

INFORMATION WARFARE AND ITS IMPACT ON NAVAL OPERATIONS*

Over the centuries one of the most significant contributing factors to a military force's effectiveness has been the availability and reliability of information about an opposing force. The knowledge of the size of such a force, its capabilities and its location has always been a significant factor that assists any adversary in dealing with a threat. We have now entered an age where communications and information technology are pervasive. Most of our daily life is underpinned by technology. It is ironic that military organisations have struggled to develop efficient communications and intelligence systems to gain a strategic advantage over an adversary and that these systems will now be the major vulnerability of any technologically advanced force. We have moved into a new era in military affairs where an attack on the information technology assets of both a country and its military force pose a significant and imminent threat. The new era has ushered in the concept of Information Warfare.

Information Warfare has been variously defined, but typically is viewed as the 'offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information based processes, information systems, and computer based networks, while protecting one's own. Such actions are designed to achieve advantage over military, political or business adversaries'¹. Whereas this definition is new and challenges the elements that underpin our modern society, the concept of information warfare is as old as warfare itself. Information warfare encompasses a wide range of techniques to demoralise or hinder the enemy such as psychological operations, deception or information attack (see editor's note). These have always been in common use by any effective military protagonist, but the attack on specific information technology infrastructure is a new and relatively unknown phenomenon. The proliferation of networked systems and the Internet that underpins the way government and business operate is now, more than ever, a desirable target to any adversary bent on seeking its political objectives.

The advent of this form of warfare poses great difficulties for government and military organisations alike. Questions such as, 'What constitutes an attack?' must be considered in light of a new paradigm for conflict. While it is clear that a physical attack upon property and person will give rise to a country's right to seek United Nations intervention to resolve the situation diplomatically, there has been no clear definition of the consequences of an information technology attack giving rise to such a right, or indeed grounds to permit

physical military intervention. The ability to even recognise an attack is also subject of concern. The penetration of a country's territorial waters by a foreign military power may permit the use of military force under UN Charter. The same cannot be said for an attack on a country's information systems. Evidentiary aspects alone can be complex and require significant expertise, while the motive and intent of the attack may also be obscure. The issue of linking the attackers to a particular country or even tracing them could cause such consternation as to render any government impotent to react.

Australia's current maritime doctrine does not describe an active information warfare role for the Navy; its warfare role is limited principally to armed conflict. This does not imply that the threat is not recognised, as the Department of Defence is committed to the security of its information systems and recognises the significance of computer security. There remains, however, a deficiency in the capability of our Navy to react to a situation where the Government would require a forward military presence to react to an attack on Australian assets through electronic means. The evolving trend towards non-state organisations being the protagonists in any conflict will necessitate the Navy having the capability to react to threats and attacks posed outside the traditional armed conflict paradigm. In such an event the Navy would need to be equipped to take the elements of computer interdiction to the theatre of operations in order to deal with a threat that might be posed to its own, or more generally our country's, information and communications systems.

The impact of attacks on Navy Command, Control, Communications, Computer and Intelligence (C4I) systems is as significant as the one posed to government and commercial organisations. The deployment of our Navy depends upon information. Consequently, the growing reliance upon these systems will also require an increasing need to protect them and determine ways in which we are able to exploit the vulnerabilities of an opposing force. This may not always be possible with conventional techniques of attacking an opponent's C4I systems, and the use of technologies within our borders may in fact be more decisive than steaming towards an adversary. It is the exploitation and recognition of these capabilities that will mark the rise of a new world order in military affairs. A technologically superior entity that has the capability to infiltrate and destroy the C4I capabilities of another country could effectively render the traditional approach of military capacity obsolete. While this at first appears a seemingly grandiose claim, we have seen, time and again, throughout history, the tide turn towards lesser adversaries through the adoption of a significant technology. Information technology will be no less important a revolution in military affairs.



