

June 2008

Spy-Ops Specialty CD Certificate Program Catalog



**Quality and Relevant Continuing Education
Made Easy and Affordable**

2007 Spy-Ops Specialty CD Catalog

Spy-Ops, Inc. offers a series of Certificate Programs. This catalog is an all inclusive list of Spy-Ops programs and provides abstracts of all briefs included herein.

Spy-Ops Specialty CD Certificate Programs

About SPY-OPS.....	1
Spy-Ops Specialty CD Certificate Program Overview.....	2
Specialty CD 1 – Counter-Terrorism.....	3
Specialty CD 2 – Corporate Crime	6
Specialty CD 3 – Industrial Safety & Security.....	8
Specialty CD 4 – Personal Protection for Elected Officials	10
Specialty CD 5 – Personal Protection for Corporate Executives.....	12
Specialty CD 6 – Advanced Security Services for Private Security Guards.....	14
Specialty CD 7 – Private Investigation Services.....	17
Specialty CD 8 – Executive Protection Services	19
Specialty CD 9 – Personal Protection for Individuals	21
Specialty CD 10 – Educator Threat Awareness	23
Specialty CD 11 – Anti-Money Laundering.....	26
Specialty CD 12 – UnRestricted Warfare	28
Specialty CD 13 – Tradecraft 101.....	31
Specialty CD 14 – Computer Information and Security	32
Specialty CD 15 – Mortgage Fraud	34
Specialty CD 16 – Terrorism: Chemical – Biological – Radioactive – Nuclear – Explosives	36
Specialty CD 17 – Enterprise Risk Management	38
Specialty CD 18 – Cyber Warfare.....	41
Specialty CD 19 – Custom Certification.....	44
Ordering Information	45

About SPY-OPS

Spy-Ops is a leading provider of security, intelligence, defense, and risk management and mitigation training. With over 500,000 training briefs distributed worldwide, our materials are used by governments, intelligence agencies, law enforcement, consultants and private security firms. Our unique insights into the critical topics within the security, intelligence, and risk management space is codified into our knowledge products. Our proprietary delivery methodology ensures skills transfer. The constant change in today's world requires professionals in every industry to update their knowledge and skills. Through our continuing education products and services, we strive to provide the opportunity for professionals in the field of Intelligence, Security, Law Enforcement, Education, Personal Protection and Defense to maximize their skills, improve on-the-job performance and increase overall productivity.

Spy-Ops Specialty CD Certificate Program Overview

Our specialty CD series addresses the continuing education needs of targeted groups and individuals. While there is no one organization in charge of certifying training in the area of defense, security and intelligence, we provide a record of your training and certificates of achievement. All of the base content used in our training programs has been developed within the last two years and is updated regularly. The topics we cover represent new information on emerging trends pertaining to threats, technology and techniques that professionals require to keep their skills sharp and up-to-date. Our network of contacts, tools, methodologies and open source intelligence techniques all provide value to increase the quality of the materials included in each training brief.

The screenshot shows the first page of a training brief. It includes a title bar with 'Spy-Ops Training Brief' and 'Corporate Espionage'. Below the title is a 'CONTENTS' table with sections like Abstract, Objectives, Brief, Key Words, Glossary, Summary, References, Exam, and On-line Exercise. The 'Abstract' section contains a short paragraph about corporate espionage. There is also a small image of a person in a dark setting.

This screenshot shows the 'Summary' section of a training brief. It contains several paragraphs of text discussing mortgage fraud, specifically mentioning the Mortgage Lender Fraud (MLF) and the Financial Crimes Enforcement Network (FinCEN). It also includes a 'REFERENCES' section with several hyperlinks to external resources.

The screenshot shows the 'Answer Sheet' for the 'Corporate Espionage' training brief. It includes a header with the title and a 'Volume #, Brief #' field. Below the header is a section for 'Applicant Information' with fields for Name, Address, City, State, Zip, E-Mail, and Phone. The 'Exam' section contains five multiple-choice questions related to corporate espionage. At the bottom right, it says 'Proprietary © 2008'.

Each CD Certificate program contains from 4 to 16 Training Briefs.

Each training brief takes approximately one and one half hours to complete and includes:

- A list of objectives
- An Abstract (note: abstracts for all available briefs are included in this course catalog)
- A 6-20 page brief which provides detailed information on the topic at hand.
- A summary.
- A list of key words, and a glossary of terms.
- Current facts, alerts, notes, etc. that are applicable to the brief topic.
- A list of references.
- A 5 question multiple choice examination.

Upon successful completion of the exam, continuing education units and a certificate of completion from the Technolytics Institute is issued.

Please see the last two pages of this catalog for ordering instructions or visit the Spy-Ops website, www.spy-ops.com.



Specialty CD 1 – Counter-Terrorism

Counter-terrorism refers to the practices, tactics, and strategies used by governments, militaries, and other groups to fight terrorism. Counter-terrorism is not specific to any one field or organization; rather, it involves entities from all levels and aspects of society. For instance, businesses have security plans and often share commercial data with government agencies. Local police, firefighters, and emergency medical personnel ("first responders") have developed plans for dealing with terrorist attacks. Armies conduct combat operations against terrorists, often using special force units and tactics. Building a counter-terrorism plan involves all segments of a society and/or many government agencies working together in cooperation with private sector organizations

In response to the global threat of terrorism, and in collaboration with the Technolytics Institute, we have created this counter-terrorism awareness training program. The program is delivered on CD or electronically, and includes eleven modules that take approximately 22 hours to complete. Once you pass all eleven exams, you will receive a Certificate in Counter Terrorism.

FACT: Terrorism and Acts of Terror are not a part of the world's fabric. They are a risk which we all must face.

Program Cost: \$ 99.95

#	Title	Abstract
1	Islamist Terrorism	<p>Terrorism has become a reality of American life. We have purposely focused this brief on Islamic terrorism, and specifically groups posing a real and present danger to the United States. There are other groups, some not motivated by Islamic religious beliefs that pose immediate danger in their section of the world and future briefs will expound on these threats.</p> <p>Counter-terrorism professionals say the greatest threat from Islamic terrorists is a group using Weapons of Mass Destruction (WMD) against an American city that results in massive destruction and loss of life. While the majority of U.S. counter-terrorism efforts are aimed at Islamist terror, domestic terror groups like Earth Liberation Front (ELF) and (apparent) lone wolves like the Unabomber and Oklahoma City bombers continue to kill and maim innocent citizens. While Al-Qaeda is the most well-know organization of Islamist terror, Hezbollah and Hamas provide counter-terror professionals with plenty of sleepless nights due to their lethal operations and capabilities. There is a wealth of resources available on the internet to both understand and track the terrorist threat.</p>
2	Dirty Bombs	<p>This course introduces Radiological or "Dirty" Bombs. A dirty bomb has a conventional high-explosive core surrounded by radiological material in a solid, gas or liquid form. It is not to be confused with a fission weapon such as the bombs used during WWII. The primary lethality of a dirty bomb depends on the type and amount of radioactive material, and the dispersal factors such as wind speed and blast location. The ease of construction and availability of radiological material make the dirty bomb's use inevitable by terrorist groups.</p>

3	Biological Weapons	Biological warfare (BW), also known as germ warfare, is the use of any living organism, whether bacteria, virus, or other replicative protein as a weapon of warfare. The use of biological weapons poses one of the greatest threats civilization is likely to face as Islamist or other extremist groups collude with states to obtain biological agents. One of the greatest problems in detecting the manufacture of biological weapons is that almost all equipment needed for the production of biological agents (also referred to as pathogens and toxins) is dual use (used in the production of drugs and vaccines) and available on the international market, thus increasing the potential for concealing illicit activities under the cover of legitimate production.
4	Chemical Weapons	<p>This brief introduces chemical weapons as they relate to possible use by terrorists against civilian non-combatants. It is not intended to be an exhaustive study of chemical weapons for military use but a high-level introduction. In a pre 9/11 study, the Center for Disease Control (CDC) listed several categories of chemical weapons whose use by terrorists presented a "threat." Among these are nerve, blood, pulmonary and incapacitating agents.</p> <p>Chemical agents conjure up horrible images, as death comes in seconds after exposure to most of these agents. However, mass casualty situations are hard to predict. This is because of dispersion factors such as wind, temperature, air pressure, length of exposure and chemical characteristics associated with these and other variables. Many of these chemicals are readily available and their use by terrorist groups is probably inevitable.</p>
5	Improvised Explosive Devices	This course is a high-level introduction to Improvised Explosive Devices (IEDs). An IED is any explosive device that has been rigged by its builder to detonate and cause death and injury through blast, shrapnel, fire or release of chemicals or bio-toxins. While IEDs have gained prominence through their daily use by insurgents in Iraq, armies and unconventional warfare practitioners have used the booby trap version IED for many years. Vehicle Borne Improvised Explosive Devices (VBIEDs) and Suicide IEDs pose significant problems to counter-terror professionals, due to their ease of manufacture, ability to be hidden in obvious places without detection, and seemingly endless supply of martyrs willing to blow themselves up in attacks.
6	Domestic Terrorism	Domestic Terrorism is loosely defined as terrorist actions originating from persons and influences within a country as opposed to outside influences or persons. Throughout the Clinton administration, domestic terrorism was erroneously seen as a greater threat than Islamic terrorism. Predictably, the Clinton administration focused on right wing terrorism just as President Nixon had focused on left wing terrorism during his administration. Counter-terrorism and law enforcement professionals agree that it is only a matter of time before a domestic terrorism group eventually exceeds the death and destruction caused by Timothy McVeigh in Oklahoma City.
7	Terrorist Recognition	In this training brief, the process of recognizing terrorists will be explored. We will explore some of the features that seem to be a common thread in known and suspected terrorists. We will look at how the characterization of terrorists via profiling is currently done and how the information is then used. We will also look into the recent changes to terrorist profiling and why the changes were necessary.
8	Extremist Groups	This training brief will dissect the complex world of the extremist group. Although there are numerous individuals and interlaced groups throughout the world, we will try to look into a basic model of the psychopathology of hate groups in general. We will also look into how this model is being used to try to control hate crimes committed by such groups.

9	Scenario Based Intelligence Analysis	Intelligence is the key component needed to combat terrorism and defend against the numerous threats we face today. Currently, less than 1/10th of the United States spending on intelligence is devoted to analysis; it is the least expensive dimension of intelligence. However, if done right, the intelligence process will provide insight into new and emerging threats, perhaps preventing them, or at the very least explaining them after the fact. Toward that end, analysts in the nation's intelligence community are under extreme public pressure to perform flawlessly. Failure to do so has catastrophic consequences. Working to improve the quality of analysis to assist the intelligence community and intelligence analysts in gathering, analyzing and reporting on global threats to our interests, has resulted in the evolution of several new methods and techniques. Scenario-Based Intelligence Analysis (SBIA) is one such method. This document will explore the use of (SBIA) within the context of many methodologies.
10	Terrorism – Strategies & Tactics	Terrorism is a fact of life and a force with which we must deal. Terrorism has impacted our business, social, political and personal lives in numerous ways. When you mention terrorism one thing is certain, there is little agreement on what exactly constitutes terrorism and terrorist activities. Generally, terrorism is a tactic used to influence the activities of one entity by another entity with an opposing view, opinion, value or culture and is used in times of peace, conflict and war. Groups employ terrorist violence in the name of many causes. The threat of terrorism is ever present, and an attack is likely to occur when least expected. Terrorism is unconventional warfare. There are no fronts, no armies, and no battlefields. This training module will provide a basic understanding of terrorism.
11 (Bonus Brief)	Nuclear Weapons	Nuclear weapons can be grouped into different classes based on the nuclear reactions that provide their destructive energy, and on the details of their design. At their simplest level, nuclear weapons are classified as fission or fusion weapons, but in reality there are variations beyond the scope of this introductory text. The greatest fear of most professional intelligence practitioners is for Islamists militants to obtain nuclear weapons—an inevitability that many believe may have already occurred.

Specialty CD 2 – Corporate Crime

Corporate crime is on the rise. A recent study suggests corporate crime, in the United States alone, has reached \$300 billion annually. The most common offenses include: antitrust violations, computer and internet fraud, phone and environmental law violations, government fraud, tax evasion, financial fraud, securities fraud, insider trading, bribery, kickbacks, public corruption, money laundering, economic espionage and trade secret theft.

Business professionals are now required to investigate all aspects of corporate crime, security breaches and compromises of internal controls. In response to the needs of the business community, and in collaboration with the Technolytics Institute, we have created this corporate crime training program. The program is delivered on CD or electronically, and includes ten modules that take approximately 20 hours to complete. Once you pass all ten exams, you will receive a Certificate in Corporate Crime.

FACT: *Corporate crime and espionage have reached epidemic proportions with annual costs exceeding \$1 trillion.*

Program Cost: \$99.95

#	Title	Abstract
1	Corporate Espionage	Corporate espionage is the dirty little secret of global business. Espionage activities are often masked under the title of competitive intelligence. But in the end, thieves or spies still acquire sensitive, restricted information assets of another entity, which may include product designs, business models, marketing plans, research and development files, customer lists, employee lists, pricing strategies and other intellectual property. This module will provide a basic understanding of the current state of corporate espionage, as well as illustrate many techniques used in committing this new type of crime.
2	Digital Spying	In this brief, you will look into the world of spyware from all angles. You will see what it is and how it is used. In addition, you will be able to tell how it is being used on you. You will also learn how to protect yourself from being a victim of spyware and, if you already are a victim, how to get rid of it and protect yourself in the future.
3	Electronic Bugging	This course provides a brief overview of electronic bugging. Espionage is the art of covertly obtaining information of value about another entity. Advances in electronics have made this easier and more economical than ever. Everyone who has information that is valuable to another individual, organization or government is at risk. This module provides an introduction to electronic bugging devices, what to look for, and most importantly the "Do's and Don'ts" for when you find electronic surveillance devices.
4	Digital Footprints	The world enjoys unlimited benefits from new technologies in an electronic world. But those 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 training brief will provide an understanding of digital footprints, their dangers and what the consequences are for all of us.

