Land Warfare Studies Centre

Working Paper No. 116

Communications Electronic Warfare and the Digitised Battlefield

by

Michael Frater

and

Michael Ryan

October 2001

National Library of Australia Cataloguing-in-publication Entry

Frater, Michael, 1965– .
Communications electronic warfare and the digitised
battlefield.

ISBN 0 642 29552 2.

1. Electronics in military engineering. 2. Communications,
Military. I. Ryan, Michael. II. Land Warfare Studies
Centre (Australia). III. Title. (Series : Working paper
(Land Warfare Studies Centre (Australia)) ; no. 116).

355.85

Land Warfare Studies Centre Working Papers

ISSN 1441-0389

Working papers produced by the Land Warfare Studies Centre are vehicles for initiating, encouraging or nurturing professional discussion and debate concerning the application of land warfare concepts and capabilities to the security of Australia and its interests. Working papers, by their nature, are not intended to be definitive.

Disclaimer

The views expressed are the authors' and not necessarily those of the Australian Army or the Department of Defence. The Commonwealth of Australia will not be legally responsible in contract, tort or otherwise for any statement made in this publication.

About the Authors

Dr Michael Frater is an Associate Professor in the School of Electrical Engineering at the Australian Defence Force Academy (ADFA). He has more than ten years experience in the development of communications systems and services, including video conferencing and video and image surveillance. He has led ADFA involvement in a number of collaborative projects, investigating tactical image and video communications. Dr Frater has been actively involved in the development of international standards for audiovisual communications and currently chairs the group within the Moving Picture Expert Group (MPEG) concerned with wireless and mobile applications of this technology. He holds a Bachelors degree in Electrical Engineering and a Doctor of Philosophy in Systems Engineering. He is the author of a number of articles on communications systems and communications services, and is the co-author of books on tactical communications architectures and electronic warfare. Captain Frater is also a part-time Army officer in the Royal Australian Signals Corps, currently serving with the Army School of Signals.

Dr Michael Ryan is a Senior Lecturer in the School of Electrical Engineering at ADFA. He has twenty years experience in battlefield communications and information systems. He is a graduate of the Royal Military College, Duntroon; the Telecommunications Engineering Management Course (UK); and of the Australian Army Command and Staff College. Throughout his military career, he has held a range of regimental and staff appointments. He holds Bachelor, Masters and Doctor of Philosophy degrees in electrical engineering. Dr Ryan is an internationally recognised expert on battlefield command systems and has studied battlefield communications systems in Australia, the United States, and Europe. He is the Editor-in-Chief of the international journal, *Journal of Battlefield Technology*, the author of a number of articles and a book on battlefield command systems, and the co-author of books on tactical communications architectures and electronic warfare. In his capacity as a part-time Army officer, Lieutenant Colonel Ryan is a Senior Research Fellow at the Land Warfare Studies Centre.

Land Warfare Studies Centre

The Australian Army established the Land Warfare Studies Centre (LWSC) in July 1997 through the amalgamation of several existing staffs and research elements.

The charter of the LWSC is to promote the wider understanding and appreciation of land warfare; provide an institutional focus for applied research into the use of land power by the Australian Army; and raise the level of professional and intellectual debate within the Army. The LWSC fulfils these roles through a range of internal reports and external publications; a program of conferences, seminars and debates; and contributions to a variety of professional, academic and community fora. Additional information on the centre may be found on the Internet at http://www.defence.gov.au/lwsc.

Comment on this working paper is welcome and should be forwarded in writing to:

The Director
Land Warfare Studies Centre
Ian Campbell Road
DUNTROON ACT 2600
Australia

Telephone: (02) 6265 9548
Facsimile: (02) 6265 9888
Email: dir.lwsc@defence.gov.au

ABBREVIATIONS AND ACRONYMS

ADFA	Australian Defence Force Academy
AS	autonomous system
C2	command and control
C2W	command-and-control warfare
CNR	combat net radio
COMINT	communications intelligence
COMSEC	communications security
COTS	commercial off-the-shelf
CSMA	carrier-sense multiple access
DF	direction finding
EA	electronic attack
EAC	Echelons Above Corps
ECCM	electronic counter-counter measures
ECM	electronic counter measures
ELINT	electronic intelligence
EMCON	emission control
EMSEC	emission security
EOB	electronic order of battle
EP	electronic protection
EPM	electronic protection measures
ES	electronic support
ESM	electronic support measures
EW	electronic warfare
GIG	global information grid
GPS	global positioning system
IEW	Intelligence and Electronic Warfare
IO	information operations
IW	information warfare
JTRS	Joint Tactical Radio System
JV2020	US Joint Vision 2020
LWSC	Land Warfare Studies Centre
MPEG	Moving Picture Expert Group
NCW	network-centric warfare
OPSEC	operations security
PCS	personal communications system
PSYOPS	psychological operations
SIGINT	signals intelligence
UAVs	uninhabited aerial vehicles

ABSTRACT

Modern land commanders are increasingly dependent on information-age systems comprising communications and information systems, networks and sensors. While these systems have the potential to produce significant changes in the conduct and character of war, their reliance on the electromagnetic spectrum also has the potential to increase their vulnerability to interdiction by electronic-warfare systems. Of all the changes likely to occur as a result of the use of information-age systems, the evolution of today's disparate battlefield communications systems into a single battlefield network is perhaps the most significant. These networks will both support electronic warfare as well as provide its targets.

There have been many books and articles describing *non-communications electronic warfare*, which is electronic warfare in the context of electronic sensor systems, particularly radar. This paper addresses the effect of electronic warfare on the battlefield communications systems that support the command-and-control process, that is, battlefield communications networks. This aspect of electronic combat is called *communications electronic warfare*. Moreover, this paper focuses on the components and techniques employed at the *tactical* level of land warfare, that is, at division and below.

The paper begins by briefly describing the operational environment of the digitised battlefield. The concept of network-centric warfare is discussed as an example of a doctrine that is emerging in the United States to harness the power of the information revolution for application to land warfare. This doctrine is then examined in the context of the heavy reliance that networked forms of warfare have on the use of the electromagnetic spectrum. The information revolution not only provides an improved ability to command and control, but also

brings with it a commensurate ability to disrupt the process.

The emergent concepts of *information warfare*, *information operations* and *command-and-control warfare* are then discussed to provide a framework within which to consider the role of electronic warfare on the digitised battlefield. A taxonomy is given for the doctrine of electronic warfare, comprising *electronic support*, *electronic attack* and *electronic protection*. These components are briefly discussed in the context of their targets—the communications systems that underpin the ability of a tactical commander to command and control.

Finally, the paper addresses the future directions of battlefield electronic-warfare systems as tactical communications continue to develop to take advantage of the opportunities offered by the information revolution. A key driver of future tactical electronic warfare will be the evolution of the target tactical communications systems towards a true battlefield network.

Communications electronic warfare has always played an important role in land warfare. With digitisation of the battlefield, the number of targets for electronic warfare will increase greatly, creating the potential for increased vulnerability of tactical communications and information systems. Greater investment is therefore required in offensive and defensive electronic warfare equipment, personnel and training.

COMMUNICATIONS ELECTRONIC WARFARE AND THE DIGITISED BATTLEFIELD

INTRODUCTION

Throughout history, technological, political and social advances have caused profound shifts in military doctrine, organisation, strategy and tactics. In recent history, six revolutions in military affairs have radically altered the conduct and character of war. The first five were the institution of universal military obligation (the French Revolution of 1789); the Industrial Revolution of the mid-19th century; the managerial revolution of the late 19th century; the mechanised revolution occurring between 1919 and 1939; and the scientific revolution that followed shortly afterwards, culminating in the production of the atomic bomb. Then, in the early 1970s, the introduction of precision-strike weapons and computers produced the latest revolution—an information revolution centred on the concept that the dominant factor in war is the ability to collect, analyse, disseminate and act upon battlefield information.[1]

These advances in technology have produced an environment on the modern battlefield that is characterised by continuous 24-hour action; increased volume, lethality, range and precision of fire; smaller, more-effective units due to better integration of technology; a disjunction between greater dispersion of more mobile, faster units and an increased tendency for combat in built-up areas with congestion of forces in short ranges; and a further dichotomy between greater invisibility (due to dispersion and speed) and increased risk of detection (due to larger numbers of more-capable battlefield sensors).

[1] D. Reimer, 'Foreword', in *War in the Information Age: New Challenges for US Security*, R. Pfaltzgraff and R. Shultz (eds), Brassey's, Washington, DC, 1997.

It has been several hundred years since a commander has had the ability to stand on a convenient hilltop and survey the disposition of friendly and adversary forces. Now, in the Information Age, the modern commander, with senses enhanced by electronic sensors and modern communications systems, is promised the ability to stand on an electronic hilltop and once again ‘see’ whatever portion of the battlefield is desired at whatever detail is appropriate.

For warfare, the major lesson from the commercial world is that, in the Information Age, conflict will largely be about knowledge, and mastery of the network and networked organisations will provide major advantage in conflict. However, these concepts can be an anathema to military commanders, who tend to see command and information (and even communications in many armies) following the same hierarchical lines. In a non-hierarchical network model, command and information flow must necessarily diverge. Sensors, commanders and weapon systems are connected via a networked grid that ensures that situational awareness data can be shared by all elements, regardless of whether they belong to the same unit. Command lines need no longer be shared with information flow. Information is shared across the network, while command and control is directed in accordance with the order of battle. Therefore the adoption of these new technologies will not only significantly affect the way armies are commanded and controlled, but will change the way they are organised and trained. Not all armies, however, will be able (or will choose) to take advantage of this revolution, and today’s information-age army must be prepared to deal with a broad spectrum of threats from agrarian and industrial-age adversaries as well as to threats from information-age foes.[2]

There are many books and articles that address the issue of warfare in the Information Age.[3] This paper focuses on the framework articulated by the US Joint Vision 2020 (JV2020),[4]

[2] A. Toffler and H. Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*, Little, Brown and Company, Boston, MA, 1993.

