Information warfare

by
WILLIAM CHURCH

For nearly ten years, rumours of a new type of war have captured the imagination of military planners, but the Kosovo crisis demonstrated that the present has caught up with the future. Some of these rumoured technologies and tactics have turned into military doctrine, and now the United Nations has been asked by a world power to explore this shift in methods of warfare.

These changes fall under the popular name of Information Warfare (IW), but in military jargon it is part of a much larger strategic shift that goes by the name of Information Operations (IO) and Revolution in Military Affairs (RMA). Regardless of the wrapping, the content is the same. It is exploiting for subversive purposes an enemy's use of high-tech computer and telephone systems in both military and civilian infrastructures.

Since the definition of Information Warfare is still in the development phase and varies according to each country that formulates it, the best method of understanding the application of such

WILLIAM CHURCH is managing editor of the Centre for Infrastructural Warfare Studies (CIWARS) and of RMA Watch, Glasgow (UK). He is currently working on a doctoral thesis at the University of Glasgow on international humanitarian law and information warfare. — This article was compiled from a range of sources. The primary source is CIWARS Intelligence Report, 1997 and 1998 issues. See www.iwar.org/ciwars.html. For a review of the United States policy on Information Operations (Warfare) see www.iwar.org/USJointIO.html. For that of other countries, see www.iwar.org/country.html.

warfare is to examine how it has been and could be used. This paper examines the use of IW by dividing it into two separate categories:

- IW without concurrent use of physical force — in time of peace;
- IW concurrent with physical force — during armed conflict.

Information warfare without concurrent use of physical force

Prior to starting this section, it is important to ask one important question: how can the term Information Warfare be used if there is no war? The answer goes back to an early 19th century definition of war by the well-known German military theoretician Carl von Clausewitz who understood war as a "continuation of politics by other means". In terms of IW, "other means" might be seen as not very different from the naval practice of firing a warning shot across the bow of a ship, except that it is done with computers in a silent but nonetheless effective mode.

Approximately two years ago, IW was used to disrupt the transfer of money from one arm of a Middle Eastern terrorist group to another. This terrorist financier's bank account was covertly broken into and the money was diverted. In a similar move at the beginning of the Kosovo conflict, methods were discussed and approved to put pressure on President Milosevic; these included tampering with or breaking into his bank accounts and disrupting his personal communications.

In the first instance, the break into the banking system was successful. Conversely, there is no evidence that an attempt was made to break into the Serbian President's accounts or to disrupt his personal communications. However, what is significant are the questions surrounding the methods and results. For example, breaking into a financial account involved breaking the laws of the State where the account was domiciled, and, if successful, it had to involve intercepting and cracking the secure communications code of the international banking system. But breaking into banking systems raises more questions with regard to criminal law than to international humanitarian law, although in that case it was carried out as a hostile act in the context of a conflict situation. The example also provides an opportunity

to speculate further about extensions of this strategy. Most stock market trading is conducted in an electronic mode today, and there have already been examples of accidents that could be duplicated by an IW tactic. For example, in 1998 a bond trader-trainee hit the wrong button on his computer and initiated a market panic that wiped out several hundred million dollars of market value in one day.

Not only could this situation be duplicated by breaking into or corrupting a stock market's computer, but it is exactly the type of scenario that is being practised for both offence and defence strategies by a number of modern armies today. The goal would be to financially cripple a nation's economy so that it could not continue an aggressive arms purchase programme.

The closer the possibility of physical force in armed conflict, the more aggressive the IW tactics. The United States' Presidential Commission on Critical Infrastructure Protection (PCCIP) in 1998 cited the need to prepare for a number of IW tactics that it believes could be used against the United States. They include the disruption of electricity and/or telecommunications systems to hinder military mobilization or induce civilians to question the cost of the pending war.

As tensions mounted in the months immediately preceding the armed intervention in Kosovo, the United States military computer infrastructure was increasingly probed and in some cases its operation was hindered. This occurrence was code-named Solar Sunrise and although it was later discovered not to have been directed by the Federal Republic of Yugoslavia or any of its supporters, it sent a strong warning signal to the US armed forces.

A similar eventuality was presented at the Future of War Conference in St. Petersburg in February 1999. This time, however, the Falklands War was used as an example. IW could conceivably have been used by Argentina to disrupt the electricity, telephone and transport services of London and thus the mobilization itself; this might have delayed the sailing of the fleet and gained Argentina more time to resupply air-to-air and air-to-ground missiles or raise the political stakes for the British Prime Minister. It might be easy to discard such "what if" scenarios if it were not for the fact that they are taken directly from current military doctrine.

