and explaining static and dynamic relationships between sets of information. Waltz calls this 'understanding'.[15] Finally, the process of applying knowledge to carry out a plan to achieve a desired goal is referred to as 'application'.[16] There is direct correlation between Waltz's views here and the OODA loop discussed earlier, in terms of the 'observe', 'orient' and 'act' elements.

With these definitions in mind, we can postulate that the effect we wish to achieve from the use of information in business is to create capital value; the effect in the military and national security is to achieve a desired end-state; and across government, it is to deliver value to the public. From this, we can say that we use information to create value and achieve a desired end-state. The business focus, military focus, national security focus or government service-delivery focus will drive the nature of the data that is necessary. For example, business seeks to define the market place (customers, buying trends, product differentiation, etc); the military seeks to define the battle place (orders of battle, terrain, targets, etc); and government seeks to define the public place (voter preferences, national economic and social issues, and so on).

In a business sense, the strategic value of IT can be exploited by gaining leverage through process innovation, by applying data and information in one process to other processes, and by sharing networks or selling excess capacity.[17] Waltz extends this thinking to the military dimension and whole-of-government dimension by arguing that leverage can be gained through the use of data links to deliver real-time targeting information to weapons; intelligence could be applied to support the competitiveness of the economy; and coalition networks with appropriate security mechanisms can burden share.[18]

In assessing the value of information, Waltz looks at six approaches – epsitemology (truth and human perception), logic, information theory (value chains in processing and communication), decision theory (measuring performance and effectiveness based on impact), and knowledge management (measuring the economic utility of information processes).[19] Waltz's analysis leads him to surmise that the greatest utility comes from acquiring the right data, transforming that data to knowledge, distributing that

---

[14] Waltz, *Information Warfare: Principles and Operations*, p. 51.
[15] *Ibid.*
[16] *Ibid.*
[17] J V McGee, L Prusak and P J Pyburn, *Managing Information Strategically: Increase your Company's Competitiveness and Efficiency by Using Information as a Strategic Tool*, John Wiley & Sons, New York, 1993, pp. 68-69.
[18] Waltz, *Information Warfare: Principles and Operations*, pp. 54-55.
[19] *Ibid*, pp. 69-70.

knowledge so that it can be applied, and protecting it all.[20] In sum, the strategic value of information is a function of its availability and reliability, and the way in which it contributes to achieving a desired effect.

In traditional military thinking, information has tended to be viewed as battlefield intelligence and tactical attacks on enemy radar and telephone networks. Based on the discussion thus far, we can now broaden that thinking and see information as a powerful lever that can alter an enemy's high-level decisions. Indeed, it becomes a strategic asset, in which opposing sides will try to shape the other's actions by manipulating the flow of intelligence and information.[21]

It was out of this thinking that Command and Control Warfare emerged in the early 1990s. David Ronfeldt and John Arquilla of the RAND Corporation in Santa Monica took this further into the realms of cyber war – turning the balance of information and knowledge in one's favour.[22]

In its simplest sense, the strategic value of information boils down to the ability to 'acquire, process, distribute and protect information, while selectively denying or distributing it to its adversaries and/or allies'.[23] In other words, the strategic value comes from providing the right information to the right people at the right time.

Hand-in-glove with this notion of providing information to the right person in the right place at the right time in the right form is the requirement to deliver the right training and education to the right person in the right place, at the right time, in the right form. Just as advanced technologies help the flow of information so too can they speed learning – in particular through simulation. All of this leads Toffler to conclude that 'knowledge is the ultimate substitute for other resources'.[24] And in effects based thinking, this knowledge that comes through effective national assessment is pivotal.

But while information or knowledge superiority might win wars, it is also highly fragile. As Toffler says, 'a small bit of the right information can provide an immense strategic or tactical advantage. The denial of a small bit of information can have catastrophic effects'.[25] This leads to the notion of information superiority, which is the capability to collect, process, and

---

[20] Waltz, *Information Warfare: Principles and Operations,* p. 73.

[21] A & H Toffler, *War and Anti-War*, p. 140.

[22] J Arquilla and D Ronfeldt, *The Advent of Netwar*, RAND Corporation, Santa Monica, CA,1996, and D.Ronfeldt and J Arquilla, *Networks and Netwars*, RAND Corporation, Santa Monica, CA, January 2002.

[23] A & H Toffler, *War and Anti-War*, p. 142.