[3] Further suggested reading on warfare in the Information Age: J. Adams, *The Next World War*, Random House, London, 1998; J. Alexander, *Future War: Non-lethal Weapons in Twenty-first Century Warfare*, St Martin’s Press, New York, 1999; C. Allard, *Command, Control, and The Common Defense*, Yale University Press, New Haven, CT, 1990; J. Arquilla and D. Ronfeldt (eds), *In Athena’s Camp: Preparing for Conflict in the Information Age*, RAND, Santa Monica, CA, 1997; A. Campen and D. Dearth, *CyberWar 2.0: Myths and Reality*, AFCEA International Press, Fairfax, VA, 1998; C. Bellamy, *The Future of Land Warfare*, St Martin’s Press, New York, 1987; M. De Landa, *War in the Age of Intelligent Machines*, Zone Books, New York, 1991; A. Gordon, *The Rules of the Game: Jutland and British Naval Command*, Naval Institute Press, Annapolis, MD, 1996; The International Institute for Strategic Studies (IIS), *Strategic Survey 1995–1996*, Oxford University Press, London, 1996, p. 30; R. Pfaltzgraff and R. Shultz (eds), *War in the Information Age: New Challenges for US Security*, Brassey’s, Washington, DC, 1997; D. Rooney, V. Kallmeier and G. Stevens, *Mission Command and Battlefield Digitisation: Human Sciences Considerations*, DERA Report, DERA/CHS/HS3/CR980097/1.0, March 1998; R. Scales, *Future Warfare*, US Army War College, Carlisle, PA, 1999; A. Toffler and H. Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*, Little, Brown and Company, Boston, MA, 1993; and H. Van Trees, ‘C3 Systems Research: A Decade of Progress’, in *Science of Command and Control: Coping with Complexity*, S. E. Johnson and A. H. Levis (eds), AFCEA International Press, Fairfax, VA, 1989.

[4] Director of Strategic Plans and Policy, J5 Strategic Division, *Joint Vision 2020*, US Government Printing Office, Washington, DC, June 2000.

which provides a useful background for our consideration of electronic warfare on the digitised battlefield. JV2020 builds upon the conceptual template established in Joint Vision 2010, and has the goal of transforming US forces to create a force that is dominant across the full spectrum of military operations. Modern armed-forces must be able to defeat adversaries across a wide range of operations, such as conventional warfighting, peace enforcement, peacekeeping, counter-terrorism, humanitarian assistance, and civil support. In this paper, the term *battlefield* is used to refer generically to land operations across the spectrum.

A key component of full-spectrum dominance is *information superiority*—the capability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Information superiority can therefore be defined as 'that degree of dominance in the information domain which permits the conduct of operations without effective opposition'.[5] Superior information is to be converted to superior knowledge, which—when combined with organisational and doctrinal adaptation, relevant training and experience, and the proper command-and-control mechanisms and tools—is to achieve *decision superiority*.

JV2020 proposes that current capabilities for manoeuvre, strike, logistics and protection will become *dominant manoeuvre*, *precision engagement*, *focused logistics* and *full-dimensional protection*. The following descriptions of these terms are taken from the definitions provided in JV2020.[6]

[5] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, Office of the Joint Chiefs of Staff, Washington, DC, 1994 (as amended to September 2000).

[6] In this paper, US doctrine is used to provide a framework for two reasons: US doctrine is more comprehensive and integrated than

Australian doctrine; and it is unclassified and in the public domain, which expands the audience for this paper. While Australian doctrine is classified and generally less coherent, it is typically similar to US doctrine in its scope and intention. The issues raised in this paper are therefore not invalidated by the use of US doctrine.

Dominant manoeuvre is defined as the ability of joint forces to gain positional advantage with decisive speed and overwhelming operational tempo in the achievement of assigned military tasks. Widely dispersed joint air, land, sea, amphibious, special operations and space forces, capable of scaling and massing force or forces and the effects of fire as required for either combat or noncombat operations, will secure advantage across the range of military operations through the application of information, deception, engagement, mobility and counter-mobility capabilities.

Precision engagement is the ability of joint forces to locate, observe, discern and track objectives or targets; select, organise, and use the correct systems; generate desired effects; assess results; and re-engage with decisive speed and overwhelming operational tempo as required, throughout the full range of military operations.

Focused logistics is the ability to provide the joint force with the right personnel, equipment and supplies in the right place, at the right time and in the right quantity, across the full range of military operations. These focused logistics will be made possible through real-time, networked information systems providing total asset visibility as part of a common relevant operational picture, effectively linking the operator and logistician across service and support agencies. Through transformational innovations to organisations and processes, focused logistics will provide the joint warfighter with support for all functions.

Full-dimensional protection is the ability of the joint force to protect its personnel and other assets required to execute assigned tasks decisively. Full-dimensional protection is achieved through the tailored selection and application of multi-layered active and passive measures within the domains of air, land, sea and space and information across the range of military operations with an acceptable level of risk. The dimensions of protection range from forward-deployed forces, through supporting logistics, to home commands and supporting space surveillance and communications systems. Just one dimension of protection, for example, is the protection of forces at garrisons and military bases. Asymmetric terrorist attacks pose a threat that must be countered by layers of defence including active human intelligence (HUMINT) on terrorist activities, passive monitoring of traffic around the base, alert conditions and procedures for tightening perimeter security, covert intrusion-detection sensors, facility decoys, and levels of physical security access.

JV2020 also places significant emphasis on *information operations*[7] as an essential element of achieving each of the elements of full-spectrum dominance. This topic is revisited shortly since electronic warfare is an important component of information operations.

Recognition is also given in JV2020 to the fact that adoption of information technologies is not sufficient to make maximum use of the opportunities made available by the information revolution. The vision of JV2020 is to be realised through a transformation of the necessary doctrine, organisation, training, materiel, leadership and education, personnel and facilities.

Perhaps the most useful elaboration of the impact of information technology is in the emergent concept of *network-centric warfare* (NCW). In current platform-centric warfare, the sensing and engaging capability normally resides in the weapon system (‘shooter’), and there is only a limited capability for the weapon

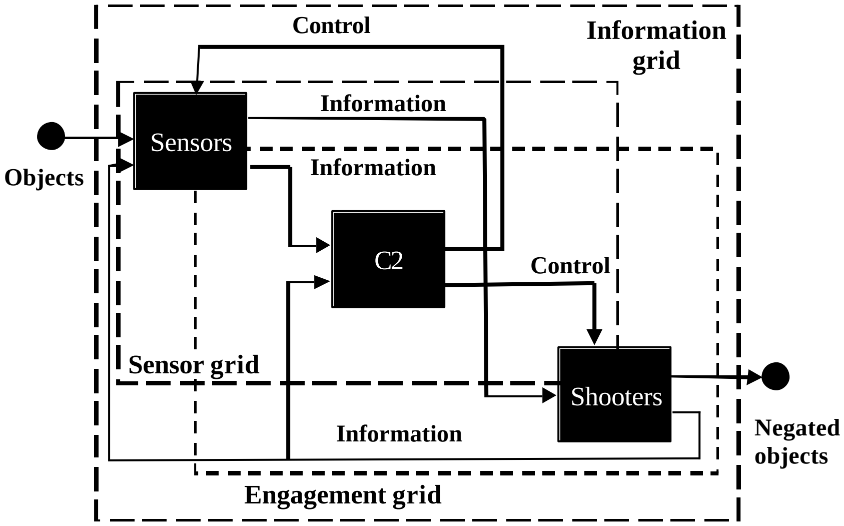
[7] *Information operations* are defined later in the paper as those actions taken to affect an adversary’s information and information systems while defending one’s own information and information systems.

to engage targets because it can only use the situational awareness generated by its own sensor. If a weapon is able to engage a target located by a remote sensor, the passage of weapon data is normally via stovepipe communications systems (that is, they connect the single weapon directly to the single sensor). By contrast, in network-centric warfare, sensors and shooters are connected by a ubiquitous network through which weapons can engage targets based on a situational awareness that is shared with other platforms. Combat power can therefore be applied with fewer weapons systems than are currently required. Note that, just because weapons and sensors are interconnected, it does not mean that targets can be engaged randomly or without authority; control is still essential to ensure that targets are engaged in accordance with the operational plan.

While there may continue to be a role for direct links from sensor to shooter, the ultimate aim of NCW is that the employment of future precision-weapons is designed around information. No single sensor has the ability to direct the application of these precision weapons—data must be integrated from a number of sensors and databases. On the modern battlefield, the network is a considerable force-multiplier. Commanders' tactical plans will not be constrained by communications, nor will they be confined to information centres (command posts). The information network must be ubiquitous across the battlespace and must be fluid, flexible, robust, redundant and real-time; have integrity and security; have access and capacity; and be joint- and coalition-capable.

Figure 1 illustrates the three interlocking grids of NCW (the *information grid*, the *sensor grid*, and the *engagement grid*), and the three major types of participants (*sensors, command elements* and *shooters*). The information grid provides the infrastructure through which information is received, processed, transported, stored and protected. The sensor grid contains all sensors, whether they are specialised devices mounted on weapon systems, carried by individual soldiers, or embedded into equipment. The engagement grid consists of all available weapon systems that are tasked to create the necessary battlefield effect. Proponents of NCW envisage that these three grids will exist in space, in the air, on land, and on and under the sea.

Figure 1: The grid arrangement of network-centric warfare[8]



NCW is not currently a formal part of US doctrine. The concept does, however, have considerable merit philosophically, and it is very likely that future land warfare will embrace most, if not all, of the above concepts. The employment of a tactical network based on wireless, non-nodal communications has the advantage that armies can disperse as required and then concentrate effects rapidly at an appropriate time and place. Less reliance is required on large information-processing centres, which can be distributed to increase physical survivability without sacrificing processing power.

[8] A. Cebrowski and J. Garstka, 'Network-Centric Warfare: Its Origins and Future', *Naval Institute Proceedings*, 1997.

This section has provided a very brief introduction to the operational environment of the future. While this section has not considered in detail many of the issues associated with the significant impact that the information revolution will have on battlefield weapon systems, the most significant effect for this discussion of electronic warfare will be on the ability of a commander to acquire information, prepare and disseminate plans, and then control their execution. This is the business of *command and control*, which has become increasingly dependent on reliable communications and effective information systems.

INFORMATION WARFARE

While the Information Age has produced a revolution in military operations that provides great promise of decisive advantage on the modern battlefield to the commander who can gather and exploit information most effectively, there is a significant dark side to the information revolution. As communications and information systems become vital to military and civilian society, they can become critical targets in war and can also serve as a major means for conducting offensive operations. Consequently, military adoption of information technology creates a new vulnerability: the same information technology that provides the fuel for the networks that support modern commanders also provides one of the major means for their destruction. An increased reliance on communications and information systems increases this vulnerability. So, while automated command-systems increase a commander’s situational awareness, they can also be turned against friendly forces and used to contribute to their uncertainty.