IW has also been speculated to be the next effective weapon to be used by terrorists and guerrilla armies as a means of compulsion. Colombian guerrilla forces are already targeting civilian electricity systems: over thirty pylons carrying power lines have been blown up in the last year. Considering that IW techniques are already being used on the battlefield to hinder the Colombian army's communications, the idea of IW actions aimed at the civilian infrastructure may not be that far-fetched. There are consequently any number of reasons to turn our attention to international humanitarian law.

Information warfare use concurrent with physical force

This section, which is intended to give a summary overview rather than a complete catalogue of IW use, details six areas thereof; for the sake of convenience, they are described in terms of primary and secondary usage. This delineation is based on known doctrine and capabilities. Considerations on primary usage are based on what is known and probable, while secondary usage is still speculative.

Primary usage

IW can be used to disrupt the use of precision bombs. Their increased use will undoubtedly be accompanied by a correlative growth in the development of IW for defence purposes. These types of bombs — popularly called "smart bombs" — premiered in the 1991 Gulf War between the Coalition countries and Iraq almost ten years ago. Since then, the use of such weapons has increased from eight per cent in that war to over 35 per cent in the Kosovo conflict. Precision bombing is meant to allow for the targeting of military facilities that are surrounded by civilian buildings, as was repeatedly the case in both the Gulf and Kosovo campaigns, and that is also the heart of the problem. The bombs are directed either by transponders surreptitiously placed on the target or by coordination of GPS (Global Positioning Satellite) signals which can identify exact locations on the earth and guide a bomb to that location. IW may be used to jam or corrupt the signals that direct the bombs.

However, a hand-held GPS jammer capable of misdirecting a precision bomb is now available at a cost of under $10,000. Considering the close proximity of some military facilities to civilians, this raises a question of responsibility:

- Who is responsible for the effects of misdirection and of collateral damage?
- If it is known that the enemy has this capability, should precision bombs no longer be used, as they might become indiscriminate weapons?

Unfortunately, GPS jammers are not the only threat to "precision bombs". The modern military have developed Electronic Magnetic Pulse (EMP) weapons capable of scrambling the operating system of computers and telecommunications facilities. These weapons are best described as similar to placing a magnet next to a computer disk and then discovering that all the information on the disk has been wiped clean. EMP weapons — used as primary weapons and as a countermeasure — have their own share of problems: they tend to be indiscriminate, with the EMP blast hitting more than its target. Civilians in hospitals on computer-controlled life-support systems, vital power-generating facilities and transport systems could be affected. Once again this raises the issue of collateral damage and responsibility for the use of IW weapons.

In both the Gulf and Kosovo conflicts, the overall infrastructure became a target and international humanitarian law experts have reviewed this tactic at length. The purpose of this paper, however, is to examine the use of IW instead of physical force. In other words, the computer systems of the targeted nation would be broken into and corrupted by inserting a computer virus or by other means, and this would naturally hinder their use for a period of time, without the cost of physical reconstruction as is now faced in Kosovo.

As far-fetched as this might seem, the facts show that this tactic was considered and rejected for the intervention in Kosovo. It can therefore only be assumed that the core capabilities were in place and that perhaps, by the next war, there will be confidence in their use. In fact, the core concept of limited damage was tested on 5 May 1999 using a device called a "soft bomb": pieces of graphite were dropped

on electric wires and caused a temporary short-circuit in the system. This test was successful, with a five-hour outage, so it only stands to reason that the search for "soft" means will continue.

The next area of IW is the potential use of these "soft" means to break into computer systems that control a country's infrastructure, with the result that the civilian infrastructure of a nation would be held hostage. Once again, this tactic was considered but rejected in Kosovo; it does, however, bring up the question of future use. Likewise rejected was the idea of electronically severing Yugoslavia's Internet connection, which would have affected both the military and civilian population and could have had a devastating effect on businesses that use the Internet to control their vital business functions, like modern electricity and water systems. Hospitals in many countries are using the Internet to access records and even for expert guidance during medical procedures.

Also, such action might disrupt any of the transnational energy-sharing agreements which are becoming increasingly popular in this globalized and privatized world. Targeting of the civilian infrastructure in this manner raises an interesting question as to the targeting process and its overall effect, which some experts have suggested could develop into indiscriminate use owing to the interrelated character of global and national infrastructures. For example, electricity is shared between Laos and Thailand, between Venezuela and Brazil, between Canada and the United States and between Indonesia and Singapore, while Malaysia, providing half of Singapore's water, is a particularly drastic case in point.