[24] *Ibid*, p. 147.

[25] *Ibid*, p. 148.

disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.[26]

Should an information attack be launched against us, we can take defensive or offensive measures. A defensive response would 'generate alerts, increase the level of protective restrictions to access, terminate vulnerable processes, or initiate other activities to mitigate potential damage'.[27] An offensive response would support targeting and specific attack options of our own.[28]

With many weapons increasingly coming to rely on information – such as smart munitions that use GPS guidance – we can expect information to become 'more directly relevant' in warfare of the future.[29] Similarly, a digitised force should be able to operate at a higher tempo than a non-digitised one through its improved ability to coordinate actions.[30] And a common relevant operating picture should lead to more efficient command and control.[31]

This can be lifted out of the military dimension and applied within a whole-of-government context. We can expect information to become 'more directly relevant' in whole-of-government activities of the future. Similarly, digitised elements from multiple agencies should be able to operate at a higher tempo than non-digitised elements through their improved ability to coordinate actions. And a common relevant operating picture should lead to more efficient coordination.

These twin related notions of effects based planning across the whole-of-government demand an ability to identify, analyse and resolve all of the interacting facets of multi-dimensional problems such that decision makers are provided with a degree of confidence that the right decision can be made at the right time by the right people. This means we need to be able to clarify both the dimensions and the drivers of any given planning issue from which an effect is desired. An outcome decision system that derives policy options for seemingly intractable strategic problems that operates on the basis of collaboration and collegiality and forges a highly participative approach across subject matter experts would seem long overdue.

---

[26] US DoD Joint Publication 3-13, 'Joint Doctrine for Information Operations'.
[27] Waltz, *Information Warfare: Principles and Operations*, p. 160.
[28] *Ibid*.
[29] Lonsdale, *The Nature of War in the Information Age*, p. 91.
[30] *Ibid*, p. 92.
[31] *Ibid*.

Strategic Information Warfare and Vulnerabilities

If, as Robert Pape suggests, measuring success 'is not about assessing *combat* effectiveness but *strategic* effectiveness',[32] then perhaps there is far more to strategic information warfare than many commentators are prepared to acknowledge. This is entirely consistent with effects based thinking. In cases where strategic information warfare cannot obtain strategic decisiveness in a military sense, then clearly traditional modes of destructive warfare would continue to prevail.

There is a note of caution that must be sounded, however. We must be careful not to overplay this significance of information in warfare and to treat warily retrospective analyses of history that 'discover' the importance of information.[33] In the end, information is an important enabler, which may at times be of great strategic value, but in essence this is usually because of other actions and effects to which it contributes.

Some of the pro-information literature tends to argue that information dominance avoids the need to use force and that it leads to an ability to disrupt the enemy rather than destroy his forces. While there may be an element of truth in that, the use of force is not incompatible with achieving a superior information position and disruption and destruction are not mutually exclusive.[34] War will continue to be a dangerous and violent clash, while improved information will tend to facilitate a more economical use of force.[35] Information is not an end in itself,[36] it is a means to an end, and increasingly nations will view that end as the achievement of an effect, whether it be diplomatic, military, or economic, or a combination of the instruments of national power.

Ed Waltz offers a basic model of warfare in terms of options for attack. He argues that one can launch a physical attack, engage in deception, carry out a psychological attack, or engage in an information attack.[37] In each of these, information plays a key role. The aim of these options is to destroy, to deceive or surprise, to disorient, and to severely dislocate (by affecting confidence in information through destruction, deception or disorientation).

It would be instructive here to examine how Information Warfare might apply to the physical, information and cognitive domains.[38] In terms of the physical

---

[32] See R A Pape, 'The Limits of Precision-Guided Air Power', *Security Studies*, vol. 7, no. 2, 1997-98, p. 95.
[33] This is expanded in Lonsdale, *The Nature of War in the Information Age*, p.71.
[34] This is discussed further in *ibid*, p. 73.
[35] R Bennett, *Behind the Battle: Intelligence in the War with Germany 1939-1945*, Pimlico, London, 1999, p .9.
[36] A Singh, 'Time: The New Dimension in War', *Joint Force Quarterly,* vol. 10, 1995-96, p. 60.
[37] Waltz, *Information Warfare: Principles and Operations*, pp. 6-7.
[38] *Ibid*, p. 27.

domain, it would involve destruction or theft of computers and destruction of facilities, data bases, communications nodes or lines. In terms of the information domain, it would involve electronic attack against information content or processes either in the network or during transmission. Finally, in terms of the cognitive domain, it would involve targeted attacks against the human mind via electronic, printed or oral means.

