COMPUTER CRIME

The IW Threat from Sub-State Groups: An Interdisciplinary Approach

Andrew Rathmell, Richard Overill, Lorenzo Valeri and John Gearson

INTRODUCTION
This article is concerned with answering the question: What is the extent and nature of the Information Warfare (IW) threat from sub-state radical political groups? Although there has been a great deal of speculation and theorising about the potential threat from terrorist groups, there has been little open source research on this subject. Even at a classified level, it appears that intelligence agencies are struggling with the construction of methodologies for threat assessment.

The article provides a preliminary discussion of findings from a research project underway at ICSA. The concept behind the project is the assumption that assessing the IW threat from sub-state radical groups requires the combined skills of computer and information security specialists, strategists, and political scientists with area expertise.

The information revolution presents today’s terrorist organisations with new opportunities to pursue their political and strategic aims. The Internet in particular can be used to spread their message by making it accessible to audiences worldwide. At the same time, weaknesses in networked systems can be exploited to raise funds or to attack Government Information Infrastructures (GII) and National Information Infrastructures (NII). As noted by Walter Laqueur, ‘...why assassinate a politician or indiscriminately kill people when an attack on the electronic switching will produce far more dramatic and lasting results?’

Scope and definitions
For the purposes of this study, the following definitional limitations have been adopted. (i) The only forms of IW that are considered are software warfare and psychological operations. (ii) The concentration is on assaults on civilian and strategic targets. Direct attacks on the Defence Information Infrastructure (DII) are not considered. Attacks on the NII, however, pose a threat to the military due to its growing reliance on the NII for operations and administration.

SOFTWARE WARFARE
Terrorist activities in cyberspace may be considered as part of a new kind of war: software warfare. When InfoWarriors plan to hack or penetrate particular networks, their goal is to modify software and, consequently, its proper functions. Conversely, the system managers of the targeted information have to make sure that software is protected and running properly. Other forms of Information Warfare, such as Command and Control Warfare (C2W), Information Infrastructure Warfare (I2W) or economic information warfare are therefore dependent on the outcome of this competition to control the software of information systems.

Software warfare techniques
Knowledge of techniques of software warfare comes from the activities of private sector hackers and crackers as well as from government-spon-
sored IW programmes. Software warfare generally involves two steps — penetration of a system and disruption.5 In practice, the majority of computer/data crimes or software attacks are perpetrated by a trusted user already inside the system. This is clearly one strategy with which terrorist groups are already familiar. Otherwise, they will need to penetrate the system.

In the UK, the most common penetrative strategy involves acquisition of an authorised user's password. This may be achieved in a number of ways. Packet sniffers installed on gateways, routers or bridges linking packet switched networks can be employed to detect usernames and unencrypted passwords in transit to remote hosts; password grabbers installed as TSR (terminate and stay resident) programs on remote workstations mimic the logon sequence of a central server in order to dupe the user into giving up their username and password. Password crackers, such as that within Crack 5.0, are employed in repeated attempts to break an encrypted password using a dictionary. Added to this, well-informed password guessing and persuasive 'social engineering' are often exploited.

More general tools, such as SATAN (Security Analysis Tool for Auditing Networks), which are publicly available, are also routinely used to probe the configurational security of target Internet hosts against more sophisticated intrusion strategies.

After penetration, an intruder requiring system manager, superuser or root capabilities will attempt to obtain these by some form of subversion, typically a Trojan Horse. Such programs are planted to replace but mimic the actions of common system utilities, but with undocumented side-effects to benefit the intruder. Thus a system manager could unwittingly confer system-wide privileges on the intruder while executing the Trojan utility. Trojans may also have palpably destructive side-effects, such as deleting or scrambling mission critical files, and as such have been used for sabotage, extortion and blackmail.

Software bombs have a similar role to destructive Trojans. Planted (and usually well concealed) within some mission critical software, they consist of a trigger and a payload. If the trigger is a date and/or time then it is termed a time bomb. If the trigger is some logical condition it is called a logic bomb. When the host application is executed, the trigger condition is tested. If it is true then the payload is activated, often with destructive consequences. Typical sabotage scenarios involve an employee setting a trigger condition that their name no longer appears on the firm's payroll and a payload which is to delete the stock control or customer files. For blackmail or extortion, the trigger might be that the employee's salary has not been increased substantially. In either case the logic bomb would be buried in the payroll program by the employee.

