

# subjects within

*EXTRACTS FROM EYE SPY INTELLIGENCE MAGAZINE*

*\* images are presented in low-res screen shots for quicker loading*

# INTELLIGENCE

*Each carefully selected feature enables the reader to understand different elements of the world of intelligence, from espionage, money laundering, biometrics and the latest spy equipment from the real-life 'Q'. Readers can also complete a test paper and acquire a certificate of completion for each module.*

*The features have been carefully researched, written and prepared by leading US intelligence analyst Kevin Coleman - all contain a plethora of useful and revealing information suitable for training and educational purposes.*

*A series presented by Eye Spy Intelligence Magazine in conjunction with Spy-Ops of America*

***PAGE 02 BIOMETRICS - THE HOTTEST TECHNOLOGY FOR SECURITY - ISSUE 31***

***PAGE 03 READER PARTICIPATION OPPORTUNITY - OVERVIEW OF THE SERIES - ISSUE 32***

***PAGE 03 FUTURE SPY TECHNOLOGY FROM 'Q's' LABORATORY - ISSUE 34***

***PAGE 04 FORENSICS AND DNA - ISSUE 35***

***PAGE 05 MONEY LAUNDERING - ISSUE 36***

***PAGE 06 DIGITAL FOOTPRINTS - ISSUE 37***

***PAGE 07 PROFILING A TERRORIST - ISSUE 38***

***PAGE 07 UNRESTRICTED WARFARE - ISSUE 40***

***PAGE 08 TRACKING TERRORIST MONEY - ISSUE 42***

***PAGE 09 TECHNOLOGY WARFARE AND PROFILE OF A CORPORATE SPY - ISSUE 43***

***PAGE 10 CYBER TERRORISM - ISSUE 44***

***PAGE 11 FINANCIAL WARFARE - THE COUNTERFEIT KINGS [PART 1] - ISSUE 46***

***PAGE 12 FINANCIAL WARFARE - THE COUNTERFEIT KINGS [PART 2] - ISSUE 47***



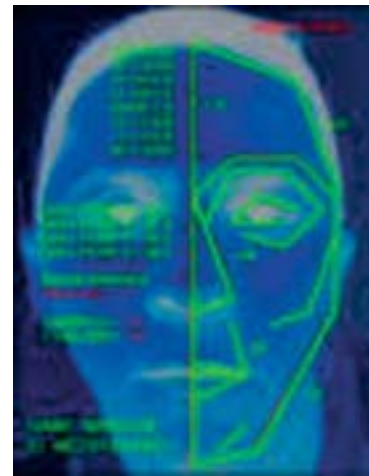
# TITLE: BIOMETRICS - THE HOTTEST TECHNOLOGY FOR SECURITY

SUB TITLE: INTELLIGENCE - LEARNING AND UNDERSTANDING  
ISSUE 31

*Basic understanding of biometrics and the different techniques being used to combat GLOBAL terrorism.*

Since the global war on terrorism began, increased emphasis has been placed on security, access control and identification. Positive identification is more critical than ever before. Historically, individuals were identified by some known piece of data or information, such as a social security number, mother's maiden name, or a personal identification number. Individual identification also took the form of things that we had such as a driver's license, an ATM card, a work ID card, or a key to the building. Today there is technology, called **BIOMETRICS** that provides positive identification using fingerprint, iris, facial, hand geometry, voice, and signature recognition.

Much attention is being given to this technology that has been under development for decades. In fact, the first commercial biometric device was produced nearly 25 years ago, and there is a good

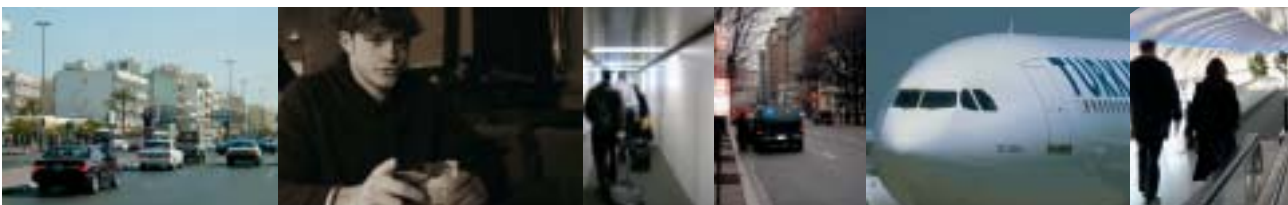


chance you may have already come across one of these biometric identification and access control systems. As advances in this specific area of technology continue, adoption will grow and you may soon see a biometric identification system built into cars and computer keyboards.

