

The BlackEagle BlackEagle Operatives Kit



Tactics and Techniques

**for Getting the Job Done,
Getting it Done Right,
and Keeping Yourself Alive
While Doing It**



1999 Edition, v2.0
Publication Number 167A
BlackEagle/BlackEagle Security and
Investigations Corporation
Logistics and Procurement Branch
Atlanta, Georgia

Forward

Back in 1994, when there were only forty or fifty people working for this company, then Senior Operative Charlie Doyle's idea of setting up a training course for new employees seemed a little ambitious. Sure, we were adding two or three offices a year and bringing in half a dozen new operatives each month. But at the time it seemed like there were enough ex-cops, FBI men, and special forces guys to fill our requirements, and these people didn't need much extra training. But Charlie figured it wouldn't be too long before we would be hiring people with more diverse backgrounds, and sending them into a broader range of assignments. He convinced me then, and it turned out he was right. We still hire our share of military veterans and secret-service retirees, but we also bring in computer specialists, law-school graduates, and even ex-cons. The Basic Operative Training Course, which Charlie first put together in 1995, has made sure that all of our operatives, regardless of their backgrounds, have a good foundation of training in the kinds of things we do.

But the truth is, we do too many things for each operative to be an expert in them all. That's why operatives work in cells—an arrangement that takes advantage of the strengths of everyone involved. Unfortunately, even this system doesn't guarantee that every cell is strong in every type of task. The Basic Training Course has been expanded three times since it was instituted, but it still barely touches on some of the tasks that are very important to your success, and even your life.

In 1998, Alex O'Grange, head of the Operations Branch, suggested a reference manual that would sort of "fill in the gaps." The proposed book would cover many of the same fundamentals taught in the Basic Training course, going into a little more detail on the kinds of activities we carry out the most. With a copy of this book in the hands of every operative, skills

that might be forgotten (or simply never fully covered in training) would stay fresh, and there would be a company SOP on common tasks. I instructed the L&P Branch to get started on this book in August of 1998, and assigned a team of four personnel from Operations and L&P's training department the task of writing it. The first edition hit the streets in early '99, and the response was overwhelming. We blew through the first printing in a week, and operatives from every office started sending in their ideas for an expanded edition. Well, here it is.

One of the most basic decisions that had to be made before writing the first book regarded our philosophy of instruction. A number of people, myself included, were worried that we would create a "book" with a capital "B," as in "by the Book." Anyone who's worked for this company long knows how we shy away from top-down commands, especially when it comes to your cell and how you carry out your operations. We didn't want to create a set of rules that people would interpret as the only, or even the best, way of doing things. The broad range of our activities means that we'd need a thousand variations of a thousand tasks to cover every contingency, and that's impractical even if we wanted to do it. What we did want to do was to gather the wisdom of experienced operatives, experts in their specialties, so that you could learn from their experiences. I think that has been achieved with this book. You, the operative who will benefit from this accumulated knowledge, must remember that these are just guidelines. Incorporate them into your own SOP, but don't feel that the methods contained here are the only methods available. As always, I encourage you to rely on your own resourcefulness.

I want to make one additional point. The strength of a BlackEagle cell is in the individual operatives, and how they act as a team. In any sort of task—especially the kind of trouble we get into—your coordination will make the difference. Learn to work together well. Practice. Develop your own ways of doing things. Act as an organism, so that your response to the unexpected is effective and smooth. Rely on one another, and be reliable.

I hope this book makes your job a little easier and a little safer. Keep your L&P rep informed of any changes you think it needs, or anything not included that should be. Like the Basic Operative Training Course, this handbook will continue to evolve over time, to meet the needs of our operatives and the constantly-changing nature of our assignments.

And best of luck out there—even the best need it sometimes.

CLIFTON BLACKEAGLE

Clifton BlackEagle, President
May 16, 1999

Table of Contents

Chapter 1: Investigation Management	8
The Investigative Process	9
Types of Investigations ... The Requirements of Evidence Your Legal Rights and Authority	
Basic Leads	16
Clients, Victims, and Witnesses ... Motive, Benefit, Knowledge, and Opportunity ... Vehicles ... Evidence Analysis and Forensics ... Criminal Records ... Informants ... Surveillance Public Record Sources ... Private and Restricted-Access Record Sources ... Other Leads	
Event Investigating	40
The Event Scene ... Preliminary Investigation ... Picking up a Cool Trail ... Continuing Investigation ... Evidence Handling	
Background Investigation and Information Searches	54
Background Checks ... Smokescreens and Hidden Information	
Chapter 2: Protecting Yourself and Those Around You	62
Home Security ... Movement and Public Activity ... Travel Protecting Yourself on the Job	
Chapter 3: Physical Security and Surveillance Systems	70
Security Systems ... Instruments of Security ... Weak Links	
Chapter 4: Tactical Operations	78
The Basics	79
Planning Tactical Actions	80
Being Prepared for the Unplanned Incident	
Tactical Principles	84
Assault and Support ... Security ... Stealth and Speed Sectors of Fire and Defense	
Rules of Engagement	96
Non-Lethal Weapons ... Appropriate Ammunition	
Command, Control, Communications	100