Computer viruses resemble software bombs in generally having a trigger and a payload, but differ in that they replicate themselves by attaching themselves parasitically to files or disk sectors which are going to be executed in the normal course of events. Six generations of virus are now generally recognised: benign, self-encrypting, stealth, armoured, polymorphic and macro. By the end of 1996 about 8,000 virus strains were known, but only about a dozen were 'in the wild'. The number of strains observed appears to almost double each year. As with software bombs, the trigger can be a date (eg Michaelangelo's birthday, Friday the 13th) or a condition (eg 99th power-up since infection).

The payload can vary from the irritating (eg playing Yankee Doodle Dandy or displaying bouncing ping-pong balls) to the devastating (eg formatting the hard disk). Different infection strategies and lifecycles have also been noted, including 'slow' viruses which only infect files that are being modified by the user, 'fast' infectors which infect every file opened by the user, and heteroclyte (or 'tunnelling') viruses which have a three-stage lifecycle moving eg from executable file to disk boot sector to memory and back to executable file again. In addition, virus authoring packages have also been made public. It is claimed that the Mutation Engine can produce four million, million variants of a given virus.

Virus attacks tend to be indiscriminate and difficult to target accurately since their spread depends on human carelessness or lack of vigilance as well as on their own intrinsic virulence. For this reason they are not particularly suitable for blackmail or extortion purposes. However, they can cause enough general panic and mayhem to be considered as candidates for disruption to business and society at large.

Worm programs are replicators which do not necessarily damage data. They simply consume
system and network resources (processor cycles, memory capacity and communications bandwidth) by exponential growth in numbers. In so doing, they render the system incapable of performing useful work. This electronic gridlock is one form of 'denial of service' attack which, when launched on an institution such as a major clearing bank, for which online transaction processing (OLTP) is business critical, can cause major financial damage and hence has great potential for sabotage, extortion or blackmail.

TERRORISTS AND IW

How might terrorist groups use IW? This study postulates three key uses. First, to carry out propaganda campaigns. Secondly, to raise funds. Thirdly, to attack the NII. The only demonstrated use so far has been in the first category but it is striking how successful small radical groups have been in leveraging Information Technologies for their psychological operations even with limited resources. The potential for using IW techniques as a force multiplier in the latter two categories is great. This section discusses the ways in which terrorists may gain access to the knowledge required for IW, specifically by tapping into the skills of hackers.

Amateur hackers and terrorists

Hollywood films like the 1983 War Games or the 1995 The Net, science fiction novels by William Gibson, or the complex police operations required for catching 'Internet stars' such as Kevin Mitnick have exposed the world of amateur hackers to the public. Because of this world-wide media exposure, terrorist organisations may be tempted to use hackers to spread their political messages or manifests by hacking web pages of particular governments or political organisations.

A perfect example was the recent violation of the web page of the Indonesian Ministry of Foreign Affairs by Portuguese hackers. Their goal was to call the attention of 'Internauts' to the situation in East Timor. The introductory message of the page was modified twice, on 10th February and 17th February, 1997, with sentences like 'Welcome to the Fascist Republic of Indonesia' and an unflattering picture of the Minister of Foreign Affairs, Ali Abdullah Alatas. Recently, other hackers' targets have included the NASA, the CIA, whose page reproduced the phrase 'Central Stupidity Agency' and US Department of Justice, the FBI and the NCAA, whose page showed racial slurs. Moreover, in the UK the web page of the Labour Party has been made ridiculous with links to sites which had nothing to do with British politics. Hackers have also targeted commercial enterprises which use the Internet to advertise their products such as the Kriegsman Fur Company. In November 1996 hackers posted messages against the fur trade on its web site.

As these examples suggest, the potential for terrorist activities in terms of publicity are enormous but the main problem is to contact and persuade hackers to work for the organisation. A possible first step would be to prepare a sociological profile of hackers although the task is quite complicated as the published sources have mostly been concerned with an analysis of penetration techniques. Nevertheless, it is possible to say that hackers are usually male, between the ages of 17 and 30. Although they may have not been successful in academic studies, hackers are highly intelligent and knowledgeable in their fields. They do not perceive themselves as a real threat to society. According to one of them, 'a hacker is someone that experiments with systems by playing with them and making them do what they were never intended to do. Hacking is also about freedom of speech and freedom of access to information.' Most hackers are, or were, employed on computer-related jobs where they have, or had, chances to monitor the development of software and hardware. For many hackers hacking is their primary occupation in life.