With its rapidly declining price, the use of this technology will begin to explode. Data centres, high value storage areas, research and development laboratories are all prime targets for use of biometric devices. In fact, it is estimated that there are about 30,000 locations actively using biometric systems for access control in the United States alone.

Biometric technologies are defined as **“automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioural characteristic.”**

The biometric identification and access control systems are based on a number of different techniques and devices. What exactly are they and how do they work? These systems can be placed in one of two categories. **Physical Biometrics** uses physical characteristics for recognition and includes fingerprints, facial, iris, retinal, and hand recognition. The second category is **Behavioural Biometrics**, and uses characteristics such as voice or handwriting for recognition. The following is a description of several of these biometric systems...





# TITLE: INTELLIGENCE EDUCATION - READER PARTICIPATION PROGRAMME

**SUB TITLE: INTELLIGENCE - LEARNING AND UNDERSTANDING  
ISSUE 32**

*Eye Spy Intelligence Magazine is pleased to announce a unique programme that will assist readers and persons working in the intelligence, security, defence and law enforcement professions to expand their knowledge and skill base. The material and forthcoming series has been developed through a cooperative agreement between Eye Spy Intelligence Magazine, Kevin Coleman's Technolytics Institute, an executive technology think-tank, and Spy-Ops, an organisation dedicated to continuing education through practical knowledge.*

Key challenges facing the intelligence industry today require professionals to continuously update their knowledge and skills. The terrorist problem, corporate espionage, identity theft and domestic violence, just to name a few, are real threats facing our cities and corporations. There are several major factors combined with these threats that influence the requirements for new and updated information including:

- the increasing pace of technological change,
- the increased pace of political change,
- the increased pace of social change, and
- the increased pace of economic change.

Professional development demonstrates your commitment to ensure that your knowledge and skills are relevant and up to date. Some people use continuing education to stay current in their present job; others use continuing education to gain promotions or recognition within their industry. What ever your reason, it is critical for individuals in the intelligence, security, protection and defence industries to continue to grow and develop professionally.

Toward that end, our combined research has identified sixteen topical areas listed below that will touch on most, if not all, of the topics germane to the intelligence industry. The information will be presented in a continuing education brief accompanied by an exam in future issues of Eye Spy. Topics for the new intelligence series are:-

1. Advanced Technology
2. Computer Security
3. Countersurveillance
4. Disguise Techniques
5. Etiquette and the Arts
6. Explosives
7. Fake Identification
8. Forensics
9. Incendiary Devices (IEDs)
10. International and Local Law
11. Languages
12. Lock and Security Devices
13. Photography
14. Psychology
15. Surveillance
16. Banking



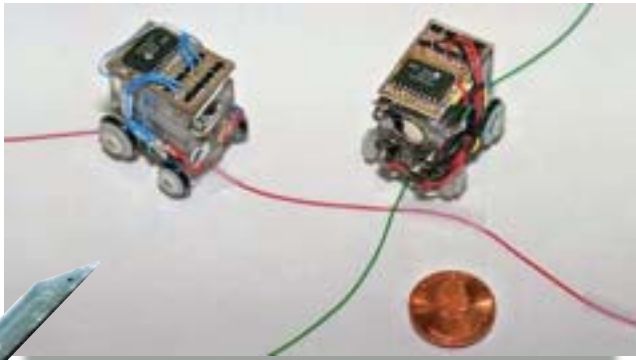
# TITLE: FUTURE SPY TECHNOLOGY FROM 'Q's' LABORATORY

**SUB TITLE: SUB TITLE: INTELLIGENCE - LEARNING AND UNDERSTANDING  
ISSUE 34**

Technology plays a critical role in defence and intelligence. Superior technology has shown to be the deciding factor when it comes to superiority on the battlefield. Whether used for intelligence, reconnaissance, surveillance or battle damage assessment, the ability to integrate technology into our strategy, planning and tactics provides a competitive edge. But where does this technology come from? What new technologies are emerging to assist the 21st century intelligence community? We will cover these topics and more.