As a potential adversary's reliance on Information Technology (IT) increases in order to carry out the first two elements of the OODA loop - observe and orient – the more options for attack are increased in the information and cognitive domains. Furthermore, as the battle space extends beyond the traditional area of operations to encompass a country's entire infrastructure and that of its allies, the number of options for attack increases further.

In an information sense, the OODA loop is about sensing and collecting information (observe), organising the information (orient), understanding it (decide) and disseminating it (act).[39] Technological and human collection of data via signals intelligence, imagery intelligence and human intelligence contribute to the 'observe' element. Data mining and data fusion contribute to the 'orient' element and are discussed in more detail below.

A mix of automation of certain simple responses and human judgment for more complex decisions contributes to the 'decide' element.[40] And it is here that I argue the need for an outcome decision system that derives options for seemingly intractable problems(whether they be whole-of-government strategic planning problems or more specific military planning problems) that operates on the basis of collaboration and collegiality and that forges a highly participative approach across subject matter experts, as mentioned earlier.

Data fusion is defined as a process in which 'diverse elements of similar observations (data) are aligned, correlated, and combined into organised and indexed sets (information), which are further assessed to model, understand, and explain (knowledge) the make-up and behaviour of a domain under observation'.[41] Data mining is a process in which 'large sets of data (or data warehouses) are cleansed and transformed into organised and indexed sets (information), which are then analysed to discover hidden and implicit but previously undefined patterns that reveal new understanding of general structure and relationships (knowledge) in the data of a domain under observation'.[42]

---

[39] Waltz, *Information Warfare: Principles and Operations*, p.127.
[40] This is explained further in Waltz, *Information Warfare: Principles and Operations*, p. 91.
[41] D Buede and E Waltz, 'Data Fusion', in *McGraw-Hill Encyclopaedia of Science and Technology*, McGraw-Hill, New York, 1998.
[42] Waltz, *Information Warfare: Principles and Operations*, p. 97.

Data fusion uses deductive reasoning while data mining searches for hidden patterns using inductive reasoning. The focus of the former is retrospective, while data mining can also be prospective.[43] Deductive reasoning is where a specific case can be inferred to be true if it satisfies the conditions of a general statement. Inductive reasoning is where the general validity of a statement can be inferred from the demonstration of its validity over an acceptable range of specific cases.[44]

The logical extension of all of this for the country that can master the information domain is to close the loop on Sun Tzu's observation that the acme of skill is to 'subdue the enemy without fighting'.[45] The US thought leader, Dick Szafranski, updated Sun Tzu's observation by arguing that the knowledge systems of an adversary (epistemology) should be the primary strategic target.[46] This is not meant to imply that information is the only option for attack, but that its importance as a partner to the more traditional physical forms of attack has increased.

In a war fighting sense, we can see that sensor technologies have extended the engagement envelope; computers and communications technologies have led to an increase in tempo of operations; and the integration of IT into weapons has made them more precise and lethal. The real transformation, therefore, has not been in sensor, weapons or IT technology *per se*, but in shifting the focus from the physical dimension to the information one. Waltz calls this the transition toward the dominant use of information and the targeting of information itself.[47] He makes a neat distinction between Information Warfare, which emphasises the use of information as a weapon or target, and Information-based Warfare, which he describes as the use and exploitation of information for advantage – often in support of physical weapons and targets.[48]

However, shifting focus to the information dimension also carries with it a physical manifestation – that of the information infrastructure. If information is so important then so too is its enabling infrastructure and that infrastructure needs to deliver three security-related effects – availability, integrity and confidentiality.[49]

Meanwhile, an adversary would be trying to achieve its own effects; wishing to use Information Warfare to achieve three different effects - disruption, corruption or exploitation. Each of these can be aligned with one of the

---

[43] *Ibid*, p. 99.
[44] Waltz, *Information Warfare: Principles and Operations,* p. 84.
[45] S B Griffith, *Sun Tzu: The Art of War*, p. 77.
[46] R Szafranski, 'A Theory of Information Warfare: Preparing for 2020', *Airpower Journal*, vol. 9, No. 1, Spring 1995, pp. 56-65.
[47] Waltz, *Information Warfare: Principles and Operations*, p. 10.
[48] *Ibid*.
[49] *Ibid*, p. 22. Although Waltz refers to these as attributes rather than effects.

security effects mentioned above. Disruption aligns with availability; corruption aligns with integrity; and exploitation aligns with confidentiality (or privacy).