Although their activities are essentially solitary, hackers usually have a minimal organisational structure. They often get together in clubs and, more importantly, through conferences and other social events which are advertised on the Net. During these meetings, hackers tend to invite guest speakers such as retired hackers or even academic and computer security specialists. A perfect case in this sense is the 'Hacking in Progress' conference held in the Netherlands last August where hackers, password crackers, phone 'phreaks' and programmers gathered in one location to build the largest open air Ethernet in the world. Throughout the conference there were live video and audio links to another hackers' meeting in New York called 'Beyond Hope'. Thanks to these on- and off-line events, hackers are able to create a world-
wide network of contacts which is useful for exchanging ideas and news.

The reasons for hacking are various; they range from personal satisfaction, amusement or pure curiosity. As the previous examples of hacked web pages have shown, some hackers are concerned about certain causes such as human rights, self-determination or animal protection. These concerns may provide a route by which terrorist groups could attract hackers to their cause. Terrorist recruiters are going to have to explore the computer underground before actually getting in contact with the hackers and convincing them that their knowledge and background can play an important role in their fight against a particular government or state. Hackers' conferences and meetings are a perfect venue where recruiters can get directly in contact with hackers. Having successfully 'hired' one or more hackers, the terrorist organisation will have among its supporters somebody who can tap into a wider global network of hackers.

**Professional hackers and terrorists**

The previous section looked mainly at the possible employment of hackers by terrorist organisations to spread propaganda. In addition, hacking activities can play an essential role in carrying out illegal activities such as fund raising or attacking government digital infrastructures by penetrating and disrupting them.

**Fund raising**

The scale of ongoing computer fraud and crime is notoriously hard to assess accurately. In the *Information Security Breaches Survey 1996*, produced by the UK's Department of Trade and Industry, only 3 per cent of respondents reported incidents of computer fraud, with a fraud of £650,000 being the largest single logical (non-physical) security breach reported. Another computer fraud survey conducted by PA Consulting Group in 1996, however, concluded that some £20bn per annum is lost to UK businesses alone, accounting for up to 3.5 per cent of turnover. The difficulty in arriving at reliable results in such surveys is exacerbated by the fact that more than 85 per cent of computer fraud goes unreported as institutions seek to preserve their reputations for secure practice.

Nonetheless, it is evident that the proliferation of information technologies and networks in the international economy has opened up to terrorist organisations new avenues for illegal fund raising. Central banks, stock markets and large finance institutions transfer among each other large amounts of money through systems such as CHIPS, SWIFT and FEDWIRE in the USA. At the same time, most banks are shifting some of their activities from branches to direct banking thanks to computer-telephone integration which provides links between the telephone system and databases, or even to the Internet as in the cases of Britain's Royal Bank of Scotland and Prudential. Customers expect absolute security from these institutions when they deposit money. The profitability of financial and commercial entities or even their survival is directly related to their ability to stay constantly on-line in order to attract customers 24 hours a day and to ensure secure methods of payments by credit cards or special schemes such as 'digicash'.

Terrorist organisations may consider this reliance of Western economies on information systems and networks as a lucrative source of funds. One approach would be to penetrate the information systems of a particular company and insert logic bombs or Trojan Horses in order to demand a ransom. This scenario was recently described in the *Sunday Times* which reported that, since 1993 City of London and New York financial institutions were attacked 40 times by sophisticated cyber criminals who were able to extort £400m. Terrorist organisations can benefit from the panicky response that many companies, especially small and medium size ones, have in the presence of computer viruses or other malicious codes. According to an anonymous computer virus writer, 'people think it is a major catastrophe when they are hit by a virus'. By playing on such misconceptions and threatening to leak the story to journalists and so damage customer confidence, terrorist organisations could extort significant sums. Alternatively, terrorist organisations may try to steal money directly by entering financial networks. The recent case of a young Russian mathematician who diverted funds from Citibank, is a perfect example of this tactic.

