THE IMPACT OF NEW TECHNOLOGIES IN THE MILITARY ARENA: INFORMATION WARFARE

PAULO FERNANDO VIEGAS NUNES

INTRODUCTION

> *We live in an information-dominated era. Technological discoveries... are changing the nature of war and the way we prepare for it.*
>
> – US Secretary of Defence William Perry

The current status of decision support systems is marked by the multiplicity and transitoriness of the information vehicles that feed them. The realm of its application is broad and decisive on the modern battlefield, which is characterised by the extensive use of technologically advanced equipment.

That fact, though not exclusive, characterises the action of the armed forces in emphasising its importance due to the critical nature of the information that flows in the command and control systems. Technology plays a key role within this context not only as a guarantor of the existing information systems' effectiveness but also as the best way to render those systems inoperable, repackaging an old but ever present concept that is now called "information warfare."

The significant technological advances witnessed in the telecommunications

Captain **Paulo Fernando Viegas Nunes**, Portuguese Army, serves at the Military Academy in Lisbon. He has a B.A. and an M.A. in electronic and computer engineering from the University of Lisbon, specialising in telecommunications. His essay on "Prototype of an ISDN Phone" won the 1994 "Innovation by Young Engineers" prize awarded by the Portuguese "Corporation of Engineers".

(The above is a rough translation of the original Portuguese-language article presented at the International Congress of Military Press held on September 13-16, 1999 in Lisbon, Portugal, and later published in Revista Militar, the sponsor of the aforementioned event. It was subsequently reproduced in the 2nd Qtr 00 issue of the Portuguese-language *Aerospace Power Journal*. We are grateful to the Editor, *Air & Space Power Journal – Chronicles Journal Online* for permission to reprint this article.)

and information systems areas have compelled us to define and restructure new and old concepts linked to the transport and use of information, making terms such as digitalisation of the battlefield, communication integration and globalisation, war games, command, control, communications and intelligence (C3I) and communications, information and intelligence (CI2), military Internet, *hackers*, etc., the order of the day.

Due to its growing importance, this issue is currently the subject of a long debate in both military and civilian realms at a moment in history when one witnesses the progressive internationalisation of conflicts and of the world economy, where globalisation is the operative term.

CONCEPTUAL FRAMEWORK OF INFORMATION WARFARE

The new era, in which science and industry play a determinant role in the destructive power of the military, is characterised by the existence of three major types of weapons that succeeded one another in importance within the age-old offensive versus defensive conflict: obstruction weapons (ditches, ramps, bastions, armour, and fortifications of all types), weapons of destruction (spears, arches, firearms, artillery pieces, missiles, etc.), and, finally, communication weapons (signal, information and transport vectors, optical telegraphy, radiotelephony, radars and satellites, among others). Each of these types of weapons dominated a particular kind of confrontation: siege warfare for the first, manoeuvre warfare for the second and *blitzkrieg* for the last one.

This historical evidence is also described in *The Third Wave* and *War and Anti-War*, in which the argument is made that the wars waged throughout several historical eras are characterised by revolutionary technological discoveries that cause "waves" of socio-economic changes. According to the authors of those works, Alvin and Heidi Toffler, the first wave (agrarian) was characterised by the cultivation of the land and the domestication of animals; the second wave (industrial) was characterised by mechanisation, large-scale production, and work division; the current wave (informational) is characterised by digitalisation, computers, and information technologies.

The arguments made by those authors include a definition of the objectives of

the wars imposed by the predominant socio-economic structures in the different epochs. Pre-industrial wars were generally materialised by the conquest and/or control of territorial resources. Industrial era wars had as their objective the reduction and limitation of the opponent's production resources. Supposing that this analogy is valid, future wars will be fought to ensure control over data, information, and knowledge.

In fact, everything henceforth hedges on information or disinformation – truthfulness or untruthfulness. That once again brings the conflict between sword and armour to the surface.

In this context, some propose that the hierarchical command structures and the heavy military industry structures created to meet the needs of the industrial era now give way to the more decentralised and horizontal structures of the information era, as is the case in business-oriented civilian organisations. The success of those organisations that have adjusted to the modern world of computer networks, communication and data processing – and the failure of those that did not – is a compelling argument for the introduction of new command and control processes and procedures in the military.