Movement in the Tactical Environment	102
Rally Points and Objective Rally Points ... Link-ups	
Approaching the Objective ... Danger Areas	
Bodyguarding and Personal Security	112
Types of Jobs and Threats ... The Rules of Bodyguarding	
Personal Security Tactics	
Urban Problems	118
Movement in the Urban Environment ... Urban Tactical	
Hazards ... Clearing a Zone ... Storming a Building	
Suppressing a Sniper	
Interior Problems	130
Moving Indoors ... Interior Tactical Hazards ... Infiltration	
Clearing a Room	
Field Problems	138
Tactical Travel in the Field ... Field Tactical Hazards	
Patrols and Patrol Bases ... Ambushes ... Recons ... Raids	
Actions on and after the Objective	154
Chapter 5: BlackEagle/BlackEagle: Company Methods and Policies	158
The Company	159
History and Scope ... Organization ... Senior Staff	
Operations Policy	164
Following Policy ... Cell Organization ... The Operations	
Roster ... Operative ... Status ... Operations Restrictions	
Contracts ... Contract Payment ... Multi-Cell Operations	
Safehouses and Relocation	
Support	176
Office Representatives ... Equipment ... Forensics ... Legal	
Aid ... Medical Support	
Security	179
Physical Security ... Operational Security ... Counter-Sur-	
veillance Measures ... Weapons Policy	
Employee Policies and Benefits	182
General Benefits	

■ **The Real Scoop**

This is the BlackEagle Operatives Kit, a book chock full of tips and tricks for successful modern roleplaying adventures. You may have noticed, if you've scanned the book already, that it's laid out not as a game supplement but as if it were a real publication—an actual handbook for BlackEagle operatives. Aside from this page, and the back cover text, you won't find a single reference to GMs, players, or the *Millennium's End* game system in this publication. Just loads of great ideas for your characters to use in their adventures.

The absence of game mechanics means there's nothing here that tells you how these tips and techniques affect game rules. That's OK—the ideas in this book aren't new rules, and their use doesn't have to be guided by skill rolls or mechanics. Your GM may want to require a Police Science, Military Science, or other appropriate skill roll to see how well your characters implement these ideas, and many of the tasks obviously require specific skills to carry out. Use common sense and the same methods you'd use to resolve any other idea or strategy your character might come up with for dealing with a hazardous or difficult situation.

There's also no specific information on how the GM can counter these techniques. That's also OK. Just remember, none of these techniques are foolproof—in most cases, many of their weaknesses are discussed in the text. Even more importantly, your GM is perfectly free to have his or her NPCs use these tricks against your characters. Players and GMs alike can benefit from the ideas in this book.

The BlackEagle Operatives Kit v2.0

Written and illustrated by Charles Ryan, with additional writing by Steve Long
Special thanks to Kelly Crane, Ryan Pendergast, Cedric Ponchy, and Joni Virolainen, and to the other supportive subscribers to the Millennium's End internet mailing list

First Printing

© 2001 Hero Games, Inc. All rights reserved. No portion of this text may be reproduced without the written consent of Chameleon Eclectic Entertainment, Inc.

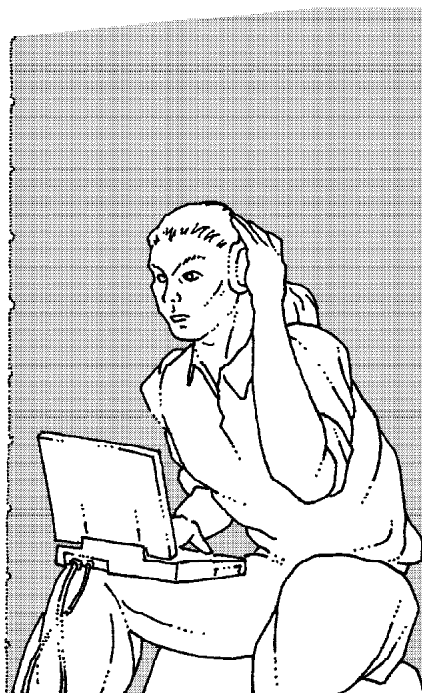
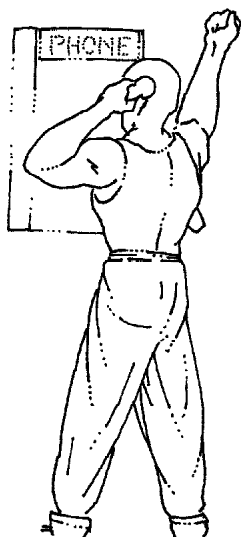
Hero Games, Inc.
35 Pamaron Way, Suite D Novato, CA 94949

www.herogames.com

Techniques Index

Using this Book	11	Radio Prowords and the Phonetic Alphabet	89
Evidence Kits	13	Hand and Arm Signals	91
What To Do if Arrested	15	Deploying Non-Lethal Gasses	95
Fundamentals of Personal Identification	17	Deploying Non-Lethal and Restraining Weapons	97
Informants and Witnesses	19	Tactical Movement Formations— the Diamond	99
Fundamentals of Vehicle Identification	21	Tactical Movement Formations— the Wedge	101
Vehicle Searches	23	Tactical Movement Formations— the File	103
Detecting Concealed Weapons	25	Tactical Movement Formations— the Line	105
Knowing Illicit Drugs and their Effects	27	The Herringbone	107
Following up on Gang Crimes	29	Breaking Contact	109
Stakeouts	31	Crossing a Danger Area	111
Shadowing	33	Scroll to the Road	113
The ABC Shadowing Method	35	Personal Security on the Road	115
Shaking Tails	37	The Hostile Meeting	117
Conducting Interrogations	39	Urban Movement Hazards	119
Holding out under Interrogation	41	Urban Movement Techniques	121
Evidence Collection	43	Diversions	123
Taking Fingerprints	45	Dealing with Hostage Situations	125
Dealing with Kidnappers	47	Searching Prisoners and Bodies	127
Getting around locks	49	Trauma in Combat	129
Cracking Secret Organizations	51	Interior Movement Hazards	131
Police Investigation Reports	53	Interior Movement Techniques	133
Autopsy Reports	55	Area Search Techniques	135
Social Security Numbers	57	Shaking Trackers	137
High-speed Pursuit	59	Field Movement Hazards	139
Bribery	61	Field Movement Techniques	141
A Home Security Kit	65	The Near Ambush	143
Countersurveillance on the Road	67	Surviving an Ambush	145
Office Security Drill	69	Field LZs	147
Security Strategy	73	Helicopter Insertions and Extractions	149
Dealing with Motion Detectors	75	The Objective Recon	151
Dealing with Wires and Beams	77	Conducting a Raid	155
Working with an OpOrder	81		
The Five-Point Contingency Plan	83		
Field Tactical Kits	85		
Passwords	87		