**Infrastructure attacks**

Although financing is an essential prerequisite of terrorist organisations, the ultimate goal of their 'cyber activities' would be the disruption or
destruction of information infrastructures including basic services such as power supply, police databases, social security transfers, medical networks, transportation signals, money transfers and telephone switching systems. Terrorist organisations may prefer to operate in cyberspace since the risks of capture are less than in the case of physical operations in a hostile country. Another reason would be to hamper the confidence of investors and operators in the security of the infrastructure of a particular region. This aspect may prove extremely damaging for local authorities trying to attract foreign investors not only through tax breaks or incentives but also by promoting the reliability of their transport and telecommunications infrastructures.

The need for professional hackers

The above-mentioned IW operations require an extensive knowledge of computer programming and networking. Moreover, when planning an IW attack, the terrorist organisation will have to carry out detailed intelligence work concerning the targeted system, including nodal analysis. Through this examination the terrorist organisation will assess the vulnerability of the targeted system and define penetration methods. In particular, the terrorist organisation will have to assess the importance of certain systems according to the information they carry or hold, identify their weaknesses and then prepare the appropriate software weapons.

Due to the complexity and sophistication of these operations, terrorist organisations may decide to 'hire' a professional hacker or cracker. The problem of finding such an individual is not hard to solve. The end of the Cold War led to the dismantling of Eastern European intelligence agencies. Most of these government agencies had developed extensive capabilities to violate computer systems in order to steal political and economic information. Moreover, some of the Eastern European states had developed an extensive knowledge in writing malicious computer codes in order to harm West European and American information systems. Today, most of the intelligence agencies have laid off software and computer hardware specialists because of budget constraints and lack of operational roles.14

In addition, the economic crisis of many Eastern European countries, and Russia, has meant that many high technology departments or research centres have been closed leaving many scientists unemployed and technicians with unpaid salaries. Throughout the 1990s, moreover, many large Western corporations carried out major internal restructuring by firing many technicians. Finally, there are a lot of Third World students with advanced degrees in computer studies but who have not been able to use their knowledge and capabilities back in their own countries.15

In spite of the deep reservoir of expertise, the recruitment of computer specialists may be risky for a terrorist organisation as it may expose them to penetration by police or security services. Although the same case can be made for the 'hiring' of amateur hackers, the situation with the professional is more complex as it can threaten the actual survival of the terrorist organisation. It may be difficult to conceive of a professional computer specialist becoming involved in terrorist activities on ideological grounds, since his or her nationality or cultural background is probably different from the terrorists. The professional, mainly motivated by financial gain, is more likely to decide to switch sides. Furthermore, the lack of computer expertise of some terrorist organisations may also prove to their disadvantage as they may recruit professionals who prove unable to actually carry out the planned IW operations.

In any case, the recruitment of professionals may not be enough for the terrorist organisation to carry out IW attacks against certain organisations. It is possible that nodal analysis carried out prior to the attack may indicate that the insertion of a malicious code may require an 'insider' from the targeted organisation. In this case, the terrorist organisation has to find the right person, in the right position and persuade them to take risks for the cause. That this is possible to do is demonstrated by a number of surveys concerning information intrusion inside companies that indicate the majority of problems are the result of wrongful employee actions.16

TERRORIST GROUP PROFILES

In order to ground the above discussion in empirical data, two very different types of sub-state organisation are considered here: Gulf radical movements and the Provisional Irish Republican Army (PIRA). The Gulf groups, mostly move-
ments opposing the Saudi Arabian regime, are representative of loosely organised, transnational Islamist-oriented movements that are becoming increasingly active in the Muslim world. Although these groups have their origins in long-standing opposition movements they are not well organised or highly structured. Their leaderships tend to be based outside the country in question and they appeal both to a domestic audience and to a diaspora in the West. The movements consider themselves very much in the early stages of rebellion and are concerned mainly with consciousness raising and propaganda operations. Some elements of these movements are engaged in a clandestine armed struggle but this aspect of their strategy is not yet highly developed.

PIRA, in contrast, is representative of the small number of highly professional underground ‘armies’ which draw on a long tradition of paramilitary resistance to the metropolitan power. Although propaganda is vital for the PIRA, it has long passed the early revolutionary stage of consciousness raising and is actively engaged in a sustained armed struggle. PIRA self-consciously mirror images its strategy on those of a conventional state at war. Thus it raises ‘taxes’ to fund its operations and adjusts its military strategy and targeting doctrine in line with Clausewitzian notions of the subordination of military means to political ends.

These two sample sub-state movements therefore have quite different requirements. IW techniques would serve different functions for the movements.