INFORMATION WARFARE: RELATED ISSUES

> *Communication without "intelligence" is noise, intelligence" without communication is irrelevant.*
>
> – Gen Alfred M. Gray, USMC
>
> *Winning 100 victories in 100 battles is not the exponent of excellence. Subjugating the opposing army without a fight is the true exponent of excellence.*
>
> – Sun Tzu, *The Art of War*

Information warfare is one of the pleasant sounding terms to which we have grown accustomed over the past decade. It is normally associated with both military and civilian arenas.

Despite the fact that this topic has been the object of several studies done by both strategy analysts and defence organisations, no one has been able to precisely define "information warfare." However, everyone agrees on one thing:

in the digital era, information and its dissemination have reached the status of a vital strategic resource. In the light of this situation, a large number of military and civilian organisations have already established their work processes and methods so as to include and integrate this "new" concept in their fields.

The term "information warfare" means to perform the same tasks we used to perform but at a much faster rate by occasionally using equipment derived from our society's technological evolution. In fact, there is nothing really new at the root of the term. One can even ascertain that the basic ideas of the information warfare concept have been around for centuries.

The real problem concerning the information warfare concept lies in the fact that we have a set of old concepts dressed in new clothing. Depending on whom we talk to, information warfare encompasses attack on command and control systems, operational security, cyberwar, and electronic warfare; hacking, information-based warfare, and even psychological warfare.

The term "information warfare" means to perform the same tasks we used to perform but at a much faster rate by occasionally using equipment derived from our society's technological evolution.

Attack on Command and Control Systems

Attack on command and control systems takes place through actions that make it more difficult for the enemy to control his forces and communicate with them. This embodies one of the oldest principles of war, and, even if our forefathers did not call it information warfare, it is probably its most important aspect. The key to the problem is the ability to make decisions faster than the opponent and then act according to those decisions.

The decision cycle contains no mysteries – it is a fact of life. Everything we do is based on decision cycles. In the military arena, the decision cycle can be encapsulated in the acronym OODA (Observe, Orient our attention toward what has just happened, Decide how to proceed, and Act). Information warfare can, for example, deny our observation. The lack of information prevents us from adequately orienting our attention, making a decision, and, most importantly, acting in an effective way.

As an example, let us suppose that a computer genius was able to enter one of the networks that serve the North Atlantic Treaty Organisation's (NATO's) information systems. The enemy hacker deleted some information and changed data so as to create a false picture of what was happening on the Kosovo battlefield. After the operation, NATO commands would see a false version of reality and would inescapably end up making disastrous decisions, such as bombing areas where Serbian munitions warehouses or armoured vehicles were supposed to be, but where in fact Albanian refugee camps are located.

Operational Security

Operational security is designed to ensure the preservation of our secrets and the places where they are kept. It is accomplished by safeguarding secret documents in safe places, thus, assuring that electronic messages be coded and not easily accessed by the enemy, and by training our troops to keep important information only to themselves. Known as OPSEC in the civilian business world, this concept gave rise to some famous World War II slogans, such as "loose lips sink ships" and "the enemy is listening."

Electronic Warfare

Electronic warfare uses electronic means to neutralise enemy command and control systems, working on their communication and electronic systems while ensuring the integrity of their own systems. This type of action has existed since the military began using the telegraph in 1850. Equipment specific to electronic warfare began to appear in an efficient and coordinated way in World War II. Today, it is a standard component of any army's inventory.

Cyberwar

The cyberwar concept, though at times referred to as being different from the electronic warfare concept, can be considered as one of its integral parts. Thus, cyberwar encompasses the use of all electronic and information systems "tools" available to bring down enemy electronic and communication systems while keeping our own systems operational. Many of the actions to be developed in

this area are still not clearly defined due basically to the fact that new equipment is emerging continuously and that only recently did the military start considering this technological area as a new way of war. Some elements typical of cyberwar appear here and there in an irregular and not very systematic way as opportunities for their use emerge. "Cybersoldiers" are normally confined to combat information centres (CIC) equipped with monitors, computers, and other high-technology equipment maintained by expert technicians. Their mission consists of ensuring that commanders receive current data about the situation on the battlefield.