5	Identity Theft	Identity theft crimes range from purse snatchings to kingpin-style fraud rings. The definition of identity theft is a crime in which an imposter obtains key pieces of personal information, such as a Social Security number, in order to impersonate someone else. Identity theft can occur when someone takes your mail, steals your wallet or swipes your records from an institution. Terrorists have a long history of assuming other individual's identities and have seized upon the use of information technology as a tool in their terrorist activities. In an article published on September 22nd, 2001 by the Times LTD titled "Terrorists' Trade in Stolen Identities" it discusses how Osama bin Laden had carefully created impostors and how his agents stole the identities and life histories of at least a dozen Western-educated young men who were all murdered in 1990. Every document and record of those men's lives were either stolen or doctored to allow the terrorists to move freely around the world. This training brief will provide a solid understanding of identity theft and implications associated with this crime.
6	White-Collar Crime	This training brief will explore the world of white-collar crime. It will look into the broad definition of the term and the most common ways it is exhibited. It will also reveal how government and law enforcement officials are trying to control and prevent these crimes from being committed. Additionally, the brief will discuss how one can protect oneself from becoming a victim.
7	Social Engineering	Social engineering is the practice of obtaining confidential information by manipulation of people. A social engineer will commonly use the telephone or internet to trick people into revealing sensitive information or get them to do something that is against typical policies. By this method, social engineers exploit the natural tendency of a person to either trust his or her word, and impart information freely, or be so busy as to take a shortcut, rather than exploiting computer security holes. It is generally agreed upon that "users are the weak link" in security, and this principle is what makes social engineering possible.
8	Computer Crime	In this training brief, we will examine the constantly evolving world of computer crimes and define a broad base of current types of crimes. We will also look at what the government is doing in an attempt to control these crimes. Finally, we will suggest some options for how individuals can protect themselves from becoming victims of such crimes.
9	Money Laundering	This training brief will define what money laundering is, walk through how it is accomplished, and examine the layers involved. The different ways money laundering effects our world will also be explored. Finally, the two necessary components required if governments are to have any hopes of controlling this area of crime will be reviewed. Although money laundering and financing terrorism are closely related, this brief addresses only money laundering. Financing terrorism is covered in a separate training brief.
10	Computer Hacking	Computer hacking, or cracking, has grown to pandemic proportions and costs businesses and governments billions of dollars in on-going computer security and countermeasure efforts. Far from its beginnings, with computer geeks breaking the security of networks, applications or communications systems, black hat hackers are now using their knowledge to commit computer crimes such as identity theft and credit card fraud. Terrorists and foreign intelligence and military personnel hack and crack to gain intelligence, conduct cyber warfare or engage in electronic sabotage.

Specialty CD 3 – Industrial Safety & Security

In early 2004, the Department of Homeland Security (DHS) advised that industrial plants are potential terrorism targets. This new reality has given momentum to industry and government initiatives aimed at enhancing the security of industrial facilities in ways that meet the ever changing threat environment.

In response to the needs of the industrial safety and security community, and in collaboration with the Technolytics Institute, we have created this unique training program. This program covers everything from terrorist attacks to white collar crime. The program includes ten modules that prepare you for the challenge of providing security in the new threat environment. The program is delivered on CD or electronically, and takes approximately 20 hours to complete. Once you pass all ten exams, you will receive a Certificate in Industrial Safety and Security.

FACT: *Industrial facilities store and use a number of hazardous substances. This is the reason they are among the 100 top terrorist targets.*

Program Cost: \$99.95

#	Title	Abstract
1	Corporate Espionage	Corporate espionage is the dirty little secret of global business. Espionage activities are often masked under the title of competitive intelligence. But in the end, thieves or spies still acquire sensitive, restricted information assets of another entity, which may include product designs, business models, marketing plans, research and development files, customer lists, employee lists, pricing strategies and other intellectual property. This module will provide a basic understanding of the current state of corporate espionage, as well as illustrate many techniques used in committing this new type of crime.
2	Dirty Bombs	This course introduces Radiological or "Dirty" Bombs. A dirty bomb has a conventional high-explosive core surrounded by radiological material in a solid, gas or liquid form. It is not to be confused with a fission weapon such as the bombs used during WWII. The primary lethality of a dirty bomb depends on the type and amount of radioactive material, and the dispersal factors such as wind speed and blast location. The ease of construction and availability of radiological material make the dirty bomb's use inevitable by terrorist groups.
3	Biological Weapons	Biological warfare (BW), also known as germ warfare, is the use of any living organism, whether bacteria, virus, or other replicative protein as a weapon of warfare. The use of biological weapons poses one of the greatest threats civilization is likely to face as Islamist or other extremist groups collude with states to obtain biological agents. One of the greatest problems in detecting the manufacture of biological weapons is that almost all equipment needed for the production of biological agents (also referred to as pathogens and toxins) is dual use (used in the production of drugs and vaccines) and available on the international market, thus increasing the potential for concealing illicit activities under the cover of legitimate production.
4	Electronic Bugging	This course provides a brief overview of electronic bugging. Espionage is the art of covertly obtaining information of value about another entity. Advances in electronics have made this easier and more economical than ever. Everyone who has information that is valuable to another individual, organization or government is at risk. This module provides an introduction to electronic bugging devices, what to look for, and most importantly the "Do's and Don'ts" for when you find electronic surveillance devices.

5	Security Systems	Security Systems (also called alarm systems) have gotten extremely sophisticated since the advent of the microprocessor (computer chip). Today's systems offer a myriad of optional sensors, signaling devices and control options that were not available just a few years ago. Most systems offer the capability to communicate with a remote monitoring station, where operators are on duty 24 hours a day to dispatch the appropriate authorities to the alarm location if a break-in or emergency arises. This training brief will cover the basics of security systems.
6	Improvised Explosive Devices	This course is a high-level introduction to Improvised Explosive Devices (IEDs). An IED is any explosive device that has been rigged by its builder to detonate and cause death and injury through blast, shrapnel, fire or release of chemicals or bio-toxins. While IEDs have gained prominence through their daily use by insurgents in Iraq, armies and unconventional warfare practitioners have used the booby trap version IED for many years. Vehicle Borne Improvised Explosive Devices (VBIEDs) and Suicide IEDs pose significant problems to counter-terror professionals, due to their ease of manufacture, ability to be hidden in obvious places without detection, and seemingly endless supply of martyrs willing to blow themselves up in attacks.
7	White-Collar Crime	This training brief will explore the world of white-collar crime. It will look into the broad definition of the term and the most common ways it is exhibited. It will also reveal how government and law enforcement officials are trying to control and prevent these crimes from being committed. Additionally, the brief will discuss how one can protect themselves from becoming a victim.
8	Extremist Groups	This training brief will dissect the complex world of the extremist group. Although there are numerous individuals and interlaced groups throughout the world, we will try to look into a basic model of the psychopathology of hate groups in general. We will also look into how this model is being used to try to control hate crimes committed by such groups.
9	Terrorism Strategies & Tactics	This training brief will define what money laundering is, walk through how it is accomplished, and examine the layers involved. The different ways money laundering effects our world will also be explored. Finally, the two necessary components required if governments are to have any hopes of controlling this area of crime will be reviewed. Although money laundering and financing terrorism are closely related, this brief addresses only money laundering. Financing terrorism is covered in a separate training brief.
10	Corporate & Industrial Terrorism	Computer hacking, or cracking, has grown to pandemic proportions and costs businesses and governments billions of dollars in on-going computer security and countermeasure efforts. Far from its beginnings, with computer geeks breaking the security of networks, applications or communications systems, black hat hackers are now using their knowledge to commit computer crimes such as identity theft and credit card fraud. Terrorists and foreign intelligence and military personnel hack and crack to gain intelligence, conduct cyber warfare or engage in electronic sabotage.

Specialty CD 4 – Personal Protection for Elected Officials

Individuals in the public eye, like elected officials, are facing mounting risks as they perform their duties. Threats, mail bombs, or face to face confrontation by unhappy citizens is becoming all too common in today's threat filled environment. No longer can you afford to be lax with your personal security. Apparent power, influence and wealth at all levels of government create the highest risk scenario for elected officials and their families. Personal protection is an important part of every elected official's skill set. Where you work, what you drive, where you live, what you wear and where you travel are all contributing factors to becoming a target. In response to the need for information related to increased security for elected officials, and in collaboration with the Technolytics Institute, Spy-Ops created a comprehensive program that incorporates the three stages of personal protection. It covers awareness, avoidance and defense in a range of topical areas critical to elected officials. The program is delivered on CD or electronically, and includes ten modules that take approximately 20 hours to complete. Once you pass all ten exams, you will receive a Certificate in Personal Protection.

FACT: *When individuals are elected to a position, they place themselves at risk. Not every decision will be popular and attacks by radicals and disgruntled individuals are a foreseeable risk.*

Program Cost: \$99.95

#	Title	Abstract
1	Digital Spying	In this brief, you will look into the world of spyware from all angles. You will see what it is and how it is used. In addition, you will be able to tell how it is being used on you. You will also learn how to protect yourself from being a victim of spyware and, if you already are a victim, how to get rid of it and protect yourself in the future.
2	Electronic Bugging	This course provides a brief overview of electronic bugging. Espionage is the art of covertly obtaining information of value about another entity. Advances in electronics have made this easier and more economical than ever. Everyone who has information that is valuable to another individual, organization or government is at risk. This module provides an introduction to electronic bugging devices, what to look for, and most importantly the "Do's and Don'ts" for when you find electronic surveillance devices.
3	Digital Footprints	The world enjoys unlimited benefits from new technologies in an electronic world. But those 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 training brief will provide an understanding of digital footprints, their dangers and what the consequences are for all of us.
4	Identity Theft	Identity theft crimes range from purse snatchings to kingpin-style fraud rings. The definition of identity theft is a crime in which an imposter obtains key pieces of personal information, such as a Social Security number, in order to impersonate someone else. Identity theft can occur when someone takes your mail, steals your wallet or swipes your records from an institution. Terrorists have a long history of assuming other individual's identities and have seized upon the use of information technology as a tool in their terrorist activities. In an article published on September 22nd, 2001 by the Times LTD titled "Terrorists' Trade in Stolen Identities" it discusses how Osama bin Laden had carefully created impostors and how his agents stole the identities and life histories of at least a dozen Western-educated young men who were all murdered in 1990. Every document and record of those men's lives were either stolen or doctored to allow the terrorists to move freely around the world. This training brief will provide a solid understanding of identity theft and implications associated with this crime.



5	Secret Intelligence	The world of intelligence is all about information. Information that is acted upon becomes intelligence. This training brief will dissect the area of secret intelligence. We will define this practice as well as discover ways it has been used throughout history by our own country and others. We will also briefly explore how secret intelligence is practiced and used in today's world.
6	Terrorism – Strategies & Tactics	Terrorism is a fact of life and a force with which we must deal. Terrorism has impacted our business, social, political and personal lives in numerous ways. When you mention terrorism one thing is certain, there is little agreement on what exactly constitutes terrorism and terrorist activities. Generally, terrorism is a tactic used to influence the activities of one entity by another entity with an opposing view, opinion, value or culture and is used in times of peace, conflict and war. Groups employ terrorist violence in the name of many causes. The threat of terrorism is ever present, and an attack is likely to occur when least expected. Terrorism is unconventional warfare. There are no fronts, no armies, and no battlefields. This training module will provide a basic understanding of terrorism.
7	Gang Activity	This brief will look at the make-up and activities of gangs. It will define what a gang is and look into how it influences the people involved in their activities as well as society as a whole.
8	Personal Protection	<p>Personal protection is critical in today's society. Home invasions, assaults, rapes, kidnappings, extortion, and carjackings are all too common in today's news headlines. Individuals must take steps to reduce the risk of becoming a victim to these crimes. Today you have about a 1 in 100 chance of becoming a victim of a violent crime. History has shown that criminals and terrorists single out businessmen and/or their families who fit a particular profile. Understanding how not to fit the profile is the first step in protecting yourself and your loved ones. Apparent power, influence and wealth create the highest risk scenario for executives and their families. Where you work, what you drive and where you live are all risk factors to be considered.</p> <p>Many individuals rely on self-defense courses as the primary way they choose to prepare. Personal protection is a broad area that covers everything from hand-to-hand combat, martial arts and the use of weaponry to the use of alarms and evasive driving techniques and many areas in-between. This brief provides a high-level introduction to personal defense and offers two important concepts central to any personal protection program. The concepts are "defense in depth" and the three stages of personal protection: awareness, avoidance and defense.</p>
9	Travel Security	<p>Travel is an integral part of our personal and professional lives. With world events and political environments rapidly changing, travelers need to exercise an increased amount of caution and take security precautions to reduce their risks. Recent political events throughout the world have changed--but not necessarily diminished--the threats you face. We will provide information about security related to travel, and preparing for and reacting to crises and emergencies while traveling. Post-September 11, several measures have been considered to improve aviation security. While air transportation security has been increased, you still have to deal with the risks on the ground. This training brief will provide you with information and tips to decrease your risks while traveling.</p> <p>Note: Technolytics provides ½ day training program on travel security as part of our corporate security suite of products and services. In addition, you should also complete the Personal Security Training Brief.</p>

10	Situational Awareness	Situational Awareness (SA) defined at the very basic level means to be aware of one's immediate environment and be prepared to take action. One of the underlying principles of personal SA is that the environment you are in controls your needed level of awareness. In any heightened threat situation, you will be looking for threat indicators that signal possible danger. Situational Awareness should be viewed as a normal extension of the biological fight or flight physiological system hardwired into everyone—not something to keep you fearful or borderline paranoid.
----	-----------------------	--

Specialty CD 5 – Personal Protection for Corporate Executives

Corporate executives make numerous decisions during each business day. These decisions frequently result in unpopular circumstances for groups and individuals. Many times these decisions are questioned and met with resentment and anger. Because of the pressure put on corporations to succeed at all costs, corporate executives are now in the spotlight and under increased scrutiny. In view of this increased scrutiny, executives must become increasingly aware of the threats they face. In response to these threats and concerns raised by executives, Spy-Ops has created an executive level training program to help reduce the risk from the daily threats corporate executives face. The program has been specifically designed to help train and educate individuals on areas important to them individually, and in their role as a corporate executive.