The Gulf and the information revolution

Governments in the states of the Gulf Cooperation Council (GCC) have been concerned for many years to control the flow of information to and from their citizens. The aim has been to protect their societies against ‘subversive’ messages — both cultural and political. Opposition movements operating in the 1960s began to overcome these controls through the use of radio. Voice of Cairo broadcasts served as a rallying cry for a generation of Nasserite Arab nationalist activists. In Oman and Saudi Arabia this propaganda had an impact but revolutionary tendencies were ultimately suppressed by the authorities.

The information revolution of the 1980s and 1990s has left these states struggling to catch up. Until the emergence of satellite TV and the proliferation of cheap satellite dishes, the residents of the GCC states were fed a diet of bland and politically conservative programming by their state channels. Access to satellite TV has in recent years enabled residents of the GCC to view a variety of international and national channels. GCC governments have sought to ban satellite dishes, a policy which is enforced in the breach in Saudi Arabia. Alternatively, as in Qatar, satellite stations are piped to cable subscribers, enabling the authorities to monitor and edit programming. More generally, Saudi finance in particular has been used to seize control of much of the Arabic satellite TV output, as it has the pan-Arab press. Saudi-owned companies such as Middle East Broadcasting Centre and Orbit TV have the resources to dominate the market and ensure that coverage of Saudi politics remains off the agenda.17

While satellite TV poses one sort of dilemma for the Gulf governments, interactive communications media such as faxes, e-mail and the Internet pose a far harder problem. The Saudi Arabian Government’s information control machinery is struggling to keep abreast of the flood of new media. The Supreme Information Council, established in 1977 under Interior Minister Prince Nayef, supervises the work of a vast network of censors. They are quite effective at dealing with domestic and foreign publications as well as controlling public spaces inside the country such as mosques18 but controlling the new electronic media poses a number of problems.

First, the connectivity of Saudi society is increasing rapidly as the economy modernises and as the populace becomes ever better educated.19 In response to these needs, the Saudis are investing $4bn in upgrading their telephone system and installing 1.5 million extra lines. Secondly, the technical problems of monitoring Internet access among a large group of subscribers have not been solved. Although the Saudi Government has promised Internet access to business users, at present access is limited to universities and hospitals where the activities of individual users can be monitored by systems administrators and security officials. Thirdly, the Saudi diaspora, consisting of students, business travellers and holidaymakers, now has regular and unfettered access to the communications networks of the West. Cyberspace is
thus accessible to many Saudis at frequent intervals even if they cannot access it from inside the Kingdom.

**Islamist psychological operations**

A number of Islamist opposition movements have been quick to seize the opportunities provided by cyberspace. These movements draw on long traditions of opposition to the Al Saud but the current conflict was sparked off by the Gulf War and the invitation to Western troops to defend the Kingdom against Iraq. The key groups are Wahhabi dissidents, the very movements that have worked in alliance with Al Saud since the 18th century but who have at various times risen up against the 'impurity' and 'corruptness' of a regime that is perceived to have made too many compromises with the infidels.

The three groups of most interest are: the Committee for the Defence of Legitimate Rights (CDLR), the Movement for Islamic Reform in Arabia (MIRA) and the Committee Against Corruption in Saudi Arabia (CACSA). All have leveraged communication technologies to ensure a psychological impact out of proportion to their size.

The CDLR was founded in May 1993. Its leading members had, in 1991 and 1992, issued a list of demands to King Fahd which demanded more Islamic domestic and foreign policies. Ignored by the monarch but encouraged by the level of informal support, the leaders of the movement hoped that the CDLR would be a vehicle through which pressures could be applied on the monarchy. Instead, the government cracked down on the dissidents, imprisoning some and sending others fleeing into exile. The most prominent, Dr Muhammad al-Masari, set up office in London where he acted as a voluble spokesman for the movement. Although well funded from private sources, Masari never had as many supporters in the Kingdom as did certain radical pan-Islamist movements who were discrediting the cause. Even smaller and less well resourced than the CDLR, MIRA's proactive and sophisticated media strategy has made it a leading voice of the Saudi Islamist opposition and a leading source for the international news media. MIRA has a well constructed Internet home page and distributes a weekly newsletter. Faqih has frequently cited plans to begin satellite TV broadcasts but so far has faced legal and financial problems which have prevented this.