The US Navy introduced the use of CIC for the first time about 50 years ago. Since then, their use has expanded. They have also been adopted by the other branches of the US military as well as by the armed forces of other countries.

Hacking

Hacking or "electronic guerrilla warfare" can be used by any person at any place in the world. All one needs are a computer, a modem, and some determination. This phenomenon is something recent due to the fact that it only has been a few years since we began to witness the introduction of international computer networks that virtually anyone can access. The Internet is the best example of this.

A large number computer programmers, technicians, and surfers with free time in their hands and malicious intentions, surf computer networks in search of security holes or breaches in information systems belonging to the armed forces or major corporations. This has been taking place on a consistent basis for more than a decade due to a certain lack of organisation in the network structures operated by the government and some corporations. Over the past decade, there have been a few attempts to turn the hacker problem into a "military weapon." This process has neither been agreed to nor easily put into practice, but in the light of the major advantage one can gain by penetrating the enemy information system in times of war, it is worthy of serious consideration. This has happened only in fiction, but many countries are already working toward using this scenario in the next conflict in which they are involved.

Today, hacking is an extremely attractive strategic activity for international terrorism. A testimony to that fact is the news disseminated by the August 21, 1991, *Correio da Manhã*, whereby Ramos Horta threatened Jakarta with computer terrorism activities to be carried out by 100 hackers (from Europe. Canada, and the United States) against the Indonesian banking systems.

Today, hacking is an extremely attractive strategic activity for international terrorism.

Information Jamming

Information jamming is a variation of the concept underlying the old practice of physically blocking an enemy's territory, thus, preventing him from receiving resources and goods. Due to the extreme importance of today's information, it is possible to effect a real "information jamming" if we shoot down the satellites and destroy the cable links and microwave antennas that channel information into enemy territory. After some time, this situation will be extremely difficult to overcome, especially in the more technical areas.

Information-Based Warfare

This is an area that is more associated with the concept we are attempting to define. In the 1960s, it was discovered that the mass media could make a decisive impact on the political decision-making process. Even before then, several governments in all parts of the world realised the importance of controlling the media (especially the print medium) and directing them to meet their own interests. As an increasing number of people began to see the way the media operates – collecting and disseminating information – more people began to participate in the handling of the news, thus, influencing what is disseminated by the mass media.

In the 1960s, it was discovered that the mass media could make a decisive impact on the political decision-making process.

A good example of information-based warfare could be observed during the 1991 Gulf War, when CNN, through Peter Arnett, showed the war live via

satellite to the whole world. We watched the US use television as a way of bringing pressure to bear on national and international public opinion.

Iraq also tried, with some success, to sway public opinion in its favour. The Iraqi cause remained popular among the general population of many Arab and Third World countries due to the way the Iraqi leadership exploited the visibility CNN and other international media gave the conflict. The "media offensive" did affect public opinion somewhat in the nations involved in the conflict.

More recent examples of the use of the mass media as elements to pressure public opinion and the international community are the recent conflict in Kosovo and the ongoing process for the independence of East Timor.

Psychological Warfare

Widely used, psychological warfare is nothing more than disseminating misleading information designed to demoralise the enemy. This type of action continues to be frequently used with marked success. However, there is another aspect of information warfare that has to be considered. Information warfare is defined largely by the way information is used as a weapon against enemy forces. Within a context of psychological warfare, we can work on the information that travels through the enemy's systems to prevent him from using it, or we can defend ourselves against this type of action by attempting to delete the information the enemy covertly handles and sends to us via computer, telephone, or even through any other means.

The Gulf War, often described as the first information war, is once again a good example of that type of action. The Coalition carried out an extremely effective psychological warfare campaign against Iraqi forces, at least if we consider the number of Iraqi soldiers and how quickly they would surrender whenever Allied ground troops would approach them. In fact, this operation went as planned since the pamphlets that were dropped over Iraqi troops told them exactly how they should surrender and showed the advantages of surrendering (becoming guests of honour of the Saudis). Both sides also used the media to reinforce the operation in an attempt to influence the enemy forces' will to fight.

THE INFORMATION WARFARE CONCEPT

Current definitions of information warfare are military in nature, despite the fact that many people are now beginning to understand that information warfare is not limited to the military realm. The information warfare concept can be described as the use of information and the equipment that it uses as tools (weapons) against opponents.