The program is delivered on CD or electronically, and includes ten modules that take approximately 20 hours to complete. Once you pass all ten exams, you will receive a Certificate in Personal Protection.

FACT: *Corporate executives are in the public eye. As such they place themselves at risk due to decisions they make daily.*

Cost of Program: \$99.95

#	Title	Abstract
1	Corporate Espionage	Corporate espionage is the dirty little secret of global business. Espionage activities are often masked under the title of competitive intelligence. But in the end, thieves or spies still acquire sensitive, restricted information assets of another entity, which may include product designs, business models, marketing plans, research and development files, customer lists, employee lists, pricing strategies and other intellectual property. This module will provide a basic understanding of the current state of corporate espionage, as well as illustrate many techniques used in committing this new type of crime.
2	Electronic Bugging	This course provides a brief overview of electronic bugging. Espionage is the art of covertly obtaining information of value about another entity. Advances in electronics have made this easier and more economical than ever. Everyone who has information that is valuable to another individual, organization or government is at risk. This module provides an introduction to electronic bugging devices, what to look for, and most importantly the "Do's and Don'ts" for when you find electronic surveillance devices.
3	Digital Footprints	The world enjoys unlimited benefits from new technologies in an electronic world. But those 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 training brief will provide an understanding of digital footprints, their dangers and what the consequences are for all of us.

4	Identity Theft	<p>Identity theft crimes range from purse snatchings to kingpin-style fraud rings. The definition of identity theft is a crime in which an imposter obtains key pieces of personal information, such as a Social Security number, in order to impersonate someone else. Identity theft can occur when someone takes your mail, steals your wallet or swipes your records from an institution. Terrorists have a long history of assuming other individual's identities and have seized upon the use of information technology as a tool in their terrorist activities. In an article published on September 22nd, 2001 by the Times LTD titled "Terrorists' Trade in Stolen Identities" it discusses how Osama bin Laden had carefully created impostors and how his agents stole the identities and life histories of at least a dozen Western-educated young men who were all murdered in 1990. Every document and record of those men's lives were either stolen or doctored to allow the terrorists to move freely around the world. This training brief will provide a solid understanding of identity theft and implications associated with this crime.</p>
5	Extremist Groups	<p>This training brief will dissect the complex world of the extremist group. Although there are numerous individuals and interlaced groups throughout the world, we will try to look into a basic model of the psychopathology of hate groups in general. We will also look into how this model is being used to try to control hate crimes committed by such groups.</p>
6	Terrorism – Strategies & Tactics	<p>Terrorism is a fact of life and a force with which we must deal. Terrorism has impacted our business, social, political and personal lives in numerous ways. When you mention terrorism one thing is certain, there is little agreement on what exactly constitutes terrorism and terrorist activities. Generally, terrorism is a tactic used to influence the activities of one entity by another entity with an opposing view, opinion, value or culture and is used in times of peace, conflict and war. Groups employ terrorist violence in the name of many causes. The threat of terrorism is ever present, and an attack is likely to occur when least expected. Terrorism is unconventional warfare. There are no fronts, no armies, and no battlefields. This training module will provide a basic understanding of terrorism.</p>
7	Surveillance	<p>This brief will describe the purpose for using surveillance, how surveillance is conducted, how surveillance can be countered, and when surveillance should be employed. We will list and explain a number of types of surveillance and the technology that is available. We will also discuss an emerging technology that will provide new and unique capabilities for the intelligence community.</p>
8	Personal Protection	<p>Personal protection is critical in today's society. Home invasions, assaults, rapes, kidnappings, extortion, and carjackings are all too common in today's news headlines. Individuals must take steps to reduce the risk of becoming a victim to these crimes. Today you have about a 1 in 100 chance of becoming a victim of a violent crime. History has shown that criminals and terrorists single out businessmen and/or their families who fit a particular profile. Understanding how not to fit the profile is the first step in protecting yourself and your loved ones. Apparent power, influence and wealth create the highest risk scenario for executives and their families. Where you work, what you drive and where you live are all risk factors to be considered.</p> <p>Many individuals rely on self-defense courses as the primary way they choose to prepare. Personal protection is a broad area that covers everything from hand-to-hand combat, martial arts and the use of weaponry to the use of alarms and evasive driving techniques and many areas in-between. This brief provides a high-level introduction to personal defense and offers two important concepts central to any personal protection program. The concepts are "defense in depth" and the three stages of personal protection: awareness, avoidance and defense.</p>

9	Travel Security	Travel is an integral part of our personal and professional lives. With world events and political environments rapidly changing, travelers need to exercise an increased amount of caution and take security precautions to reduce their risks. Recent political events throughout the world have changed--but not necessarily diminished--the threats you face. We will provide information about security related to travel, and preparing for and reacting to crises and emergencies while traveling. Post-September 11, several measures have been considered to improve aviation security. While air transportation security has been increased, you still have to deal with the risks on the ground. This training brief will provide you with information and tips to decrease your risks while traveling.
10	Situational Awareness	Situational Awareness (SA) defined at the very basic level means to be aware of one's immediate environment and be prepared to take action. One of the underlying principles of personal SA is that the environment you are in controls your needed level of awareness. In any heightened threat situation, you will be looking for threat indicators that signal possible danger. Situational Awareness should be viewed as a normal extension of the biological fight or flight physiological system hardwired into everyone—not something to keep you fearful or borderline paranoid.

Specialty CD 6 – Advanced Security Services for Private Security Guards

A significant amount of the nation's critical infrastructure is protected by private security forces. In the eyes of most customers, these private security forces require additional training in several areas to provide adequate protection. Customers and employers are now examining training when evaluating suppliers of security guard services. Advanced Security Services for Private Security Guards will prepare you to work in the security industry, in such areas as corporate security, security consulting and private protection, as well as for specialization within the multi-faceted field of private security.

In response to new threats, and in collaboration with the Technolytics Institute, we have created this training program. The program is delivered on CD and includes ten modules that take about 20 hours to complete. Once you pass all ten exams, you will receive a Certificate in Protective Services.

FACT: 85% of the infrastructure in the United States is privately owned. Security services are on the front line providing protections for these and other assets.

Program Cost: \$99.95

#	Title	Abstract
1	Corporate Espionage	Corporate espionage is the dirty little secret of global business. Espionage activities are often masked under the title of competitive intelligence. But in the end, thieves or spies still acquire sensitive, restricted information assets of another entity, which may include product designs, business models, marketing plans, research and development files, customer lists, employee lists, pricing strategies and other intellectual property. This module will provide a basic understanding of the current state of corporate espionage, as well as illustrate many techniques used in committing this new type of crime.

2	Islamist Terrorism	<p>Terrorism has become a reality of American life. We have purposely focused this brief on Islamic terrorism, and specifically groups posing a real and present danger to the United States. There are other groups, some not motivated by Islamic religious beliefs that pose immediate danger in their section of the world and future briefs will expound on these threats.</p> <p>Counter-terrorism professionals say the greatest threat from Islamic terrorists is a group using Weapons of Mass Destruction (WMD) against an American city that results in massive destruction and loss of life. While the majority of U.S. counter-terrorism efforts are aimed at Islamist terror, domestic terror groups like Earth Liberation Front (ELF) and (apparent) lone wolves like the Unabomber and Oklahoma City bombers continue to kill and maim innocent citizens. While Al-Qaeda is the most well-know organization of Islamist terror, Hezbollah and Hamas provide counter-terror professionals with plenty of sleepless nights due to their lethal operations and capabilities. There is a wealth of resources available on the internet to both understand and track the terrorist threat.</p>
3	Dirty Bombs	<p>This course introduces Radiological or “Dirty” Bombs. A dirty bomb has a conventional high-explosive core surrounded by radiological material in a solid, gas or liquid form. It is not to be confused with a fission weapon such as the bombs used during WWII. The primary lethality of a dirty bomb depends on the type and amount of radioactive material, and the dispersal factors such as wind speed and blast location. The ease of construction and availability of radiological material make the dirty bomb’s use inevitable by terrorist groups.</p>
4	Biological Weapons	<p>Biological warfare (BW), also known as germ warfare, is the use of any living organism, whether bacteria, virus, or other replicative protein as a weapon of warfare. The use of biological weapons poses one of the greatest threats civilization is likely to face as Islamist or other extremist groups collude with states to obtain biological agents. One of the greatest problems in detecting the manufacture of biological weapons is that almost all equipment needed for the production of biological agents (also referred to as pathogens and toxins) is dual use (used in the production of drugs and vaccines) and available on the international market, thus increasing the potential for concealing illicit activities under the cover of legitimate production.</p>
5	Chemical Weapons	<p>This brief introduces chemical weapons as they relate to possible use by terrorists against civilian non-combatants. It is not intended to be an exhaustive study of chemical weapons for military use but a high-level introduction. In a pre 9/11 study, the Center for Disease Control (CDC) listed several categories of chemical weapons whose use by terrorists presented a “threat.” Among these are nerve, blood, pulmonary and incapacitating agents.</p> <p>Chemical agents conjure up horrible images, as death comes in seconds after exposure to most of these agents. However, mass casualty situations are hard to predict. This is because of dispersion factors such as wind, temperature, air pressure, length of exposure and chemical characteristics associated with these and other variables. Many of these chemicals are readily available and their use by terrorist groups is probably inevitable.</p>

6	Security Systems	Security Systems (also called alarm systems) have gotten extremely sophisticated since the advent of the microprocessor (computer chip). Today's systems offer a myriad of optional sensors, signaling devices and control options that were not available just a few years ago. Most systems offer the capability to communicate with a remote monitoring station, where operators are on duty 24 hours a day to dispatch the appropriate authorities to the alarm location if a break-in or emergency arises. This training brief will cover the basics of security systems.
7	Improvised Explosive Devices	This course is a high-level introduction to Improvised Explosive Devices (IEDs). An IED is any explosive device that has been rigged by its builder to detonate and cause death and injury through blast, shrapnel, fire or release of chemicals or bio-toxins. While IEDs have gained prominence through their daily use by insurgents in Iraq, armies and unconventional warfare practitioners have used the booby trap version IED for many years. Vehicle Borne Improvised Explosive Devices (VBIEDs) and Suicide IEDs pose significant problems to counter-terror professionals, due to their ease of manufacture, ability to be hidden in obvious places without detection, and seemingly endless supply of martyrs willing to blow themselves up in attacks.
8	Extremist Groups	This training brief will dissect the complex world of the extremist group. Although there are numerous individuals and interlaced groups throughout the world, we will try to look into a basic model of the psychopathology of hate groups in general. We will also look into how this model is being used to try to control hate crimes committed by such groups.
9	Terrorism – Strategies & Tactics	Terrorism is a fact of life and a force with which we must deal. Terrorism has impacted our business, social, political and personal lives in numerous ways. When you mention terrorism one thing is certain, there is little agreement on what exactly constitutes terrorism and terrorist activities. Generally, terrorism is a tactic used to influence the activities of one entity by another entity with an opposing view, opinion, value or culture and is used in times of peace, conflict and war. Groups employ terrorist violence in the name of many causes. The threat of terrorism is ever present, and an attack is likely to occur when least expected. Terrorism is unconventional warfare. There are no fronts, no armies, and no battlefields. This training module will provide a basic understanding of terrorism.
10	Corporate and Industrial Terrorism	Corporate & Industrial terrorism costs U.S. businesses billions of dollars each year and the threats continue to grow in frequency and sophistication. From left wing domestic terrorists like Earth Liberation Front (ELF) to global terrorists like al-Qaida, the challenges to a company's security have been redefined. Top-notch corporate security should no longer viewed as an expense, but as a necessity — a cost-saving, asset preserving investment that needs to be reviewed on an on-going basis.

Specialty CD 7 – Private Investigation Services

The demand for private investigative services is expected to exceed \$50 billion in the U.S. market by 2010. Despite varying crime rates, many perceive a high risk of crime and harbor a belief that public safety officials are overburdened and ill prepared for hi-tech crimes. These perceptions, as well as the perceived risk from non-traditional threats such as cyber criminals, white collar crimes and terrorism, present significant opportunities for private investigative services. The winners and losers will be determined by the quality of the individuals who perform these services. The challenge is how do you keep up with the ever changing threat environment, new technologies and emerging techniques? The answer is the Spy-Ops continuing education certificate program in private investigation services. This ten module program covers the topics you need to stay abreast of the changes in crime, threats and technology. The program is delivered on CD or electronically, and takes approximately 20 hours to complete. Once you pass all ten exams, you will receive a Certificate in Private Investigation.

FACT: *The use of private investigative services is growing rapidly. However, the demand is greatest for those with education and experience in the latest crime and espionage techniques.*

Program Cost: \$99.95

#	Title	Abstract
1	Corporate Espionage	Corporate espionage is the dirty little secret of global business. Espionage activities are often masked under the title of competitive intelligence. But in the end, thieves or spies still acquire sensitive, restricted information assets of another entity, which may include product designs, business models, marketing plans, research and development files, customer lists, employee lists, pricing strategies and other intellectual property. This module will provide a basic understanding of the current state of corporate espionage, as well as illustrate many techniques used in committing this new type of crime.
2	Human Intelligence Techniques	This brief will explore a portion of the large world of human intelligence. It will define what is meant by the term for spy purposes. It will explore different ways that one approaches gathering valuable information and what that information might be used for.
3	Digital Spying	In this brief, you will look into the world of spyware from all angles. You will see what it is and how it is used. In addition, you will be able to tell how it is being used on you. You will also learn how to protect yourself from being a victim of spyware and, if you already are a victim, how to get rid of it and protect yourself in the future.
4	Interrogation	Interrogation is a critical tool when it comes to gathering intelligence. Selecting the wrong technique can ruin the chance to gain valuable information that can be turned into intelligence. Likewise, poorly using a technique can have the same dire consequences. Interrogation techniques have been studied and developed over the years. In addition new technology has been tightly coupled to interrogation to enhance our ability to detect deceptive practices by those being pumped for information. In this brief we will explore several facets of interrogation. We will discover that interrogation is not simply a method of questioning, but a skill that is hard to learn. We will look at the abilities that a skilled interrogator possesses and what he or she must do in order to complete a thorough interrogation.