This problem also extends to telecommunications. East and South-East Asia would be a good example, as the entire land and underwater telephone cable system is linked and is susceptible to interruption at any point. For example, action against one of the countries there would strand much of Asia's telecommunication traffic and force it all to fall back on limited satellite capacity. This raises the issue of damage to neutral or third-party countries.

The third primary area of IW with concurrent physical force is the "hacking" of military systems as reported in the Kosovo conflict. It has been confirmed that the Yugoslav air force's missile

defence system was manipulated; an example would be placing false targets on the computer screen or a simple disruption of the system. Much of this activity falls into the category of ruses of war, but it has a much larger potential.

One of the most obvious examples is hacking into nuclear missile systems and causing an inadvertent launch, or changing the target acquisition database on conventional missiles or bombs so as to cause intentional civilian damage and thereby sway public opinion. This is not as far-fetched as it sounds. Many of these functions are controlled by a targeting database that is constantly updated, even in peacetime. That database might become a primary target for destruction and corruption. This will be especially true as modern military thinking moves to what is called a direct-fire concept, which involves a combination of instant battle damage assessment by remote means, simulation analysis, and subsequent retargeting by feeding the information into on-site fire systems which then fire again with very little human intervention. It might be appropriate to examine, from the standpoint of international humanitarian law, the liability for a misdirected strike based on IW techniques, or the responsibility for supervising a direct-fire system (which would obviously hinder the effectiveness of that system in a combat situation).

Secondary usage

This part deals with issues more directly related to the conventional battlefield and revolves around acts of perfidy or the targeting of sick and wounded soldiers. Unlike most of the areas summarized above there is no hard evidence that these tactics have been used, but they have been considered at military seminars and in discussion groups.

An act of perfidy may involve the use of the enemy's flag or uniform or the feigning of injury or death, with the intent to betray the enemy's confidence and to inflict damage upon him. It is this intent — meaning to draw the enemy closer by deception in order to kill him — that distinguishes perfidy from a battlefield ruse. The concept of perfidy may be relatively easy to define in the physical world. However, as we have already seen, the new battlefield is not always

visually physical. Modern armies use a combination of electronic sensors worn by their personnel or placed on their equipment. Infrared and motion detectors are used to highlight enemy movements which might be hidden by darkness or obstacles. This electronic battlefield is displayed on a combat-hardened laptop so that the entire battlefield can be monitored. This is the environment that is most susceptible to IW.

One countermeasure would be for an enemy to use or wear the other army's transponders so as to look like a friendly force, and might be deemed equivalent to wearing the enemy's uniform. This could be done by hacking into the system, altering the image and bypassing the encryption verification process, or by simple physical possession of the transponder.

An enemy might also mask the infrared signal — by an adaptation of the technology used by the Stealth bomber — so as to appear to be dead or immobile and giving off very low body heat. An army unit on patrol using the infrared identification combat system would register the object and the very low level of heat emitted. Seeing no movement and assuming that the object was lifeless, the unit might approach it with less caution. — Such signal-masking, however, presupposes the use of technology that is still at an experimental stage. There is no documented use of it at this stage.

Finally, an effective target might be the medical records of the enemy, for the purpose of delaying treatment or causing death once the soldier is under treatment. In this scenario, the enemy's computer system would be entered and selective data fields, such as blood type, would be altered. Such action could cause additional deaths. Once the problem was discovered, it would cause additional confusion and delays in the treatment of patients. It is believed that such interference is still very much theoretical. But it belongs to a category of capabilities that need exploration in order to forestall them, especially if the civilian population might become the target.

The above discussion covers the most obvious uses of IW, but there is one final area that needs exploration. It is the use of IW in psychological warfare and in the intelligence arena. While psychological warfare (PSYOP) is not new, some of its techniques might be

creating new problems. The goal of PSYOP is to affect the attitudes of the enemy soldiers and of the civilians who support them. Operations Tokyo Rose and Axis Sally during World War II are two examples. Another is the dropping of leaflets urging soldiers to surrender because of an impending invasion or giving a civilian population an unfavourable view of the war in the hope that they will cease to support it. There is no uniform answer as to whether modern uses of PSYOP are contrary to criminal law or international humanitarian law, but there may well be grounds for discussion of moral issues, as the Internet is being increasingly used for PSYOP and intelligence efforts.