CACSA emerged recently on the Internet in the USA and, unlike MIRA and CDLR, does not promote any individual as its leader. Instead it claims to represent a Saudi technocratic and business elite in general. There is some evidence that the group is an outgrowth of Shiite opposition movements that were active in the early 1990s. This earlier movement, which called itself the Reform Movement after 1992, operated out of London and Washington from where it published an authoritative newsletter distributed by fax to Saudi Arabia. This group made its peace with the Saudi Government in 1994 and agreed to cease its propaganda activities. Complaints have, however, emerged that the Saudi Government has not kept its end of the agreement and CACSA may be the work of dissident Shiites.

The common theme from an examination of the propaganda activities of all of these groups is the striking extent to which they have been able to leverage information technologies to circumvent Saudi Government controls on information collection and dissemination. There are three key ele-
ments: first, a very small and poorly resourced group, if it is skilled in the use of communication technologies, can have a major propaganda impact both internationally and in the Kingdom. Secondly, the Saudi authorities have been unable to find technical or security methods of controlling new information channels. They have had to resort to using diplomatic influence and traditional foreign covert operations to disrupt the activities of groups such as the CDLR. Thirdly, a key feature of the new technologies is that, unlike radio or TV, they are interactive. Opposition sympathisers in Saudi Arabia can use fax, phone and e-mail to send information to opposition activists in exile. The activists can then package and redistribute this information from their safe haven. Opposition movements therefore become information providers which greatly enhances their credibility and influence.

The final point to note is that the groups mentioned above have not even begun to consider more advanced IW psychological operations. Offensive techniques such as spoofing official Saudi broadcasts and hacking into official web sites have not yet been tried. Similarly, these groups have as yet shown no inclination to use a wider range of offensive IW or software warfare techniques. This may be because they do not yet understand what is possible but it is also because they are in the early stages of their campaigns and are focused on consciousness raising rather than on physical operations against the regime.

The two bomb attacks carried out by Saudi dissidents against US forces in 1995 and 1996 were probably carried out by militants inspired by the exile leaderships but with no direct connections to them.24 The comparative levels of technological sophistication between the IT and media-literate exiles and the combat-experienced militants are, for now, quite different. It is clear, though that the dissidents running the IT-intensive propaganda campaigns could turn their hands to more disruptive IW attacks if they so desired.

The current 'Troubles' began in 1969 after a series of civil rights marches. The PIRA emerged in 1969 when it split from the 'Official' IRA, which has adopted a class warfare form of struggle as opposed to the Provisional's concentration on revolutionary warfare.25

PIRA is a minority revolutionary movement with a hard core of perhaps 500 activists and several thousand sympathisers. In the past 20 years some 5,000 members have passed through its ranks, been imprisoned or killed. The PIRA's political wing, Sinn Fein, is a legal party in British elections and Northern Ireland local politics. In 1983, its vote peaked at over 10 per cent of the population of Northern Ireland or around 40 per cent of the nationalist vote. In the light of its small base of popular support, the movement has refrained from mass action such as strikes and demonstrations. Instead it has forged a dedicated and professional cadre of paramilitary operatives. Its strategy is to make the cost of 'occupying' Northern Ireland unbearable for the British state so as to bring about a British withdrawal. According to the PIRA, this would result in Northern Ireland joining Eire and becoming a sovereign state.26

PIRA has two key problems in carrying out its campaign. First, it needs to fund its activities. Unlike the Saudi groups discussed above, individual supporters of the PIRA do not enjoy large amounts of disposable income. Instead, the organisation must raise its funds either from supporters abroad, such as NORAID in the USA, or from the community. In the Province, PIRA raises funds from a range of legitimate businesses and illegal activities — running taxi services, contracting, controlling gambling rackets, bank robbery and money laundering.

Secondly, it needs to select and implement a politico-military strategy that leverages its limited resources into politically and strategically significant damage to the British Government. Over time, PIRA's military strategy has altered according to political and strategic circumstances. Its main focus has been on undermining the government of Northern Ireland by attacks on the security forces or targets linked to them. Its tactics have consisted mainly of ambushes and bombings, with a number of tactical variations on the theme. It has also sought to raise the costs of governance by hitting commercial targets, such as the city centre of Bel-
fast. The problem for the PIRA has, however, been to create a sense of irresistibility. In order to raise the costs for Britain and to sustain morale among its supporters, it needs to demonstrate that, even though the struggle may take decades, it can continue to cause damage and disruption. It is in this area that there is the greatest potential for the application of IW techniques.