5	Improvised Explosive Devices	This course is a high-level introduction to Improvised Explosive Devices (IEDs). An IED is any explosive device that has been rigged by its builder to detonate and cause death and injury through blast, shrapnel, fire or release of chemicals or bio-toxins. While IEDs have gained prominence through their daily use by insurgents in Iraq, armies and unconventional warfare practitioners have used the booby trap version IED for many years. Vehicle Borne Improvised Explosive Devices (VBIEDs) and Suicide IEDs pose significant problems to counter-terror professionals, due to their ease of manufacture, ability to be hidden in obvious places without detection, and seemingly endless supply of martyrs willing to blow themselves up in attacks.
6	Digital Footprints	The world enjoys unlimited benefits from new technologies in an electronic world. But those 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 training brief will provide an understanding of digital footprints, their dangers and what the consequences are for all of us.
7	Identity Theft	Identity theft crimes range from purse snatchings to kingpin-style fraud rings. The definition of identity theft is a crime in which an imposter obtains key pieces of personal information, such as a Social Security number, in order to impersonate someone else. Identity theft can occur when someone takes your mail, steals your wallet or swipes your records from an institution. Terrorists have a long history of assuming other individual's identities and have seized upon the use of information technology as a tool in their terrorist activities. In an article published on September 22nd, 2001 by the Times LTD titled "Terrorists' Trade in Stolen Identities" it discusses how Osama bin Laden had carefully created impostors and how his agents stole the identities and life histories of at least a dozen Western-educated young men who were all murdered in 1990. Every document and record of those men's lives were either stolen or doctored to allow the terrorists to move freely around the world. This training brief will provide a solid understanding of identity theft and implications associated with this crime.
8	White-Collar Crime	This training brief will explore the world of white-collar crime. It will look into the broad definition of the term and the most common ways it is exhibited. It will also reveal how government and law enforcement officials are trying to control and prevent these crimes from being committed. Additionally, the brief will discuss how one can protect themselves from becoming a victim.
9	Forensic DNA Identification	This training brief will explore the use of DNA in the world of forensic science. It will look at DNA as a key tool in human identification and the role it plays in solving many types of crimes. Finally, it will open up how DNA procedures have improved in recent history and what scientific advances we can expect in the near future.
10	Computer Crime	In this training brief, we will examine the constantly evolving world of computer crimes and define a broad base of current types of crimes. We will also look at what the government is doing in an attempt to control these crimes. Finally, we will suggest some options for how individuals can protect themselves from becoming victims of such crimes.

Specialty CD 8 – Executive Protection Services

Executive Protection Services for individuals, politicians, executives, celebrities, diplomats, world leaders, and other public figures from people who might want to interfere with them is growing rapidly. As the current culture continues to grow more violent, and with increasing terrorism and risks, it is imperative for individuals and companies to choose qualified professionals to provide protection to executives. The decision often relies not just on experience, but continuous improvement and updating of the security provider's education. Spy-Ops is uniquely qualified to provide the continuous education you need in the ever changing risk environment. We like many others believe in "brains before brawn" and that the modern day Executive Protection Specialist bares no resemblance to the old fashioned "Bodyguard" of the past. Gain the knowledge you need to protect clients. Understand new threats. Train for the future with our ten module certificate program. The program is delivered on CD or electronically, and includes ten modules that take approximately 20 hours to complete. Once you pass all ten exams, you will receive a Certificate in Protective Services.

FACT: Due to the enormous risks executive face today, the demand for executive protection services is growing rapidly. The competitive difference between firms in this space is the education of those providing the protection.

Program Cost: \$99.95

#	Title	Abstract
1	Corporate Espionage	Corporate espionage is the dirty little secret of global business. Espionage activities are often masked under the title of competitive intelligence. But in the end, thieves or spies still acquire sensitive, restricted information assets of another entity, which may include product designs, business models, marketing plans, research and development files, customer lists, employee lists, pricing strategies and other intellectual property. This module will provide a basic understanding of the current state of corporate espionage, as well as illustrate many techniques used in committing this new type of crime.
2	Body Armor	This brief will examine the aspects of protection provided by forms of body armor. It will look at both hard and soft body armor and take a brief glance at situations in which both are used. The composition of materials and the construction of soft and hard body armors will be reviewed. In addition, we will see how body armor not only stops a blow from penetrating the body of the protected person, but disperses the force so that blunt trauma is minimized.
3	Armored Vehicles	This brief will explore the various types of armored vehicles in use today. It will present both civil and military category situations in which such vehicles are in use. It will also look into the use of armored protection in the three main categories of physical transportation: air, land and sea. You will broaden your knowledge around the type of materials used to create a protective surface in armored vehicles and learn when certain materials are more beneficial than others.
4	Digital Spying	In this brief, you will look into the world of spyware from all angles. You will see what it is and how it is used. In addition, you will be able to tell how it is being used on you. You will also learn how to protect yourself from being a victim of spyware and, if you already are a victim, how to get rid of it and protect yourself in the future.

5	Islamist Terrorism	<p>Terrorism has become a reality of American life. We have purposely focused this brief on Islamic terrorism, and specifically groups posing a real and present danger to the United States. There are other groups, some not motivated by Islamic religious beliefs that pose immediate danger in their section of the world and future briefs will expound on these threats.</p> <p>Counter-terrorism professionals say the greatest threat from Islamic terrorists is a group using Weapons of Mass Destruction (WMD) against an American city that results in massive destruction and loss of life. While the majority of U.S. counter-terrorism efforts are aimed at Islamist terror, domestic terror groups like Earth Liberation Front (ELF) and (apparent) lone wolves like the Unabomber and Oklahoma City bombers continue to kill and maim innocent citizens. While Al-Qaeda is the most well-know organization of Islamist terror, Hezbollah and Hamas provide counter-terror professionals with plenty of sleepless nights due to their lethal operations and capabilities. There is a wealth of resources available on the internet to both understand and track the terrorist threat.</p>
6	Long Range Microphones	<p>Long range microphones have been in use for decades. With advances in electronics, noise elimination technology and digital audio processing, this stand-off surveillance device is an effective way to gain intelligence. It should be noted that these devices do not require a warrant for their use. This course will explore the world of long range microphones. It will look at their components, and the details of how they work. It will also look at situations in which long range microphones may be needed or beneficial.</p>
7	Security Systems	<p>Security Systems (also called alarm systems) have gotten extremely sophisticated since the advent of the microprocessor (computer chip). Today's systems offer a myriad of optional sensors, signaling devices and control options that were not available just a few years ago. Most systems offer the capability to communicate with a remote monitoring station, where operators are on duty 24 hours a day to dispatch the appropriate authorities to the alarm location if a break-in or emergency arises. This training brief will cover the basics of security systems.</p>
8	Improvised Explosive Devices	<p>This course is a high-level introduction to Improvised Explosive Devices (IEDs). An IED is any explosive device that has been rigged by its builder to detonate and cause death and injury through blast, shrapnel, fire or release of chemicals or bio-toxins. While IEDs have gained prominence through their daily use by insurgents in Iraq, armies and unconventional warfare practitioners have used the booby trap version IED for many years. Vehicle Borne Improvised Explosive Devices (VBIEDs) and Suicide IEDs pose significant problems to counter-terror professionals, due to their ease of manufacture, ability to be hidden in obvious places without detection, and seemingly endless supply of martyrs willing to blow themselves up in attacks.</p>
9	Digital Footprints	<p>The world enjoys unlimited benefits from new technologies in an electronic world. But those 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 training brief will provide an understanding of digital footprints, their dangers and what the consequences are for all of us.</p>
10	Corporate & Industrial Terrorism	<p>Computer hacking, or cracking, has grown to pandemic proportions and costs businesses and governments billions of dollars in on-going computer security and countermeasure efforts. Far from its beginnings, with computer geeks breaking the security of networks, applications or communications systems, black hat hackers are now using their knowledge to commit computer crimes such as identity theft and credit card fraud. Terrorists and foreign intelligence and military personnel hack and crack to gain intelligence, conduct cyber warfare or engage in electronic sabotage.</p>

Specialty CD 9 – Personal Protection for Individuals

“It can’t happen to me” and “if it’s going to happen, it’s going to happen” is extremely dangerous thinking. Recent political events throughout the world have changed the threats you face. A criminal attack against you or your family can take place at any time, as can a fire or other disaster. However, you can influence what happens to you by assuming more responsibility for your own security. Don’t just become a victim. Invest in your and your family’s security. Get a certificate in personal protection for you and the ones you love. The Personal Protection for Individuals program is delivered on CD or electronically, and includes ten modules that take approximately 20 hours to complete. Once you pass all ten exams, you will receive a Certificate in Personal Protection.

FACT: *The world is a dangerous place. Whether at home or traveling, individuals need to be aware of the risks they face and know how to protect themselves and their families from these threats.*

Program Cost: \$99.95

#	Title	Abstract
1	Digital Spying	In this brief, you will look into the world of spyware from all angles. You will see what it is and how it is used. In addition, you will be able to tell how it is being used on you. You will also learn how to protect yourself from being a victim of spyware and, if you already are a victim, how to get rid of it and protect yourself in the future.
2	Electronic Bugging	This course provides a brief overview of electronic bugging. Espionage is the art of covertly obtaining information of value about another entity. Advances in electronics have made this easier and more economical than ever. Everyone who has information that is valuable to another individual, organization or government is at risk. This module provides an introduction to electronic bugging devices, what to look for, and most importantly the “Do’s and Don’ts” for when you find electronic surveillance devices.
3	Digital Footprints	The world enjoys unlimited benefits from new technologies in an electronic world. But those 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 training brief will provide an understanding of digital footprints, their dangers and what the consequences are for all of us.
4	Identity Theft	Identity theft crimes range from purse snatchings to kingpin-style fraud rings. The definition of identity theft is a crime in which an imposter obtains key pieces of personal information, such as a Social Security number, in order to impersonate someone else. Identity theft can occur when someone takes your mail, steals your wallet or swipes your records from an institution. Terrorists have a long history of assuming other individual’s identities and have seized upon the use of information technology as a tool in their terrorist activities. In an article published on September 22nd, 2001 by the Times LTD titled “Terrorists’ Trade in Stolen Identities” it discusses how Osama bin Laden had carefully created impostors and how his agents stole the identities and life histories of at least a dozen Western-educated young men who were all murdered in 1990. Every document and record of those men’s lives were either stolen or doctored to allow the terrorists to move freely around the world. This training brief will provide a solid understanding of identity theft and implications associated with this crime.

5	Terrorism – Strategies & Tactics	Terrorism is a fact of life and a force with which we must deal. Terrorism has impacted our business, social, political and personal lives in numerous ways. When you mention terrorism one thing is certain, there is little agreement on what exactly constitutes terrorism and terrorist activities. Generally, terrorism is a tactic used to influence the activities of one entity by another entity with an opposing view, opinion, value or culture and is used in times of peace, conflict and war. Groups employ terrorist violence in the name of many causes. The threat of terrorism is ever present, and an attack is likely to occur when least expected. Terrorism is unconventional warfare. There are no fronts, no armies, and no battlefields. This training module will provide a basic understanding of terrorism.
6	Surveillance	This brief will describe the purpose for using surveillance, how surveillance is conducted, how surveillance can be countered, and when surveillance should be employed. We will list and explain a number of types of surveillance and the technology that is available. We will also discuss an emerging technology that will provide new and unique capabilities for the intelligence community.
7	Gang Activity	This brief will look at the make-up and activities of gangs. It will define what a gang is and look into how it influences the people involved in their activities as well as society as a whole.
8	Personal Protection	<p>Personal protection is critical in today's society. Home invasions, assaults, rapes, kidnappings, extortion, and carjackings are all too common in today's news headlines. Individuals must take steps to reduce the risk of becoming a victim to these crimes. Today you have about a 1 in 100 chance of becoming a victim of a violent crime. History has shown that criminals and terrorists single out businessmen and/or their families who fit a particular profile. Understanding how not to fit the profile is the first step in protecting yourself and your loved ones. Apparent power, influence and wealth create the highest risk scenario for executives and their families. Where you work, what you drive and where you live are all risk factors to be considered.</p> <p>Many individuals rely on self-defense courses as the primary way they choose to prepare. Personal protection is a broad area that covers everything from hand-to-hand combat, martial arts and the use of weaponry to the use of alarms and evasive driving techniques and many areas in-between. This brief provides a high-level introduction to personal defense and offers two important concepts central to any personal protection program. The concepts are "defense in depth" and the three stages of personal protection: awareness, avoidance and defense.</p>
9	Travel Security	<p>Travel is an integral part of our personal and professional lives. With world events and political environments rapidly changing, travelers need to exercise an increased amount of caution and take security precautions to reduce their risks. Recent political events throughout the world have changed--but not necessarily diminished--the threats you face. We will provide information about security related to travel, and preparing for and reacting to crises and emergencies while traveling. Post-September 11, several measures have been considered to improve aviation security. While air transportation security has been increased, you still have to deal with the risks on the ground. This training brief will provide you with information and tips to decrease your risks while traveling.</p> <p>Note: Technolytics provides ½ day training program on travel security as part of our corporate security suite of products and services. In addition, you should also complete the Personal Security Training Brief.</p>

10	Situational Awareness	Situational Awareness (SA) defined at the very basic level means to be aware of one's immediate environment and be prepared to take action. One of the underlying principles of personal SA is that the environment you are in controls your needed level of awareness. In any heightened threat situation, you will be looking for threat indicators that signal possible danger. Situational Awareness should be viewed as a normal extension of the biological fight or flight physiological system hardwired into everyone—not something to keep you fearful or borderline paranoid.
----	-----------------------	--

Specialty CD 10 – Educator Threat Awareness

It seems you can not pick up a paper or log on to the web without news of another incident occurring at a school. Violence, drugs, gangs and the threat of terrorism in our schools has educators concerned. They are concerned not only for their students but also their own personal security. This program provides a basic understanding of 14 key areas that are all related to educator threat awareness.