While there are clearly warfare dimensions that need to be considered in the strategic value of information, there are also positive opportunities that can be leveraged in terms of more open networks and communication. This will help promote an exchange of ideas, democratic processes, humane values, and rapid and continuous exchange of information at national leadership levels. All of this can lead to less misunderstanding, more informed decisions, and help counter oppressive regimes, thus ranging across the full spectrum of effects that a national leadership may wish to contemplate.

With all of this information potentially available, there is the question of information overload. We do not really understand the breakdown of human performance under heavy information loads, yet we are accelerating both the pace of change and the amount of information. Compounding all of this is the increasing tempo of decision-making and the need (whether real or perceived) for a rapid response to a situation. Increasingly, the situations in which 'programmed' decisions can be made is reduced, which leads to disorganisation, exhaustion and anxiety.

Increasing the number of choices increases the amount of information needed and tests show the more the choices, the slower the reaction time. Hence, we are faced with incompatible pressures as we combine the effects of decision stress with sensory and cognitive overload.[50] Alvin Toffler argues that people tend to suffer at three different levels – sensory (perceiving), cognitive (thinking), and decisional (deciding).[51] It is at the cognitive level that information overload manifests itself and people find it difficult to make reasonably correct assessments that characterise rational behaviour. Studies have shown that there are limitations on the amount of information a person can receive, process and remember.[52]

As a counter to Toffler's views, the newer generations who have been exposed to computers at an early age will get better and better at taking in information and making decisions quickly. They will have new skill sets and indeed they are more likely to be calling for more information and for better tools to filter and search through that information. They won't want to see any information being held back. So there will be a challenge in balancing the different expectations and skill sets of different generations who come together at the pinnacle of national security effects based planning.

---

[50] A Toffler, *Future Shock*, Bantam Books, August 1971, p. 358.
[51] *Ibid*, p. 348.
[52] *Ibid*, p. 351, where Toffler cites the work of Rockefeller University psychologist George A. Miller.

VULNERABILITIES

This information dimension that we have identified will, increasingly, underpin almost every aspect of a modern nation's way of life, economy and security. We depend so much on the interrelated trio of electrical energy; the telecommunications system; and the interconnected, networked information systems that service society.[53] This dependence does make the electrical energy, communications and computers trio a key vulnerability.

Unfortunately, there is no silver bullet solution to protect against information warfare attacks.[54] That said, the technology and tools do exist to defeat and defend against the information warrior;[55] defensive measures are part of many information systems;[56] and there are well-developed countermeasures in a thriving anti-virus industry.[57] Resilience, redundancy and robustness have been built in to our information infrastructure. Consider Robert Anderson's point that the US's infrastructure is 'very resilient, as various natural disasters and various incidents to date have shown'.[58] And Greg Rattray argues that the complexity of information infrastructure has brought with it an 'inadvertent robustness'.[59]

Furthermore, when it comes to attacks against a population's will, we must be mindful of Robert Pape's point that losing modern infrastructures through a strategic information attack is simply not comparable to being firebombed.[60] Indeed, as Lonsdale notes, if a population's will can withstand Dresden and Tokyo, it will surely hold up in the face of all but the most destructive acts of Strategic Information Warfare.[61] The most destructive act would be a major nuclear incident.

But what is more likely? Carlo Kopp refers to Electro-Magnetic Pulse (EMP) weapons as 'the nuclear weapons of the information age' and notes that apart from major electrical systems, commercial networked computer

---

[53] See both *Critical Foundations: Protecting America's Infrastructures,* Report of the President's Commission on Critical Infrastructure Protection, October 1997, <www.pccip.gov>; and F J Cilluffo and C H Gergely, 'Information Warfare and Strategic Terrorism', *Terrorism and Political Violence*, vol. 9, no. 1, 1997, p. 87.

[54] D E Denning, *Information Warfare and Security*, Addison-Wesley, Boston, MA, 1999, p. xiv.