The information warfare concept can be described as the use of information and the equipment that it uses as tools (weapons) against opponents.

Non-military uses of information warfare can take the shape of industrial or economic espionage that is used through government or private agents to gain a competitive advantage over an opponent by revealing his secrets while protecting those belonging to their sponsor. Of course, that situation will have a direct military effect if those "infospies" select military technology as the focus of their activity.

There is no need for weapons of physical destruction to conduct information warfare, but, as we will have the opportunity to see next, that may happen at times. In fact, most tools used in information warfare are of the non-violent type, since information assumes visible form as data even if it sometimes is linked to military information systems. Even the primitive peoples, armed only with bows and arrows, had a very real understanding of the value of information: on the current enemy position, his organisation, his combat tactics, and on the battlefield in general. Accordingly, the primitive man could afford not to have a lot of technology, but needed a lot of information, and used it. From the primitive man to the man of our time, we can see that there has been an evolution in the amount of available information and the degree of dependence we have in relation to the information that we do not control.

The military in industrialised nations has become increasingly dependent on its communication systems and electronic equipment. The superiority of modern weapon systems is basically due to the fact that they transfer their data quickly across the battlefield. If we interrupt that flow of information, we will disable those high-technology systems.

Information warfare encompasses everything that can be done to protect our information systems from being exploited, corrupted or destroyed while simultaneously exploiting, corrupting or destroying the enemy's information systems.

So, in seeking to define this concept, we can say that information warfare encompasses everything that can be done to protect our information systems from being exploited, corrupted or destroyed while simultaneously exploiting, corrupting or destroying the enemy's information systems. That will enable us to gain a necessary information advantage if we become involved in an armed conflict.

Even if the use of force becomes imperative in the event combat breaks out, that is not the natural order in information warfare, as we have already seen. Information warfare is often nothing more than obtaining information faster that the enemy and assessing it in a more careful and effective way.

TYPES OF INFORMATION WARFARE WEAPONS

Much has been written recently on the various shapes information warfare can take. Within this realm, scenarios have been developed involving hacker wars, electronic warfare, information jamming, etc. However, this type of approach is a product of a vertical analysis that has only a few specific capabilities. There is no systematic approach to a taxonomy adapted to the weapons of information warfare. If instead of adopting a definition based on a weapon's physical configuration, we distinguished them according to their effects, we will arrive at an analysis matrix that will enable us to have greater relational objectivity. So, there are currently three major types of weapons capable of being used to carry out information warfare. They can produce physical, "syntax", and "semantics" effects.

Physical Effects

The use of a physical weapon will result in the permanent destruction of the information structure's physical components. A direct consequence of this is the corresponding denial of services. The complexity associated with these types of weapons is low, and their use is linear. To attain this objective, we have a wide gamut

of means that encompass traditional weapon systems such as missiles, explosives, sabotage, etc. There are also the so-called directed-energy weapons that are under development. These weapons, also known as radio frequency (RF) weapons, are devices that destroy through the emission of electromagnetic radiation in an RF with a wavelength greater than 1mm(a frequency less than 3000 GHz). This specific pulse type could cause more damage in the World Trade Centre's information systems than that caused by the bomb that exploded there recently.* These weapons are seen as a very important development because they allow the use of non-lethal force.

"Syntax" Effects

A "syntax" weapon is designed to attack an information system's operational logic by introducing delays or unpredictable behaviours in its operation. New computer viruses, as well as their counter-measures (anti-virus software), are being created at an alarming rate. Currently, there are programming environments in the market that "incubate" viruses according to the attacker's wishes. The objective of this class of weapon is to control or deactivate the logic of the networks and information systems targeted. Using the operational system's software or other systems tools, a virus can make the system work differently than expected or simply experience major delays in its execution. Here lies the central axiom of information warfare – control the enemy information systems and you will control his decision-making process and his ability to see and understand events. In that case, there is no need to destroy the enemy information or systems if we can control it. The use of viruses as an information warfare weapon has as its designated target the structural component of the information infrastructure – that is, the system's operational logic. As such, the use of this type of weapon becomes somewhat complex and follows a statistical model in the targeting process.