In response to the needs of educators, and in collaboration with the Technolytics Institute, Spy-Ops has created the Educator Threat Awareness training program. The program is delivered on CD or electronically, and includes fourteen modules that, in its entirety, take about 28 hours to complete. Once you pass all fourteen exams, you will receive a Certificate in Educator Threat Awareness.

FACT: *School violence is now a foreseeable threat, and as such, educators and administrative staff must be trained to spot potential problems as well as respond to issues as they arise.*

Program Cost: \$99.95

#	Title	Abstract
1	School Violence	While America braces for violence from outside our borders, we must prepare now for the possibility of violent acts taking place where children are learning – schools and the areas around them. Every day we witness violence in our schools or on our school campuses. When you consider gangs, drugs, guns, violent attacks, and child exploitation, it is no wonder why many of our teachers are feeling overwhelmed and not in control of their classroom or school environment. Teachers are trained to teach students and are often not prepared to deal with violence or criminal acts. Many believe the situations listed above are a major contributing reason for underperforming students and even entire schools. This training brief informs educators and other administrative staff about the current state of the threats that they face both inside and outside of the classroom.
2	On-Line Child Exploitation	Child exploitation is not new; it has been occurring for years. Each day our children are exposed to this hideous risk. The internet has provided the mechanism that created the infrastructure that has allowed this industry to explode over the past decade. Today, child exploitation is a \$20+ billion international industry that ruins the lives of our children. The problem is not just found online. There are organizations that arrange complete travel packages for adults to travel abroad for the sole purpose of having sex with children in other countries. This training brief will provide a basic understanding of the problem, the signs of sexual exploitation, a profile of the sexual predators, and suggest ways to protect the children.

3	Cyber-bullying	<p>Our school systems are under attack and face numerous risks. One risk that is rapidly becoming a critical issue is that of bullying. Today, bullying has taken on a new and perhaps even more sinister form. Through the use of technology (cell phones and computers), young people are threatened, harassed, and embarrassed in ways that go beyond the realm of acceptable school behavior. The use of computers and cell phones to attack a student causes young people to become anxious, depressed and angry, and there have been numerous incidents where they have released that anger in the form of violent acts.</p> <p>Many experts believe that cyber-bullying is a major contributing factor as to why students may perform poorly in school or harm themselves and others. Educators need to become aware of this evolving issue in order to protect themselves and their students. Cyber-harassment is a crime. It is just as lethal as robbery, rape or murder. It destroys lives and reputations. It is not First Amendment protected and supports moral and ethical bankruptcy. This training brief informs educators and parents about the current state of cyber-bullying and how to recognize the behavior and prevent future attacks.</p>
4	Gang Activity	<p>This brief will look at the make-up and activities of gangs. It will define what a gang is and look into how it influences the people involved in their activities as well as society as a whole.</p>
5	Domestic Terrorism	<p>Domestic Terrorism is loosely defined as terrorist actions originating from persons and influences within a country as opposed to outside influences or persons. Throughout the Clinton administration, domestic terrorism was erroneously seen as a greater threat than Islamic terrorism. Predictably, the Clinton administration focused on right wing terrorism just as President Nixon had focused on left wing terrorism during his administration. Counter-terrorism and law enforcement professionals agree that it is only a matter of time before a domestic terrorism group eventually exceeds the death and destruction caused by Timothy McVeigh in Oklahoma City.</p>
6	Extremist Groups	<p>This training brief will dissect the complex world of the extremist group. Although there are numerous individuals and interlaced groups throughout the world, we will try to look into a basic model of the psychopathology of hate groups in general. We will also look into how this model is being used to try to control hate crimes committed by such groups.</p>
7	Islamist Terrorism	<p>Terrorism has become a reality of American life. We have purposely focused this brief on Islamic terrorism, and specifically groups posing a real and present danger to the United States. There are other groups, some not motivated by Islamic religious beliefs that pose immediate danger in their section of the world and future briefs will expound on these threats.</p> <p>Counter-terrorism professionals say the greatest threat from Islamic terrorists is a group using Weapons of Mass Destruction (WMD) against an American city that results in massive destruction and loss of life. While the majority of U.S. counter-terrorism efforts are aimed at Islamist terror, domestic terror groups like Earth Liberation Front (ELF) and (apparent) lone wolves like the Unabomber and Oklahoma City bombers continue to kill and maim innocent citizens. While Al-Qaeda is the most well-know organization of Islamist terror, Hezbollah and Hamas provide counter-terror professionals with plenty of sleepless nights due to their lethal operations and capabilities. There is a wealth of resources available on the internet to both understand and track the terrorist threat.</p>

8	Terrorist Recognition	In this training brief, the process of recognizing terrorists will be explored. We will explore some of the features that seem to be a common thread in known and suspected terrorists. We will look at how the characterization of terrorists via profiling is currently done and how the information is then used. We will also look into the recent changes to terrorist profiling and why the changes were necessary.
9	International Drug Trafficking	International crime is a growing threat to the way of life in our country. This brief will look at one of the major types of international crime; one that is labeled as a significant threat to the lives and property of Americans: drug trafficking. It will also address what is being done to control this threat.
10	Dirty Bombs	This course introduces Radiological or "Dirty" Bombs. A dirty bomb has a conventional high-explosive core surrounded by radiological material in a solid, gas or liquid form. It is not to be confused with a fission weapon such as the bombs used during WWII. The primary lethality of a dirty bomb depends on the type and amount of radioactive material, and the dispersal factors such as wind speed and blast location. The ease of construction and availability of radiological material make the dirty bomb's use inevitable by terrorist groups.
11	Biological Weapons	Biological warfare (BW), also known as germ warfare, is the use of any living organism, whether bacteria, virus, or other replicative protein as a weapon of warfare. The use of biological weapons poses one of the greatest threats civilization is likely to face as Islamist or other extremist groups collude with states to obtain biological agents. One of the greatest problems in detecting the manufacture of biological weapons is that almost all equipment needed for the production of biological agents (also referred to as pathogens and toxins) is dual use (used in the production of drugs and vaccines) and available on the international market, thus increasing the potential for concealing illicit activities under the cover of legitimate production.
12	Chemical Weapons	<p>This brief introduces chemical weapons as they relate to possible use by terrorists against civilian non-combatants. It is not intended to be an exhaustive study of chemical weapons for military use but a high-level introduction. In a pre 9/11 study, the Center for Disease Control (CDC) listed several categories of chemical weapons whose use by terrorists presented a "threat." Among these are nerve, blood, pulmonary and incapacitating agents.</p> <p>Chemical agents conjure up horrible images, as death comes in seconds after exposure to most of these agents. However, mass casualty situations are hard to predict. This is because of dispersion factors such as wind, temperature, air pressure, length of exposure and chemical characteristics associated with these and other variables. Many of these chemicals are readily available and their use by terrorist groups is probably inevitable.</p>
13	Improvised Explosive Devices	This course is a high-level introduction to Improvised Explosive Devices (IEDs). An IED is any explosive device that has been rigged by its builder to detonate and cause death and injury through blast, shrapnel, fire or release of chemicals or bio-toxins. While IEDs have gained prominence through their daily use by insurgents in Iraq, armies and unconventional warfare practitioners have used the booby trap version IED for many years. Vehicle Borne Improvised Explosive Devices (VBIEDs) and Suicide IEDs pose significant problems to counter-terror professionals, due to their ease of manufacture, ability to be hidden in obvious places without detection, and seemingly endless supply of martyrs willing to blow themselves up in attacks.

14 Bonus Brief	Personal Protection	<p>Personal protection is critical in today's society. Home invasions, assaults, rapes, kidnappings, extortion, and carjackings are all too common in today's news headlines. Individuals must take steps to reduce the risk of becoming a victim to these crimes. Today you have about a 1 in 100 chance of becoming a victim of a violent crime. History has shown that criminals and terrorists single out businessmen and/or their families who fit a particular profile. Understanding how not to fit the profile is the first step in protecting yourself and your loved ones. Apparent power, influence and wealth create the highest risk scenario for executives and their families. Where you work, what you drive and where you live are all risk factors to be considered.</p> <p>Many individuals rely on self-defense courses as the primary way they choose to prepare. Personal protection is a broad area that covers everything from hand-to-hand combat, martial arts and the use of weaponry to the use of alarms and evasive driving techniques and many areas in-between. This brief provides a high-level introduction to personal defense and offers two important concepts central to any personal protection program. The concepts are "defense in depth" and the three stages of personal protection: awareness, avoidance and defense.</p>
----------------------	------------------------	--

Specialty CD 11 – Anti-Money Laundering

When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention.

In response to mounting concern over money laundering, the Patriot Act requires that all financial institutions and businesses take measures to identify and report possible money laundering and terrorist financial transactions. Included in this legislation is a requirement for ongoing training. The program addresses money laundering, sources of funds laundered, as well as terrorism financing and more. The program is delivered on CD or electronically, and includes seven modules that take about 14 hours to complete. Once you pass all seven exams, you will receive a Certificate in Anti-Money Laundering.

FACT: Individuals and companies may become an unwilling participant in money laundering. Without proper education that covers the latest techniques used, individuals and organizations are placing themselves at great risk.

Program Cost: \$59.95

#	Title	Abstract
1	Money Laundering	This training brief will define what money laundering is, walk through how it is accomplished, and examine the layers involved. The different ways money laundering effects our world will also be explored. Finally, the two necessary components required if governments are to have any hopes of controlling this area of crime will be reviewed. Although money laundering and financing terrorism are closely related, this brief addresses only money laundering. Financing terrorism is covered in a separate training brief.

2	Tracking Terrorist Financing	This brief will explore the domain of terrorist financing. It will reveal what activities are involved in raising money for terrorist activities and how money is filtered back to the terrorist groups. It will explore the methods and the tools that the government is using to track such activities and look into the benefits of the information gained from tracking their financing patterns.
3	White-Collar Crime	This training brief will explore the world of white-collar crime. It will look into the broad definition of the term and the most common ways it is exhibited. It will also reveal how government and law enforcement officials are trying to control and prevent these crimes from being committed. Additionally, the brief will discuss how one can protect themselves from becoming a victim.
4	International Drug Trafficking	International crime is a growing threat to the way of life in our country. This brief will look at one of the major types of international crime; one that is labeled as a significant threat to the lives and property of Americans: drug trafficking. It will also address what is being done to control this threat.
5	Smuggling	This brief will look into the broad area of smuggling items over the United States borders. It will detail three of the most active types of smuggling in this country: cigarette smuggling, contraband item smuggling, and people smuggling. It will also describe steps that are being taken to help remedy the situation.
6	Computer Crime	In this training brief, we will examine the constantly evolving world of computer crimes and define a broad base of current types of crimes. We will also look at what the government is doing in an attempt to control these crimes. Finally, we will suggest some options for how individuals can protect themselves from becoming victims of such crimes.
7 Bonus Brief	Identity Theft	Identity theft crimes range from purse snatchings to kingpin-style fraud rings. The definition of identity theft is a crime in which an imposter obtains key pieces of personal information, such as a Social Security number, in order to impersonate someone else. Identity theft can occur when someone takes your mail, steals your wallet or swipes your records from an institution. Terrorists have a long history of assuming other individual's identities and have seized upon the use of information technology as a tool in their terrorist activities. In an article published on September 22nd, 2001 by the Times LTD titled "Terrorists' Trade in Stolen Identities" it discusses how Osama bin Laden had carefully created impostors and how his agents stole the identities and life histories of at least a dozen Western-educated young men who were all murdered in 1990. Every document and record of those men's lives were either stolen or doctored to allow the terrorists to move freely around the world. This training brief will provide a solid understanding of identity theft and implications associated with this crime.

Specialty CD 12 – UnRestricted Warfare

A new emerging area of conflict is called Unrestricted Warfare or URW. Spy-Ops has developed a series of training briefs to educate multiple industry disciplines on this type of warfare. This new range of options combined with the escalating cost (both political and financial) of waging traditional warfare has resulted in the rising dominance of the new alternatives to traditional military action. Anyone that does not heed these warnings is placing themselves, and the organization or country that they are affiliated with at great risk. In response to the new threat of UnRestricted Warfare (URW), and in collaboration with the Technolytics Institute, we have created this first-ever URW training program. The program is delivered on CD or electronically, and includes seventeen modules that take approximately 34 hours to complete. Once you pass all seventeen exams, you will receive a Certificate in UnRestricted Warfare.