Chapter 1: Investigation Management



Not every BlackEagle assignment is an investigation, but most require some investigating. Even in a totally tactical assignment, you may need to do some background research or gather intelligence on your objective. If only for this reason alone, solid investigative skills are necessary even for the total grunts amongst us.

■ The Investigative Process

An investigation is a process of searching for facts, then assembling those facts into an understanding of the person, event, or thing being investigated. Good investigation requires several things. You must understand your objective. You must know the sources and resources available to you. But more than anything else, you must have imagination, curiosity, and stamina. Great analytical minds are few and far between, but thousands of investigators in the public and private sector make up for average IQs by imaginatively seeking out leads and pursuing them with tenacity and genuine interest.

Types of Investigations

In our line of work, there are three basic sorts of investigations that we carry out: event investigations; background investigations; and information searches. Although the distinction between these three types is vague and they often overlap, there are important differences in their objectives.

- **Event investigations** seek to understand given events—usually crimes—to determine what happened and how, and who was responsible. Missing persons, thefts, murders, acts of piracy and terrorism, and sabotage are just a few of the many types of events that B/E ops are hired to investigate. Most of these are crimes, but the focus of an event investigation may be civil, like investigating the cause of an accident for an insurance company. Some espionage assignments, including private-sector espionage, include event investigations.

- **Background investigations** gather a large quantity of information on a particular subject, like a terrorist organization, a business, or a criminal suspect, with the intent of gaining a greater degree of insight into the subject's activities, motives, and day-to-day existence. Background investigations may be assignments in and of themselves—for example, you may be hired to investigate a company that is suspected of ties to organized crime. Or, the background investigation might be a subset of

a larger event investigation—like learning all you can about one of your main suspects while investigating a murder.

- **Information searches** look for specific pieces or types of information. Information searches are most often part of another investigation, but may be required in an assignment that is otherwise totally non-investigative. For example, you may want to track down a set of construction plans for a building you wish to enter. Often, carrying out an information search is as easy as glancing through a GenNet directory. But when a particular piece of information is carefully guarded, a search for it can be a long and difficult task.

These general types of investigations can be hierarchical. An event investigation frequently includes background investigations of important individuals and organizations, each of which may involve dozens of information searches. When carrying out a large and complex investigation, break it down into its subset background checks and information searches. This will help you organize the tasks and carry out each thoroughly. Be certain, however, to fully integrate the results of each segment with the whole—to see the big picture. The key to solving complicated mysteries often lies simply in seeing a relationship between two otherwise insignificant pieces of information. Don't overlook such a relationship because your information is too fragmented, especially when you split up different tasks amongst the members of your cell.

The Requirements of Evidence

The role of evidence in an investigation varies greatly depending on the type of investigation you are carrying out and the needs of the client. Law enforcement investigators always look to provide evidence admissible in court, and sufficient to prosecute beyond reasonable doubt. This is not generally the case with BlackEagle cells. Sometimes you will need to create a watertight case supported by undeniable, legally admissible evidence. Other times you will only need to satisfy yourself. There are a thousand variations in between. To generalize, however, we can say that there are three cases:

- **Evidence for your use.** Often, an assignment will call for a physical result, with no stipulation for how it comes about. You may be asked to recover a piece of stolen merchandise, to locate and retrieve a hostage, or carry out some other task that will have to start with some investigating. Any evidence recovered in that investigation is for your use only—you don't have to satisfy anyone else as to its importance or validity. The evidence is sufficient if it gets results.

- **Evidence for the client's use.** Other assignments may require you to investigate on your client's behalf, bringing him or her your