[55] W Schwartau, ed, *Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age*, 2nd edition, Thunder's Mouth Press, New York, 1996, p. 589.

[56] L Freedman, *Information Warfare: Will Battle Ever Be Joined?*, International Center for Security Analysis (Launch), 14 October 1996, p. 8.

[57] G Smith, 'An Electronic Pearl Harbor? Not Likely', *Issues in Science and Technology Online*, Fall 1998.

[58] R H Anderson, 'Risks to the US Infrastructure from Cyberspace', verbal testimony to the Permanent Subcommittee on Investigations, 25 June 1996, and cited in Lonsdale, *The Nature of War in the Information Age*, p. 164.

[59] G Rattray, *Strategic Warfare in Cyberspace*, MIT Press, Cambridge, MA, 2001, p .133.

[60] R A Pape, 'The Limits of Precision-Guided Air Power', p. 103.

[61] Lonsdale, *The Nature of War in the Information Age*, p.166.

---

systems are also vulnerable to EMP weapons.[62] Taking Carlo Kopp's thoughts a little further, one area of concern that received some attention by the US Congress in 2004 was the effect of high-altitude electromagnetic pulses. High-altitude electromagnetic pulses are by-products of nuclear explosions in space and can have devastating effects on critical infrastructure that is not sufficiently hardened. Indeed, a Congressional Commission argued that much of the critical infrastructure is insufficiently hardened and recovery plans are incomplete or non-existent.[63] While EMP effects do not directly harm people, they can damage and disrupt electronics.

A briefing from the Commission stated that 'America's ability to reconstitute following such an EMP attack is inadequate; full recovery might take months to years. This threat also places our national economy and worldwide military forces at risk'.[64] The Commission briefing went on to state that the US was as vulnerable to a 'cheap shot' as well as to a 'high-tech threat'. Potential adversaries would have to be aware of this as a strategic attack option.

The infrastructure that might be affected by EMP attacks includes power grids, telecommunications systems (including cell phone, satellite and Internet communications, as well as high-frequency, VHF and UHF receivers), financial markets and networks (such as the various international stock exchanges), transportation, energy distribution, water supply and sanitation, fuel supply and refineries, chemical plants, emergency services, health care, and the military, among others. Home computers and other systems would also be affected.

US and Australian infrastructure is increasingly dependent on microelectronics in computers and other systems, making facilities and systems 'simultaneously at serious risk over a large geographic area'.[65] A large-scale attack would undermine the integrity and coherence of government and its public services.

The results from some 'hands-on' testing carried out by the Commission indicated greater vulnerability of control and communications systems, and concerns over the interdependence of many systems. The oil and gas industry, for example, is connected in various ways to power plants, the transportation industry, communications systems, even legislative offices

---

[62] See C Kopp, 'The E-Bomb – A Weapon of Electrical Mass Destruction' in W Schwartau, ed, *Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age*.
[63] See 'Panel Says Society At Great Risk From Electromagnetic Pulse Attack', *Inside The Pentagon*, 15 July 2004, p. 1.
[64] *Ibid.*
[65] *Ibid.*

and military installations. Similarly, banking and finance are tied to various industries and government entities.[66]

Strategic information warfare is anonymous and insidious says Lonsdale; threats are difficult to quantify; entry costs are low; new target sets are presented (such as the finance and banking system); society can be disrupted without being destroyed; and strategic information warfare has global reach without an in-theatre footprint.[67] These points lead Lonsdale to conclude that strategic information warfare does offer the potential for intense and simultaneous attacks without precedent; however, it is more in terms of operational efficiency rather than strategic efficacy.[68]

Strategic information warfare is not a solution for every occasion. There are far too many intangibles. Vulnerability of information systems does not automatically mean an adversary would achieve strategic success if it attacked these systems. The key systems that can be attacked and that need to be defended revolve around the information infrastructure as mentioned above.

The Information Infrastructure

Conceptually, we can look at the information infrastructure at three levels – globally, nationally and locally (for Defence). Hence, we have the Global Information Infrastructure (GII), the National Information Infrastructure (NII), and the Defence Information Infrastructure (DII). These are discussed in more detail below.