Have you ever wondered where the ideas for all the gadgets used in espionage come from? Spy technology has on multiple occa-

sions been modelled after the technology showcased in Hollywood spy thrillers. As you may well know, 'Q' is the fictional character in the James Bond novels and movies. 'Q', which stands for Quartermaster, is a job title rather than a name. Q is the head of 'Q-branch', the fictional research and development division of the British Secret Intelligence Service. The Q character actually appears only fleetingly in Ian Fleming's novels, but comes into his own in the successful Bond movie series. The character of Q has appeared in each of the 007 films except for *Live and Let Die*.



**Spy technologies once believed fanciful or derived from the pen of a Hollywood script writer, are emerging every year**

Major Boothroyd, a.k.a. Q, is the man responsible for the creation of all the spy gadgets used by Bond. Q's mission was to go beyond traditional thinking and develop imaginative, innovative and often high risk research ideas. These ideas offer a significant technological impact, and the pursuit of these ideas will be from the demonstration of technical feasibility through the development of fielded systems.

weapons systems and platforms. Countries with poor records in R&D are unlikely to have viable civilian technology industries and advanced infrastructures, which makes it difficult for them to develop sophisticated technology for military and intelligence use.

During the 1980s and 1990s, the USA and Japan both used research and development (R&D) findings to establish their positions at the forefront of global science and technology. In addition, as a result of the change to the basic threats faced today, R&D spending has acquired even greater importance in preparing and allowing military forces to make use of advanced

A look at emerging spy technology...



# TITLE: FORENSICS AND DNA INTELLIGENCE

**SUB TITLE: INTELLIGENCE - LEARNING AND UNDERSTANDING**

**ISSUE 35**

Numerous television shows have glamorised the field of forensic science. Most people do not realise the scope of this area of study. Forensics or forensic science is the application of science to questions which are of



interest to the legal system. There are several sub-areas of forensics. For example, forensic pathology is the study of the human body to determine cause and manner of death. Criminalistics is the application of

various sciences to answer questions relating to examination and comparison of biological evidence, trace evidence, impression evidence, drugs and firearms.

The study of DNA (DeoxyriboNucleic Acid) is perhaps the most noted area of advancement in forensics. Forensic scientists have the wide-scope job of using these several areas of science to analyse the evidence collected at crime scenes. Forensic science **DOES NOT** establish innocence or guilt. Forensic science contributes information about *who, what, where, why and how.*

DNA is the key piece to several puzzles in many realms of science. It can be used to discover the starting points of medical maladies and trace heredity. It can be used to diagnose diseases and identify remains. For our purposes, we will dissect the use of DNA evidence as collected and used in the area of forensic science.

**DNA AND COLLECTION OF DNA AS EVIDENCE**

DNA is the most well known type of forensic evidence. It plays a significant role in cases where it can be of use. It is a large part of several puzzles since it is so uniquely identified. It is an individual's very own genetic blueprint and basic building block of life. It is stored within the physical parts of a body in the cells that make it up and within fluids that come from the body. Both can be of great use in forensic science.

**SOURCES OF DNA**

- Blood
- Semen
- Tissue
- Bone (Marrow)
- Hair Root
- Saliva
- Urine
- Tooth (Pulp)



Note: Spies, terrorists and criminals believe by wearing gloves and other garments it will conceal their covert activities. Now, due to DNA forensics, they have to be concerned about other evidence gathering measures...



**TITLE: MONEY LAUNDERING**

**SUB TITLE: INTELLIGENCE - LEARNING AND UNDERSTANDING**  
**ISSUE 36**



*This training brief defines what money laundering is, analyses how it is accomplished, and examines the various layers involved*

Throughout history, tracking laundered money has led to the capture of criminals and the break up of criminal rings, drug cartels, and organised crime gangs. And although money laundering and the financing of terrorism are closely related, this brief addresses only money laundering. Financing terrorism is covered in a separate training brief.

