

April 2011

# Spy-Ops Training Brief Catalog



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

# Spy-Ops Training Brief Catalog

Spy-Ops Provides Individual Training Briefs on a variety of topics. Our Training Briefs provide a comprehensive and in-depth review of a topic that is directly related to current events and targeted threats.

The collage displays four distinct training materials:

- Corporate Espionage Training Brief:** Features a table of contents, an abstract, a brief overview, a summary, and a list of references.
- Corporate Espionage Answer Sheet:** Contains a red-bordered box with instructions for completing the exam and an application information form.
- Corporate Espionage Exam:** A multiple-choice test with five questions regarding espionage statistics and motivations.
- Corporate Espionage On-Line Exercise:** A section for a research-based writing exercise with a provided space for answers.

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.
- An on-line exercise to reinforce key learning objectives.

Upon successful completion of the exam as well as the on-line exercise, continuing education units and a certificate of completion from the Technolytics Institute is issued.

Spy-Ops training briefs can be ordered individually for \$12.95 each. Please see the last page of this catalog for ordering instructions or visit the Spy-Ops website, [www.spy-ops.com](http://www.spy-ops.com).



## Course List

Spy-Ops Training Briefs cover a wide variety of topics. Each is updated on a regular basis to insure they remain current. New briefs are continually being added. If a topic of interest is not available in this list, please send an e-mail to [info@spy-ops.com](mailto:info@spy-ops.com), and we will consider developing a brief for this additional topic.

Brief 0	Corporate Espionage	Brief 39	Personal Protection
Brief 1	Unmanned Aerial Vehicles (UAVs)	Brief 40	Travel Security
Brief 2	Body Armor	Brief 41	Situational Awareness
Brief 3	Armored Vehicles	Brief 42	International Drug Trafficking
Brief 4	Creating a Microdot	Brief 43	Smuggling
Brief 5	Human Intelligence Gathering Techniques	Brief 44	Tracking Terrorist Financing
Brief 6	Global Positioning Systems	Brief 45	Nuclear Weapons
Brief 7	Digital Spying	Brief 46	UnRestricted Warfare
Brief 8	How Spies Get Caught	Brief 47	International Law Warfare
Brief 9	Interrogation	Brief 48	Economic Warfare
Brief 10	Islamist Terrorism	Brief 49	Critical Infrastructure Protection
Brief 11	Long Range Microphones	Brief 50	On-line Child Exploitation
Brief 12	Dirty Bombs	Brief 51	Technology Warfare
Brief 13	Biological Warfare	Brief 52	Political Warfare
Brief 14	Electronic Bugging	Brief 53	Psychological Warfare
Brief 15	Chemical Weapons	Brief 54	Cyber Terrorism (Telecommunication and Network Warfare)
Brief 16	Security Systems	Brief 55	Environmental Warfare
Brief 17	Introduction to Intelligence Technology	Brief 56	Financial Warfare
Brief 18	Improvised Explosive Devices	Brief 57	Cultural Warfare
Brief 19	Domestic Terrorism	Brief 58	School Violence
Brief 20	Biometric Security Devices	Brief 59	Resource Warfare
Brief 21	Directed Energy Weapons	Brief 60	Cyber-Bullying
Brief 22	Terrorist Recognition	Brief 61	Mortgage Fraud
Brief 23	Digital Footprints	Brief 62	Bombs and Explosives
Brief 24	Identity Theft	Brief 63	Transient Electro-Magnetic Devices (TEDS)
Brief 25	Secret Intelligence	Brief 64	Business Continuity Planning
Brief 26	White-Collar Crime	Brief 65	Body Language
Brief 27	Extremist Groups	Brief 66	Poisoning
Brief 28	Forensic-DNA Identification	Brief 67	Insider Threats
Brief 29	Scenario Based Intelligence Analysis	Brief 68	eCrime
Brief 30	Social Engineering	Brief 69	Suicide Bombers
Brief 31	Terrorism – Strategies & Tactics	Brief 70	Intellectual Property Theft
Brief 32	Computer Crime	Brief 71	Fraud in Business
Brief 33	Money Laundering	Brief 72	Social Networking Sites
Brief 34	Corporate & Industrial Terrorism	Brief 73	Secret Codes and Encryptions
Brief 35	Information Warfare	Brief 74	e-Discovery
Brief 36	Surveillance	Brief 75	Satellite Imagery
Brief 37	Gang Activity		
Brief 38	Computer Hacking		

## Detailed Abstracts

To help with your training brief selection process, please review the following abstracts. This will give you an overview of the information that is included in the brief.

