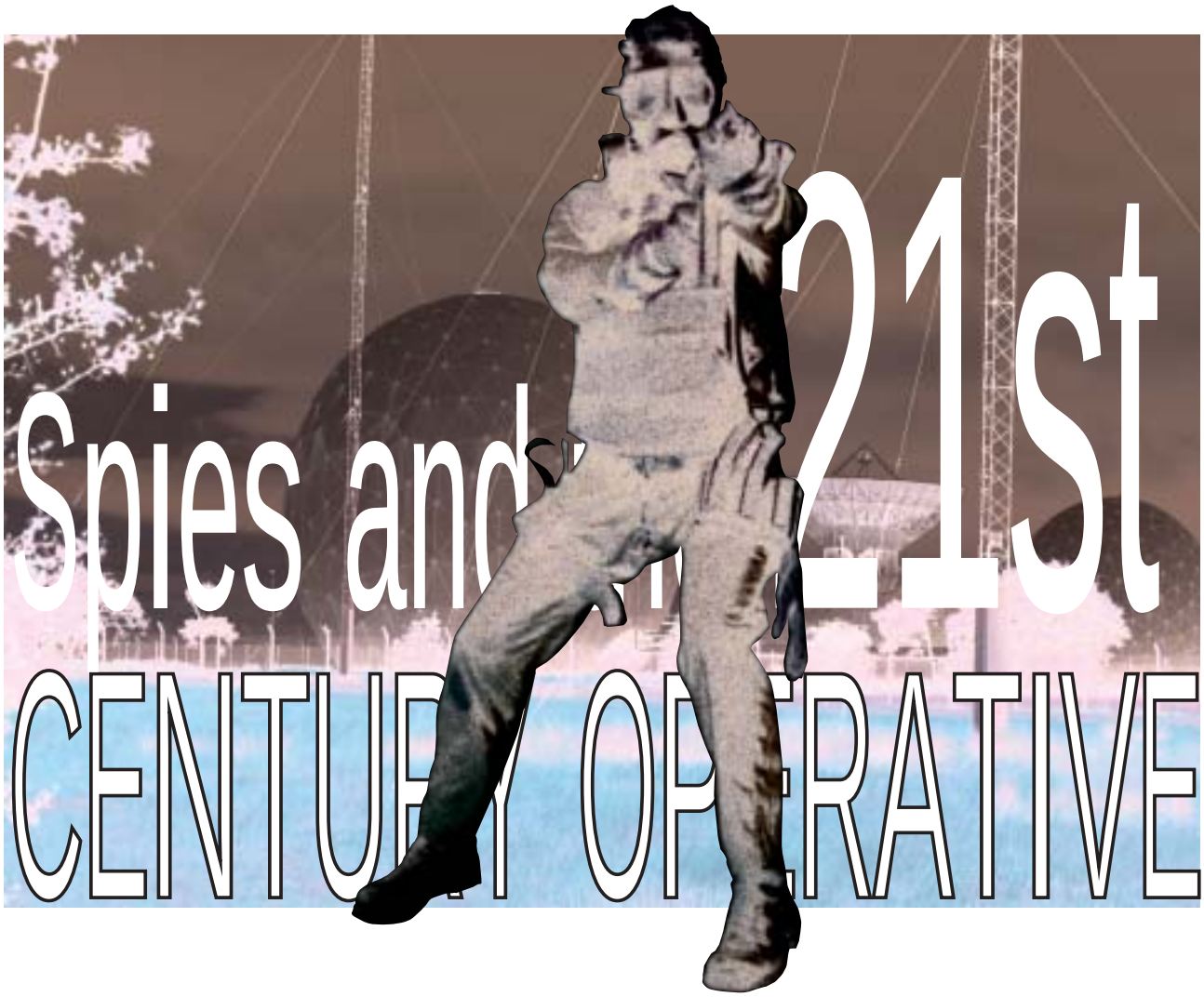


Spy-Ops of America in conjunction with Eye Spy Intelligence Magazine examine a number of highly important issues relevant to the intelligence operative. The following overview looks at emerging technologies including directed energy weapons, biometrics, nano-electronics and what is expected of the '21st Century Operative'