It is evident from the preceding discussion that movement through the command and control (C2) cycle[9] on the modern battlefield depends heavily on the use of the electromagnetic spectrum, whether for surveillance and target acquisition, passage of information, processing of information or destruction of adversary forces. This reliance is a vulnerability that must be exploited in attacking adversary command-systems while being protected in own-force systems. Operations to counter the C2 cycle are generically termed *information warfare* (IW), which is a term that recognises a range of actions taken during conflict to achieve information superiority over an adversary, and may be defined as:

> Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending ones own information, information-based processes, information systems, and computer-based networks. [10]

The terminology and techniques of IW are still relatively ill-defined and without universal agreement, although there have been a number of comprehensive descriptions of the topic.[11]

[9] For more detail on the C2 Cycle, see M. Ryan, *Battlefield Command Systems*, Brassey's, London, 2000.

[10] US Army Field Manual FM100-6, *Information Operations*, HQ Department of the Army, Washington, DC, August 1996.

[11] Further reading can be found in: US Army Field Manual FM100-6, *Information Operations*, HQ Department of the Army, Washington, DC, August 1996; Joint Publication 3-13, *Joint Doctrine for Information Operations*, Office of the Joint Chiefs of Staff, Washington, DC, 1998; Joint Publication 3-13.1, *Joint Doctrine for Command and Control Warfare (C2W)*, Office of the Joint Chiefs of Staff, Washington, DC, 1996; M. Libicki, *What is Information Warfare?*, Institute for National Strategic Studies, National Defense University, Washington, DC, 1996; A. Brosnan, 'Information Operations—What is IO?', *Journal of Battlefield Technology*, vol. 4, no. 2, July 2001, pp. 32–36; and J. Rothrock, 'Information Warfare: Time for Some Constructive Skepticism?', in J. Arquilla and

Again, this paper is not concerned with the detail of IW and related concepts, but is focused on those aspects that impact on the field of electronic warfare.

The objective of IW is to attain a significant information advantage that enables the rapid domination and control of an adversary. The US Army recognises that the current definition of IW is more narrowly focused on the impact of information during actual conflict and has chosen a somewhat broader approach to the impact of information on ground operations and has adopted the term *information operations* (IO). IO integrate all aspects of information to support and enhance the elements of fighting power, with the goal of dominating the battlespace at the right time, at the right place and with the right weapons or resources. IO are defined by FM100-6 as:

> Continuous military operations within the military information environment that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations; IO include interacting with the global information environment and exploiting or denying an adversary's information and decision capabilities. [12]

JV2020 adds that IO also includes actions taken in a noncombat or ambiguous situation to protect one's own information and information systems as well as those taken to influence target information and information systems.

The warfighting application of IW in military operations is called *command-and-control warfare (C2W).* The aim of C2W is *to influence, deny information to, degrade, or destroy adversary C2 capabilities while protecting C2 capabilities*

D. Ronfeldt (eds), *In Athena's Camp: Preparing for Conflict in the Information Age*, RAND, Santa Monica, CA, 1997.

[12] US Army Field Manual FM100-6, *Information Operations*, HQ Department of the Army, Washington, DC, August 1996.

against such actions. C2W therefore comprises two major branches: C2-attack and C2-protect. C2W operations integrate and synchronise the capabilities of *psychological operations (PSYOPS), deception*, *operations security (OPSEC)* and *electronic warfare (EW).*[13]

It is the EW component, in particular communications EW, that is of interest in this paper. Although IW has the potential to have an impact much wider than the tactical environment, the following discussion focuses on the warfighting application of communications EW on the digitised battlefield.

[13] Ibid.

ELECTRONIC WARFARE

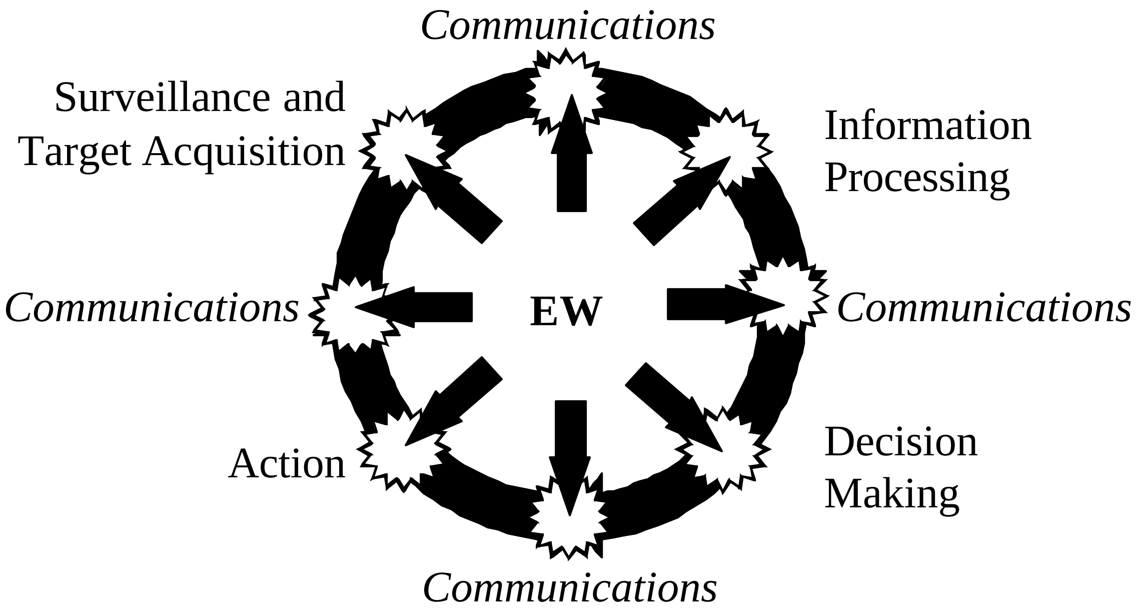
Domination of the electromagnetic spectrum is a crucial component of most modern military operations. There are few battlefield elements that do not rely on communications and information systems. As discussed earlier, the C2 cycle depends very heavily on the electromagnetic spectrum to maximise the effectiveness of surveillance and target acquisition, communications and information systems. If these systems are destroyed, degraded or deceived, the commander and staff are unable to prosecute war adequately. For example, without communications on the modern battlefield the commander is deaf, dumb and blind. Therefore, the capability to conduct electronic combat and dominate the electromagnetic spectrum is now a recognised component of any modern force structure.

Electronic Warfare (EW) can be defined as the use of the electromagnetic spectrum to degrade or destroy an adversary's combat capability (including degrading or preventing use of the electromagnetic spectrum as well as degrading the performance of adversary equipment, personnel and facilities); or to protect friendly combat capability (including protecting friendly use of the electromagnetic spectrum as well as friendly equipment, personnel and facilities that may be vulnerable to attack via the electromagnetic spectrum).

The targeting of personnel is beyond the scope of this paper, which is focused on EW conducted against adversary communications and information systems. The paper therefore only considers EW that is targeted against adversary communications, EW and electronics. EW is also only considered as it is applied in the tactical context of the battlefield.

Figure 2 illustrates how EW pervades all aspects of the modern battlefield and has the potential to have an impact on all elements of the C2 cycle. In summary, EW resources are used to monitor adversary activities in the electromagnetic spectrum, indicate adversary strength and dispositions, give warning of adversary intentions, deceive and disrupt sensors and command-and-control processes, and safeguard the friendly use of the electromagnetic spectrum.

Figure 2: The potential impact of EW on the C2 cycle



Although EW is targeted against the technology, the ultimate effect is on a commander’s ability to move through the C2 cycle. The human element of the command system is both the strongest and weakest link, and can be fairly rapidly enshrouded in the fog of war if supporting communications and information systems are disrupted, degraded or deceived.

The activities of EW are applicable across the whole spectrum of military operations and are not confined to warfare, conventional or otherwise. In peacetime, armies attempt to intercept, locate and identify the source of a potential adversary’s electronic emissions. Analysis may then reveal details of capabilities as well as vulnerabilities that can be used to gain an advantage in times of conflict.

EW is an area of considerable innovation. Inevitably, and often very rapidly, advantages gained by technological or procedural change are met with equally effective countermeasures. In order to maintain the edge in any future conflict, information on friendly methods of electronic protection and attack must be safeguarded. Therefore, much of the parametric data associated with EW capabilities is highly classified. However, the underlying techniques and relationships can readily be obtained from open-source publications.

Communications and Non-communications EW

The field of EW is normally divided into two main areas: *communications EW* and *non-communications EW*. Communications EW is almost as old as electronic communications itself and, on the battlefield, is mostly concerned with communications sources that transmit in frequency bands between HF and SHF. Intercept and analysis of transmissions is usually more important than measurement of transmitter characteristics. Non-communications EW has been developed since the early employment of radars in World War II and is primarily concerned with platform protection, and is in most cases specifically oriented towards radar systems in the UHF and higher bands. In non-communications EW, measurement of emitter characteristics is central as they are used to detect the presence of, and possibly identify, an equipment and/or its performance.

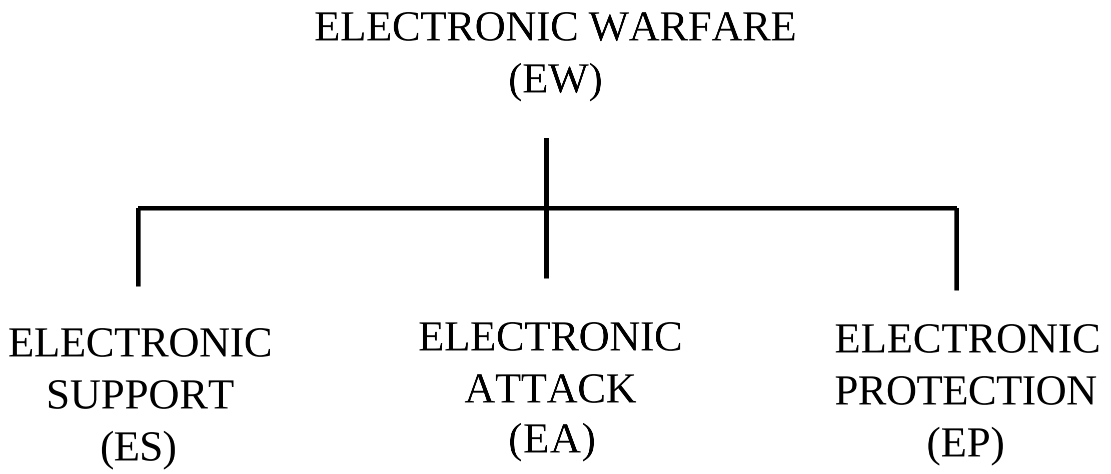
As an aside, EW is also associated with *signals intelligence* (SIGINT), which contains two main sub-components: *communications intelligence* (COMINT) and *electronic intelligence* (ELINT). To a large extent, these components mirror the functional areas of communications and non-communications EW, but take place in the strategic rather than the tactical environment.