**PIRA’s campaign against the mainland infrastructure**

Since the early 1990s, the PIRA leadership has adopted a revised targeting strategy which they hope will better achieve their goals. It has become clear that low-level violence in Northern Ireland is of little concern to the public or politicians in Britain. Similarly, it is evident that major outrages on the mainland, such as the bombings of pubs in the 1970s, serve mainly to strengthen the determination of Britain not to compromise. Instead, the PIRA have adopted a strategy of targeting the commercial and transport infrastructure of the mainland. This is in addition to targeting British military and political symbols on the mainland, but these have become less important targets over time.

This strategy has not aimed to cause casualties, although these are often a by-product. Instead, it aims at causing economic losses to commerce and the government and disruption to the general public. The campaign began in 1991 and used bombings, backed up by hoax calls, to hit shopping centres and the railway network. In the wake of the 1992 General Election campaign, large vehicle bombs devastated commercial targets in the City of London and badly damaged a key motorway flyover in north London. In 1993 a series of bombs targeted British Gas installations and an oil terminal. In April 1993 the largest bomb ever detonated in peacetime in London went off in the heart of London’s financial district. The PIRA enthusiastically noted that this attack alone may have cost between £350m and £2.5bn in damage and lost business. In 1994 the campaign continued, with small bombings of shopping centres and railways. In March 1994 an attack on Heathrow Airport demonstrated a commitment to hit high visibility targets.

Later in 1994 the PIRA agreed to a ceasefire in the hope of entering the negotiating process in Northern Ireland. This ceasefire, however, broke down and in 1996 and 1997 the organisation resumed its operations. Once again, attacks focused on the national infrastructure. In July 1996 police arrested seven terrorists who had planned to bomb a number of electrical substations around London. Had they succeeded, there would have been ‘serious and widespread loss of electricity to London and the South-East’.

In the run up to the British General Election, on 1st May, 1997, the PIRA carried out a coordinated campaign of small bombings and hoax calls targeted at the London rail network and the national motorway network. On 3rd April, for instance, the country’s central motorway network was put out of action for a whole day. The Freight Transport Association estimated that the disruption had cost British industry £3.5m.

**PIRA and IW**

There is no open source evidence of the exploitation of IW techniques by the PIRA. Clearly, though, the group could make use of IW for both fund raising and targeting.

As discussed above, the PIRA raises some of its funds from sources such as bank robberies and fraud. There would appear to be significant benefits for the PIRA in employing hackers just as they employ more traditional criminals — to raid banks for instance. There is no evidence that the PIRA has tapped into this potentially lucrative source of funds but their experience with more traditional forms of crime and fraud mean that they may well move into this area.

In terms of the military campaign, the PIRA’s shift to targeting the UK transport and commercial infrastructure raises intriguing parallels with the work of strategic theorists who argue for coordinated attacks, including IW, on national infrastructures in order to hit the enemy state’s centre of gravity. The PIRA is using traditional methods (high explosive and incendiary devices delivered by covert operators) against a traditional target set (roads, railways, energy supplies, shopping centres and financial institutions). It is correct in its assumption that such attacks on key points are effective in causing embarrassment and cost to the British Government. What it does not yet appear to have considered, however, is the potential benefit of using software warfare techniques to simultaneously target the British NII.

Although the British NII is not as sophisticated
and extensive as its US counterpart, and therefore less vulnerable to such attacks, considerable damage and disruption could be inflicted on a variety of targets. Moreover, these attacks could generally be carried out at less risk and at lower cost than the current operations. Current mainland operations require several trained and trusted operatives, supported by a covert network of transport routes, safe houses and weapons. These operations are therefore vulnerable at many points to surveillance and interception by the British authorities. A software warfare attack, in contrast, could be carried out by one or two specialists operating with minimal infrastructure from a safe haven abroad.

In spite of the potentially huge leverage that such an IW campaign could have, there are a number of reasons why the PIRA may be reluctant to adopt IW. First, it does not fit with the organisational culture and group self-image of the movement. The Irish Republican movement places great store by, even glorifies in, physical violence. Overt, violent operations such as bombing fit this self-image. Subtle software attacks do not, though this may change if the PIRA realises the amount of physical destruction that could be caused by attacking certain components of the NII.