"Semantics" Effects

The objective of a "semantics" weapon is to destroy the trust the user places in the information systems and its supporting network, as well as to influence the interpretation of the information that flows in them. The focus of this type of

* This refers to the World Trade Centre bombing in 1993 – *Editor*

weapon is to manipulate, change, and destroy the decision models, the perception and representation of reality built through the use of an information system belonging either to a military command and control system or to a civilian organisation. The complexity associated with this type of weapon is high, since it does not seek to affect the information systems proper but rather the behaviour of its users, thus, influencing their decisions. In a not so distant future, information systems in multimedia environments will be the main information management tool. As a direct consequence of this situation, the user will have to place an even greater trust in automated processes to seek, access, collect and present information during the critical phase of intensive processing of information that as a rule occurs in a crisis situation. The existing danger (or opportunity) lies in the fact that what we believe to be objective information always resides in a specific point of view and, as such, is open to manipulation. As we can logically infer, this situation will greatly affect the correct decision-cycle performance.

Framework for the Use of Information Warfare Weapons

The technology associated with information warfare weapons is not a limiting factor nowadays. Its use is limited only by the lack of organisational, doctrinal, and legal knowledge on this issue.

Determining how these information warfare weapons are to be used, in terms of offence or defence, sparked a heated debate on the legitimacy of activities classified as information warfare actions. The US resolved this dilemma by dividing information warfare into two different components: offensive information warfare (OIW) and defensive information warfare (DIW).

The US military is working especially hard on the development of a defensive capability. This option is seen as acceptable, and it is classified by many as a legitimate information warfare activity. However, conducting information warfare activities does not eliminate the need to develop research processes, offensive in nature. These capabilities are activated due to the need know the weaknesses within the system itself. The fact is that we are led to conclude that the development of this type of action requires an offensive information warfare

capability. So, if we talk about defensive information warfare without alluding to offensive information warfare, we will be studying only one side of the coin, disregarding the synergy required from those who wish to maintain strategic superiority in information warfare.

The capability to assess weaknesses is one of the ways to ensure that information is effectively and safely configured. Classifying networks according to their size, locating all their structural elements, determining all access points, and installing sensors to monitor and exploit the processes are some of the important activities that have to be carried out to make a correct analysis of the vulnerabilities. To conduct war games, defensive information warfare needs an offensive information warfare capability to reach a relatively safe risk management level.

THE INTERNET AND INFORMATION WARFARE

The Internet: Birth and Evolution

In the late 1970s, personal computers (PCs) equipped with modems became progressively more common not too long after the emergence of computer networks. Many of those computers belonged basically to private corporations, where some programmers had designed information database software that allowed users to share files and messages with other users. This system involved nothing more than a single modem-equipped computer running a BBS (Bulletin Board System). Anyone who knew the phone number of the line to which the modem was connected could make a call and be connected to the system. Some private companies also began to adopt this system, though with some additional security procedures to prevent access from unauthorised persons.

However, the system that would drastically change this situation was the Internet. Designed in the early 1960s under the aegis of the US Department of Defence (DoD), it was first called ARPANET (Advance Research Project Agency Network). This network started to be more widely used only in the 1970s. Thus, military and university computers were connected through telephone lines. Researchers from the scientific community and military personnel could now

communicate more easily over technical projects in which written communication was much more effective than verbal. The experimental nature of this network allowed quick progress in solving a large number of technical problems. The system was built in such a way as to enable any network user to access any other computer within the same network. Although this situation could expose all network computers to sabotage, it seldom happened, at least in the beginning. Everything went smoothly until the network grew so large that the small number of hackers, who had always existed, increased considerably.

In early 1990, the Internet was already an international platform with more than 10 million users. Many of those mischievous hackers decided that it was much more fun to destroy the system than to promote its expansion or sustainability. Although people who use their personal computers connected to the Internet are generally aware of their vulnerabilities, not all of them improve their own systems to inhibit computer vandals. Besides, there is still some doubt as to whether or not the use of the Internet will become completely secure. The Internet was developed as a poorly organised project. The US government, which funded its initial design, has encouraged its growth as a very "loose" network. That means that if major parts of the network were destroyed in a nuclear war, for instance, the surviving parts could still work. People who build the network, many of them volunteers, also see the advantage of a decentralised network free from the tutelary control of a central authority.