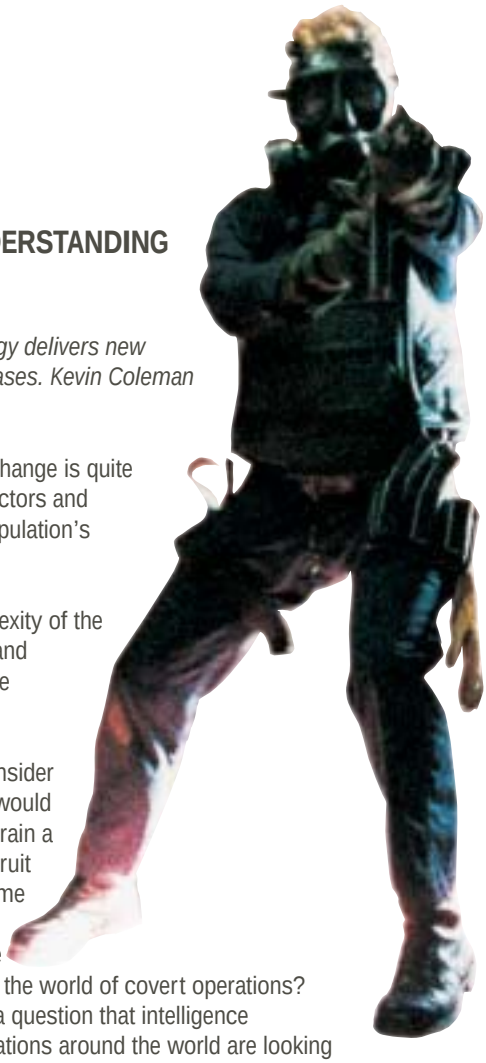
TITLE: TRAINING THE 21st CENTURY COVERT OPERATIVE

SUB TITLE: SPY-OPS INTELLIGENCE - LEARNING AND UNDERSTANDING
ISSUE 28

As the stability of the operational environment declines and the advancement of technology delivers new tools, the requirement for training intelligence operatives, both officers and agents, increases. Kevin Coleman lifts the cloak of secrecy surrounding the training for the 21st century covert-operative.

We live in a very dynamic world. The process for social, political, economic and cultural change is quite complex and not well understood. This evolutionary change may involve many different factors and multiple processes operating concurrently. Many scholars are questioning much of the population's ability to cope with such a high degree of change.

The accelerated rate of technological, political and social change has increased the complexity of the work done by the global intelligence community. In addition, the proliferation of terrorism and extremism globally has created a new challenge with unique characteristics that require the intelligence community to retool and rethink their operational modalities.



Ever consider what it would take to train a new recruit to become a valuable asset in the world of covert operations? That is a question that intelligence organisations around the world are looking to answer. As you can imagine, the task of training agents is enormous. If recruitment started today, it would take years, rather than months, to develop a highly skilled agent. However, a larger challenge exists. The dynamics of all aspects of international intelligence is such that continuous updates to training are now the most critical factor in the success equation.

TITLE: SUPERIOR TECHNOLOGY

SUB TITLE: SPY-OPS INTELLIGENCE - LEARNING AND UNDERSTANDING
ISSUE 24

In the Intelligence - Learning and Understanding series, we provide the high level understanding required to increase your skills and prepare you for the high tech intelligence world of tomorrow. As you prepare for the future we will also provide information to enhance your skills and value as an intelligence agent or operative. The articles are based on reality rather that academic vision of what the future might hold.

EXTRACT:

The world is addicted to information. It has become the life blood of corporations and governments. This is clearly indicated by the explosion of data over the past several years. Overall data production is growing about

30% a year. In 2002 there was about 5 exabytes of data. What is an exabyte? An exabyte is 5 billion gigabytes or 83,333,333 average PC hard drives. If you look at the growth of information you will discover the value of having this information has never been higher nor in more demand.