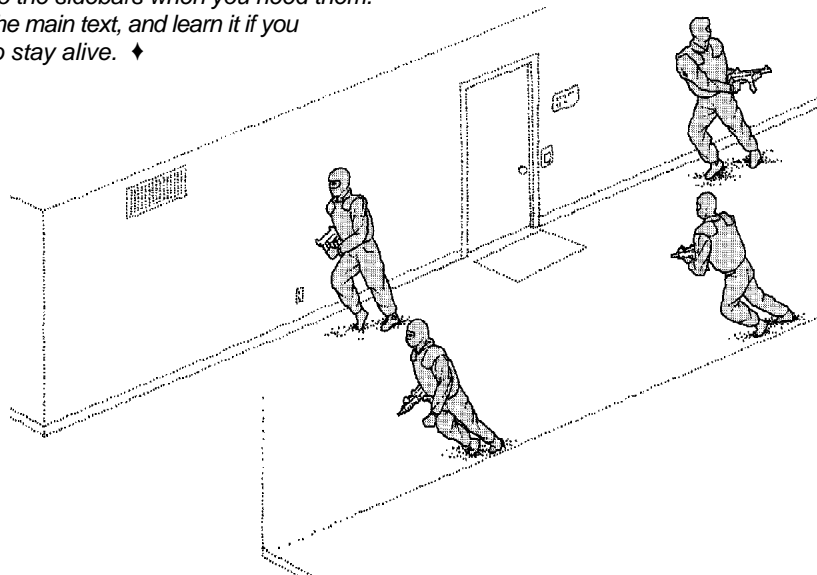
Techniques: Using this Book

The advice and guidelines in this book are presented in two bodies of information: the main text (like that opposite); and the sidebars (on every right-hand page, like this one, throughout the first four chapters). The main text covers investigations and tactical operations, important topics in overview, and general methods for getting things done and keeping alive while doing them. It includes plenty of details and examples, but focuses mainly on theory—the fundamental concepts underlying specific techniques. The sidebars illustrate specific situations, techniques, and tips. They provide more in-depth information on the material in the main text, and give examples of specific techniques that you can use on assignment—how to detect and slip past tripwires; how to conduct an ambush or survive one sprung on you; how to tail a suspect, or shake a tail that's following you. Being separated, and located on each right-hand page, they're handy for quick look-ups. The original edition of this book featured nineteen such "Techniques" sidebars—this edition has been dramatically increased, with almost seventy.

Nevertheless, a book like this couldn't possibly cover every difficulty you'll encounter in the field. That's why the main text is so important—the principles it contains are good, solid guidelines that you can apply to a wide array of situations. They are the foundation upon which all the techniques and tips in the sidebars are based. Learn them. Use them. They'll help you finish your assignments and live to talk about them.

As for the Techniques sidebars, remember that every situation is different, and these tips and how-tos are only examples. If you understand what they're showing you—why they work—you'll learn how to adapt them to the unique situations you'll face while out in the jungle or on the streets. That takes us back to the importance of the main text, and the fundamental principles that are so important to understanding your work.

Refer to the sidebars when you need them.
Read the main text, and learn it if you
want to stay alive. ♦



conclusions. You may be asked to discover an information leak, look into a competing corporation's activities, or identify the perpetrator of a crime. In such cases, the client sets the standard of proof—you must provide enough evidence to convince him that your conclusions are correct. Keep in mind that sometimes the client may have to convince someone else—like his or her boss, for example. You may need to go beyond the level of proof that satisfies both you and the client.

- **Evidence for legal prosecution.** Sometimes you will be hired by a government agency to investigate a crime, or by a private organization or citizen that doesn't trust the results or methods of the government. In the latter case, you may be working for the prosecution or the defense. The prosecution must prove guilt beyond a reasonable doubt, while the defense tries to show that reasonable doubt remains. Your evidence must be legally admissible, support the goals of your side, and be able to withstand the legal scrutiny of the opposition. Physical evidence is very important in legal cases, and requires special handling and accountability (see Evidence Handling, below).

The use of evidence in investigations is three-fold. Obviously, evidence can generate investigative leads. Some of the most common types of leads generated by physical evidence and testimony are covered below under Basic Leads. Process and consider every piece of evidence you can get your hands on, even those that seem irrelevant, because you never know how important a piece of information will be at a later stage in your investigation.

Evidence can also be used to limit leads. This can be an equally important function, because it can narrow your field of suspects and help you refine your theory of events. Take advantage of opportunities to use eliminative evidence. For example, take fingerprints from everyone with regular access to the scene of a crime, even if you don't really suspect them. When lab comparisons with the prints left by the perpetrator turn up negative, you can safely remove those people from your list of suspects.

Finally, evidence is used in legal prosecution. Legal evidence can't just tell you who committed a crime—it must prove it. This is a very important distinction, because if a defense can find any reasonable doubt in the evidence provided by the prosecution, the verdict will be innocent regardless of how obvious the guilt of the accused (at least in the United States). When you are investigating for legal prosecution, be sure you have good accountability of physical evidence, and that your methods don't threaten the evidence's admissibility. Then, when putting together the case, go through the evidence accumulated, and figure out how much of it is legally relevant (much of your lead-generating and eliminative evidence won't be). Bolster it with additional forensics and testimony until the case is as airtight as possible. Be sure to consult with your office legal

Techniques 1: Evidence Kits

You need a good evidence kit to process an event scene, and it's a good idea to keep some basic evidence gathering supplies on hand all the time. The two lists below cover a complete, heavy-duty kit and another, more portable kit you can keep handy.

Full-sized Evidence Kit

- flashlight and portable floods.
- 50-foot tape measure.
- 18-inch ruler.
- photographic equipment, including still and video cameras, tripod, lenses, flash, and color and B&W film.
- tweezers, forceps, scissors, and razor blades.
- zip-lock bags in a variety of sizes.
- jars and boxes in a variety of sizes.
- garment bags.
- masking and duct tape.
- graph paper, notebook, pens, chalk and crayons.
- a magnifying glass and hand mirror.
- a fingerprint digitizer or kit.
- a plaster mold kit.
- a thermometer.
- a basic tool kit.
- a compass.
- a tape recorder.
- towels.

This complete kit can be put together in two or three good-sized duffle bags or tool boxes. In addition to these items, it's a good idea to have specialized equipment, like vacuum samplers and chemical sniffers, available.