EW in the tactical land environment is mostly concerned with communications EW, which is therefore the focus of this paper.[14]

EW Subdivisions

As shown in Figure 3, there are three fundamental subdivisions within EW that are applicable to both communications and non-communications EW, albeit with the different degrees of emphasis noted earlier.

Figure 3: Major subdivisions of EW



Electronic Protection

[14] Readers with interest in non-communications EW are referred to F. Neri, *Introduction to Electronic Defense Systems*, Artech House, Boston, MA, 1991; and D. Schleher, *Electronic Warfare in the Information Age*, Artech House, Boston, MA, 1999.

Formerly known as *electronic protection measures* (EPM) or *electronic counter-countermeasures* (ECCM), *electronic protection* (EP) comprises those actions taken to protect personnel, facilities and equipment from any effects of friendly or adversary employment of EW that degrade, neutralise or destroy friendly combat capability. While EP is traditionally most concerned with protecting communications equipment, it is applicable to the protection of all systems.[15]

EP is usually divided into *passive EP* and *active EP*. Passive EP comprises measures that are not detectable by an adversary, and is concerned with tactics and procedures for providing electronic protection, including terrain shielding. Active EP, whose measures are detectable by an adversary, is concerned with providing protection by the use of special equipment or special operating modes of equipment.

One important way in which EP differs from the other EW subdivisions is that all tactical units should practise it, not just by specialist EW units. Unlike other aspects of EW, EP is directly associated with the tactical communications system. Its techniques relate to the employment of the tactical communications system or to specific features of the equipment that makes up the tactical communications system.

Electronic Support

Formerly known as *electronic support measures* (ESM), e*lectronic support* (ES) involves actions undertaken to search for, intercept, identify and locate sources of intentional and unintentional radiated electromagnetic energy for the purposes of immediate threat recognition and constructing an *electronic order of battle (EOB).* [16] An EOB includes information on the

[15] US doctrine for EP is contained in U.S. Army Field Manual FM 24-33, *Communications Techniques: Electronic Counter-Countermeasures,* HQ Department of the Army, Washington, DC, July 1990.

[16] US doctrine on ES is covered in: U.S. Army Field Manual FM 34-1, *Intelligence and Electronic Warfare Operations,* HQ Department of the Army, Washington, DC, September 1994; U.S. Army Field Manual FM 34-2, *Collection Management and Synchronisation Planning,* HQ Department of the Army, Washington, DC, March 1994; U.S. Army Field

nature and the deployment of all electromagnetic emitting equipment of a military force, including equipment types, frequencies, modes of operation, locations and other relevant data. The main functions of ES are to produce operational intelligence, to provide steerage for electronic attack, and to cue surveillance and target acquisition resources.

The major ES activities are:

- *Search.* Before any other EW processes can be carried out, it is necessary to search for and classify electromagnetic signals of interest.
- *Intercept.* Once identified in the search process, signals of interest are examined for their technical characteristics, such as bandwidth and modulation type, as well as their content, which may be monitored and recorded either by an operator or electronically.
- *Locate.* The physical location of transmitters is identified by the direction finding (DF) process, based on steerage provided by the search process.
- *Analyse.* The information gained from the other ES processes is used to construct an EOB of the adversary, and attempt to infer the adversary commander's intent.

Traditionally, each of these processes has been carried out separately using its own special-purpose equipment. More recent technology makes possible the integration of two or more

Manual FM 34–36, *Special Operations Forces Intelligence and Electronic Warfare*, HQ Department of the Army, Washington, DC, September 1991; U.S. Army Field Manual FM 34-37, *Echelons Above Corps (EAC) Intelligence and Electronic Warfare (IEW) Operations*, HQ Department of the Army, Washington, DC, January 1991; and U.S. Army Field Manual FM 34-40-9, *Direction Finding Operations*, HQ Department of the Army, Washington, DC, August 1991.

processes into a single receiver. The discussion below deals separately with each process so as to highlight its special characteristics and because, even if implemented in one equipment or detachment, there are still four distinct processes involved.

ES may target *adversary communications systems*, *adversary electronic-attack systems* or *adversary electronics*. The electromagnetic emissions of adversary communications systems are the primary traditional targets for ES, obtaining information for use in targeting and intelligence. Electronic-attack systems, like communications systems, emit electromagnetic radiation that can be exploited by ES. The targeting of adversary electronics other than communications systems is possible with specialised forms of ES equipment, although only over very short ranges. As a result of the short range, this type of target is accessible only on rare occasions.

As collectors and processors of tactical information about an adversary, ES activities are closely related to other intelligence functions. In many cases, ES makes up the bulk (as high as 60–80 per cent) of tactical information obtained about an adversary.

Electronic Attack

Formerly known as *electronic countermeasures* (ECM), *electronic attack* (EA), is the division of EW involving the use of electromagnetic energy to attack personnel, facilities or equipment, with the intent of degrading or destroying adversary combat capability. In a similar manner to indirect fire, EA aims to minimise the effect of adversary devices that rely on the EM spectrum.[17]

EA comprises *jamming, electronic deception* and *neutralisation*. Jamming aims to impair the effectiveness of the adversary's electronic equipment or systems by degrading the quality of the signal at a receiver. Electronic deception aims to confuse or mislead the adversary or the adversary's electronic systems. Neutralisation is the use of electromagnetic energy to either disrupt or permanently damage adversary communications or electronic equipment. The power required for neutralisation is typically many times larger than that required for effective jamming of a receiver.[18]

EA can target adversary communications systems through jamming, deception and neutralisation; adversary ES through jamming, deception and neutralisation; and adversary electronics, primarily through neutralisation. EA does not exist in isolation, but rather as part of a force's fire plan, which in turn is part of the operational plan.

ES provides a variety of information required for EA, including frequencies to be used. While EA is being carried out ES also provides monitoring of the effectiveness of the EA.

[17] US doctrine on EA can be found in U.S. Army Field Manual FM 6-20-10, *Tactics, Techniques, and Procedures for the Targeting Process*, HQ Department of the Army, Washington, DC, May 1996; U.S. Army Field Manual FM 34-1, *Intelligence and Electronic Warfare Operations*, HQ Department of the Army, Washington, DC, September 1994; and U.S. Army Field Manual FM 34-45, *Tactics, Techniques, and Procedures for Electronic Attack*, HQ Department of the Army, Washington, DC, June 2000.

[18] M. Frater and M. Ryan, 'Vulnerability of Digitized Platforms to Modern RF Electromagnetic Weapons', *SPIE Aerosense 2000* conference, Orlando, 18–20 April 2001.

Other Categories of EW

EW can be categorised as either *offensive* or *defensive*. ES and EA tend to be offensive, in that they are targeted towards an adversary and involve the process of *searching, intercepting, direction finding* (or *locating* or *position fixing*), *analysing* and engaging adversary electronic systems through *jamming, deception* and *neutralisation*. Mastery of offensive techniques, capabilities and limitations is vital to the effective conduct of electronic combat. EP tends to be more defensive and protects own-force use of the electromagnetic spectrum against an adversary's offensive EW. EP is the concern of all users of electronic equipment and encompasses practices such as *emission security* (EMSEC) and *communications security* (COMSEC).

In turn, EW techniques can be characterised as either *passive* or *active* in nature. Passive activities are not detectable, and can be implemented and practised in peacetime with limited risk of compromise. As active measures are detectable, they should be carefully controlled on the battlefield and only permitted in peacetime under strict conditions. ES tends to be passive, while EA is active. EP contains both active and passive measures.

The diagram in Figure 4 gives an overall view of the interrelated activities associated with EW.

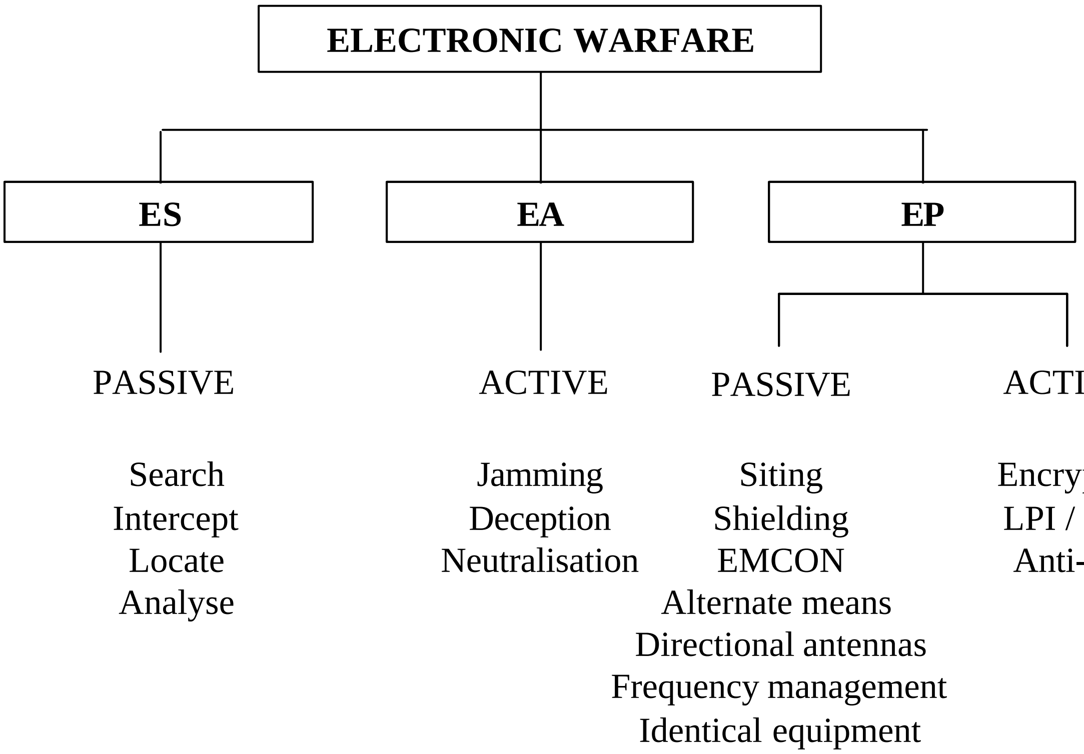


Figure 4: Overall view of EW

CURRENT LAND EW

In this section, an overview of the architecture of the tactical communications system is presented, followed by a discussion of its vulnerability to EW.