On a different level there is the use of the Internet by groups in East Timor and Mexico to gain world support and expose alleged human rights abuses. However, following the same line of thinking, if such acts lead to vandalizing websites or sending "e-mail bombs" — flooding an e-mail account with messages — they may be seen as acts of terrorism.

The moral question comes into play when misinformation is knowingly put on the Internet to incite domestic tension. Last year Malaysia arrested two people who were allegedly spreading rumours on the Internet about racial strife between the Malays and the ethnic Chinese. Since neighbouring Indonesia was already experiencing ethnic violence, there may have been justifiable fear of it spreading. During the Asian financial crisis of 1997 rumours of bank collapses were spread on the Internet, no doubt with the intention of creating additional unrest. No State was found to be behind the above incidents, but the fact that they occurred begs the question of possible recurrences in the future.

The path forward

In November 1998, Russia requested the United Nations to examine the use of IW and develop an opinion regarding the need to amend international humanitarian law to govern IW or to promote some form of arms control agreement. With its Resolution A/RES/53/70 of 4 January 1999, entitled "Developments in the field of information and telecommunications in the context of international security", the General Assembly agreed to examine these issues.

One of the first questions to explore might be the relationship between IW acts and the UN Charter's prohibition of the use of force. The question is: is the use of IW without physical force as a coercive strategy a use of force in the sense of the Charter? That same question has for example been answered by the negative with respect to economic pressure.

Finding an answer to the issues raised by IW may not be as simple as it sounds. What about situations where the use of IW produces the same end results as physical force? For example, disrupting telecommunications systems by means of a computer virus can be viewed as comparable to bombing the telephone switchboard. Both can be repaired and the intention of neither is to cause the loss of human life. If the destruction of Kosovo's oil pumping and distribution system were computer-focused, or if the Yugoslav command and control systems were silenced by using IW means to corrupt the entire nation's telephone, satellite, radio and television installations, would such action be considered as a prohibited use of force? In addition, and perhaps more importantly, how could Yugoslavia have responded to these acts, and with which justification? This last question is perhaps addressed more to nuclear-capable countries, since some countries have already classified IW as a potential weapon of mass destruction.

The starting point of any reflection might be to rationalize IW in terms of current thinking on the use of force. Since much of IW focuses on infrastructure facilities shared both by civilians and by the military, international humanitarian law may be an appropriate forum to examine this issue.

A high priority might be to examine the use of precision bombs and the effect of their being corrupted. Is such use covered by the provisions of Protocol I? The same question must be asked with respect to the corruption of the targeting database and the use of EMP weapons. It is my opinion, based on military experience and not on legal expertise, that the perfidious use and targeting of medical records will sort itself out over time, once practical experience has shown its lethal effect for both sides. Combatants may develop a tacit understanding to abstain from this behaviour because of the complications it adds to the battlespace.

This situation is reminiscent of the relative ease in which the 1995 Protocol on Blinding Laser Weapons was concluded. Everyone involved understood that such weapons were not good for the waging of war and some even doubted their practical application. The Protocol stands today as one of the few examples of a weapon being prohibited before its actual use.

IW will not lend itself to easy solutions in terms of arms control. The equipment needed to wage effective IW can be as simple as a personal computer, a telephone line, and "hacker" software that is readily available on the Internet. This does not mean that we have a world full of potential "cyber soldiers", because it is a long way from the possession of a single machine to developing a coordinated strike capability that uses the modern command and control system needed to wage a military campaign, as opposed to a single hack into a computer system.

Conclusion

I hope I have given an idea of the potential problems involved in the use of IW and indicated a number of possible solutions. IW has been tabled by the United Nations, which will work its way through the various issues. The discussion would benefit if experts in international humanitarian law would also examine the issues raised in this paper. It should be possible to discover a path forward in the right direction.

●

Résumé

La guerre des systèmes d'information (« Information Warfare »)

par WILLIAM CHURCH

Depuis quelques années, une nouvelle notion est apparue dans le vocabulaire des personnes s'intéressant aux affaires militaires et de sécurité internationale : la guerre des systèmes d'information ou, en anglais, Information Warfare. *Cette méthode de guerre permet à un belligérant d'affecter et de perturber les programmes informatiques de l'adversaire, par exemple en modifiant les données qui devraient guider un missile dit « intelligent » vers son objectif. L'auteur en examine différents aspects, notamment sous l'angle du droit international humanitaire en vigueur. Il conclue que la récente décision des Nations Unies de s'intéresser à ce sujet est fondée et nécessaire.*