Money laundering can be simple or very complex, but in all cases the object is to utilise funds from previously committed criminal activity. Rather than being a crime in itself, it is actually a necessary component to other crimes.

Criminal activity is often focused on financial gain. Criminals cannot openly reveal the origin of their profits since they are in fact illegal. This creates the climate for money laundering. The end result is that profits made via illegal activities can be used or invested without the person having to divulge the true source of their income.



## How Money Laundering is Accomplished

Money laundering can be a lengthy process. Large sums of money made from criminal activity (bribery, computer fraud schemes, embezzlement, insider trading, drug dealing and numerous other areas) is not immediately spent or simply banked. Some crimes generate substantial amounts of cash that could attract unwanted attention from the authorities. This could lead to the source of their wealth. By disguising the source of funds, changing the form of funds (cash to gold or physical property) and transferring monies, crime gangs can keep their money 'anonymous'.

The general process followed in money laundering involves three steps: *placement*, *layering* and *integration*...



## TITLE: DIGITAL FOOTPRINTS

SUB TITLE: INTELLIGENCE - LEARNING AND UNDERSTANDING  
ISSUE 37

*This training brief examines how 'digital footprints' can betray more than just your everyday movements.*

### EXTRACT

The world enjoys unlimited benefits from new technologies in an electronic world. But electronic services send information in two directions, and the access to our personal data has never been more open. As we go about our daily lives, the use of electronic devices and systems create digital trails of where we are, what we do, whom we talk to, what we buy and more. This article will provide an understanding of digital footprints, their dangers, sources and what the consequences are for all of us.

Tracks can be followed, and being followed means you can be caught. Just as we leave behind footprints on a sandy beach, we leave behind digital footprints as we go about our daily lives. Most of our interaction and activities occur through the miracles of technology. Using technology often *creates* a digital footprint. This could be the product of a credit card transaction, web activity, a cell phone call, and even your vehicle. They could also be tied to your computer keystrokes if you work for an untrusting company. You may think these are the only ways you could be tracked digitally, but this is not the case. As technology progresses and wireless connections of sensors, cameras and other devices expand, so too do our digital footprints. Failure to understand these digital footprints puts individuals who work in security, law enforcement and intelligence at risk. Understanding how information about you flows throughout the digital world, will help protect your anonymity. It's also an important consideration if you want to protect your identity from being stolen.



**A cell phone call will leave a 'digital footprint'**



### BLACK BOXES IN VEHICLES

One of the best-kept secrets in the auto industry is that along with their airbags, many late-model cars now have electronic devices installed called Black Boxes to record data. These devices working with Global Positioning System systems and systems like ONSTAR create huge digital footprints. They track the vehicle, its duration at a particular point, how fast the vehicle is travelling and much more. Electronic vehicle tags also create a digital footprint....

### So too will a credit card transaction





# TITLE: PROFILING A TERRORIST

SUB TITLE: INTELLIGENCE - LEARNING AND UNDERSTANDING  
ISSUE 38

*In this training brief the process of recognising the characteristics of terrorists and terrorism is explored, so too some of the features that seem to be a common thread in known and suspected terrorists. How profiling is currently achieved and how the information is used is also examined. Similarly, Kevin Coleman looks into the recent changes to terrorist profiling and why these changes were necessary.*

**EXTRACT:**

Before 9/11, the practice of racial profiling as used by police and others was considered unacceptable and even illegal. Today, adjusted profiling practices are being used to protect against the all too real threat of terrorist activity. With the numerous threats that are possible in today's society, it is necessary for the government to vigilantly watch for any suspicious persons or activity. We are waging an overt war against terrorists and terrorism, but the enemy in this war is a concealed and yet obvious threat. This 21st century enemy forms hidden cells of terrorists who are preparing for and awaiting the right time to strike. Ideally, it would be best to catch such a threat before it becomes a reality. In order to accomplish this daunting task, guidelines of terrorist profiling are being developed and continually revised. In these methods of profiling, red-flag traits and activity signals are combined to single out possible threats to our society.