The Tactical Communications System

The primary purpose of the tactical communications system is to enable effective command and control by providing effective communications between commanders and their subordinates. Differing requirements for communications dictate that the tactical communications system is not provided as a single homogeneous network, but that a variety of different subsystems are used. These subsystems are illustrated in Figure

5.[19]

At the lower level, combat troops carry a device that must be a network node as well as an access terminal. Limited battery power and the need for small omnidirectional antennas mean that ranges and capacities are constrained. At the higher level, the large capacities necessary for trunk communications will require semi-mobile platforms for the foreseeable future. Large power requirements must be met by the use of generators, and high-gain antennas must be deployed on guyed masts to provide reasonable ranges. This variation in requirements has led to the traditional (and ongoing) subdivision of the tactical communications system into *combat net radio* (CNR) and *trunk* subsystems.

[19] M. Ryan and M. Frater, 'An Architectural Framework for Modern Tactical Communications Systems', *IEEE Military Communications Conference (MILCOM 2000),* Los Angeles, 23–25 Oct. 2000. See also: M. Frater and M. Ryan, *Electronic Warfare for the Digitized Battlefield*, Artech House, Boston, 2001; and M. Ryan and M. Frater, *A Tactical Communications System for Future Land Warfare*, Working Paper no. 109, Land Warfare Studies Centre, Duntroon, ACT, March 2000.

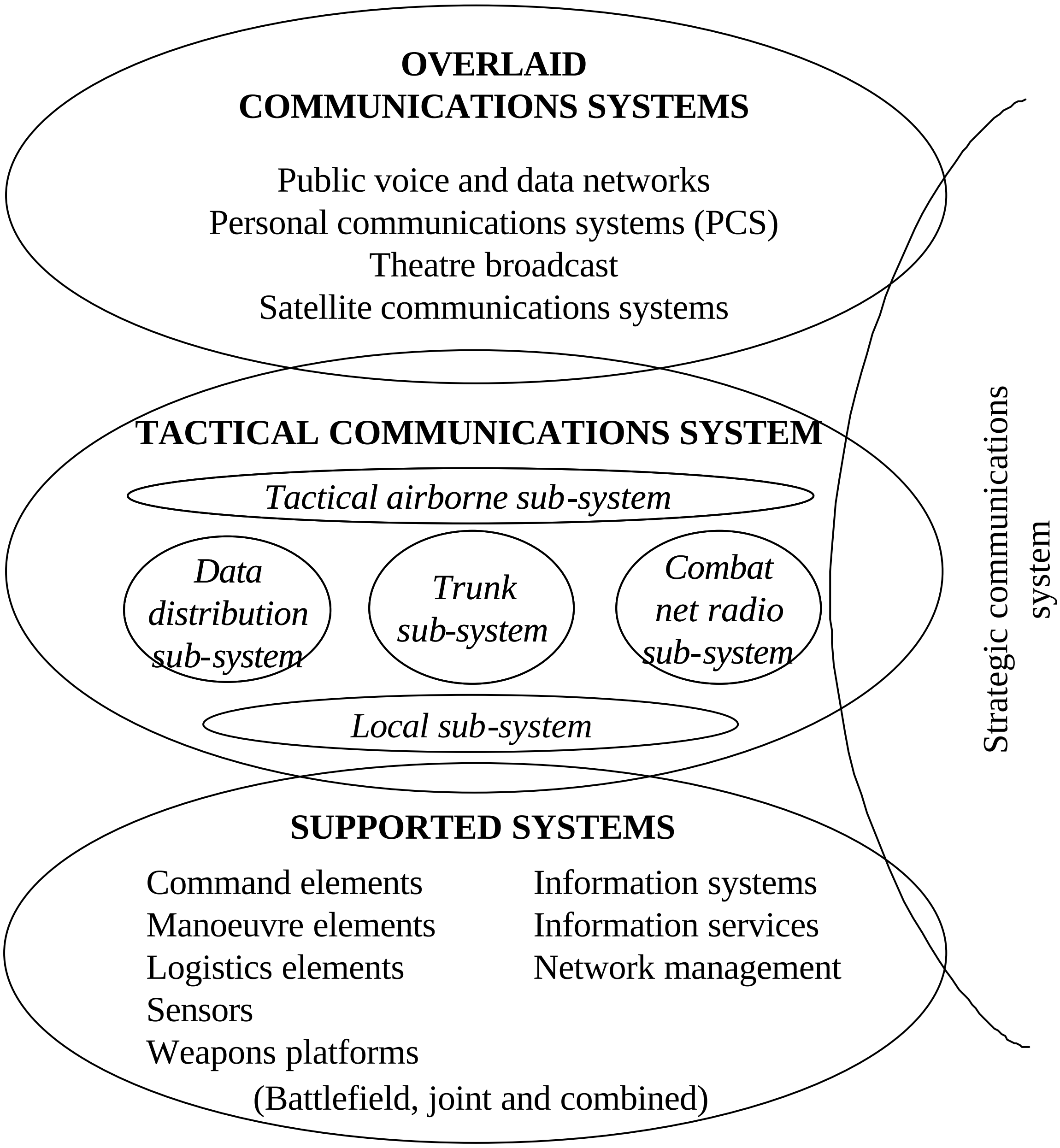

OVERLAID
COMMUNICATIONS SYSTEMS
Public voice and data networks
Personal communications systems (PCS)
Theatre broadcast
Satellite communications systems
TACTICAL COMMUNICATIONS SYSTEM
Tactical airborne sub-system
Data distribution sub-system
Trunk sub-system
Combat net radio sub-system
Local sub-system
SUPPORTED SYSTEMS
Command elements
Manoeuvre elements
Logistics elements
Sensors
Weapons platforms
Information systems
Information services
Network management
(Battlefield, joint and combined)
Strategic communications system

Figure 5: An architectural framework for the tactical communications system

The CNR subsystem provides the highly mobile, low-capacity, short-range communications for the command and control of combat troops. The trunk subsystem provides much higher capacity and range at higher levels, but at the sacrifice of mobility.

The data-handling capacity of the trunk communications system will generally be sufficient to cope with the volumes of data required to be transmitted between command posts. The CNR subsystem's ability is severely limited, however, especially since it is still required to transmit voice information. An additional, purpose-designed, data distribution system is therefore required to provide sufficient capacity to transfer situational awareness data across the lower levels of the battlefield. CNR must, however, still be voice- and data-capable to allow organic communications of both types within subunits, should they be deployed individually or beyond the range of the data distribution subsystem. The additional (albeit limited) data capacity in the CNR subsystem would also provide an overflow capability should the tactical data distribution subsystem be unable to meet all the data needs.

Neither the CNR subsystem nor the trunk communications subsystem is able to cover the large ranges required for dispersed operation. The only solution to providing high-capacity, long-range communications is to elevate the antennas. In the extreme, the provision of a satellite-based or an airborne repeater or switch will greatly increase the ranges between network nodes.
A satellite-based solution is not considered desirable due to its inability to meet the requirements of a minimum organic communications system in most armies (even in those large armies that could afford integral satellite communications, such assets are likely to be provided sparingly and are relatively easily interdicted). An airborne subsystem is therefore required to support long-range operations. In addition, an airborne system will increase the capacity of lower-level tactical communications by removing the range restriction on high frequencies that can provide additional capacity from small omnidirectional antennas.

By its very nature, a minimum organic tactical communications system will only be able to provide a basic level of service and must be able to be augmented where possible by overlaid communications systems such as the public-telephone network, satellite-based systems, and personal-communications systems. These overlaid systems cannot be guaranteed to be available and cannot therefore be included in the minimum organic system. If they are available, however, great advantage is to be gained from their use.

In order to simplify the user interface to these subsystems, a local communications subsystem (most probably containing a level of switching) is required. This local subsystem could take a number of forms, from a vehicle harness to a local-area network around brigade headquarters.

Until recently, manual handling was required to pass data between different subsystems. Most Western armies are taking advantage of recent advances in networking technology to implement interfaces that allow the subsystems making up the tactical communications system to be integrated into a single logical network. In the foreseeable future, however, it is unlikely that advances in technology will make possible a single homogeneous battlefield network.

Target Impact

The various subsystems of the tactical communications system have different vulnerabilities to hostile EW and protection against it. These differences arise from different use (for example, close to an adversary or in rear areas) and from differences in equipment (for example, the use of directional antennas or provision of EP). Table 1 illustrates the relationship between ES and the adversary’s tactical communications system, with the relationship between EA and the adversary’s tactical communications system summarised in Table 2.[20] Broadly speaking, an adversary's CNR subsystem presents the most attractive target for both ES and EA, due to its use of omnidirectional antennas and likely close proximity to ES and EA assets.

Table 1: ES and the tactical communications system

Tactical communications subsystem	**Vulnerabilities**	**Protection**
Trunk	Omnidirectional antennas for mobile subscriber access	Directional antennas, long distance between transmitter and ES facility, line-of-sight frequencies
CNR	Omnidirectional antennas, short distance between transmitter and ES facility, transmission only when messages sent	Low-power, low antennas, terrain screening
Tactical data distribution	Omnidirectional antennas, short distance between transmitter and ES facility	Extensive EP
Airborne	Height, omnidirectional antennas	Only downlinks likely to be detected by tactical EW assets

Table 2: EA and the tactical communications system

Tactical communications subsystem	**Vulnerabilities**	**Protection**
Trunk	High antennas	Directional antennas, long distance between receiver and EA
CNR	Omnidirectional antennas Short distance between receiver and EA asset	Frequency hopping (sometimes), terrain screening
Tactical data distribution	Omnidirectional antennas, short distance between receiver and EA asset	Heavy use of EP, including spread spectrum

[20] M. Frater and M. Ryan, *Electronic Warfare for the Digitized Battlefield*, Artech House, Boston, 2001.

Airborne	Receivers on uplinks are exposed	Receivers on downlinks may be protected from ground-based EA

It can be expected that the vulnerabilities of communications systems to adversary EW will generally remain on the digitised battlefield. The evolution to the battlefield network will, however, create additional EW opportunities, which are the subject of the next section.

FUTURE LAND EW

The key change in the nature of EW on a future digitised battlefield will be its orientation towards the *network*, leading to a proliferation of opportunities for EW. While many of the EW techniques in the future will be the same as the ones currently used, the focus will change from being primarily on the physical layer to focusing on attacks on network security and the security services that protect against these attacks. This same network technology will also greatly increase the capability of friendly EW.

Network Issues

In the foreseeable future, the most significant change likely to occur in the targets for EW is the evolution from a collection of related, but separate, communications systems to a network. This network will facilitate the passage of information between any two points on the battlefield, as well as between any point on the battlefield and terminals associated with other networks, such as joint and even multinational systems.