Of the eight characteristics of a maritime power (mobility in mass, readiness, access, flexibility, adaptability, reach, poise and persistence, and resilience²), the resilience of our on-board systems to attack has been recognised as increasing in importance as these systems become even more integral to the functioning of the fleet. No less is the capability of our force to poise and be persistent which will undoubtedly require more complex technology to infiltrate and monitor an adversary's C4I systems. Even as poise and resilience imply that our Navy serves its most useful function by being in a position to bring force of arms to bear at short notice, it will also become increasingly important to bring information technology interdiction capabilities to bear. In a sophisticated technological environment the Navy will not only have to protect its own systems from attack but also participate in waging similar attacks to be able to disable an adversary's capabilities. A situation could arise where a conflict has occurred as a result of an attack on our information infrastructure, which does not warrant physical intervention, but may necessitate the requirement for our Navy to disable the attacking force through technological means. Not as dramatic as a physical attack, it is no less significant in its effect. The disablement of the Australian banking system, for example, would throw our society into chaos. Such an incident, if recurrent, deliberate, and traceable may justify a Navy that possesses more than a physical force capability. In addition, were Navy to be involved in a physical confrontation, the ability of an opposing Navy to debilitate our C4I through electronic means would effectively relegate its effectiveness to that of a pre-WWII fleet; relying on sight and sound to conduct operations. Such an electronic attack could range from a security infiltration via a virus, worm, or similar into a central communications mechanism such as a satellite uplink through to an Electro Magnetic Pulse (EMP) designed to knock out onboard systems or other critical infrastructure such as communications satellites.

Clearly, the current approach to naval operations is the rapid deployment of naval forces to a theatre in order to bring force to bear and control access to and from a country involved in conflict. The capability of Navy to conduct interdiction operations and launch offensive operations is among a range of capabilities that the military relies upon to effectively mount a campaign. The use of information technology to deny an adversary its communications (without physically attacking it) or to infiltrate its command and control networks will become increasingly important in any environment where the existence of a conflict scenario is ambiguous. An involvement in a conflict without physical attack will necessitate the application of like force. Such a capability must therefore be inherent in any force deployed in an environment where such a situation could arise.

The challenge for any military organisation in the face of this new environment is to have information technology architecture that can not only withstand attack but also operate in an environment where it seamlessly supports our forces. At present this is a struggle for any large

military organisation that has created stove-pipe solutions for a range of different environments. This struggle is compounded when a force interacts with allies, who may have developed their own systems and architectures. The ability of an opposing force to exploit these inconsistencies is a new challenge for modern navies but also presents an opportunity for us to be at the forefront of this challenge. The complexity of this task is formidable. The ability of Navy to communicate and to be interoperable with Army and Air Force, our allies and, at the same time, appreciating the capabilities of other countries and the deficiencies inherent in our own and their systems will present significant challenges to the military into the future. The ability to react to a threat and deal effectively with it in this new age, where warfare may not be as easily identifiable, will bring with it challenges all countries are yet to face.

References

1. Golberg, I.K. *Definition of Information Warfare*. Institute for the Advanced Study of Information Warfare, (<http://www.psycom.net/iwar.1.html>), 1999.
2. *Australian Maritime Doctrine (RAN Doctrine 1)*. Department of Defence, Canberra, 2000.

Editor's Note: For an interesting example of WWII deception, see Ewan Montagu, *The man who never was: World War II's boldest counter-intelligence operation*. Naval Institute Press, MD, 1953

***About the author:** LEUT Guy Forsyth is a Naval Reserve Officer who has worked for the Maritime Command Information Systems Agency and also, in his professional capacity, with the Directorate of Information Systems - Navy to develop the Navy Information Network and associated Network Management systems. In his civilian life, Guy has over 20 years experience in the Information and Communications Technology industry and specialises in project management. He has an undergraduate Commerce degree with a major in Information Systems from the UNSW, a Masters degree in Corporate Law from the University of Canberra and is now pursuing doctoral studies focusing on Information Warfare, through the Centre for Maritime Policy at the University of Wollongong in New South Wales.

Published by: The RANR Professional Studies Program, Office of the Director General Reserves (Navy).

The opinions expressed in this paper are those of the author alone and should not be taken to represent the views of the Department of Defence, The Australian Defence Force, the RAN or the Professional Studies Program.