Portable Evidence Kit

- a flashlight.
- a 12-foot tape measure.
- an 18-inch ruler.
- a still camera with flash and film.
- tweezers, forceps, and scissors.
- zip-lock bags in several sizes.
- graph paper, a notebook, and pens.

These items can be kept in a small duffle bag or tool box. Keep a kit like this in the trunk of your car or some other handy location where it can be left indefinitely (you never know when you'll need this sort of stuff). Always have a kit like this nearby when working on investigative assignments. ♦

counsel, to make certain you have done everything possible to meet your legal requirements.

Your Legal Rights and Authority

The issue of legal authority is well covered in the BlackEagle Basic Operative Training course, but the basics are worth covering again here. It is important that you understand your rights and authorities clearly, so that you can protect yourself from litigation. Operatives who injudiciously overstep their bounds make themselves, and the company, liable to suit or prosecution for anything from false arrest to assault with a deadly weapon.

In general, an operative has the same legal authority as any other private citizen. In the United States, that means that you can arrest a suspect if the crime was committed in your presence. Only a sworn law officer may make an arrest based upon suspicion—and you aren't a law officer. You must have caught the person in the act, and be able to prove it, or you can be prosecuted or sued by the offender (even if he's guilty).

Arrest means detaining someone, then forcibly turning him or her over to the proper authorities. The law allows considerably more leeway to *detain* someone without arresting him. Businesses in most states, for example, are permitted to use "reasonable force" to detain someone for a "reasonable period of time" if there is probable cause to believe that the person has committed a crime on the premises, like trespassing or shoplifting. However, legal interpretations of "reasonable force," "reasonable period of time," and "probable cause" are vague, and may vary from locality to locality. As with arrest, detention can be a tricky proposition if you are not absolutely certain of what you are doing.

Searching another person is even thinner ice. In general, you are only safe if the suspect gives you permission to search—that includes searching the suspect's belongings as well as their person. The law is vague concerning involuntary searches—and that vagueness is more likely to work against you in court than to protect you. Generally speaking, if you're searching a person because you know or have good reason to suspect that they're carrying a weapon, you're on better legal ground than if you're simply looking to see what he's carrying.

Interrogation, however, is one area that is relatively safe. You can ask a suspect anything you want, without giving advice of rights as a police officer must, and he or she may or may not answer. But there are a couple of pitfalls. Questioning a suspect within earshot of bystanders may make you liable for slander, if the questions imply any sort of criminal wrongdoing. Furthermore, coercive questioning techniques run the risk of assault and battery charges. A suspect can also go back on statements

Techniques 2: What to do if Arrested

Arrest and legal difficulties are an occupational hazard for the BlackEagle operative. All operatives and cells should be prepared for the possibility, whether operating in their home cities or halfway around the world.

What happens on arrest varies dramatically from country to country. In all cases, the arrested persons are removed to a police station, jail, or similar official location, where they are generally separated, in-processed (identified and fingerprinted), questioned, and held. In developed countries, and most Third World countries, the arrestee is allowed contact with the outside world—the proverbial “one phone call” is a minimum, and many municipalities allow more or even place pay phones within holding cells.

At your first opportunity after arrest, call your office. Call the office before trying to reach anyone else—including your cell, your family, the embassy, your lawyer, your friends, anyone. There should be someone at the office to take your call any time of day or night, and the office can reach anyone that needs word of your situation. Furthermore, your Senior Cell Leader and office legal aide can work effectively for your freedom from the moment you contact them, and can coordinate the efforts of your fellow operatives as needed.

Regardless of your guilt or innocence, make no statement to the police without the legal assistance provided by the office. The police may attempt to get you to talk by insisting that only the guilty need lawyers, or that your fellow operatives have already made statements. Do not believe them—there is no law or regulation that prevents police from using misdirection and deceit in their interrogations, even in the U.S., where police conduct is constantly subject to legal scrutiny. Even if you are 100% completely innocent of all charges, say nothing without legal help—anything you do say can be used against you, and it’s not unheard of for operatives to face trumped-up or fabricated charges—or even frame-ups—brought by corrupt officials or enemies of the company.



If (once you’re in contact with your cell or the company) you must discuss issues related to your current assignment, be careful. You are not any guaranteed privacy while in jail, and conversations with visitors or on the phone may be monitored and used against you.

As in any case in which you’re in someone else’s hands (see the sidebar on being interrogated, on page 41), avoid confrontation with your captors. Behave reasonably and subserviently, regardless of the behavior or professionalism of your arrestors.

The American legal system assumes innocence until guilt is proven. Most of the rest of the world—even the developed world—does not. In any case, unless the charges against you are very serious and the evidence very compelling, the company should be able to get you out of jail on short order—but be mentally prepared for the worst. ♦

made under threat, meaning that coerced information may be of little legal significance unless backed up by good evidence.

Finally, there is the issue of lethal force. Restrictions on the use of lethal force are the same for civilians as they are for police: lethal force may be used in the immediate protection of your life or the life of another, *not* in the protection of property. If you reasonably believe that your life is in immediate danger (being threatened is not enough, unless the threat is backed up by the display or use of a deadly weapon), you may use lethal force against the threat. In all other cases, using lethal force makes you liable for criminal prosecution for anything from assault to capital murder.

There are, of course, exceptions to all of these cases. Some security jobs, particularly some connected to the federal government or industries with high national security priority, have special guidelines. Make sure that you and your client understand any such guidelines, and include them as contract clauses.