Benefits and Vulnerabilities Associated with Internet Use

The Internet consists of millions of personal computers interconnected by telephone lines using software and common formats to send and receive information. A user can access the Internet through his or her personal computer or through a mainframe shared by thousands of users. Each computer has its own address within the Internet domain, such as *brown.edu* (a university), *army.mil* (US Army), *mobil.com* (multinational corporation), or *aol.com* (large commercial chain). Although all these computers use a common software to communicate with one another, they can individually use a great variety of operating systems. By the early 1990s, the system became so large and complex that no one could exactly say

who controlled it. Even today, we still don't know all the nasty things that can be done to the different types of computers connected to the Internet. Some of these computers are more vulnerable than others. All it takes is to access a computer connected to the Internet to get passwords and other information that will enable access to many more computers that are also connected to the Internet. As a response to this situation, many corporations began to develop firewall software for their own use or for sale. This software allows isolating the computer. However, since almost all computers (from the personal computer to the mainframe) can be connected to the Internet and not all firewall systems are identical, it is impossible to reach the same level of effectiveness.

The Internet as an Element in Information Warfare (IW)

The local area network (LAN) saw increased use in the 1970s. A LAN, as its name indicates, consists of computers usually located in the same building and connected by electric cables. When a LAN computer is connected to the Internet, all other computers within that LAN can, in most cases, be accessed by any other computer connected to the Internet. The Internet has become too valuable not to be used, but also too risky for an intrusion in a PC or LAN from vandals. This situation is now much more dangerous than it was 50 years ago, when the only existing networks were the telephone networks.

The Internet brought something slightly different from the original telephone networks. These new networks now carry multimedia information (voice, database, text, and video) using satellites and microwave systems in addition to the traditional cable systems. There is an increasing number of automated systems in which machines communicate with machines with minimal human intervention. These "machines" control electric power systems, communications and a large number of tasks in factories or wherever easy and repetitive tasks are involved. Although these tasks are easy and repetitive, they are often vital. If one of these machines makes an error or if it is sabotaged, a whole city can be without power, a telephone network can become inoperable in a large area, or a bank can be without power, a telephone network can become inoperable in a large area, or a bank can be robbed.

This situation has contributed to the increasing importance of information warfare. If a person has the chance to access one of these "robots", he or she can often neutralise its decision-making process. That, of course, will not directly cause anyone's death, but the fact of the matter is that military systems use several of these automated systems. For example, it is estimated that 90 per cent of military communications use commercial data connections. The individual user, the banking system and DoD all use the same telephone lines. Although most of the data is sent from a machine to another with no human intervention, it is possible to interfere in the process if we are able to access the system. We can use secret codes to send data, but these codes can be broken. Any computer network user is vulnerable.

Since it is true that we cannot afford not to use computer networks nowadays, we find that information warfare consists basically of exploiting that vulnerability. Many weapon systems, radars and headquarters (HQs) depend on the speed and functionality offered by computer networks to ensure their operability. The country that tries to manage its armed forces without these networks will find itself at an enormous disadvantage before an opponent who is completely interconnected by communication networks. We must not forget that the first objective targeted during the Gulf War comprised the Iraqi communication networks. Once those networks were cut, the Iraqis never regained their full operational capability. That is the embodiment of an information war accompanied by smart bombs, themselves a product of the modern technological evolution. However, it is also possible to perform information warfare actions using a personal computer and a telephone line. Never before was there a situation in which a war was open to anonymous individuals sitting at their desks from distant locations and armed with personal computers and other electronic devices.

The first objective targeted during the Gulf War was the Iraqi communication networks. Once those networks were cut, the Iraqis never regained their full operational capability.