FACT: *The face of conflict has changed as technology has evolved. New technology brings new weapons and threats that must be understood before they can be countered.*

Program Cost: \$159.95

#	Title	Abstract
1	UnRestricted Warfare	UnRestricted Warfare is a relatively new concept first defined by two Chinese colonels in a book written in the late 1990s for the Chinese People's Liberation Army. In this book, they described un-conventional tactics that could be used by an enemy on a larger more powerful target such as the United States. This concept has continued to evolve and now consists of fifteen different modalities of warfare employed against an enemy. This concept poses a unique threat to the United States and other leading world powers that have increasingly been targeted with small scale, stealth, focused attacks on nonmilitary targets. With respect to the United States, the book points out that the U.S. has 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, the United States currently is highly vulnerable to attack along these lines.
2	Cultural Warfare	The clash of cultures has occurred throughout the entire course of human history. The ability to manipulate the cultural aspects of adversarial populations can create a driving force for change, even in the 21st century. Using outside influence to bring about a cultural change is a powerful weapon in the realm of UnRestricted Warfare. This brief will look into the use of modern day cultural warfare tactics. You will discover the meaning of cultural warfare, and how it is currently being used around the world. Issues in China and Iraq, involving elements of cultural warfare and the response of those countries to the measures being taken, are specifically addressed.
3	Economic Warfare	This training brief will focus on the use of economic warfare by using economic aid dependency to control a targeted adversary. It will describe examples of areas in which economic warfare may be used and how it is accomplished. Finally, it will look into selected examples of the use of economic warfare in recent history.
4	Environmental Warfare	Environmental Warfare has been called the ultimate weapon. This brief will define and look into the use of environmental warfare as a modality of UnRestricted Warfare. It will look at the capabilities of environmental warfare and environmental engineering as they have developed and what continues to emerge from scientific and covert studies. It will look at the dangers of using environmental warfare and prospective uses against entire populations.



5	Financial Warfare	In a statement by Osama Bin Laden, it was made very clear that a major objective of this terrorist conflict is to “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. While financial attacks of this nature have occurred in the past, the globalization and integration of financial systems and the ubiquitous nature of the internet has increased the impact of these types of attacks and augmented the likelihood that they will occur. Current trends indicate an increased level of sophistication and coordination of attacks with initiation points coming from multiple locations and countries. Many experts believe that the likelihood of such an attack, while high, has slim chances of success. This training will explore the financial warfare modality of UnRestricted Warfare and whether such attacks have the footprint of success.
6	Illegal Drugs Warfare	International crime is a growing threat to the way of life in our country. This brief will look at one of the major types of international crime; one that is labeled as a significant threat to the lives and property of Americans: drug trafficking. It will also address what is being done to control this threat.
7	International Law Warfare	This brief will explore the make up and functions of international law. It will describe what comprises international law, the basic rules of international law and its overall purposes in the area of security. In addition, it will examine how international law is incorporated and used in the concept of UnRestricted Warfare. Finally, it will define INTERPOL and its role within the world of international law.
8	Information Warfare	In this training brief, the world of information warfare will be explored. Various ways this crime is committed will be revealed and the masterminds behind it will be profiled. The results of the work of these criminals will also be examined.
9	Telecommunications and Network Warfare (Cyber Terrorism)	Cyber-terrorism or attacks on telecommunications and computer networks have been called the invisible threat to our national economy and security. Day after day, digital warriors defend our information systems and infrastructure against thousands of unseen attacks by criminals and terrorists. This 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 will be actual intelligence and scenarios that pose a significant threat to our national information and telecommunications infrastructure.
10	Political Warfare	This brief will investigate the world of political warfare and regime change. The brief will provide a basic understanding of the essence of political warfare. It will also describe what a regime change actually entails and how it is attempted and/or accomplished in a region. It will also look into modern day examples where political warfare is being waged and regime change is currently underway. Keep in mind, regime change is just one strategic weapon that is used in political warfare. While regime change is by far the most visible and widely publicized weapon, there are numerous other aspects of political warfare as well.

11	Psychological Warfare	Psychological warfare is a tactic that has been used for hundreds of years by military and non-military forces. It is sometimes referred to as psychological operations. A psychological warfare campaign or operation focuses on a war of the mind. This brief will look into the use of psychological warfare. It will define, in general, what psychological warfare is and how it is used. This brief will also look into the use of psychological warfare by the U.S. government and the area of the government devoted to this task. It will then explore the ways psychology is used to attempt to control an adversary's perception of their own capabilities, and how psychological warfare is used in general, against opponents.
12	Resource Warfare	This brief will look into an additional modality of UnRestricted Warfare known as Resource Warfare. This tactic withholds strategic resources (materials, energy, water, etc...) from an adversary to disrupt normal activities and cause harm. This brief will review how it is used and what resources can be applied in the worldwide system to control the actions and behaviors of others. This brief will also look at key examples of the use of resource warfare in history and more recently in the contemporary modern period.
13	Smuggling Warfare	This brief will look into the broad area of smuggling items over the United States borders. It will detail three of the most active types of smuggling in this country: cigarette smuggling, contraband item smuggling, and people smuggling. It will also describe steps that are being taken to help remedy the situation.
14	Technology Warfare	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 our economic and military engine. Without a strong technology base we as a nation 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.
15	Terrorism – Strategies & Tactics	Terrorism is a fact of life and a force with which we must deal. Terrorism has impacted our business, social, political and personal lives in numerous ways. When you mention terrorism one thing is certain, there is little agreement on what exactly constitutes terrorism and terrorist activities. Generally, terrorism is a tactic used to influence the activities of one entity by another entity with an opposing view, opinion, value or culture and is used in times of peace, conflict and war. Groups employ terrorist violence in the name of many causes. The threat of terrorism is ever present, and an attack is likely to occur when least expected. Terrorism is unconventional warfare. There are no fronts, no armies, and no battlefields. This training module will provide a basic understanding of terrorism.
16	Gang Warfare	This brief will look at the make-up and activities of gangs. It will define what a gang is and look into how it influences the people involved in their activities as well as society as a whole.
17 Bonus Brief	Improvised Explosive Devices	This course is a high-level introduction to Improvised Explosive Devices (IEDs). An IED is any explosive device that has been rigged by its builder to detonate and cause death and injury through blast, shrapnel, fire or release of chemicals or bio-toxins. While IEDs have gained prominence through their daily use by insurgents in Iraq, armies and unconventional warfare practitioners have used the booby trap version IED for many years. Vehicle Borne Improvised Explosive Devices (VBIEDs) and Suicide IEDs pose significant problems to counter-terror professionals, due to their ease of manufacture, ability to be hidden in obvious places without detection, and seemingly endless supply of martyrs willing to blow themselves up in attacks.

Specialty CD 13 – Tradecraft 101

Have you ever thought about becoming a secret agent? Have you ever wished you could go through the training they do? With Tradecraft 101 you are on your way. The seven training modules included in this program provides you the basic understanding of critical topics in espionage and spying. This training is real and is used worldwide by government agencies, security firms and others.

The program is delivered on CD or electronically, and includes seven modules that take approximately 14 hours to complete. Once you pass all seven exams, you will receive a Certificate in Tradecraft.

FACT: *Spying is one of the oldest professions. It is the subject of countless books and movies. The passion to learn the art of spying is what tradecraft is all about.*

Program Cost: \$29.95

#	Title	Abstract
1	Digital Spying	In this brief, you will look into the world of spyware from all angles. You will see what it is and how it is used. In addition, you will be able to tell how it is being used on you. You will also learn how to protect yourself from being a victim of spyware and, if you already are a victim, how to get rid of it and protect yourself in the future.
2	Secret Intelligence	The world of intelligence is all about information. Information that is acted upon becomes intelligence. This training brief will dissect the area of secret intelligence. We will define this practice as well as discover ways it has been used throughout history by our own country and others. We will also briefly explore how secret intelligence is practiced and used in today's world.
3	Creating a Microdot	This brief will explore the topic of microdots. We will define what they are and what they are used for. Finally, we will look in some detail at how they are made. We will see how a simple set-up can allow a person to reduce a page of text to an area of 1.0 by 1.2 millimeters. Creating a microdot is not as complicated as one might think. With a rather easy setup, a simple microdot can be made in ones own home and used for reducing print at a ratio of 210:1. Here we will not only see how to do this, but look at why one would want to do it and how useful it can be.
4	Introduction to Intelligence Technology	From the corporate wars fought in the board room to the war on terrorism fought in virtually every corner of the world, technology provides organizations and governments with the ability to both protect and destroy. Globally, a significant amount of effort and funding is given to collecting, analyzing and disseminating all types of intelligence. This training brief will examine technology and the role it plays in secret intelligence.
5	How Spies Get Caught	In this brief we will look at the ways spies are caught. We will learn how they are caught firsthand through former spies who were sought out and caught in the act. Through their actual experiences, we see, in hindsight, the mistakes they made and the ways that the same weapons available to them for their work were used against them.
6	Forensics DNA Identification	This training brief will explore the use of DNA in the world of forensic science. It will look at DNA as a key tool in human identification and the role it plays in solving many types of crimes. Finally, it will open up how DNA procedures have improved in recent history and what scientific advances we can expect in the near future.
7	Human Intelligence Gathering	This brief will explore a portion of the large world of human intelligence. It will define what is meant by the term for spy purposes. It will explore different ways that one approaches gathering valuable information and what that information might be used for.

Specialty CD 14 – Computer Information and Security

Computer and information security are areas of study that are rapidly growing in importance and visibility. With the increased ease with which an unscrupulous person can access the internet and commit eCrimes with and against computers, and with the increased emphasis on homeland defense in this country, there is a growing need for all those in the security field to update their skills to minimize these threats. This continuing education program will cover a wide variety of topics such as computer crime and digital spying. You will learn different aspects of computer crime and ways in which to uncover, protect and exploit digital evidence. You will also be exposed to different types of tools, both software and hardware, and be able to use them to perform rudimentary investigation. Update your eCrime skills with our Computer Information and Security certificate program.

The program is delivered on CD or electronically, and includes thirteen modules that take approximately 26 hours to complete. Once you pass all thirteen exams, you will receive a Certificate in Computer Information and Security.

FACT: *eCrime has burst onto the scenes and has become a formidable challenge for businesses, governments, and individual users.*

Program Cost: \$ 99.95

#	Title	Abstract
1	Digital Spying	In this brief, you will look into the world of spyware from all angles. You will see what it is and how it is used. In addition, you will be able to tell how it is being used on you. You will also learn how to protect yourself from being a victim of spyware and, if you already are a victim, how to get rid of it and protect yourself in the future.
2	Electronic Bugging	This course provides a brief overview of electronic bugging. Espionage is the art of covertly obtaining information of value about another entity. Advances in electronics have made this easier and more economical than ever. Everyone who has information that is valuable to another individual, organization or government is at risk. This module provides an introduction to electronic bugging devices, what to look for, and most importantly the "Do's and Don'ts" for when you find electronic surveillance devices.
3	Security Systems	Security Systems (also called alarm systems) have gotten extremely sophisticated since the advent of the microprocessor (computer chip). Today's systems offer a myriad of optional sensors, signaling devices and control options that were not available just a few years ago. Most systems offer the capability to communicate with a remote monitoring station, where operators are on duty 24 hours a day to dispatch the appropriate authorities to the alarm location if a break-in or emergency arises. This training brief will cover the basics of security systems.
4	Biometric Security Devices	Biometrics involves using the different parts of the body, such as the fingerprint or the eye, as a password or form of identification. All biometric systems work in the same manner. First, a person is enrolled into a database using a specific type of biometric identification device. Initially, information about a certain characteristic of the person is captured, for example a fingerprint or hand geometry. This information is subsequently processed by an algorithm, coded and stored in a data base for future reference. When the person needs to be identified, the system will ask for specific personal information, translate it using an algorithm, and then compare the new code with existing data base information. If a match is made, the identification process is complete. This training brief will introduce you to biometrics and its use in security applications.

5	Digital Footprints	The world enjoys unlimited benefits from new technologies in an electronic world. But those 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 training brief will provide an understanding of digital footprints, their dangers and what the consequences are for all of us.
6	Identity Theft	Identity theft crimes range from purse snatchings to kingpin-style fraud rings. The definition of identity theft is a crime in which an imposter obtains key pieces of personal information, such as a Social Security number, in order to impersonate someone else. Identity theft can occur when someone takes your mail, steals your wallet or swipes your records from an institution. Terrorists have a long history of assuming other individual's identities and have seized upon the use of information technology as a tool in their terrorist activities. In an article published on September 22nd, 2001 by the Times LTD titled "Terrorists' Trade in Stolen Identities" it discusses how Osama bin Laden had carefully created impostors and how his agents stole the identities and life histories of at least a dozen Western-educated young men who were all murdered in 1990. Every document and record of those men's lives were either stolen or doctored to allow the terrorists to move freely around the world. This training brief will provide a solid understanding of identity theft and implications associated with this crime.
7	Social Engineering	Social engineering is the practice of obtaining confidential information by manipulation of people. A social engineer will commonly use the telephone or internet to trick people into revealing sensitive information or get them to do something that is against typical policies. By this method, social engineers exploit the natural tendency of a person to either trust his or her word and impart information freely, or be so busy as to take a shortcut, rather than exploiting computer security holes. It is generally agreed upon that "users are the weak link" in security, and this principle is what makes social engineering possible.
8	Computer Crime	In this training brief, we will examine the constantly evolving world of computer crimes and define a broad base of current types of crimes. We will also look at what the government is doing in an attempt to control these crimes. Finally, we will suggest some options for how individuals can protect themselves from becoming victims of such crimes.
9	Information Warfare	In this training brief, the world of information warfare will be explored. Various ways this crime is committed will be revealed and the masterminds behind it will be profiled. The results of the work of these criminals will also be examined.
10	Computer Hacking	Computer hacking, or cracking, has grown to pandemic proportions and costs businesses and governments billions of dollars in on-going computer security and countermeasure efforts. Far from its beginnings, with computer geeks breaking the security of networks, applications or communications systems, black hat hackers are now using their knowledge to commit computer crimes such as identity theft and credit card fraud. Terrorists and foreign intelligence and military personnel hack and crack to gain intelligence, conduct cyber warfare or engage in electronic sabotage.
11	Technology Warfare	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 our economic and military engine. Without a strong technology base we as a nation 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.