The motivations for migrating to a network architecture are to maximise the effectiveness of the passage of information between sensors, command elements and weapon systems. Because of the trade-off between mobility, capacity and range in communications links, it is unlikely in the near future that this network can be provided with a single communications technology. In other words, it is unlikely that an evolution of the equipment and protocols associated with the CNR subsystem will be able to meet all the requirements of the tactical communications system; the same applies to the trunk and tactical data distribution subsystems. Furthermore, there is no single technology on the horizon that could replace all of these systems.

While a single homogeneous network is not likely, a single logical network is both desirable and achievable using current and developing technology. The major changes that will occur in this evolution to a network are seamless integration of all subsystems, provision of truly mobile networking and the use of ad-hoc network technology. Seamless integration of all subsystems will enable the passage of information between any two points on the battlefield. Mobile networking technology will allow stations to move at will through the network without being constrained in their location. Ad-hoc network technology will allow the network to be self-forming, without the need for large numbers of dedicated base-stations throughout the area of operations.

Seamless Integration

Given the lack of a suitable technology from which to build an homogeneous tactical communications network, a smooth integration between a number of subsystems is the only means of providing a single logical network. While this integration has not occurred previously in the tactical communications system, it is becoming increasingly common in commercial systems. Examples include the global telephone network, containing interfaces both for fixed telephones (both analog and digital) and mobile telephones. The telephone network has also evolved to carry data as well as voice. Another example is the Internet, whose terminals are connected by a range of interfaces, including high-performance local-area networks providing capacities of 10 Mbit/s or more, cable modems (approximately 0.5 Mbit/s), dial-up modems (up to 56 Kbit/s) and mobile dial-up connections (up to approximately 10 Kbit/s).

Practical implementation of a single logical network requires the use of common protocols and ubiquitous encryption to provide security for the network. Given current commercial technology, it is most likely that the majority of information-processing equipment that will operate across future tactical communications systems will be based on ruggedised computers using the same TCP/IP protocol employed within the Internet.

An outline view of a typical modern network is illustrated in Figure 6. It is based on a hierarchical structure. Each terminal is connected to a local network. Each local network is connected to one or more other networks via a router, denoted R in Figure 6. The purpose of the router is to route data between the various local networks. A group of networks and routers forms an *autonomous system* (AS). In a tactical network, a local network may be the internal network of a headquarters, while an AS may consist of all the networks and routers in a formation.

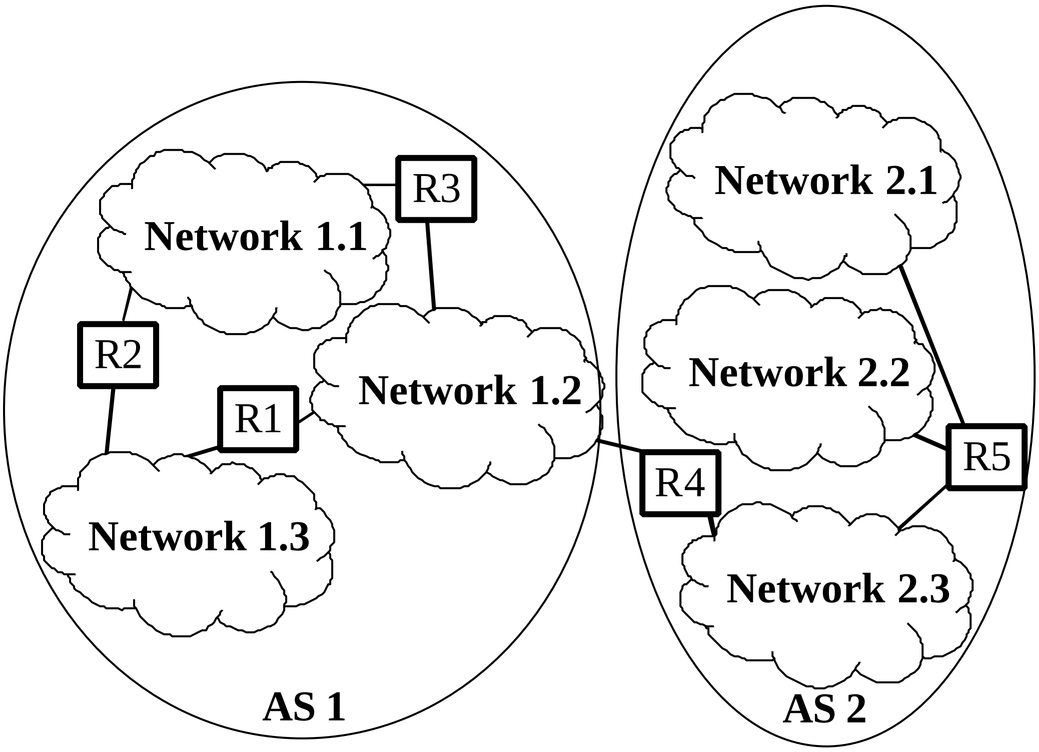


Figure 6: Outline structure of a TCP/IP network

One of the advantages of the hierarchical structure shown in Figure 6 is that it minimises the requirement for network terminals to understand the structure of the network. Terminals only need two pieces of knowledge about the network: the identities of the other terminals attached to their local network (to which they can therefore transmit data directly) and the address of the router to which all other traffic should be sent. Routers require knowledge of the next hop to route data between terminals with their local AS and the identity of the router that handles traffic destined for outside the AS. Only these boundary routers require explicit knowledge of the outside network, and even here the knowledge required relates only to the first hop outside the AS.

Seamless integration will provide the network for network-centric warfare, underwritten by a variety of technologies, including those associated with evolutions of cellular mobile telephone systems (especially third-generation systems), satellite technology, network protocols and miniaturisation of electronics. The move to network-centric warfare will lead to a proliferation in transmitters, each of which is a potential target for ES, and even EA.

This organic, tactical network will be supported by a range of overlaid communications systems, including operational- and strategic-level military systems. The US *global information grid* (GIG) is one such concept, aiming to provide seamless integration throughout a reliable, assured, cost-effective, global network. An important means for providing this level of connectivity will be the incorporation of multiple layers of airborne rebroadcast using aircraft, UAVs and satellites.[21]

Mobile Networks

Users in the tactical communications system should be able to move from one part of the network to another, and receive the same services in their new location. Depending on the equipment used, this roaming may be provided using a wireless connection or require connection to a wired network at the new location. Recently developed mobile networking protocols provide this service using a forwarding agent (Figure 7). Station *B* is in its home network in case (a), and roaming in a different network in case (b). When station *B* moves from network 1.3 to network 1.2, it changes its address to a value lying in network 1.2. One station (labelled *F*) in network 1.3 acts as a forwarding agent, receiving any data addressed to *B* and forwarding it to *B* at its network 1.2 address. So long as a forwarding agent exists

[21] Policy for the GIG is defined in: US Department of Defence Chief Information Officer Guidance and Policy Memorandum 10-8460, *GIG Network Operations*, August 24, 2000; US Department of Defence Chief Information Officer Guidance and Policy Memorandum 7-8170, *GIG Information Management*, August 24, 2000; and US Department of Defence Chief Information Officer Guidance and Policy Memorandum 4-8460, *GIG Networks*, August 24, 2000.

for each local network, stations can roam at will through the network. Mobility is provided at the cost of some double-handling by a forwarding agent of data destined for a roaming station.

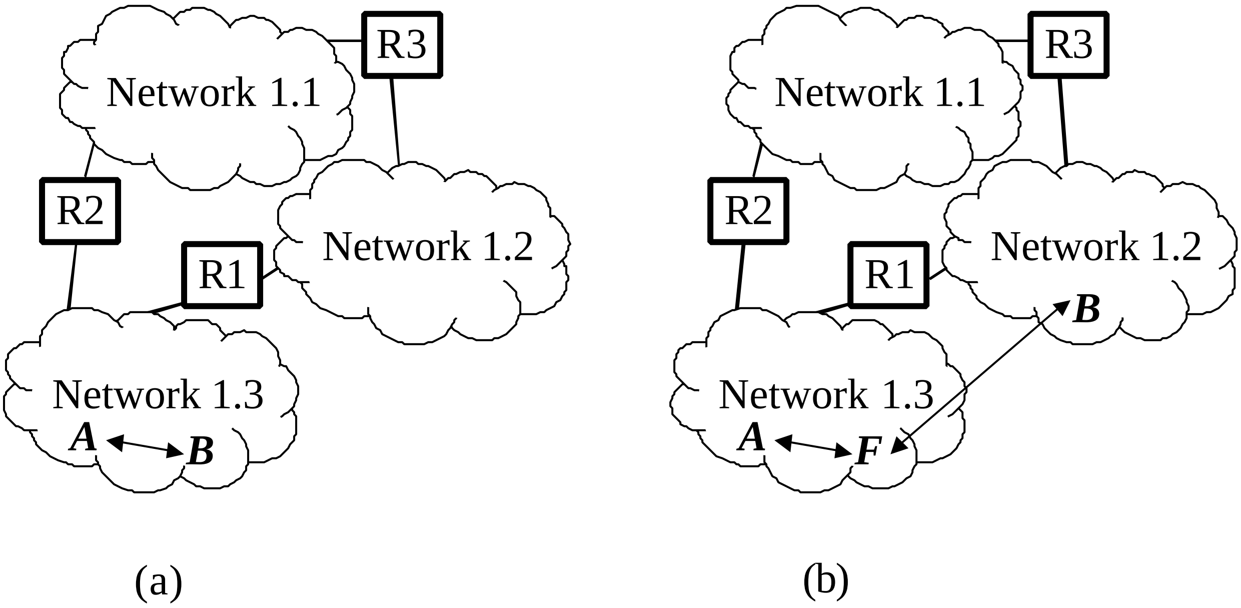


Figure 7: Mobile networking

Implementation of mobility, particularly wireless mobility, has implications for the management of encryption keys. It will be necessary to provide either a common key for use across the whole network or to provide mobile users keys for use in different parts of the network, imposing difficulty in guaranteeing the security of such widely distributed keys. The use of wired network connections may reduce difficulties with security by allowing individual stations to connect to the network without the use of encryption systems.