Please see the last page of this catalog for ordering instructions or visit the Spy-Ops website, [www.spy-ops.com](http://www.spy-ops.com).

Volume/ Training Brief #	Title	Abstract
Brief 0	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.
<b>VOLUME 1</b>		
Brief 1	Unmanned Aerial Vehicles (UAVs)	In this brief, you will learn what an Unmanned Aerial Vehicle (UAV) is. We will take a look at various uses for them and the types of situation they may be needed for. UAVs have a number of advantages to regular piloted aerial vehicles. These advantages will be explored, and it will become clear why UAVs can be a much better choice than regular piloted vehicles in some instances.
Brief 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.
Brief 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.
Brief 4	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.

Brief 5	Human Intelligence Gathering 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.
<b>VOLUME 2</b>		
Brief 6	Global Positioning System	In this brief, you will learn the basics behind the Global Positioning System (GPS). You will discover how GPS was developed, and explore the components used to make the system work. You will see the basics of how points are found using the tracking system and identify some of the main uses for the system today.
Brief 7	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.
Brief 8	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.
Brief 9	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.
Brief 10	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>

<b>VOLUME 3</b>		
Brief 11	Long Range Microphones	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.
Brief 12	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.
Brief 13	Biological Warfare	Biological warfare (BW), also known as germ warfare, is the use of any living organism, whether bacteria, virus, or other replicating 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.
Brief 14	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.
Brief 15	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>

<b>VOLUME 4</b>		
Brief 16	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.
Brief 17	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.
Brief 18	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.
Brief 19	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.
Brief 20	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.

<b>VOLUME 5</b>		
Brief 21	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.
Brief 22	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.
Brief 23	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.
Brief 24	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.
Brief 25	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.
<b>VOLUME 6</b>		
Brief 26	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.

Brief 27	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.
Brief 28	DNA-Forensics 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.
Brief 29	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.
Brief 30	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 a person into revealing sensitive information, or getting 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 or 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.
<b>Volume 7</b>		
Brief 31	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.
Brief 32	Computer Crimes	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.

Brief 33	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.
Brief 34	Corporate & 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.
Brief 35	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.
<b>VOLUME 8</b>		
Brief 36	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.
Brief 37	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.
Brief 38	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.

Brief 39	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>
Brief 40	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>
<b>VOLUME 9</b>		
Brief 41	Situational Awareness	<p>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.</p>
Brief 42	International Drug Trafficking	<p>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.</p>
Brief 43	Smuggling	<p>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.</p>
Brief 44	Tracking Terrorist Financing	<p>This brief will explore the domain of terrorist financing. It will reveal what activities are involved in raising money for terrorist activities and how</p>

		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.
Brief 45	Nuclear Weapons (Bonus Brief)	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.
<b>VOLUME 10</b>		
Brief 46	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.
Brief 47	International Law	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. Finally, it will define INTERPOL and its role within the world of international law.
Brief 48	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.
Brief 49	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.
Brief 50	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.
<b>VOLUME 11</b>		
Brief 51	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.
Brief 52	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.
Brief 53	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.
Brief 54	Cyber Terrorism- Telecommunications & Network Warfare	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.
Brief 55	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.