Terrorist profiling is no longer a matter of picking out only obvious signals of suspicion. We are no longer living in a world that can be naive to the reality of our vulnerability. Since 9/11, the profile guidelines must be broadened to include more obscure activity and individuals or groups who try to blend into our own way of life. A terrorist profile now includes not just those in training camps overseas, but suspicious (or even not so suspicious) people using our own country's various methods and centres of learning to prepare for actions against us.

Terrorist profiling is **NOT** simple *racial profiling* where a person of a certain descent, religion, colour or creed is automatically singled out. The United States, for example, is home to a vast array of peoples with different practices and backgrounds who enjoy freedoms that do not exist in other parts of the world. Because of this, looks alone are not an acceptable single point of reference when it comes to suspecting a person or group of persons of terrorist or threatening activity. Unfortunately, media portrayal has caused many innocent persons of Middle Eastern appearance or background in general, to be categorised by society as "suspicious". We must be sure to protect rather than automatically label. This is why terrorist profiling **MUST** include expanded categories beyond race...



Osama bin-Laden



# TITLE: UNRESTRICTED WARFARE

SUB TITLE: INTELLIGENCE - LEARNING AND UNDERSTANDING  
ISSUE 40

*In this training brief, Eye Spy examines the emerging threat of UNRESTRICTED WARFARE and identifies several new and important areas that individually or combined pose a major threat to world governments. The implications for the intelligence world are significant...*



UnRestricted Warfare is a relatively new concept first defined in 1999 by two Chinese colonels in a book written in the late 1990s for the Chinese People's Liberation Army. The authors, colonels Qiao Liang and Wang Xiangsui describe unconventional tactics that could



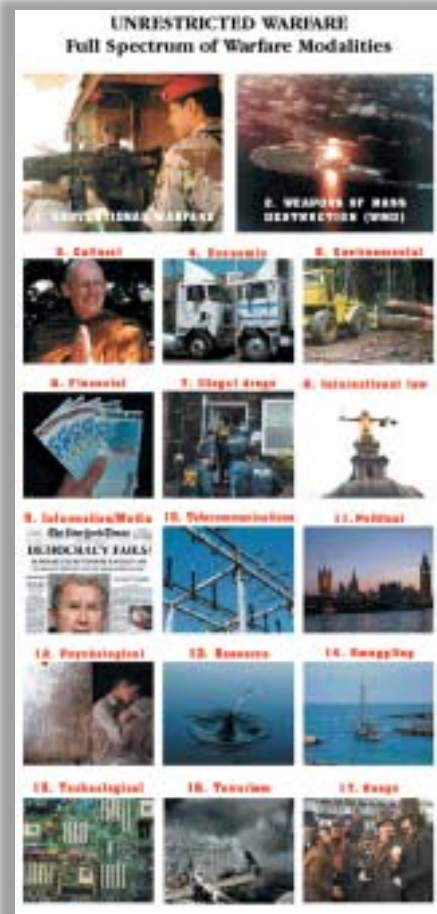
be used by an enemy against more powerful targets. This concept has continued to evolve and now consists of fifteen different modalities of warfare employed against an enemy and poses a unique threat to leading world powers that have increasingly been targeted with small scale, stealth-focused attacks on non-military targets. The book

points out that leading powers have not considered the wider picture of military strategy, which includes legal and economic factors as a method of warfare. Since no consideration has been given to these aspects of conflict, major powers are highly vulnerable to attacks along these lines.

**FULL SPECTRUM OF WARFARE MODALITIES**

Warfare is defined as organised conflict between groups for political, economic, or religious purposes. Each group is motivated by a common purpose. We can categorise it using modalities or types of warfare. Traditionally we have only considered two types - Conventional and Weapons of Mass Destruction. However with the technological advancements that have been occurring in the world, 15 new areas, or modalities of warfare are recognised. These are now known as the modalities of UnRestricted Warfare.

Here is a brief description of each of these modalities...