There is another factor to keep in mind. Disregarding the above guidelines will make you vulnerable to legal attack if the suspect fully understands his rights and is inclined to prosecute. If the suspect has no legal recourse—if, for example, he is an underworld figure or wanted criminal—you might be able to act without fear of prosecution. Also, many people are ignorant of the limitations that we in the private sector face. People are impressed by an ID card, a gun, and air of authority. You may be able to bend the rules a little, to act with more authority than you really have. Keep the possible consequences in mind, though, because you always face some legal risk.

■ **Basic Leads**

The investigative process consists of identifying your leads, then following them through. Every investigation is unique, and no two sets of leads are the same, regardless of the similarity of the cases. Nevertheless, there are a number of leads or lead sources that show up again and again, and almost always get you somewhere when you run them down. These are covered in this section.

Clients, Victims and Witnesses

The client and, when applicable, the victim, are generally the first leads available to you in your investigation. Use them to develop an understanding of the context of the investigation, to reconstruct specific events, and to establish your initial leads. Additional witnesses, when available,

Techniques 3: Fundamentals of Personal Identification

Ask a typical witness to describe a suspect, and you'll probably get something like "average height, brown hair." Not very helpful. However, most witnesses retain a lot of useful information, they just need some help turning their mental picture into an accurate and concise verbal description. Knowing what to ask can help get that information out of a witness. It's also useful to have a mental checklist of details for recalling your own experiences—when you want to remember someone you've seen, go through these points mentally when you observe him or her, for easier and more accurate recollection later.

For your own recollections, it's always best to focus on telling details rather than generalities. Build and hair color are necessary, of course, but hardly telling—a birthmark, lisp, or tattoo is much more concrete. Also, remember that apparent information is far more important than factual info—in describing a person, how old she is isn't nearly as important as how old she looks.

Identifying points include:

- **Gender, race, and skin color.** The latter is important even when race is identified, as there can be a great deal of variation.
- **Age.** Avoid general terms such as "old" or "young"—such terms mean completely different things to different people. Get an estimate of age in years, even if your witness isn't confident about his or her accuracy.
- **Height and Weight.** These can be difficult to guess, but a witness may be able to make comparisons to bystanders or objects in the area. Many retailers (especially convenience stores) actually mark the door jamb, so that employees have a point of reference when they see a criminal enter or exit.
- **Build.**
- **Speech and Mannerisms.**
- **Scars, Marks, Deformities, and Tattoos.**
- **Hair.** Look for not just color, but also length, part (right, left, center or none), texture, and hairline.
- **Eyes.** Get expression and shape as well as color.
- **Facial Features.** Most people's faces can be described as oval, round, triangular, or long. Nose, mouth, chin, jawline, cheekbones, placement of the eyes, and facial hair are all notable features.
- **Clothing.**

Be sure to ask witnesses about all of these potential features, and make a note of them yourself whenever you see someone you might need to remember or describe in the future. ♦



can help flesh out your understanding of events and give you more leads to follow.

In any type of assignment, the first information you get is about the client. When you meet with a client for the first time, you see what he looks like and you size him up. You get a feel for his personality, you learn something of his goals, and you are probably told who he works for. The first step in your investigation is to learn even more about the client. What is his relationship to the subject of the investigation? To the victim of the crime, if it isn't him? To the perpetrator, if known? What are the client's suspicions or concerns? Why does he hold them? Does the client have a criminal past, or has he been a past victim? Most of these questions can be answered in the initial meeting with the client. The answers can give you a great deal of insight into the situation, as well as pointing to some beginning leads.

If this is an event investigation, especially one that involves a crime, turn your attention next to the victim, who may be your only available witness. If the victim is not the client, ask the questions in the above paragraph concerning the victim's relationships with the client and suspect, the victim's own suspicions, and the victim's criminal past. Regardless, find out the following: if it was a violent event, did the victim have a weapon? Did he or she use it? Does the victim have an aggressive personality? Could the victim have been mistaken for someone else? If the event was a property crime, what specifically could the criminal have been after?

Now you are ready to move on to other witnesses. Usually, Black-Eagle operatives aren't the first called to a crime scene. Chances are, therefore, that you will be dealing with witnesses well after the fact, possibly after they have already spoken with police. In any event, you want to identify and question witnesses as quickly as possible. The fresher the witness, the more willing he or she is to talk, the more truthful he or she will be, and less likely you are to get an "I don't remember" response.

Ask your witnesses to describe what he or she saw, briefly, but omitting nothing. Get an overview of the event as perceived, as well as specifics like description of the perpetrator or perpetrators, vehicles, direction of flight, and other activities. Be certain to get the witness's name, address and phone and GenNet numbers, so you can recontact him or her as necessary.

In all of the above contacts, you want to remain pleasant, sincere, and accessible. Witnesses and victims tend to be more open if you seem friendly and interested. Remember that they're on your side, even if they aren't particularly helpful or cooperative. You want them to come back to you if they learn or remember additional information. Make sure they have some way of reaching you, even if you are concealing your identity. For more tips, see the "Informants and Witnesses" sidebar, opposite.

Techniques 4: Informants and Witnesses

Getting information out of your witnesses and informants is sometimes harder than finding them. Witnesses are often frightened, mistrustful, or downright hostile. They usually want to know why you are questioning them, and sometimes you can't tell them. Successfully interviewing informants and witnesses, especially reluctant ones, requires a certain knack. Nevertheless, there are certain tricks and techniques that can make your interviews a little easier and more successful.