VOLUME 12		
Brief 56	Financial Warfare	<p>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.</p> <p>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.</p>
Brief 57	Cultural Warfare	<p>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.</p>
Brief 58	School Violence	<p>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.</p>
Brief 59	Resource Warfare	<p>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.</p>

Brief 60	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>
<b>VOLUME 13</b>		
Brief 61	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 Americans are staggering. This epidemic has now also spread to Canada. During fiscal 2005-2006, the Financial Transactions and Reports Analysis Canada (FINTRAC), the Canadian equivalent to the Financial Crimes Enforcement Network (FinCEN) in the United States, made 168 mortgage case disclosures, of which:</p> <ul style="list-style-type: none"> <li>• 134 were for suspected money laundering,</li> <li>• 33 were for suspected terrorist activity financing, and</li> <li>• 1 case disclosure involved both suspected money laundering financial fraud.</li> </ul> <p>In 2005, the U.S. Mortgage Brokers Association (MBA) mortgage estimation topped \$2.7 trillion. Experts estimate that 10% to 15% of loans involves some kind of fraud. This means that between 2 to 3 home loans originated this year could be fraudulent; that equates to new fraudulent loans every business day. As the mortgage market and innovative ways to defraud financial institutions will appear.</p>
Brief 62	Bombs and Explosives	<p>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 understand of bombs and explosives and their use in terror attacks.</p>

Brief 63	Transient Electromagnetic 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 <b>call</b> 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.
Brief 64	Business Continuity Planning	In the 21 <sup>st</sup> century, few business professionals realize the vulnerability of their businesses to any outside force that will disrupt normal business operations. It is now generally recognized that operational risk assessment planning and disaster recovery planning are vital activities. However, the creation of (and maintenance of) a sound business continuity and disaster recovery plan, is a complex undertaking, involving a series of steps.
Brief 65	Body Language	Everyone is looking for an edge. What if you could tell how people are really feeling? What if you could interpret subtle gestures? Every subtle gesture has a meaning that can give you the edge when it comes to intelligence gathering and working with human assets. Equally important, you need to be aware of the same gestures that could give away your secrets. This brief will look into the use and interpretation of body language. It will describe what selected voluntary and involuntary bodily reactions can mean and how these interpreted meanings can be used by others.
<b>VOLUME 14</b>		
Brief 66	Poisoning	Poisons have been used throughout history as an effective assassination tool. The danger of these poisons, well known to pathologists, is that their effects can be both cumulative and insidious. When such toxic elements are easy to obtain, particularly when they occur in one's everyday surroundings, one can be slowly poisoned without ever becoming aware that something is wrong. Many leave little trace evidence in the body, and they are easily produced and delivered to the victim. These lethal products are supplied by Department 12 of Directorate S of the SVR (the Russian foreign intelligence of service) or FSB/KGB, which deals with biological warfare. This brief will look into the world of poison as a political and corporate weapon. It will look at the history of rising concern over poisoning capabilities. In addition, it will look at instances in both areas where poisoning has been used or suspected.

Brief 67	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, they 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 and that makes 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 insiders have risen to the top of the threat matrix. This brief will examine why the CIA, FBI, DoD, Secret Service and others have all completed significant research on this topic.
Brief 68	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 January 15, 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. This brief provides an understanding of eCrimes.
Brief 69	Suicide Bombers	Since the 1980s terrorist organizations have begun using suicide attacks as a way to invoke massive casualties on a location, as well gain the attention of their enemies and invoke a reaction from the international world community. The method of suicide attacks has increased in numbers especially in areas where major conflicts are occurring. The possibility of a future suicide attack within the continental United States is a real and frightening reality.
Brief 70	Intellectual Property Theft	Intellectual property has become the prized product of the 21st century. Authoritative sources have estimated that nearly 80% of an organization's value is held in its information, and the vast majority of that data is considered Intellectual Property. This is clearly proven when you consider IBM generates more revenue form licensing intellectual property than it does from product sales. This brief will examine and define the different areas of intellectual property and their importance in today's economy. IP has been targeted by competitors and foreign powers as a means to gain an advantage over their adversaries. This brief will explain why the protection of such property is so important, and describe the measures the government is taking to protect it.
<b>VOLUME 15</b>		
Brief 71	Fraud in Business	While the crime rate in the United States has dropped over the past few decades, one area of crime has continued to increase and be discovered in the American business community. Business fraud has continued to threaten the existence of companies as well the lives of their employees. White collar criminals through acts of criminality and greed have continued to engage in various fraud activities to enrich themselves at the expense of many. This brief will introduce the reader to various types of fraud in the American business community.