**TITLE: TRACKING TERRORIST MONEY**

**SUB TITLE: INTELLIGENCE - LEARNING AND UNDERSTANDING  
ISSUE 42**

*Kevin Coleman examines how terrorists are financed, what activities are used to raise money and how it is filtered to groups and individuals. Watching the 'terror bankers' are government agencies. How do they track illegal activities and what can be achieved by tracking financing patterns.*



**EXTRACT:**

Besides the obvious dangers, operating an active terrorist group is time consuming and expensive. Those charged with its leadership must find money to fund activities. In order to keep operations covert, the trail, often created between money-making schemes and direct funding, must be travelled in ways that make it difficult for the authorities to trace.

**What is terrorist financing?**

Terrorist financing (TF) is the process of illegally disguising the transfer of money with the purpose of obscuring the

origination, ownership or control of the financial assets, or promoting an illegal activity with illicit or legal source funds.

**Why track terrorist finances?**

In recent years there has been an upsurge in terrorism. Many terrorist operations have been successfully accomplished. Governments are seeking to block and identify the financiers of groups such as al-Qaida and their numerous 'franchises'. Without some form of financing, such groups could not function properly, especially when planning major attacks. Most security services believe it is crucial to uncover the 'BANKERS', though acknowledge it is impossible to block or trace all monies. However, measures have been taken to track and drastically reduce income.

**Terrorist financing is two dimensional**

Finance is necessary for the actual existence and daily activity of a terrorist group (including precursors and planning efforts for major events) and the execution of the operation itself. Funds are used to provide housing and daily expenses for cell members living abroad, dubbed "pre-crime" expenses. These include elements like communication, as seen in the Madrid bombings. Cell phones were used to coordinate activities, purchase items, hire rental cars, and ultimately pay for the explosives. Some 200 people were involved with the Madrid attacks, it's highly unlikely the group did not receive exterior finance of some sort. In the case of 9/11, funds were used to finance accommodation and pay for flying lessons. This was not only an expensive and lengthy endeavour, it also emphasised to the world the extent to which terrorists use the finances they obtain.

Fund raising includes smuggling, illegal sales, drug trafficking and under-the-counter donations from wealthy donors. Agencies have also been established in the guise of charities, and shadowy financial institutions to keep the money flowing. Al-Qaida's web of activities spans the globe and has resulted in a worldwide infrastructure of financing. In recent times, governments have established special intelligence units to target the global financing of terrorism.

**How is terrorist financing tracked?**

Tracking terrorist money is an extremely difficult task since all transactions are perfectly legal until they can be linked to support for a criminal act or known or suspected terrorist. They are also minute in terms of monetary value and therefore, extremely hard to detect in the absence of other indicators regarding the identity of the persons involved. Such profiles raise a number of legal and civil liberties' issues. Detecting the movement of money is difficult if cash is used and the formal financial system is by-passed....



**TITLE: TECHNOLOGY WARFARE AND PROFILE OF A CORPORATE SPY**

**SUB TITLE: INTELLIGENCE - LEARNING AND UNDERSTANDING ISSUE 43**

*Few people would dispute how significant a role technology plays in our lives and in defending a nation. Many believe that technology has become the foundation for an economic and military engine. Without a strong technology base, nations are extremely vulnerable. This brief will cover technology warfare as one of the 15 modalities of UnRestricted Warfare (URW). The concept of technology warfare is to gain a technological or economic advantage over your adversary through the unlawful acquisition of technology, information about technology or information about the technical capabilities of an adversary.*



## Espionage Tactics

There are numerous tactics employed by industrial spies to acquire technology or intellectual property. They range from the very basic to sophisticated and complex plots. The following is a list of the top 10 techniques currently being employed:

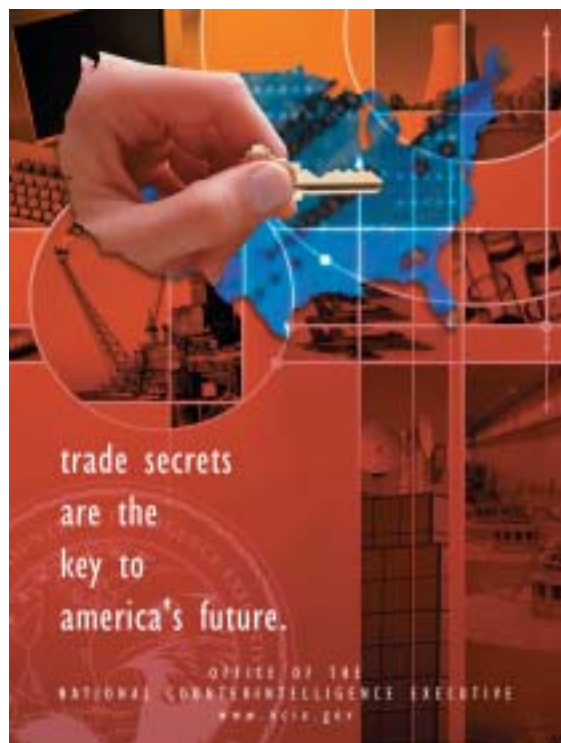
1. Use of private sector organisations, front companies, and joint ventures.
2. Classic agent recruitment (getting employees to turn over materials).
3. Employees looking to sell materials, information and samples.
4. Elicitation during international conferences and trade fairs.
5. Kidnapping and extortion of corporate executives.
6. Eavesdropping of employees in hotel, meeting rooms, and public places.
7. Dumpster diving (looking in a company's trash).
8. Surveillance and surreptitious or covert entry.
9. Hacking computer systems.
10. Laptop computer theft.

High-tech spying has become common place, and hackers and spies are being actively recruited. While the above list covers about 80% of the techniques used, industrial spies are very resourceful and often come up with new innovative techniques to achieve their goals. Employee accessibility to corporate databases and information networks makes it easy for workers to steal from their employers. Technology gives job-hopping employees an easy way to take reams of data with them. This is an area of significant concern to security professionals.

### Key Triggers and Warning Signs

1. An employee has been given a bad performance review.
2. An employee is not given a pay rise.
3. A sales person's key customer just cancelled business.
4. An employee changes work habits and comes in early or stays late.
5. Key employees leaving for no reason....

*An invaluable feature that everyone interested in technology loss and espionage should read....*



## TITLE: CYBER TERRORISM

**SUB TITLE: INTELLIGENCE - LEARNING AND UNDERSTANDING  
ISSUE 44**

*Cyber-terrorism or attacks on telecommunications and computer networks have been called the invisible threat to national economies and security. Day after day, digital warriors defend our information systems and infrastructure against thousands of unseen attacks by criminals and terrorists. This intelligence brief will help you fully appreciate the growing threat of cyber terrorism, the offensive capabilities of cyber terrorists, and the defensive measures that can be taken in response to such dangers. Included in this brief are actual scenarios that pose a significant threat to our national information and telecommunications infrastructure. Plus a listing of all major cyber attacks, viruses and related incidents.*

### EXTRACT:

Terrorism and information technology are related in two ways. First, the Internet has become a forum for both terrorist groups and individual terrorists to spread their messages of hate and violence. The internet allows terrorists to communicate with one another



**Monitoring chat rooms is an invaluable method of identifying terror suspects and their supporters**

against information, computer systems, computer programmes, networks and data, which results in violence, disruption or damage against non-combatant targets by sub-national groups or clandestine agents.

One of the first recorded cyber-terrorist attacks was in 1996. A computer hacker who was allegedly associated with the White Supremacist movement temporarily disabled a Massachusetts Internet Service Provider (ISP) and damaged part of the ISP's record keeping system. The ISP had attempted to stop the hacker from sending out worldwide racist messages under the ISP's name. The hacker signed off with the threat, "you have yet to see true electronic terrorism... this is a promise..."



and with sympathisers. Secondly, individuals and groups use the Internet to attack computer networks and systems via cyber-terrorism or cyber-warfare activities.