12	Telecommunications and Network Warfare (Cyber Terrorism)	Cyber-terrorism or attacks on telecommunications and computer networks have been called the invisible threat to our national economy and security. Day after day, digital warriors defend our information systems and infrastructure against thousands of unseen attacks by criminals and terrorists. This 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 will be actual intelligence and scenarios that pose a significant threat to our national information and telecommunications infrastructure.
13	Transient Electro-Magnetic Devices (TEDS)	The reliance of the world on electronics and computers has made them a prime target for espionage and terrorist attacks. This is particularly relevant now that the military's Net-Centric Warfare strategy is becoming a reality. Many call them e-Bombs, but the proper name is Transient Electromagnetic-pulse Devices or TEDs. The EMP or electromagnetic pulse typically associated with a nuclear detonation can now be generated using a small amount of conventional explosives and readily available components from your local electronics store. The massive disruption to business, government and society, and the relative ease of construction with readily available components increases the likelihood of a TEDs attack. This brief will present TEDs and the potential impact of such an attack.

Specialty CD 15 – Mortgage Fraud

Predatory mortgage lending / mortgage fraud drains wealth from families, destroys the benefits of homeownership, and often leads to foreclosure. The Center for Responsible Lending estimates that predatory mortgage lending / mortgage fraud costs Americans more than \$9.1 billion each year. Mortgage fraud generally involves material misrepresentation or omission of information with the intent to deceive or mislead a lender into extending credit that would likely not be offered if the true facts were known. The motivation behind mortgage fraud is money. Fraud for profit is often committed with the complicity of industry insiders such as mortgage brokers, real estate agents, property appraisers, and settlement agents such as attorneys and title examiners. Protect yourself, your family, and your business by updating your knowledge and skills.

The program is delivered on CD or electronically, and includes four modules that take approximately 8 hours to complete. Once you pass all four exams, you will receive a Certificate in Mortgage Fraud.

FACT: *Mortgage fraud has wrecked our economy and has a negative impact on all of us. Everyone must become involved in the identification and elimination of these criminal acts.*

Program Cost: \$39.95

#	Title	Abstract
1	Digital Footprints	The world enjoys unlimited benefits from new technologies in an electronic world. But those 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 training brief will provide an understanding of digital footprints, their dangers and what the consequences are for all of us.

2	Identity Theft	<p>Identity theft crimes range from purse snatchings to kingpin-style fraud rings. The definition of identity theft is a crime in which an imposter obtains key pieces of personal information, such as a Social Security number, in order to impersonate someone else. Identity theft can occur when someone takes your mail, steals your wallet or swipes your records from an institution. Terrorists have a long history of assuming other individual's identities and have seized upon the use of information technology as a tool in their terrorist activities. In an article published on September 22nd, 2001 by the Times LTD titled "Terrorists' Trade in Stolen Identities" it discusses how Osama bin Laden had carefully created impostors and how his agents stole the identities and life histories of at least a dozen Western-educated young men who were all murdered in 1990. Every document and record of those men's lives were either stolen or doctored to allow the terrorists to move freely around the world. This training brief will provide a solid understanding of identity theft and implications associated with this crime.</p>
3	Money Laundering	<p>This training brief will define what money laundering is, walk through how it is accomplished, and examine the layers involved. The different ways money laundering effects our world will also be explored. Finally, the two necessary components required if governments are to have any hopes of controlling this area of crime will be reviewed. Although money laundering and financing terrorism are closely related, this brief addresses only money laundering. Financing terrorism is covered in a separate training brief.</p>
4	Mortgage Fraud	<p>Mortgage fraud is an epidemic in America. One may think that "epidemic" sounds overly harsh as a way to describe the fraud that is besieging the real estate mortgage market in America, but the facts regarding the current problems for many Americans are staggering. This epidemic has now also spread to Canada. During fiscal 2005-2006, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), the Canadian equivalent to the Financial Crimes Enforcement Network (FinCEN) in the United States, made 168 mortgage fraud case disclosures, of which:</p> <ul style="list-style-type: none"> • 134 were for suspected money laundering, • 33 were for suspected terrorist activity financing, and • 1 case disclosure involved both suspected money laundering and financial fraud. <p>In 2005, the U.S. Mortgage Brokers Association (MBA) mortgage origination estimation topped \$2.7 trillion. Experts estimate that 10% to 15% of mortgage loans involves some kind of fraud. This means that between 2 to 3 million home loans originated this year could be fraudulent; that equates to over 7,500 new fraudulent loans every business day. As the mortgage market grows, new and innovative ways to defraud financial institutions will appear.</p>

Specialty CD 16 – Terrorism: Chemical – Biological – Radioactive – Nuclear – Explosives

First responders, law enforcement and many diverse workers including drivers, loaders/unloaders, vehicle maintenance workers, warehouse workers, truck stop personnel, dispatchers, security personnel, engineers, conductors, car men, track and signal workers, in-plant rail workers, and yardmasters all need CBRNE training. Participants stressed that many workers have received basic health and safety training but lack CBRNE knowledge. This course is designed to equip military and civilian personnel and management professionals with skills, knowledge, and information resources to carry out their responsibilities in the event of a chemical, biological, radiological nuclear, explosive (CBRNE), or improvised explosive event.

The program is delivered on CD or electronically, and includes eight modules that take approximately 16 hours to complete. Once you pass all eight exams, you will receive a Certificate in CBRNE.

FACT: *With every tick of the clock we become one step closer to the next terrorist attack. Chemical, biological, radiation, nuclear, explosive or Improvised explosives are the most likely weapons of choice for the terrorist's next attack.*

Program Cost: \$ 99.95

#	Title	Abstract
1	Terrorism Awareness	Terrorism is now a fact of life. The goals of terrorism are usually political, social, or religious in nature. Sometimes terrorists try to address their issues legally, but they become frustrated over the lack of change. They often feel ignored or as if they are being treated unjustly. Terrorists truly believe they are working toward a better world and that is what makes this so dangerous. This module is designed to help you understand the threat to our society, your part in protecting your community, and measures you can take to protect against acts of terror.
2	Terrorism – Strategies & Tactics	Terrorism is a fact of life and a force with which we must deal. Terrorism has impacted our business, social, political and personal lives in numerous ways. When you mention terrorism one thing is certain, there is little agreement on what exactly constitutes terrorism and terrorist activities. Generally, terrorism is a tactic used to influence the activities of one entity by another entity with an opposing view, opinion, value or culture and is used in times of peace, conflict and war. Groups employ terrorist violence in the name of many causes. The threat of terrorism is ever present, and an attack is likely to occur when least expected. Terrorism is unconventional warfare. There are no fronts, no armies, and no battlefields. This training module will provide a basic understanding of terrorism.
3	Chemical Weapons	<p>This brief introduces chemical weapons as they relate to possible use by terrorists against civilian non-combatants. It is not intended to be an exhaustive study of chemical weapons for military use but a high-level introduction. In a pre 9/11 study, the Center for Disease Control (CDC) listed several categories of chemical weapons whose use by terrorists presented a “threat.” Among these are nerve, blood, pulmonary and incapacitating agents.</p> <p>Chemical agents conjure up horrible images, as death comes in seconds after exposure to most of these agents. However, mass casualty situations are hard to predict. This is because of dispersion factors such as wind, temperature, air pressure, length of exposure and chemical characteristics associated with these and other variables. Many of these chemicals are readily available and their use by terrorist groups is probably inevitable.</p>

4	Biological Weapons	Biological warfare (BW), also known as germ warfare, is the use of any living organism, whether bacteria, virus, or other replicative protein as a weapon of warfare. The use of biological weapons poses one of the greatest threats civilization is likely to face as Islamist or other extremist groups collude with states to obtain biological agents. One of the greatest problems in detecting the manufacture of biological weapons is that almost all equipment needed for the production of biological agents (also referred to as pathogens and toxins) is dual use (used in the production of drugs and vaccines) and available on the international market, thus increasing the potential for concealing illicit activities under the cover of legitimate production.
5	Dirty Bombs	This course introduces Radiological or “Dirty” Bombs. A dirty bomb has a conventional high-explosive core surrounded by radiological material in a solid, gas or liquid form. It is not to be confused with a fission weapon such as the bombs used during WWII. The primary lethality of a dirty bomb depends on the type and amount of radioactive material, and the dispersal factors such as wind speed and blast location. The ease of construction and availability of radiological material make the dirty bomb’s use inevitable by terrorist groups.
6	Nuclear Weapons	Nuclear weapons can be grouped into different classes based on the nuclear reactions that provide their destructive energy, and on the details of their design. At their simplest level, nuclear weapons are classified as fission or fusion weapons, but in reality there are variations beyond the scope of this introductory text. The greatest fear of most professional intelligence practitioners is for Islamists militants to obtain nuclear weapons—an inevitability that many believe may have already occurred.
7	Bombs and Explosives	For individuals and groups that wish to cause fear and panic, the use of bombs and explosives are the weapons of choice. Unlike a random crime, the use of bombs and explosives requires a certain level of knowledge, organization, equipment, materials, and a place to create such explosive devices. By increasing one’s knowledge of bombs and explosives, a person may be able to prevent a potential event. In this age of terror and violence, no one can afford not to have at least some knowledge about bombs and explosives. This training brief will provide a fundamental understanding of bombs and explosives and their use in terror attacks.
8	Improvised Explosive Devices	This course is a high-level introduction to Improvised Explosive Devices (IEDs). An IED is any explosive device that has been rigged by its builder to detonate and cause death and injury through blast, shrapnel, fire or release of chemicals or bio-toxins. While IEDs have gained prominence through their daily use by insurgents in Iraq, armies and unconventional warfare practitioners have used the booby trap version IED for many years. Vehicle Borne Improvised Explosive Devices (VBIEDs) and Suicide IEDs pose significant problems to counter-terror professionals, due to their ease of manufacture, ability to be hidden in obvious places without detection, and seemingly endless supply of martyrs willing to blow themselves up in attacks.

Specialty CD 17 – Enterprise Risk Management

Enterprise Risk Management (ERM) represents a fundamental shift in the way businesses must approach risks. Recent years have seen heightened concern and focus on risk management. Terrorist attacks, computer system breaches, espionage and other emerging threats have made it clear that a need exists to effectively identify, assess, and manage risk. Among the most critical challenges for managements is to stay abreast of changing and emerging risks to the enterprise. Failure to adapt to the dynamics of the enterprise risk environment will result in unmanaged risks. The ERM program was designed using the knowledge and experience of top enterprise risk management experts. Its purpose is to address this issue, as well as update your knowledge and understanding of the threat facing CEOs and shareholders in corporations and governments around the world.

The program is delivered on CD or electronically, and includes fourteen modules that take approximately 28 hours to complete. Once you pass all fourteen exams, you will receive a Certificate in Enterprise Risk Management.

Program Cost: \$ 99.95

#	Title	Abstract
1	Corporate Espionage	Corporate espionage is the dirty little secret of global business. Espionage activities are often masked under the title of competitive intelligence. But in the end, thieves or spies still acquire sensitive, restricted information assets of another entity, which may include product designs, business models, marketing plans, research and development files, customer lists, employee lists, pricing strategies and other intellectual property. This module will provide a basic understanding of the current state of corporate espionage, as well as illustrate many techniques used in committing this new type of crime.
2	Digital Spying	In this brief, you will look into the world of spyware from all angles. You will see what it is and how it is used. In addition, you will be able to tell how it is being used on you. You will also learn how to protect yourself from being a victim of spyware and, if you already are a victim, how to get rid of it and protect yourself in the future.
3	Digital Footprints	The world enjoys unlimited benefits from new technologies in an electronic world. But those 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 training brief will provide an understanding of digital footprints, their dangers and what the consequences are for all of us.
4	Social Engineering	Social engineering is the practice of obtaining confidential information by manipulation of people. A social engineer will commonly use the telephone or internet to trick people into revealing sensitive information or get them to do something that is against typical policies. By this method, social engineers exploit the natural tendency of a person to either trust his or her word, and impart information freely, or be so busy as to take a shortcut, rather than exploiting computer security holes. It is generally agreed upon that “users are the weak link” in security, and this principle is what makes social engineering possible.

5	Computer Crime	In this training brief, we will examine the constantly evolving world of computer crimes and define a broad base of current types of crimes. We will also look at what the government is doing in an attempt to control these crimes. Finally, we will suggest some options for how individuals can protect themselves from becoming victims of such crimes.
6	Information Warfare	In this training brief, the world of information warfare will be explored. Various ways this crime is committed will be revealed and the masterminds behind it will be profiled. The results of the work of these criminals will also be examined.
7	Computer Hacking	Computer hacking, or cracking, has grown to pandemic proportions and costs businesses and governments billions of dollars in on-going computer security and countermeasure efforts. Far from its beginnings, with computer geeks breaking the security of networks, applications or communications systems, black hat hackers are now using their knowledge to commit computer crimes such as identity theft and credit card fraud. Terrorists and foreign intelligence and military personnel hack and crack to gain intelligence, conduct cyber warfare or engage in electronic sabotage.
8	Critical Infrastructure Protection	The attacks of September 11th caused the government to re-examine the vulnerability of the assets that allow the country to operate normally every day. The title given to this group of assets is Critical Infrastructure. Terrorists often focus their attacks on targets that disrupt their enemy's way of life. Attacking our critical infrastructure would certainly accomplish that task. This brief will provide information needed to understand what the challenges of protecting the critical infrastructure are.
9	Technology Warfare	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 our economic and military engine. Without a strong technology base we as a nation 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.
10	Cyber Terrorism	Cyber-terrorism or attacks on telecommunications and computer networks have been called the invisible threat to our national economy and security. Day after day, digital warriors defend our information systems and infrastructure against thousands of unseen attacks by criminals and terrorists. This 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 will be actual intelligence and scenarios that pose a significant threat to our national information and telecommunications infrastructure.
11	Transient Electro-Magnetic Devices (TEDS)	The reliance of the world on electronics and computers has made them a prime target for espionage and terrorist attacks. This is particularly relevant now that the military's Net-Centric Warfare strategy is becoming a reality. Many call them e-Bombs, but the proper name is Transient Electromagnetic-pulse Devices or TEDs. The EMP or electromagnetic pulse typically associated with a nuclear detonation can now be generated using a small amount of conventional explosives and readily available components from your local electronics store. The massive disruption to business, government and society, and the relative ease of construction with readily available components increases the likelihood of a TEDs attack. This brief will present TEDs and the potential impact of such an attack.