Brief 72	Social Networking Sites	<p>The evolution of the internet continues. One of the latest and most rapidly growing subsets of the web are what have commonly become known as social networking sites. In the past five years, social networking websites have become increasingly popular among Internet users, especially teenagers, as a place where they can meet other people. Social networking sites increase a person's circle of friends, increase an organization's ability to interact with their employees and expand a company's ability to communicate with customers. Social networking may sound fluffy, but it can translate into real benefits for an organization. While these sites are extremely valuable to individuals and organizations, they also can increase an organization's risk and exposure to people with less than friendly intentions.</p>
Brief 73	Codes & Encryption	<p>Secret codes and encryption are not just for spies; they protect your online credit-card purchases, and other important and sensitive information. Secure ways of communicating are hugely important to companies as more and more of their business is now being done electronically. Cryptography is the discipline of using codes, ciphers and encryption to obscure a message and make it unreadable unless the recipient knows the secret to decrypt it. For thousands of years secret messages, sent in code, have been used by various cultures throughout the world. The techniques used to cloak messages have become more and more complicated. Now, thousands of words can be hidden in a pixel of a photograph with little hope of being found by anyone but the intended receiver. Secret codes and encryption are the primary tools that are required for the tradecraft. This training brief will provide the basic information necessary to understand and use codes and encryption.</p>
Brief 74	eDiscovery	<p>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 eDiscovery. This training brief will provide the eDiscovery background needed to understand its implications to citizens and corporations alike in today's environment.</p>

Brief 75	Satellite Intelligence	Satellites affect our lives every day, and we often don't even realize it. They make our lives safer, more convenient, and provide entertainment. In little more than a generation, the launching of a satellite has gone from stopping the nation's business to guaranteeing that it runs like clockwork. Today, satellites, like clocks, telephones, and computers are commonplace tools of technology. They help us navigate, communicate, monitor the environment and forecast weather. Appropriately, the word satellite means an "attendant." This brief provides an overview of satellite technologies that can be used to provide a multitude of services. In the brief we provide a snapshot of the current and future satellite capability. The last section explores the key issue of intelligence and data collection as well as integration.
----------	------------------------	---

## About SPY-OPS

Spy-Ops is a leading provider of security, intelligence, defense and risk management & 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. 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 through effective continuing education.

## Ordering Information

The cost for each Spy-Ops Training Brief is \$12.95. We accept credit card, check, money order or PayPal payments.

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

To order training briefs:

Option 1) Order online at [www.spy-ops.com](http://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](mailto: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](mailto:info@spy-ops.com)

---

### Spy-Ops Training Brief Order Form

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

     Name on Card \_\_\_\_\_  
Payment Request Will be Sent Card Number \_\_\_\_\_  
Expiration Date \_\_\_\_/\_\_\_\_ Security Code \_\_\_\_\_

Authorizing Signature: \_\_\_\_\_

I prefer to receive the Training Briefs I have selected by:

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

## Spy-Ops Training Brief Order Form (Page 2)

Name: \_\_\_\_\_

Order	Course #	Training Brief Name	Order	Course #	Training Brief Name
<input type="checkbox"/>	A	Corporate Espionage	<input type="checkbox"/>	38	Computer Hacking
<input type="checkbox"/>	B	Disaster Preparedness Kit	<input type="checkbox"/>	39	Personal Protection
<input type="checkbox"/>	1	Unmanned Aerial Vehicles	<input type="checkbox"/>	40	Travel Security
<input type="checkbox"/>	2	Body Armor	<input type="checkbox"/>	41	Situational Awareness
<input type="checkbox"/>	3	Armored Vehicles	<input type="checkbox"/>	42	International Drug Trafficking
<input type="checkbox"/>	4	Creating a Microdot	<input type="checkbox"/>	43	Smuggling
<input type="checkbox"/>	5	Human Intelligence Gathering Techniques	<input type="checkbox"/>	44	Tracking Terrorist Financing
<input type="checkbox"/>	6	Global Positioning Systems	<input type="checkbox"/>	45	Nuclear Weapons
<input type="checkbox"/>	7	Digital Spying	<input type="checkbox"/>	46	UnRestricted Warfare
<input type="checkbox"/>	8	How Spies Get Caught	<input type="checkbox"/>	47	International Law Warfare
<input type="checkbox"/>	9	Interrogation	<input type="checkbox"/>	48	Economic Warfare
<input type="checkbox"/>	10	Islamist Terrorism	<input type="checkbox"/>	49	Critical Infrastructure Protection
<input type="checkbox"/>	11	Long Range Microphones	<input type="checkbox"/>	50	On-line Child Exploitation
<input type="checkbox"/>	12	Dirty Bombs	<input type="checkbox"/>	51	Technology Warfare
<input type="checkbox"/>	13	Biological Warfare	<input type="checkbox"/>	52	Political Warfare
<input type="checkbox"/>	14	Electronic Bugging Systems	<input type="checkbox"/>	53	Psychological Warfare
<input type="checkbox"/>	15	Chemical Weapons	<input type="checkbox"/>	54	Cyber Terrorism
<input type="checkbox"/>	16	Security Systems	<input type="checkbox"/>	55	Environmental warfare
<input type="checkbox"/>	17	Introduction to Intelligence Technology	<input type="checkbox"/>	56	Financial Warfare
<input type="checkbox"/>	18	Improvised Explosive Devices	<input type="checkbox"/>	57	Cultural Warfare
<input type="checkbox"/>	19	Domestic Terrorism	<input type="checkbox"/>	58	School Violence
<input type="checkbox"/>	20	Biometric Security Devices	<input type="checkbox"/>	59	Resource Warfare
<input type="checkbox"/>	21	Directed Energy Weapons	<input type="checkbox"/>	60	Cyber-Bullying
<input type="checkbox"/>	22	Terrorist Recognition	<input type="checkbox"/>	61	Mortgage Fraud
<input type="checkbox"/>	23	Digital Footprints	<input type="checkbox"/>	62	Bombs and Explosives
<input type="checkbox"/>	24	Identity Theft	<input type="checkbox"/>	63	Transient Electro-Magnetic Devices (TEDs)
<input type="checkbox"/>	25	Secret Intelligence	<input type="checkbox"/>	64	Business Continuity Planning
<input type="checkbox"/>	26	White-Collar Crime	<input type="checkbox"/>	65	Body Language
<input type="checkbox"/>	27	Extremist Groups	<input type="checkbox"/>	66	Poisoning
<input type="checkbox"/>	28	Forensics-DNA Identification	<input type="checkbox"/>	67	Insider Threats
<input type="checkbox"/>	29	Scenario Based Intelligence Analysis	<input type="checkbox"/>	68	eCrime
<input type="checkbox"/>	30	Social Engineering	<input type="checkbox"/>	69	Suicide Bombers
<input type="checkbox"/>	31	Terrorism - Strategies & Tactics	<input type="checkbox"/>	70	Intellectual Property Theft
<input type="checkbox"/>	32	Computer Crime	<input type="checkbox"/>	71	Fraud in Business
<input type="checkbox"/>	33	Money Laundering	<input type="checkbox"/>	72	Global Intelligence Estimate
<input type="checkbox"/>	34	Corporate & Industrial Terrorism	<input type="checkbox"/>	73	Secret Codes and Encryptions
<input type="checkbox"/>	35	Information Warfare	<input type="checkbox"/>	74	E-Discovery
<input type="checkbox"/>	36	Surveillance	<input type="checkbox"/>	75	Satellite Imagery
<input type="checkbox"/>	37	Gang Activity			

I have selected \_\_\_\_\_ Training Briefs at a cost of \$12.95 each.

Total Cost for this Order: \_\_\_\_\_ Training Briefs x \$12.95 = \_\_\_\_\_

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

**Thank you for placing an order with Spy-Ops!**