GLOBAL INFORMATION INFRASTRUCTURE (GII)

The GII comprises 'the international telecommunications computer networking, and command services (such as air traffic management and global navigation services administered by the ICAO[69] regulated by international laws and treaties and accessible to the international community)'.[70] While intercontinental cables have underpinned development of the GII, increasingly it will rely on a commercial network of broadband communications satellites. These future satellite constellations will use space and ground-based switching but will also seek to use inter-satellite links to improve traffic efficiency. For nations to be on the GII, they will need to integrate their terrestrial fibre-optic links and wireless communications

---

[66] *Ibid.*
[67] Lonsdale, *The Nature of War in the Information Age*, pp. 167-168.
[68] *Ibid*, p. 168.
[69] The International Civil Aviation Organisation (ICAO) is a United Nations organisation that provides oversight and regulation of international air traffic control operations.
[70] Waltz, *Information Warfare: Principles and Operations*, p. 175.

systems with these satellite networks. Increased connectivity will provide greater access, but it will also increase vulnerability.

NATIONAL INFORMATION INFRASTRUCTURE (NII)

The NII includes the public switched telecommunications network (PSTN), the Internet, and the millions of private, commercial, academic and government computers. The information infrastructure is probably the most critical of all national critical infrastructures (the others being infrastructures such as banking, energy, physical distribution, and so on). In Australia, we define critical infrastructure as those physical facilities, supply chains, information technologies and communications networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation, or affect Australia's ability to conduct national defence and ensure national security.[71]

Attacks against the NII would seek to reduce security, weaken public welfare or reduce economic strength.[72] Indeed, the increased dependence of government, business and the military on the NII is cause for alarm.[73] A US study noted two capabilities required of the NII to address its vulnerabilities. First is infrastructure protection – defences to prevent and mitigate the effects of physical or electronic attack; and second is infrastructure assurance – ability to ensure readiness, reliability and continuity so as to restrict damage and provide for reconstitution after an attack.[74]

DEFENCE INFORMATION INFRASTRUCTURE (DII)

The DII is the 'web of communications networks, computers, software, databases, applications, weapon system interfaces, data, security services, and other services that meet the information processing and transport needs of Defence users across the range of military operations'.[75]

ROLE OF INFORMATION INFRASTRUCTURE IN WARFARE

Operations in the electronic sphere include electronic warfare (where targets are attacked over the radiated electromagnetic spectrum) and network

---

[71] I am indebted to my colleague Mike Rothery, from the Attorney General's Department for this definition. Critical infrastructure protection is a topic in its own right and is not discussed further in this Chapter.

[72] Waltz, *Information Warfare: Principles and Operations*, p.178.

[73] Concerns in the US are expressed in K B and E Wilson, eds, *National Information Infrastructure Initiatives: Vision and Policy Design*, MIT Press, Cambridge, MA, 1996; N Munro, 'The Pentagon's New Nightmare: An Electronic Pearl Harbor', *Washington Post*, 16 July 1995; and S K Black, 'A Sobering Look at the Contours of Cyberspace', *Viewpoints 96*, Ridgeway Center for International Security Studies and the University of Pittsburgh, 3 June 1996.

[74] *Information Warfare Legal, Regulatory, Policy and Organizational Considerations for Assurance*, The Joint Staff, Washington, DC, 2d ed., 4 July 1996.

[75] Waltz, *Information Warfare: Principles and Operations*, p. 187.

operations (attacks against the GII, NII and DII).[76] A specific form of electronic warfare that attacks tactical radio navigation aids or global positioning system is known as navigation warfare or 'navwar'.

In the main, network operations can be seen in three segments:
- Network attack – attacks over the information infrastructure aimed at penetrating security and exploiting, acquiring, degrading, neutralising or destroying infrastructure or information itself.
- Network protection – actions taken to protect the information infrastructure from network attacks.
- Network support – actions taken to search for, map, identify, characterise, and locate information infrastructure elements, or actions to intercept and exploit information.[77]

INFORMATION ATTACK AND INFORMATION ASSURANCE

Offensive Information Operations seeks to breach privacy, invalidate the integrity of data or degrade the availability of services.[78] Malicious attacks can be achieved through:[79]

- Bacteria – independent, self-replicating agent program that creates multiple versions of itself, taking up storage space and processing time. It denies service to legitimate users, but does not attach to a host program.
- Worm – independent, self-replicating agent program that seeks to spread itself across computers on a network. It too seeks to consume network resources and deny service.
- Virus – dependent, self-replicating agent program that needs a host program to attach itself to and once executed, 'infects' other host programs.[80]
- Trojan horse – an apparently legitimate program containing a hidden hostile function, which is usually activated by a conditional test.
- Bomb – deceptive, disruptive or destructive function that is activated by time or a logical condition.
- Back door/trap door – installed logic that provides a covert channel of information or covert access to the system.