The term "cyber-terrorism" conjures up many different images. The truth is, cyber terrorism has been around longer than most people think. Cyber terrorism did not evolve after the terror attacks on 11 September 2001. According to the Federal Bureau of Investigation, cyber terrorism is any premeditated, politically motivated attack



# TITLE: FINANCIAL WARFARE - THE COUNTERFEIT KINGS [PART 1]

**SUB TITLE: INTELLIGENCE - LEARNING AND UNDERSTANDING  
ISSUE 46**

*Rucksack bombs, hijackings and other terrorist tactics can be countered and defeated, but there is another form of terrorism that is emerging...*

*In a statement by Osama Bin Laden, it was made very clear he intended to strike at the West financially and "bankrupt the United States". In the new order of UnRestricted Warfare, an attack on the financial infrastructures and resources of nations remains one of the most feared and effective modalities in the tool box of terrorists and rogue nation states. However, most people do not view financial institutions as a part of an enemy's attack plan, even in the 21st century.*

*A fascinating trade feature that also covers Internet attacks, hackers and currency counterfeiting.*

If you want to cripple an adversary, you simply have to find a way to disrupt their finances. This is the essence of financial warfare. Without the ability to acquire, transfer and receive money and financial resources, a country would grind to a screeching halt. An example of such can be seen in Gaza where the newly elected government of Hamas received no international financial support.





Within weeks Palestinian officials ran out of money, wages could not be paid and the shops ran dry. Suddenly the blame game began and infighting soon turned to open warfare.

**Disruption of Transactions**

Attacking the computer network or the computers processing the transactions is a well tested technique to disrupt the financial infrastructure. Called a 'denial of service' attack or DOS, this technique bombards the target with electronic traffic thus overloading the network of computers. Once the network is overloaded, legitimate transactions cannot be processed. The five most common denial of service attacks are:

- 1. BUFFER OVERFLOW** - Buffer overflows have become a common attack against applications, and have proven to be very dangerous. This happens when more data is put into a buffer or holding area than the buffer can handle. This is due to a mismatch in processing rates between the producing and consuming processes. This can result in system crashes or the creation of a back door leading to system access.
- 2. PING OF DEATH (POD)** - This is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer. A ping is normally 64 bytes in size; many computer systems cannot handle a ping larger than 65,535 bytes which is the maximum IP packet size. Sending a ping of this size often crashes the target computer.
- 3. SMURF ATTACK** - This is a denial-of-service attack which uses spoofed broadcast ping messages to flood a target system.

**4. TCP SYN ATTACK** - This attack consists of a sender transmitting a volume of connections that cannot be completed. This causes the connection queues to fill up, thereby denying service to legitimate users.

**5. TEAR DROP** - A tear drop is a widely available attack tool that exploits the vulnerability created by improper handling of fragmentation re-assembly code and overlapping IP fragments....



# TITLE: FINANCIAL WARFARE - THE COUNTERFEIT KINGS [PART 2]

**SUB TITLE: INTELLIGENCE - LEARNING AND UNDERSTANDING  
ISSUE 47**

*Intelligence analyst Kevin Coleman continues his investigation on the implications of a financial attack on the West and how big business and the individual can protect themselves...*

**SOME KEY FACTS**

In fiscal year 2003, the US Secret Service and international authorities seized \$63 million in counterfeit notes before they ever made it into circulation. About 42% of the counterfeit notes being passed in the US (detected), originated outside of the country.



Currency counterfeiting by traditional offset-printing operations is more prevalent abroad, while digital counterfeiting is more prevalent in the United States.

Nearly two million Americans have had their bank accounts raided by criminals in the past 12 months, according to a survey by market research group Gartner. Consumers reported an average loss per incident of \$1,200, pushing total losses higher than \$2 billion for the year.

Eighty-eight percent of the \$5.5 billion check fraud attempts were caught by banks' prevention measures or systems before any losses were incurred.

An "unauthorized individual" infiltrated the computer network of a third-party payment processor and may have stolen up to 40 million credit card numbers. All brands of credit cards were exposed in the attack; about 14 million of the 40 million accounts exposed were MasterCard accounts. This breach, as reported by MasterCard International, was the largest security breach made public in recent memory.

Five million elderly people are victims of financial exploitation every year. With an enormous number of baby boomers heading for retirement, are we on the verge of an elder fraud epidemic?

It is estimated that more than 2.2 million "bad cheques" enter the system each day. In the United States, for example, merchants take in over \$13 billion dollars in bad cheques annually.

Of the checks that are stolen or forged, the number of these that are written each year comes out to about 500 million checks and over \$10 billion in lost revenue....