First of all, plan your interview. Even if you take just a few seconds to review your goals, it helps to know what you think you can learn, how you will approach your questions, and what your objective is. If you are conducting a covert interview, in which you are masking your identity or your intent, you must know your cover story before approaching the target.

You can't always choose the time and place for your interview, but at least try to pull the target aside, away from other people and background distractions. This will help your witness concentrate, and free him or her to say things he or she might not otherwise. For example, a witness is unlikely to badmouth an acquaintance in front of a mutual friend, and is very unlikely to say anything self-incriminating in front of anyone. Don't give group interviews, and never get a witness's name or address within earshot of a potential suspect.

When you've worked out your plan and chosen a location, your next concern is approach. You always want to align yourself with the witness. Be open, even sympathetic, as friendly as the circumstances allow, but businesslike. Show an interest in what the witness has to say. Always give the witness room to save face—never use terminology that appears to incriminate or accuse. Ask questions that invite lengthy answers. Ask the witness' opinion on the events you discuss. Avoid expressing opinions of your own.

Don't give the witness any information that telegraphs your own intent or knowledge, even with a seemingly harmless witness or in a completely overt investigation. Sprinkle in questions with little or no relevance, or questions for which you already have the answer. This will keep witnesses from second-guessing you, or divining your intent, and gives you a check on the witness's veracity.

A truly hostile informant, especially one involved with your target or adversary, is particularly demanding. The temptation is to try to convince him that he's in real trouble—that you already know enough to be a threat. But never say things like "we know such and such—we just need the details." That gives away too much of your information, and if you're wrong, you've just demonstrated incompetency to the witness. If you keep asking the right questions, he'll get the picture that you're a force to be reckoned with, and that realization is more convincing when it comes from within than when you try to force it on him.

If you must get coercive, remember all the above rules. Play "good cop-bad cop." Have the questioner remain open and approachable, while one or more other operatives do the intimidating. And remember that coercion is more a psychological activity than a physical one. Torture, besides being unethical and legally risky, is also counterproductive when its threat can be just as effective. ♦

Motive, Benefit, Knowledge and Opportunity

Crimes are rarely totally random. There is usually a motive—the perpetrator commits the crime for some benefit, be it financial, emotional, or psychological. When investigating a crime or event, or even when trying to understand information unearthed in a background check, look for possible benefit, knowledge, and opportunity.

Who gains from a crime? Does a murder eliminate competition? Was there an opportunity for profit? Was jealousy or revenge a factor? Was the perpetrator simply a psychopath? You need to look carefully at possible motives, but do not get fixated on the obvious.

Next, look at the question of knowledge. Who knew about the opportunity to commit the crime? Who had access to the premises, or was familiar with them? Are there service, security, maintenance, or delivery personnel that might be involved? How about a spouse or employee, present or former? Could neighbors be involved? Look into all of the above, as well as criminal connections that any might have. Also ask about persons recently in the vicinity of the event, loitering, applying for work, soliciting, or just acting strangely.

Next, look at opportunity. Start with the list of names generated by the questions above, but check out everyone if you have time. Get alibis from each of them, and check them out.

Discovering motive, knowledge, and opportunity will shorten your list of suspects involved in an event. Use your examination of these factors to generate new leads and lines of investigation, and to narrow your list of suspects to a manageable level (as discussed under Continuing Investigation, below, a criminal perpetrator will always have motive, means, and opportunity). Then you can gather harder evidence on these leads. Remember, though, that these elements do not prove involvement—you may end up with several suspects with motive, benefit, knowledge, means, and opportunity, most or all of whom are completely innocent of the crime being investigated.

Vehicles

Vehicles are very commonly used in criminal acts, and they provide a unique source of leads. They are easily spotted, remembered, and described by witnesses. Even more importantly, in the U.S. and most other countries, they are well monitored by the state, which keeps useful and easily-accessible vehicle records.

An automobile registration search must begin with a license plate number, although in some states you can initiate a search with the owner's name. Auto registration records are kept by the state revenue office, and contain the plate number, the name of the owner, and the year,

Techniques 5: Fundamentals of Vehicle Identification

As with personal identification, it's always a good idea to have a mental checklist for assembling an accurate and useful description of a vehicle. In descending order of relative importance, try to focus on the following factors—even if you can only get the facts on a few of them, you'll develop enough of a description to accurately identify the vehicle later, or usefully describe the vehicle to other operatives or law enforcement officials.

- *Make and model.* If you or your witness can't tell the exact make, at least determine the vehicle configuration: sedan, coupe, mini-van, sport-utility vehicle, pickup truck, etc. If the vehicle seemed like a foreign or domestic style, note that.
- *Year.* Most people can't guess the year of a vehicle at a single glance—but they can probably tell if it is a relatively new (late-model) or fairly outdated style.
- *Color.* Two-toned vehicles are referred to by police as color "over" color—tan over red, for example. If the vehicle has a vinyl top, note that fact as well as its color.
- *License Plate.* Even if you can't catch the plate number, you may be able to tell at a glance, by its color, whether it's an in-state or out-of-state license plate. If you can get a plate number, fantastic—but beware that many criminals put stolen plates on vehicles, an act known as "hot-plating" or "cold-plating," depending on whether the plates are stolen from active cars or out of junk yards, long-term storage yards, or other places where they won't be missed or reported.
- *Body Damage.* Note the extent and general location.
- *Markings.* Commercial vehicles usually have names or logos, and even private cars are sometimes decorated (especially with bumper stickers).
- *Windows.* Note whether they've been tinted, have stickers on them, or are damaged.
- *Modifications.* Note any customization to the vehicle.
- *Interior.* If you or your witness happens to notice the interior upholstery color, or whether there is anything to distinguish the inside, make a note of it.