Secondly, the sociological background of most PIRA leaders and activists is not conducive to use of IW. The educational profile of typical activists is limited and 'professional' terrorist training has so far focused on skills such as bomb making, small arms and intelligence work. The latter area would be a particular problem since the PIRA's intelligence professionals would need educating in nodal analysis. Nonetheless, the PIRA does employ a number of electronics experts who have become proficient in fighting a low level electronic warfare campaign against the British Army's surveillance and Explosive Ordnance Disposal (EOD) specialists.

Thirdly, the PIRA places a very high value on operational security. A strictly compartmentalised cell structure was introduced in the 1970s in response to successful penetration by the British security forces. Active Service Units (ASU) operating on the mainland generally separate their operatives by function, for example reconnaissance, arms storage, safe house preparation and attacks. Lateral communication between cells is minimal. This emphasis on security has made the PIRA much harder to penetrate in recent years. This mind set would make the PIRA very reluctant to employ freelance hackers and crackers, whether amateur or professional. The risks of interfacing with possibly penetrated hacking groups may well outweigh the benefits from using their skills to launch IW attacks.

CONCLUSIONS

This article aimed to present the preliminary findings of an inter-disciplinary research project recently initiated at ICSA. The main intention was to demonstrate an approach rather than to derive detailed conclusions. Each section of the research outlined here needs to be fleshed out with further desk research, interviews and surveys. This is being done through multiple channels, using the different skills and expertise of the principal researchers.

This article has demonstrated that, to derive a useful threat assessment, it is necessary first to understand network and NII vulnerabilities, secondly, to understand the community which has the skills to cause damage and, thirdly, to understand the groups that may potentially use these skills for political and paramilitary purposes.

This article draws a number of interesting preliminary conclusions. First, that there exists a pool of knowledge and skilled personnel able and willing to carry out IW operations, ranging from propaganda to software warfare. Secondly, that even authoritarian and wealthy states such as Saudi Arabia have been unable to respond effectively to opposition groups that make sophisticated use of modern communications methods.

Thirdly, that Islamist opposition movements are making effective use of IW and that they are able thereby to leverage their limited resources to achieve a major impact. Fourthly, that although the potential impact of software warfare attacks on the NII by groups such as the PIRA could be highly disruptive and cost-effective, for reasons of organisational culture and operational security, they may be reluctant to go down this road.

REFERENCES

(2) Psychological warfare is, of course, a much broader activity than purely being a subset of IW.
(3) The concept of software warfare has been developed by Squadron Leader Peter Emmet of Britain's Defence Evaluation and Research Agency. See (1996) 'Information
(5) Disruption is used here as a shorthand for any form of unauthorised activity in a system.
(7) The original and modified version of these web-pages can be seen by visiting the sites of 2600 Magazine, the main publications for hackers at http://www.2600.com
(16) The British Information Security Breaches Survey 1996 confirmed the findings of the 1991 UN Commission on Criminal Justice Survey of 3,000 sites in the USA, Canada and Europe where by far the greatest security threat was posed by employees. The 1996 survey of US corporate security directors by Carter & Katz also mirrors this trend in finding that the primary threat came from full-time employees, followed by part-time and contract employees, with computer crackers (hackers) a close third.
(18) Sermons at mosques have been used to attack the regime but the clerics in question have usually been rapidly removed. Nonetheless, the authorities have been unable to stem the widespread distribution of audio tapes of such sermons.
(21) CDLR’s home page is at: http://www.ummah.org.uk/cdlr
(22) MIRA’s home page is at: http://www.miraserve.com/
(23) CACSA’s home page is at: http://www.saudhouse.com/
(26) Two problems with this analysis are that, first, the majority Protestant population of Northern Ireland does not want to withdraw from the UK and is determined to oppose the republicans by force; second, Sinn Fein’s objectives receive the support of just 1 per cent of the electorate of Eire.
(31) The authors of this paper have no wish to assist the IRA in selecting targets and hence this point will not be elaborated. Suitable target sets are, however, discussed extensively in the IW literature.

Dr Andrew Rathmell, International Centre for Security Analysis, Department of War Studies, King’s College London.

The International Centre for Security Analysis (ICSA) is a new collaborative venture designed to maximise the synergy between academic research in the field of War Studies and industrial expertise in Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) technologies. It is located within the Department of War Studies at King’s College and supported by Anite Systems. This paper was presented at the Third International Command and Control Research and Technology Symposium.