Information assurance includes:
- Availability – accessibility and usability when needed.

---

[76] *Ibid*, pp. 213-14.
[77] *Ibid*, p. 218.
[78] *Ibid*, p. 255.
[79] *Ibid*, pp. 283-85.
[80] By 'infects', I mean the program inserts a copy of itself.

- Integrity – secure from unauthorised tampering, through use of encryption, digital signatures and intrusion detection.
- Authentication – whereby only authorised users have access to information and services.
- Confidentiality – protects a connection, traffic flow and information content from disclosure.
- Non-repudiation – ensures that transactions legitimately authorised cannot be denied and they can be independently verified to establish proof of origin and delivery.
- Restoration – assures information and systems can survive an attack and their availability can be resumed.[81]

Beyond the ability to detect and respond to attacks discussed earlier, other survivability characteristics include:
- Fault tolerance – ability to withstand attacks, gracefully degrade and allocate resources to respond.
- Robust, adaptive response – ability to detect anomalies, allocate critical tasks as necessary, isolate failed nodes, and develop appropriate responses.
- Distribution and variability – no single-point vulnerability and sufficient diversity to avoid common design vulnerabilities that can be attacked by a single mechanism.
- Recovery and restoration – ability to assess damage, plan recovery and achieve full restoration of services and information.[82]

'With the ever-increasing complexity of computer and telecommunications networks (and the software that operates them), control of the potential vulnerabilities makes assurance a daunting challenge'.[83] Secure and assured networks depend on control over delivery (ensuring robust and high performance communications between systems), control over use (access control through authentication and firewalls), and control over the threat (detecting and removing malicious traffic or data from the network before it causes harm or destruction). These are indeed daunting challenges that require policy, process and procedural solutions as much as they demand technical ones.[84]

---

[81] Waltz, *Information Warfare: Principles and Operations*, pp. 301-02.
[82] *Ibid*, p. 334.
[83] *Ibid*, p. 350.
[84] Secure and assured networking is discussed in more detail in 'Transforming Defense Networks: Infranet Concepts and Secure and Assured Networking for Defense Transformation in the 21st Century' <http://www.juniper.net/solutions/literature/solutionbriefs/351094.pdf>.

Conclusion

Information has become an intrinsic factor in planning and operating in the 'effects age'. It has strategic value in supporting all 'effectors' and can be used to generate an effect in its own right, and as such is characterised by inherent vulnerabilities that have to be managed. The information infrastructure is now of such importance that it should no longer be viewed simply in terms of IT service delivery. If effects based planning and operations become the heart of future success in national security activities, then surely information becomes its very life-blood. In a military sense, we need to balance the promise of networks, information flows and flexible command and control structures with the human aspects of the art of command. Extending this to effects based operations, we can say that we also need to balance the promise of networks and improved information flows with the human and cultural aspects evident in the multiplicity of players in the national security agenda. To that end, an outcome decision system that derives policy options for seemingly intractable strategic problems that operates on the basis of collaboration and collegiality and forges a highly participative approach across subject matter experts would seem long overdue.

Gary Waters spent thirty-three years in the Royal Australian Air Force, retiring as an Air Commodore in 2002. From 2002-2005 he was as a senior public servant in the department of Defence before joining Jacobs Sverdrup Australia as a strategy analyst. As a military one-star Gary served in London as Head of the Australian Defence Staff from 1998-2000, and then as Head of the Theatre Headquarters Project (Defence's operational headquarters), and finally as Director General Operation Safe Base. As a public servant he was the inaugural Assistant Secretary Knowledge Planning in Defence, and was then appointed to Assistant Secretary Information Strategy and Futures within the Office of the Chief Information Officer. Gary has written ten books on doctrine, strategy and historical aspects associated with the use of military force. His latest book, co-authored with Professor Des Ball, was released in 2005, entitled 'Transforming the Australian Defence Force for Information Superiority'. He currently serves as a Board member of the Kokoda Foundation, and is also studying for his PhD at the Australian National University, where the working title of his research is 'Information the lifeblood of transformation'. Gary.Waters@sverdrup.com.au