12	Insider Threats	Few people would dispute the fact that we all rely on computers in our personal lives and in business. Each device holds a significant amount of data about ourselves as individuals as well as sensitive financial data and much more. With all the value stored in these computers that have become prime targets for attacks. Preventive measures have almost exclusively focused on attacks from the outside. Firewalls, access control software and other measures are all designed to defend against external attacks. Insiders already have access to the systems. They also have inside knowledge about the systems that make them extremely dangerous. Insiders are now thought to be responsible for well over half of all system security breaches. Couple that with their access to physical documents and the insiders has risen to the top of the threat matrix. This brief will examine why the CIA, FBI, DoD, Secret Service and other have all completed significant research on this topic.
13	eCrime	There is no question that the Internet has had a positive impact on today's global society. However, it also has had its negative implications as well. The Internet has all but become a playground for criminals who create new scams and plots. Using the Web, they are able to defraud, extort and swindle users around the world easier than ever before. The topic of eCrimes is a diverse and not-easily-defined subject matter. The deception offences are notoriously technical. There are several different terms used to describe eCrimes, as well as a number of types of criminal activities that fall within the boundaries of what are considered to be eCrimes. After a considerable gestation period, the Fraud Act of 2006 came into force on 15th January 2007 and is designed to address the epidemic of eCrime. This brief will explore a wide range of sections within the whole of e-criminal activity as well as ways the government is attempting to control this type of crime.
14	eDiscovery	The emergence of eDiscovery as a legal requirement came onto the scene late in 2006. Electronic discovery (also called e-discovery or eDiscovery) refers to any process in which all electronic (digital) data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case. The characteristics of digital data make it extremely well-suited to investigation. Given the value of electronic data, evidence of destruction or failure to protect electronic data during eDiscovery can lead to costly penalties, sanctions, and dismissal of the lawsuit. Lawsuits are a fact of life for organizations today. Electronic Discovery is the number one litigation-related burden for general counsel at companies with annual revenues exceeding \$100 million. It should be noted that court-ordered or government sanctioned hacking for the purpose of obtaining critical evidence is also a type of e-discovery. This training brief will provide the eDiscovery background needed to understand its implications to citizens and corporations alike in today's environment.

Specialty CD 18 – Cyber Warfare

Business, governments, industry and society have all become addicted to computers. With our heavy reliance on computer systems, they have become a primary military target as well as a prime target for terrorist attacks. The world realized in the late spring of 2007 that we had entered a new age of conflict when the country of Estonia experienced the first cyber war. The Estonia attack was unprecedented in size and scope and should alarm every nation around the world. Offensive cyber weapons have been developed by multiple countries that could create havoc and inflict significant damage to our information infrastructure. Cyber Arms have become easier to obtain, easier to use, and much more powerful. These weapons are a fraction of the cost of traditional weapons such as a tank. Therefore, state or group-sponsored attacks against information systems using computer viruses and other techniques should be considered an act of war. As such, governments must be proactive and establish parameters, definitions and regulations around cyber war. This Certificate Program provides you the fundamental knowledge you need in the age of cyber warfare.

The program is delivered on CD or electronically, and includes fifteen modules that take approximately 30 hours to complete. Once you pass all fifteen exams, you will receive a Certificate in Cyber Warfare.

FACT: *In the past minute there have been over 5,000 reports of serious computer attacks reported.*

Program Cost: \$ 119.95

#	Title	Abstract
1	Corporate Espionage	Corporate espionage is the dirty little secret of global business. Espionage activities are often masked under the title of competitive intelligence. But in the end, thieves or spies still acquire sensitive, restricted information assets of another entity, which may include product designs, business models, marketing plans, research and development files, customer lists, employee lists, pricing strategies and other intellectual property. This module will provide a basic understanding of the current state of corporate espionage, as well as illustrate many techniques used in committing this new type of crime.
2	Digital Spying	In this brief, you will look into the world of spyware from all angles. You will see what it is and how it is used. In addition, you will be able to tell how it is being used on you. You will also learn how to protect yourself from being a victim of spyware and, if you already are a victim, how to get rid of it and protect yourself in the future.
3	Introduction to Intelligence Technology	From the corporate wars fought in the board room to the war on terrorism fought in virtually every corner of the world, technology provides organizations and governments with the ability to both protect and destroy. Globally, a significant amount of effort and funding is given to collecting, analyzing and disseminating all types of intelligence. This training brief will examine technology and the role it plays in secret intelligence.
4	Directed Energy Weapons	A new class of weapons is currently under development by several countries around the world. Directed Energy Weapons (DEW) or Kinetic Energy Weapons (KEW) make up this new class and could change the balance of power and create a new arms race. DEWs are among the latest high-tech arms of the 21st century. The training brief will provide you with a basic understanding of Directed Energy Weapons, how they operate and how they can be used. In addition we will explore the implications of these weapons.

5	Digital Footprints	The world enjoys unlimited benefits from new technologies in an electronic world. But those 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 training brief will provide an understanding of digital footprints, their dangers and what the consequences are for all of us.
6	Scenario Based Intelligence Analysis	Intelligence is the key component needed to combat terrorism and defend against the numerous threats we face today. Currently, less than 1/10th of the United States spending on intelligence is devoted to analysis; it is the least expensive dimension of intelligence. However, if done right, the intelligence process will provide insight into new and emerging threats, perhaps preventing them, or at the very least explaining them after the fact. Toward that end, analysts in the nation's intelligence community are under extreme public pressure to perform flawlessly. Failure to do so has catastrophic consequences. Working to improve the quality of analysis to assist the intelligence community and intelligence analysts in gathering, analyzing and reporting on global threats to our interests, has resulted in the evolution of several new methods and techniques. Scenario-Based Intelligence Analysis (SBIA) is one such method. This document will explore the use of (SBIA) within the context of many methodologies.
7	Social Engineering	Social engineering is the practice of obtaining confidential information by manipulation of people. A social engineer will commonly use the telephone or internet to trick people into revealing sensitive information or get them to do something that is against typical policies. By this method, social engineers exploit the natural tendency of a person to either trust his or her word, and impart information freely, or be so busy as to take a shortcut, rather than exploiting computer security holes. It is generally agreed upon that "users are the weak link" in security, and this principle is what makes social engineering possible.
8	Computer Crime	In this training brief, we will examine the constantly evolving world of computer crimes and define a broad base of current types of crimes. We will also look at what the government is doing in an attempt to control these crimes. Finally, we will suggest some options for how individuals can protect themselves from becoming victims of such crimes.
9	Information Warfare	In this training brief, the world of information warfare will be explored. Various ways this crime is committed will be revealed and the masterminds behind it will be profiled. The results of the work of these criminals will also be examined.
10	Computer Hacking	Computer hacking, or cracking, has grown to pandemic proportions and costs businesses and governments billions of dollars in on-going computer security and countermeasure efforts. Far from its beginnings, with computer geeks breaking the security of networks, applications or communications systems, black hat hackers are now using their knowledge to commit computer crimes such as identity theft and credit card fraud. Terrorists and foreign intelligence and military personnel hack and crack to gain intelligence, conduct cyber warfare or engage in electronic sabotage.

11	UnRestricted Warfare	UnRestricted Warfare is a relatively new concept first defined by two Chinese colonels in a book written in the late 1990s for the Chinese People's Liberation Army. In this book, they described un-conventional tactics that could be used by an enemy on a larger more powerful target such as the United States. This concept has continued to evolve and now consists of fifteen different modalities of warfare employed against an enemy. This concept poses a unique threat to the United States and other leading world powers that have increasingly been targeted with small scale, stealth, focused attacks on nonmilitary targets. With respect to the United States, the book points out that the U.S. has 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, the United States currently is highly vulnerable to attack along these lines.
12	Critical Infrastructure Protection	The attacks of September 11th caused the government to re-examine the vulnerability of the assets that allow the country to operate normally every day. The title given to this group of assets is Critical Infrastructure. Terrorists often focus their attacks on targets that disrupt their enemy's way of life. Attacking our critical infrastructure would certainly accomplish that task. This brief will provide information needed to understand what the challenges of protecting the critical infrastructure are.
13	Technology Warfare	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 our economic and military engine. Without a strong technology base we as a nation 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.
14	Cyber Terrorism	Cyber-terrorism or attacks on telecommunications and computer networks have been called the invisible threat to our national economy and security. Day after day, digital warriors defend our information systems and infrastructure against thousands of unseen attacks by criminals and terrorists. This 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 will be actual intelligence and scenarios that pose a significant threat to our national information and telecommunications infrastructure.
15	Transient Electro-Magnetic Devices (TEDS)	The reliance of the world on electronics and computers has made them a prime target for espionage and terrorist attacks. This is particularly relevant now that the military's Net-Centric Warfare strategy is becoming a reality. Many call them e-Bombs, but the proper name is Transient Electromagnetic-pulse Devices or TEDs. The EMP or electromagnetic pulse typically associated with a nuclear detonation can now be generated using a small amount of conventional explosives and readily available components from your local electronics store. The massive disruption to business, government and society, and the relative ease of construction with readily available components increases the likelihood of a TEDs attack. This brief will present TEDs and the potential impact of such an attack.

Specialty CD 19 – Custom Certification

Each situation is unique. We recognize that you have special requirements for your training and skills development. To address your specific needs we have created this custom certification. Participants must demonstrate that they have actually achieved learning objectives before they complete this program. With a custom certification course, you can define specific criteria for success and measure your performance.

You select ten of our training briefs (see the Spy-Ops Training Brief Catalog for a complete listing of the 75 training briefs that are available) that are related to your specific situation, you define the title of the certification and once you complete the program we issue you a custom certificate.

The program is delivered on CD or electronically, and includes 10 modules that take approximately 20 hours to complete. Once you pass all 10 exams, you will receive a Certificate in the subject you have chosen.

NOTE: Spy-Ops reserves the right to reject titles that misrepresent the content of the program.

FACT: The work environment is undergoing constant change. New threats, specialization of job profiles, technical complexities for jobs, and increased work pressure are now major aspects of the work environment that require individuals to update their skills regularly. Currently, 93 percent of employers provide professional development opportunities/reimbursement for their employees. Check with your employer to see if they will cover the cost of your program.

Program Cost: \$ 129.95

#	Title	Abstract
1-10	Choose 10 Titles based on your area of study.	See individual Brief Abstracts listed in the Spy-Ops Training Brief Catalog.

Ordering Information

Please see the next page for pricing of Certificate CD Programs. We accept credit card, check, money order or PayPal payments.

Certificate Programs will be delivered via CD-Rom or e-mail and contain all necessary materials in Adobe Acrobat format (PDF).

To order individual or multiple Certificate CD Programs, please follow the instructions below:

Option 1) Order online at www.spy-ops.com





Option 2) Fill out the order form on this page and continued on the next page, and either mail, fax, or e-mail to:

Spy-Ops
4017 Washington Road MS 348
McMurray, PA 15317 USA
Fax: 412-291-1193
e-Mail: orders@spy-Ops.com

If you have any questions, please call us at: 888-650-0800, or e-mail us at info@spy-ops.com

Spy-Ops Certificate CD Program Order Form

Name: _____
Address: _____
City: _____ State: _____
Country: _____ Postal Code: _____
Phone: _____ Fax: _____
e-Mail: _____
Occupation: _____

  
Payment Request Will be Sent Name on Card _____
 Card Number _____
Expiration Date ____/____ Security Code _____

Authorizing Signature: _____

I prefer to receive the Certificate CD Program(s) I have selected by:

e-Mail CD-Rom (this will be mailed via USPS)

Spy-Ops Certificate CD Program Order Form (Page 2)

Name: _____

Please check the briefs you would like on this table:

Quantity	Title	@	Price
_____	CD-1 Counter-Terrorism	@	\$99.95 USD
_____	CD-2 Corporate Crime	@	\$99.95 USD
_____	CD-3 Industrial Safety & Security	@	\$99.95 USD
_____	CD-4 Personal Protection for Elected Executives	@	\$99.95 USD
_____	CD-5 Personal Protection for Corporate Executives	@	\$99.95 USD
_____	CD-6 Advanced Security Services	@	\$99.95 USD
_____	CD-7 Private Investigation Services	@	\$99.95 USD
_____	CD-8 Executive Protection Services	@	\$99.95 USD
_____	CD-9 Personal Protection	@	\$99.95 USD
_____	CD-10 Educator Threat Awareness	@	\$99.95 USD
_____	CD-11 Money Laundering	@	\$59.95 USD
_____	CD-12 UnRestricted Warfare	@	\$159.95 USD
_____	CD-13 Tradecraft 101	@	\$29.95 USD
_____	CD-14 Computer & Information Security	@	\$99.95 USD
_____	CD-15 Mortgage Fraud	@	\$39.95 USD
_____	CD-16 Terrorism CBRNE	@	\$99.95 USD
_____	CD-17 Enterprise Risk Management	@	\$99.95 USD
_____	CD-18 Cyber Warfare	@	\$119.95 USD
_____	CD-19 Custom Certification*	@	\$129.95 USD

TOTAL CD's Ordered: _____ Total Cost _____

**Please Fill out Form on Next Page for the Custom Certification Program*

Please include payment with this order to insure quick fulfillment of your request.

Thank you for placing an order with Spy-Ops!



Custom Certification Program Form

Please fill out this form to request the approval of your custom certification program.

Name: _____ Date: _____
Address: _____
Address: _____
City: _____ State: _____ Zip: _____
Country: _____
Phone: _____
e-Mail: _____

Please provide the title you wish to appear on your certification.

Certification Title: _____

Please list the ten briefs you wish to use for your certification.

Brief Number _____	Title _____
Brief Number _____	Title _____
Brief Number _____	Title _____
Brief Number _____	Title _____
Brief Number _____	Title _____
Brief Number _____	Title _____
Brief Number _____	Title _____
Brief Number _____	Title _____
Brief Number _____	Title _____
Brief Number _____	Title _____