In areas exposed to an adversary EA threat, it is likely that the capacity of wide-area, fully mobile, tactical wireless communications systems, such as CNR or developments on it, will remain limited. There is nonetheless the potential for local-area communications systems, based on technologies such as

Bluetooth,[22] to offer high-capacity, mobile communications. These systems may offer ranges of no more than tens of metres, operate in parts of the electromagnetic spectrum that are not regulated (overcoming the need to take spectrum away from other tactical uses) and offer data rates up to 2 Mbit/s. They are likely to employ a range of EP techniques, including frequency hopping,[23] to reduce their susceptibility to both natural and man-made interference. The combination of short range and the use of EP will enable communications with very low transmit powers, maximising battery life.[24]

Provision of such a local-area communications system will enable networking of the sensors, weapons and communications systems carried by an individual soldier without the weight and inflexibility of connecting cables. It will also enable the networking of small groups of soldiers, providing a 'section LAN' on which data from sensors and weapons can be shared.

Ad-hoc Networks

In current commercial networks the term *mobile communications* means only that the user terminal is mobile. The network itself is very much fixed in place. In a cellular-telephone system, for example, all communications pass from a mobile handset to a base-station, which is in turn connected to

[22] *Specification of the Bluetooth System,* Bluetooth SIG, Version 1.1, February 2001.

[23] The implementation of frequency hopping in Bluetooth is designed to provide protection against natural or unintentional interference. It is not designed to protect against adversary jamming.

[24] D. Farber, 'Predicting the Unpredictable: Technology and Society', in R. Anderson, *The Global Course of the Information Revolution: Technological Trends: Proceedings of an International Conference,* CF-157-NIC, RAND, Santa Monica, CA, 2000.

the fixed network. In tactical communications systems, not only is the user mobile, but the whole network must be able to move with the force it supports, and adapt its structure to changes in the disposition of forces as required.

In an *ad-hoc network*, stations cooperate to build the network and communicate using a common wireless channel. Each station can communicate directly with one or more of the other stations in the network, but it is unlikely that any one station can communicate directly with all of the other stations. Stations on the network are therefore required to act as relays. Data is carried through from source to destination by being passed from one relay to the next. Each station maintains a list of the stations with which it can directly communicate. Connectivity information is built up and distributed by each station.[25]

[25] D. Johnson and D. Maltz, 'Protocols for Adaptive Wireless and Mobile Networking', *IEEE Personal Communications*, vol. 3, no. 1, February 1996.

In the example network shown in Figure 8, *B* can communicate directly with *A* and *G*. *B* may send data to *E* via the path *BGE* or the path *BACE*. Each of these paths would have an associated cost, which may be as simple as the number of hops involved. *B* would choose the least-cost path, transmitting the data over the first hop. The relay station (say *G*) then transmits the data over the next hop, with this process continuing until the data reaches its destination.

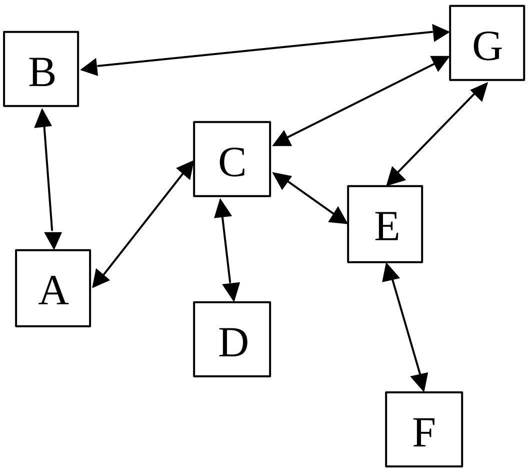


Figure 8: Example of connectivity within an ad-hoc network

In larger ad-hoc networks, stations may form themselves into clusters. A small number of stations may then take on the role of communicating between clusters, possibly using higher transmission power to do so. The forming of clusters helps to maximise frequency reuse and battery life by minimising transmission power. In the example in Figure 9, *E* and *F* have taken on the role of inter-cluster communication.

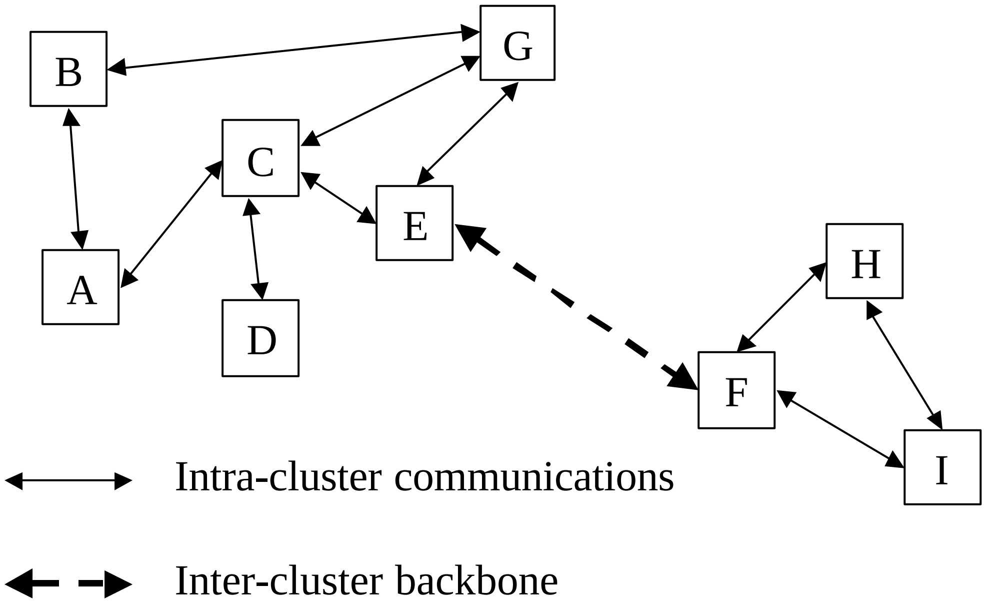


Figure 9: Example of clustering in an ad-hoc network

An ad-hoc network may be integrated with a wider network by one of the stations on the ad-hoc network acting as a gateway.

The major utility of an ad-hoc network in the tactical communications system is in the way in which the network is formed by the terminals, without the requirement for a specific infrastructure to be deployed.

Implications for EW

The advent of the battlefield network will bring with it a number of characteristics already found in commercial networks. One of the most important of these characteristics in the context of EW is the concept of *security services*.[26] These services are a generalisation of the use of encryption to protect information against unauthorised access. The security services are *confidentiality*, *authentication*, *integrity*, *non-repudiation*, *access control* and *availability.*

[26] See, for example, W. Stallings, *Network and Internetwork Security*, 2nd edn, Prentice Hall, Englewood Cliffs, NJ, 1995.

- *Confidentiality.* Information transmitted through the network should be available for reading only by authorised parties. This service is traditionally provided in military systems by encryption. The confidentiality service may conceal the contents of the message; the contents of the message and header information, such as the identities of the sender and receiver; or the very existence of the message, as is provided by the bulk encryption used in the trunk sub-system or by low-probability of intercept techniques such as spread-spectrum communications (in which case confidentiality can be seen as protecting the location of the transmitter).[27]

- *Authentication.* Each party to an exchange of information across the network should be able to guarantee the identity of the other parties involved. This guarantee applies to both senders and recipients of information.

- *Integrity.* Information transmitted though the network should be protected against modification by an adversary.

- *Non-repudiation.* A receipt should be returned to the sender of a message to guarantee that the message has been delivered to the intended recipient, preventing the recipient from later denying receiving the message. Similarly, the recipient of a message should be sent an attachment to the message that can be used to prove that the message was sent by a particular party. One impact of non-repudiation is to protect against

[27] This definition of confidentiality goes further than would usually be the case for a fixed network. It is required, however, to encompass protection against traffic analysis.

counterfeit information being inserted into the network. Non-repudiation cannot exist without authentication.

- *Access control*. Access to systems connected to the network should be limited to authorised parties. Access control includes physical security, and electronic measures such as the use of passwords.

- *Availability*. The capacity of the communications system should be protected, preventing an adversary from degrading system performance.

Exploitation of an adversary's network, whether by using ES or EA, can be seen as an attack against one or more of these security services. Possible attacks include *interception*, *modification*, *fabrication* and *interruption*.

- *Interception*. An unauthorised party may attempt to gain access to data transmitted across the network, or to a portion of this data, such as its external characteristics. Interception is an attack on confidentiality and possibly also on authentication, and encompasses all of the aspects of ES discussed above.[28]

- *Modification*. Following interception, an unauthorised party may modify this data and reinsert it into the network. Modification is an attack against integrity.

- *Fabrication*. An unauthorised party may insert counterfeit information into the network. Protection against fabrication is provided by authentication and non-repudiation.

[28] There is an unfortunate clash of terminology in the use of the term *interception* between ES and that used for network security.

- *Interruption.* Also known as a *denial-of-service* attack, interruption aims to make communications unavailable or unusable. It is an attack on availability.

The taxonomy of these attacks is based on what the attacker is trying to achieve, which means that there is not a simple one-to-one correspondence between the types of attack and the security services used to protect against them.

The division of EW into ES, EA and EP still makes sense in the context of the network. They should, however, be seen in the context of the security services that they are aiming to degrade or provide, rather than purely in terms of their relationship to the electromagnetic spectrum. ES is the means of exploiting an adversary's use of the electromagnetic spectrum using only passive systems, that is, receivers. In the language of security services, ES involves interception, that is, an attack on confidentiality (in the broad sense defined above). EA is the means of exploiting an adversary's use of the electromagnetic spectrum using active means, that is, transmitters. Defined in terms of the desired outcome on the adversary's network, these attacks may take the form of modification, fabrication or interruption. When applied to communications and information systems, EP is the provision of security services to protect friendly capabilities from the effects of friendly EA, and adversary ES and EA.

The traditional subdivision of ES into search, intercept, DF and analysis remains valid. Details of the equipment will change to enable, for example, an intercept receiver to monitor digital network traffic. ES is primarily used as an attack on confidentiality, whether of the contents of a message, the external characteristics of a message or the location from which it is transmitted.

Similarly, even though the aims of EP may be reframed in terms of network security services, the basic techniques for providing low probability of intercept and resistance to jamming will not change.

The application of EA in the context of security services and the associated attacks can be understood in terms of the mission given to an EA asset. This mission will include a task (for example, to jam the adversary command net) and a required outcome (to deny communications). The outcome specified here is interruption. For example, an outcome ‘in order to force the net to operate in plain’ specifies an interruption attack, leaving the adversary vulnerable to a later interception attack. EA can be used to provide modification, fabrication and interruption attacks. Jamming and neutralisation are exclusively associated with interruption; electronic deception may be associated with all three.