Strategic advantage can be defined as having information that your adversary does not. How does this play into intelligence? A good working definition of intelligence is the ability to derive benefit from information or the application of information to a specific issue or problem. So how does one get the information? Well, espionage is the act of collecting or the use of agents to collect information about what another government or company is doing or plans to do.

Today in the corporate world odds are that trusted employees in your company are right now stealing your product designs, business models, marketing plans, research and development files, and other intellectual property. Given most of this information is generated and stored electronically; the ability to acquire massive amounts of this information has become much easier. The high tech industry is particularly susceptible to these activities. The Internet is one of the fastest growing areas of intelligence gathering by foreign governments and potential enemies of the United States and her allies. It is believed that foreign entities are making extensive use of the "net" in an attempt to both gather military and commercial information, as well as to spread disinformation....

TITLE: GREATEST TECHNOLOGY INNOVATIONS

SUB TITLE: SPY-OPS INTELLIGENCE - LEARNING AND UNDERSTANDING

ISSUE 25

EXTRACTS:

The value of intelligence to combat current and evolving threats can not be understated. However, the current way in which we go about the business of intelligence is problematic to say the least. Even with the proposed changes the fundamental structure and operating principles of most of the intelligence agencies remains aged and flawed. The organisational architecture used by many in the global intelligence community was designed decades ago and is outdated to say the least. The entrenched architecture will be exceedingly difficult to change. Those who currently possess power and influence will resist the changes because their power and influence will likely change. While those who benefit, receiving additional power and influence, will shallowly support the changes until they become inevitable.

PROMISE

When you examine any organisation it is helpful to use a common framework for analysis. PROMISE is one such framework created specifically to address organisational change brought about by many different influencing factors. PROMISE is an acronym that stands for:

- PROCESS & PROCEDURES
- ROLES & RESPONSIBILITIES
- ORGANISATION & OPERATIONS
- MANAGEMENT & MEASURES
- INFORMATION & INFRASTRUCTURE
- SYSTEMS & SOFTWARE
- EMPLOYEE RELATIONS & EDUCATION

DATA FUSION

Technology is another area where significant change is required. Most attention is being given to the technology that allows analysts to combine data that is derived from multiple sources. This is often referred to as data fusion and is no trivial task....

TITLE: DIRECTED ENERGY WEAPONS (DEW)

SUB TITLE: SPY-OPS INTELLIGENCE - LEARNING AND UNDERSTANDING
ISSUE 26

As new materials for optics are created and advances are made in electronics, a new form of weapon looms on the horizon. Based on our analysis the new weapons system will without question be 'Directed Energy Weapons' **(DEW).**

No, this is not a science fiction movie script. We are not talking about the phasers/disruptors from Star Trek nor the turbo laser from Star Wars. We are talking about the next evolution in weapons technology - Directed Energy Weapons (DEW). This new addition to the United States already vast arsenal promises to change the face of warfare. Multiple defence agencies have research and development programmes currently underway that focus on this area. These programmes (at various stages of technological evolution) have already demonstrated many aspects of this new class of weapon. Scientists working in the field of directed energy weapons place a strong emphasis on integrating and transitioning these technologies into rapid deployment systems and platforms rather than building a single capability.

Directed energy weapons are among the latest high-tech arms of the 21st century. They hurt and kill with electromagnetic particles or waves. Simply put, these weapons direct a beam, particles, or an electromagnetic wave or a combination of the three that has a concentrated effect on the target. The speed-of-light attack and fast destruction of targets are both unique capabilities of these new weapons. DEW systems can be made variable in strength, thus, allowing both lethal and non-lethal applications of force. However, because of the early stages of research and development, little is known about the long term effects on humans. They have strong physical and psychological effects and can be used in military and civil applications. Besides obvious targets like people and buildings, microwave weapons can be aimed at computers and other electronic devices disrupting their functions or even rendering them inoperable. Probably the most interesting characteristic of these weapons is that they can be deployed and used in such a way that almost no one would know except the victims and the weapon operators. They leave no trail or trace evidence. These weapons could be devastating in the hands of terrorists. They are in essence the perfect terrorist weapon or weapon of choice for assassination.

A new technology that every budding intelligence officer should know about...