So far as we know, it has not been organised hackers who have usually created all existing

computer viruses or attempted to penetrate networks. In fact, most of these acts are perpetrated by individual hackers and freelancers. Some of these independent hackers have made arrangements with spy agencies for ideological, monetary or even other specific or unknown reasons. Some of them have already been detected and arrested, but the uncertainty over how many are yet to be found dictates the dire need to ensure an effective control capability over information warfare. What at times goes unnoticed in all this fear associated with information warfare is that most of the damage inflicted on information systems is (and has always been) caused by human error. These problems are usually caused by users, programmers, hardware designers, and system integrators. It is often impossible to determine if a system malfunction is a result of poor programming, a physical defect, or an information warfare attack. This led to a development of standard diagnostic procedures to check usual system defects to enable the detection of information warfare attacks. What makes this perspective interesting is that a smart information warfare attack would attempt to create defects in the enemy's networks so as to appear to be hardware defects or software problems. But the most immediate and popular idea, insofar as information warfare is concerned, is to hit the enemy fast and hard using all means at our disposal to bring down his information systems. However, several nations look at information warfare as a means to decisively defeat the enemy. With a few exceptions, the industrialised nations have the majority of computers and hackers.

The former Communist nations educated more people than they could actually employ. This led to an abundance of computer experts with time on their hands and a certain resentment against society. Since the 1980s, Bulgaria, strange as it may seem, was identified as a source of most of the current computer viruses. Non-Communist nations, such as Pakistan, which has a large number of highly skilled unemployed people, have also produced many hackers over the past few years. On the other hand, India, which was certain to employ the computer programmers it had trained, has a small number of hackers and a high potential for information warfare. Although it is also possible to hire mercenary hackers, one learns that, as with any weapon, the nation that better

On the other hand, India, which was certain to employ the computer programmers it had trained, has a small number of hackers and a high potential for information warfare.

organises and leads them will gain the advantage. Although a handful of super hackers working for a small nation can inflict heavy damage on a superpower's information systems (the US, for example), the odds of that happening are somewhat remote. The industrialised nations take the information-warfare-related threat very seriously, making that scenario even less likely.

Today, military information systems are consistently threatened by foreign governments and criminal organisations. The impact of hacker activities and attempts to penetrate information systems have grown largely due to the fact that there is a greater military dependence on the Internet.

Thus, the Internet has played a major role in breaking down boundaries, and, as we have already seen, it is currently one of the best platforms for the development of information warfare actions.

INFORMATION WARFARE: STRATEGIC DIMENSION

The term "information warfare" has been increasingly used to broadly designate a large set of concepts associated with warfare phenomena of the information age. These new emerging war concepts are directly linked to the idea that the fast cyberspace evolution – the global information infrastructure—can bring both opportunities and vulnerabilities. Most of the existing studies on this issue focus on one of those vulnerabilities: that this situation may jeopardise high-value national resources usually located off the battlefield and outside a country's power projection theatre in such a way as to affect its military strategy and national security strategy.

Today, the term "information" has just a general meaning in our common language and is known for being necessarily dynamic in nature. However, there is an emerging element in information warfare that appears to be common to all uses of this constantly evolving term. We define this emerging conflict area

where nations can use cyberspace to affect strategic military operations and damage national information infrastructure as "strategic information warfare." We believe that strategic information warfare deserves special attention and recognition as a legitimate new facet of warfare with profound implications to both military and national security strategies.

In recent years, the new cyberspace culture and infrastructure (Table 1) have evolved almost exclusively outside the military arena – although the contribution made by the DoD's ARPANET to the creation of the Internet is well-known – and now offer new opportunities for information warfare.

Table 1: Strategic Information Warfare

- Information Technologies
- Cyberspace Infrastructure/Culture
- Information Warfare
- Post-Cold War International Politics
- War
- Strategy
- Strategic Information Warfare

Parallel to that, we are witnessing the continuing evolution of international politics and, in this context, the inevitable evolution of war, as Clausewitz pointed out, as a political instrument. In this environment, new interests emerge naturally for the various nations, leading to new dilemmas and new strategic targets over which influence should be exercised, including the threat of the employment of new (and old) types of strategic forces. New threats and strategic vulnerabilities appear as well. Now it becomes increasingly clear, as we intend to show, that the strategic warfare evolution will include a cyberspace threat and vulnerability dimension that should be defined as "strategic information warfare."