The use of wireless-networking protocols creates new vulnerabilities, making interruption possible not only by jamming but deception. Transmitting signals that imitate the transmissions of an adversary’s data communications systems, especially for protocols based on carrier-sense multiple access (CSMA), may trick the adversary’s systems into thinking that a channel is active and prevent them from attempting to transmit. Hence, interruption may sometimes be achieved at much lower powers than those required for jamming. This opens up a new class of electronic deception, aimed principally at the adversary’s network rather than the adversary commander. The detailed coordination of this type of electronic deception is probably more closely involved with jamming rather than the force’s deception plan.

New vulnerabilities will also be created by the use of ubiquitous wireless networking of sensors and weapon systems, increasing the potential impact of electronic minefields. These wireless networks will add an electromagnetic dimension to the signature of the smallest groupings of soldiers wherever they operate.

The digitisation of the battlefield will cause the number of targets available for EW to increase significantly. This increase will place a greater strain on the already-scarce EW assets, especially on ES. The use of encryption throughout the network may reduce the need for interception if the algorithms are strong. If the algorithms are susceptible to cryptanalysis, network-centric warfare will facilitate the coordination of collection and processing or the intercepted traffic.

Universal encryption will increase the difficulty of obtaining internal information from intercepted transmissions. The use of network encryption keys, rather than separate keys for individual links or nets may, however, introduce new vulnerabilities. The larger the volume of data that is transferred using a key, the more vulnerable that key is to cryptanalysis. The interception of preambles used in the affiliation of mobile stations to networks, and their retransmission in other parts of the network, makes possible the use of electronic deception to carry out interruption attacks. The value of encryption keys stored in captured equipment may also be increased, potentially allowing that equipment to be used in a wide range of deception attacks. The extensive use of ad-hoc networks potentially increases this vulnerability. One method for overcoming the vulnerabilities created by the use of preambles is to employ an alternative means of synchronisation for encryption and spread-spectrum communications. The use of a common time reference, which may be derived from GPS, is one possibility.

The extensive use of commercial off-the-shelf (COTS) equipment in modern tactical communications systems is also a source of increased vulnerability. Much of this equipment does not conform to military standards for EP. Furthermore, commercial wireless-network protocols are not designed to operate in a hostile electromagnetic environment, and are vulnerable to a variety of attacks, especially interruption. In general, COTS equipment will be more vulnerable to jamming, deception and neutralisation.

As well as providing new targets, network-centric warfare will transform the planning and coordination of EW itself. It will enable better coordination of EA as a fire and will ensure more effective use of ES assets. In this context, ES assets are simply sensors and EA assets are weapons platforms.

Software Radio

An ideal software radio is a multi-band, multi-mode radio with a dynamic capability defined entirely in software in all layers of the protocol stack, including the physical layer.[29] This ideal radio allows such features as the electromagnetic interface (including modulation technique, data rate and channel bandwidth), voice coding, encryption and network protocols to be reprogrammed, potentially over the air. A simplified architecture for a transmitter that meets this ideal is shown in Figure 10, with a corresponding receiver architecture shown in Figure 11. In the transmitter, only two functions are performed after the digital-to-analog conversion: up-conversion to the transmission frequency and power amplification. Likewise in the receiver, analog processing is used only where it is absolutely required, mostly in the initial RF amplification and in the analog-to-digital conversion. Practical systems may compromise on software programmability, most likely because of the limited power of available signal-processing technology.

[29] J. Mitola, ‘Technical Challenges in the Globalisation of Software Radio’, *IEEE Communications Magazine*, vol. 37, no. 2, February 1999, pp. 86–98.

Figure 10: Simplified software radio transmitter architecture

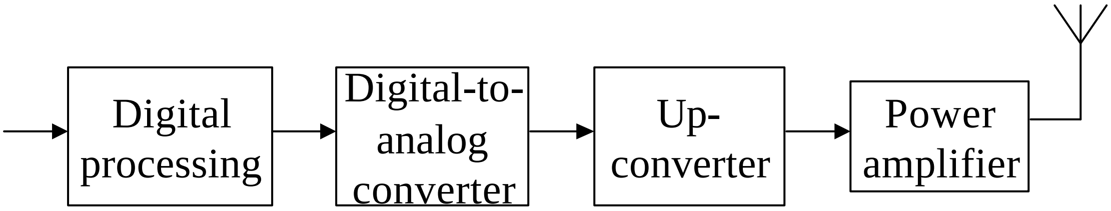
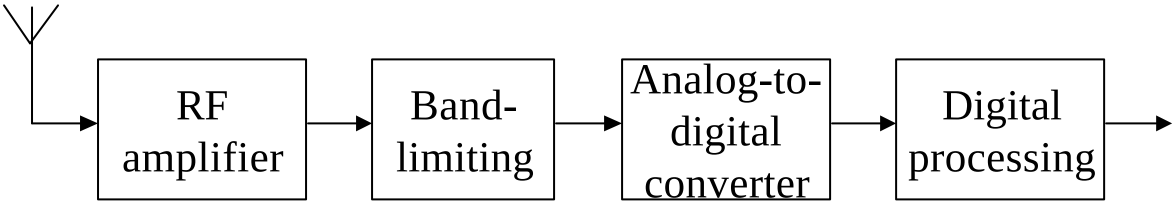


Figure 11: Simplified software radio receiver architecture



The use of software radio technology will see some convergence of equipment in the various subsystems of the tactical communications system, especially between the trunk and CNR subsystems. In comparison with the CNR subsystem, however, the trunk subsystem will continue to be characterised by longer ranges, favouring the use of elevated, directional antennas and higher transmit powers, preserving the traditional trade-off between capacity, range and mobility. Software radio technology will be a key enabler of the battlefield communications network, allowing previously separate communications systems to cooperate in forming the network.

Key Software Radio Technologies

There are a number of key technologies requiring development for software radio, including antennas, receiver RF processing and down-conversion, analog-to-digital conversion, signal-processing technology and general-purpose processors.

Antennas. One of the major aims for software radio is the construction of multi-band radios. For the tactical communications system, efficient operation across the HF, VHF and UHF bands is desirable, using a single antenna. It is also desirable that a single re-configurable antenna be used for the various applications, allowing control (exercised by an operator or automatic controller) over such parameters as directivity and null-steering. Such antennas are likely to be based on arrays, possibly containing thousands of elements.

Receiver RF processing and down-conversion. Because little or none of the selectivity of the software radio is contained in its RF stage, the requirement for low distortion is greater than that for conventional radios, especially for tactical systems that must operate in a hostile electromagnetic environment. Any distortion introduced in this stage will cause leakage of power from one channel to another, possibly allow a narrow-band jammer to jam signals in many channels and leave a receiver vulnerable to inadvertent jamming from closely located friendly transmitters.

Analog-to-digital conversion. The use of software radio systems in cellular telephone systems has led to a significant improvement in the speed and precision of analog-to-digital converters. Very low distortion and high precision are required in analog-to-digital converters in order to avoid leaving software radios vulnerable to off-channel jamming. A receiver's analog front-end and its analog-to-digital converter are possibly the most critical parts of the system for operation in a hostile electromagnetic environment.

Signal-processing technology. Recent years have seen significant improvements in the speed and precision of signal-processing hardware, based on field-programmable gate arrays or application-specific integrated circuits, and software, based on programmable digital signal processors. Further gains are required in transmitter and receiver architectures and in the power of both hardware and software to make a truly programmable radio possible, into which almost completely arbitrary new waveforms can be introduced via software updates.

General-purpose processors. To reach their full potential, software radios must implement not only physical-layer protocols, such as modulation, but complete protocol stacks. Higher layers are best implemented on a high-performance, general-purpose processor.

The most ambitious tactical software-radio project is the US

Joint Tactical Radio System (JTRS),[30] which aims to develop a family of software radios based on a common architecture, providing a range of services including voice, video and data, and operating over a frequency range from 2 MHz to 2 GHz. European projects include the *Multi-role Multi-band Radio—Advanced Demonstrator Model* funded by the German and French governments, and the *Programmable Digital Radio* funded by the UK Ministry of Defence. Commercial applications are also under investigation for third-generation cellular telephone systems.

Implications for EW

Extensive deployment of software radio will create both opportunities and difficulties for EW. The use of COTS software-radio technology is likely to increase vulnerability to jamming, with cost pressures limiting the quality of the analog front-ends of receivers and their analog-to-digital converters. The ability to change a transmitter's or receiver's EP, modulation scheme, data rate and channel bandwidth in software will demand corresponding flexibility in ES and EA systems.

The flexibility offered by software radio will also reduce the cost of some EP techniques, such as frequency hopping and other spread-spectrum techniques, increasing their use in the tactical communications system. Responsive jammers capable of following a hopper will also be much easier to build.

ES receivers based on software radio will feature high levels of flexibility. They offer the potential for automated search, intercept and DF of short-term and fast-changing signals, such

[30] Joint Tactical Radio System (JTRS) Joint Program Office, *Software Communications Architecture Specification MSRC-5000SCA,* Version 2.0, December 2000.

as those generated using EP techniques, including frequency-hopping and burst transmission.

CONCLUSION

Although the promise of command and control in the Information Age may stop short of completely dissipating the fog of war, it has significant potential to improve a commander's awareness, to achieve spans of control that can be measured in global terms, and to mass collective combat power without massing forces.[31] The enduring lesson from recent conflicts since the Gulf War is that what can be seen can be hit, and what can be hit can be killed. The function of 'seeing' is now much more sophisticated and entails electronic, optical and acoustic sensors that can have up to global coverage. These sensors can be linked in real time to computer-controlled weapon systems with unparalleled accuracy and lethality. However, such qualities are not enough. The decisive advantage on the modern battlefield will go to the commander who can gather and exploit information most effectively. While this is greatly assisted by the technologies associated with the information revolution, the human element is arguably the most significant.

As a result of the information revolution, future commanders can have unparalleled information available to them; they will be able to 'see' the full extent of the battlefield even if it spans the globe. Commanders will not have it all their own way, however. Future command-and-control systems will be heavily reliant on communications and information systems that cannot operate if access to the electromagnetic spectrum is denied. So, while the information revolution promises to deliver an enormous

[31] C. Allard, *Command, Control, and the Common Defense*, Yale University Press, New Haven, CT, 1990, p. 263.

improvement in capability to commanders, it also creates the potential for new vulnerabilities. These new vulnerabilities offer new opportunities for the application of electronic warfare on the digitised battlefield. Greater investment is therefore required in offensive and defensive EW equipment, personnel and training. As armies expend large sums of money seeking to attain the advantages of digitisation, consideration must be given to the flipside of the information revolution—the increased role of electronic warfare on the modern digitised battlefield. Arguably, for every dollar that is spent on battlefield communications and information systems, one dollar should be spent on the EW capabilities required to protect these systems and to target an adversary’s systems.