TITLE: TRACKING BIOLOGICAL WEAPONS

SUB TITLE: SPY-OPS INTELLIGENCE - LEARNING AND UNDERSTANDING
ISSUE 27

Much has been said about the threat posed by terrorists using biological and chemical weapons. How real is the threat and what must the global intelligence community do to protect against this threat? These questions are addressed as well as other critical areas in biological weapons counter-proliferation.

Technology continues to advance at a pace many people find troubling. With the advent of new technologies and breakthroughs in fundamental sciences, critics are quick to identify and espouse the negative aspects of the most recent advances. Few people would dispute that **Biotechnology** will bring about unprecedented change in many aspects of life. The medical breakthroughs in genetic engineering, tissue engineering and other Biotechnology related areas will significantly impact all living things. Biotechnology holds perhaps the greatest benefits for all mankind but like all technologies, it also

creates new threats. History has proven this fact time and time again. Just as a primitive axe can be used as a tool to cut wood and clear vegetation - it can also be used as a weapon to kill other human beings.

A basic understanding of Biotechnology is required by the intelligence community for many reasons. The first is to understand what the current capabilities of biotechnology are and how it can be used to create biological weapons (BIO-WMD). This information will also provide the knowledge to understand dual-use equipment that increases the complexity of monitoring efforts to create biological weapons.

An important feature that provides a unique insight into this important area of intelligence and counterterrorism.

TITLE: SENSOR NETWORKS, NANOELECTRONICS AND SURVEILLANCE

SUB TITLE: SPY-OPS INTELLIGENCE - LEARNING AND UNDERSTANDING

ISSUE 29

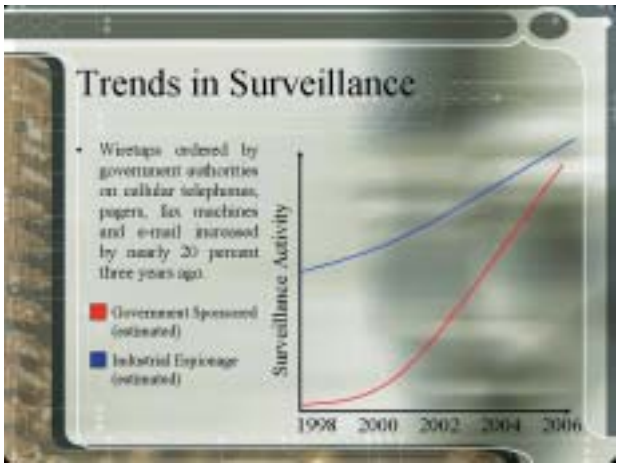
Electronic surveillance has become a core requirement for any organisation gathering intelligence. It does not matter if your are a government agency or one of the new private intelligence companies that are bursting on the scene, the art of surveillance provides the raw materials necessary for the **production** of intelligence.

Government-sponsored surveillance activities are conducted by intelligence services, other government agencies-such as foreign trade offices and S & T (science and technology) attaches-and private corporations. A number of foreign countries pose various levels and types of threats to economic and technological information. Some have been considered military adversaries for decades. Their targeting of economic and technological information is not new, but has continued as an extension of a concerted intelligence assault conducted throughout the world.

From eavesdropping on cell phone conversations to listening in on satellite communications to multifunction sensors, the intelligence we gather is the fundamental protection against terrorism and other threats.

Industry victims have reported the loss of hundreds of millions of dollars, lost jobs, and lost market share. Understandably, global industry is reluctant to publicise occurrences of foreign economic espionage. Such publicity can adversely affect stock values, customers confidence, and ultimately competitiveness and market share.

Security professionals all agree the loss of information is by far the most damaging type of theft that can occur. How big is the problem? No one knows for sure. In commercial and industrial surveillance and espionage matters, there are:



- No accurate statistics
- No common reporting methods
- No standard definitions

Successful attacks and thefts of information go unnoticed for all but a small percentage. Most unsuccessful attacks go unreported. And the rest are just news stories. No one is officially keeping track, but you can bet the monetary losses are significant and growing...

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...