Strategic Information Warfare

Today, most of the industrialised countries such as the US already have an impressive number of information-based resources, including complex systems

US allies and potential coalition partners are equally dependent on several informational infrastructures. Conceptually, when a potential foe tries to damage these systems through information warfare techniques, it inevitably takes on strategic overtones.

that control electric power, currency circulation, air traffic, oil, gas, and other information-dependent items. US allies and potential Coalition partners are equally dependent on several informational infrastructures. Conceptually, when a potential foe tries to damage these systems through information warfare techniques, it inevitably takes on strategic overtones.

The above scenario contains a fundamental aspect of strategic information warfare: there is no "front line". Strategic targets located in the US can be as vulnerable to this sort of attack as its C3I (command, control, communications and intelligence) systems positioned in the theatre of operations. When responding to information warfare attacks of this nature, military strategy cannot afford to focus solely on its area of interest when conducting and supporting operations. At the present time, we have to examine in detail all information warfare implications to the infrastructures that depend on free information management.

Strategic Information Warfare: Related Issues

Interconnected networks are subject to attacks and interruptions caused not only by states but also by private organisations, including different groups and even individuals. Thus, the number of potential threats to the interests of countries such the US can rise substantially.

Some believe that the degree of difficulty in accessing the systems, alluded to in the discussion of the different types of information warfare attacks, can increase if easy access to the networks and control systems is denied through the use of new software cryptography techniques. Others admit that this could reduce some of the threats, but point to the fact that this approach would not remove other kinds of threats to a network systems made by a corrupt operator,

a direct physical attack, or both. This, by its own nature, would also make it more difficult to develop intelligence (strategic, operational and tactical) actions against strategic information warfare opponents.

The great variety of potential enemies, weapons and strategies makes it increasingly difficult to distinguish internal from external information warfare actions and threats.

The great variety of potential enemies, weapons and strategies makes it increasingly difficult to distinguish internal from external information warfare actions and threats. This particular kind of warfare basically creates new problems in a cyberspace environment. One of the basic problems in distinguishing an attack from others caused by this type of information warfare is that we at times may not be able to detect when an attack is taking place, who is mounting it, or how it is being conducted. Another consequence of this uncertainty phenomenon is the lack of a clear definition of the different levels of actions against a state that can range from crime to war. In the light of this uncertainty, nation-states opposed to the strategic interests of a certain country could abstain from traditional military or terrorist operations and instead use individuals or transnational criminal organisations to conduct criminal operations.

There is also a growing possibility that information warfare agents will be able to manipulate key information to be disseminated to the public. For example, some political groups and other non-governmental organisations can use the Internet to galvanise political support. There is also a possibility of using multimedia techniques to manipulate the "facts" about a certain event and disseminate them. Since it is true that there may also exist a reduced ability to build and maintain domestic support for controversial political actions taken by government leaders, one of the ways to adequately cope with this problem is to use the Internet as part of any public information campaign.

CONCLUSIONS

The threat of a strategic information war completely erases the distinction between military and civilian systems. The connection between them

complicates the process of detecting an attack and developing an affective defence. So, the disturbing question still remains of figuring out how a government can protect its information infrastructure, which it neither owns nor controls.

Information technologies are being developed in strategic-level planning as an offensive weapon and, at the same time, as a "logistical attack" weapon. They are considered a means of disrupting the civilian infrastructure upon which the enemy's military systems depends.

We should always bear in mind that information warfare is a two-edged sword. The countries that are most capable of waging it are also the ones most vulnerable. The growing dependence on sophisticated information systems brings an increasing vulnerability to hostile actions, to include terrorist acts.

Information warfare is a two-edged sword. The countries that are most capable of waging it are also the ones most vulnerable.

Information-based technology attacks are extremely easy to execute. The means are relatively cheap, easy to smuggle, virtually undetectable, and hard to associate. All this, along with the vulnerability of civilian communication networks (which are extremely attractive to terrorists), affords information warfare actions a prominent place in the terrorist arsenal.

Current security solutions are far from ready to face the potential threat posed by information warfare actions. This situation will probably remain unchanged until the threat becomes a reality. Only then will we be compelled to seriously consider preventive measures.

Disclaimer

The conclusions and opinions expressed in this document are those of the author, cultivated in the freedom of expression, academic environment of the Air University. They do not reflect the official position of the US Government, Department of Defence, the United States Air Force or the Air University. This article has undergone security and policy content review and has been approved for public release IAW AFI 35-101.