As with personal identification factors, ask witnesses about all of these points, and note them yourself if you might have to remember a vehicle later. ♦

make, and model of the vehicle. Similar information is kept on boats and aircraft, and in some states the records are more detailed for these types of vehicles. However, it is not uncommon for boats and aircraft to be registered out-of-state, so finding a record might be more difficult. Also, witnesses are less likely to notice boat registration numbers than car license plates.

Once you have the registration information, you can learn more about the owner by checking out his Operator's License record (see [Private and Restricted-Access Record Sources](#), below).

Vehicle records are accessible by the state DMV and revenue agencies, local and state law enforcement agencies, and county revenue agencies (which must access the data in order to assess property taxes). If you cannot access the state databases directly, a friend or contact in any of these agencies should be able to get the information quickly and easily.

Evidence Analysis and Forensics

Modern forensic technology makes it harder and harder for a criminal to avoid leaving traces of his actions at the scene, or, rather, makes it more and more possible for investigators to interpret the very subtle clues that have always been left. Fingerprint analysis was one of the first major breakthroughs in forensic technologies, and the more recent development of DNA analysis is an equivalent step forward. These important techniques help investigators learn the identity of their suspects, but there are a number of other techniques that identify equipment, tools, clothes, and vehicles, and which can be just as valuable.

The key to nearly all forensic investigation is the comparison of evidence collected at the event scene with recorded information or other pieces of evidence found elsewhere. For example, a DNA sample from an event scene means nothing if you have no records, or samples from suspects, with which to compare it.

Even with those records and control samples, evidence analysis will generate two types of results: class characteristics and individual characteristics. Class characteristics identify a piece of evidence as coming from a class of sources, but not a specific one. Individual characteristics tie the evidence to a specific source. For example, the chemical composition and surface pattern of a shard of broken glass may identify it as coming from a certain make of car headlight, maybe even from a particular model of car (class identification). If the fragment can be fitted together with other shards, it may show that it is a piece from a specific broken headlight, and hence a specific vehicle (individual identification).

Class identification is inexact in proving the involvement of a given suspect. But class identification can be used to reduce your suspect list.

Techniques 6: Vehicle Searches

A clever criminal can hide a small object in a vehicle such that it's nearly impossible to find in a quick search. If you can tear apart a vehicle at your leisure, almost anything can be found. If you don't have that luxury, a few pointers can help you search a vehicle quickly and efficiently, to find items hidden by all but the most clever and meticulous of hidiers.

For best results, it's a good idea to have a flashlight and a mirror—preferably one on an angled handle. That'll make searches of the vehicle's underside easier, along with areas such as the underside of the dashboard and the engine compartment.

On the inside, be sure to check:

- *on the dashboard, and in the groove between the dash and the windshield.*
- *behind the sun visors.*
- *under the front and rear seats, and the floormats and carpeting.*
- *behind the back seat.*
- *in the ashtrays, glove compartment and other storage spaces.*
- *in cuts or tears in the upholstery.*
- *in the space between the seat cushion and the back cushion.*
- *in the dome light.*
- *in the springs and padding of the seats (accessible from underneath).*
- *inside loose door panels.*

Outside, check

- *behind the license plates.*
- *inside the gas cap cover, and in the tank (probably tied by a string from the gas cap).*
- *under the bumpers.*
- *inside the wheel wells.*
- *under the vehicle.*
- *inside the hub caps.*
- *behind retractable headlights.*
- *behind the front grille.*
- *inside the taillight lenses.*

In the trunk, check:

- *in, under, and around the spare tire, and in the spare tire well.*
- *in the inside of the back seat.*
- *in any compartments for tools or the jack.*
- *in the underside of the trunk lid.*
- *under the carpet or mat.*

In the engine compartment, check:

- *in the underside of the hood, and inside any molded air scoops.*
- *inside auxiliary components.*
- *inside the radiator, battery, or fluid wells (again, perhaps tied to the cap or lid).*
- *inside the air filter.*

These locations cover most of the simplest hiding spots, but for a thorough search the vehicle must be totally dismantled. ♦

For example, bruises left by long, thin fingers on the throat of a strangled corpse rule out suspects with short, stubby hands.

Check with your L&P coordinator or the L&P support labs in Atlanta or London to find out what forensic options are available to you. Here are a few of the many types of evidence analysis carried out by BlackEagle, other private organizations and labs, and law enforcement agencies:

- **Fingerprints** are very commonly left at an event scene or on other physical evidence. Fingerprint records are very extensive, covering everyone in the country with an arrest record, and many others without. Recovering fingerprints is relatively easy, with a digitizer or by hand, and they can be used to positively identify a suspect or to eliminate others. Fingerprints are matched using a system of identifying points, so a clear partial print can be more useful than a blurry full print. Palm, toe, and foot prints can also be used in identification, although records for them are not nearly as extensive.

- **DNA traces**, like fingerprints, are frequently left at an event scene, although collection can be significantly more difficult. Hair, blood, skin and bone samples can all yield DNA traces, often even after extensive decomposition (although fresh blood yields the best results). Even when you have no overt samples—like pools of blood, or skin under the victims’s fingernails—you may still be able to capture microscopic hair and skin samples. Bedsheets and clothing are great sources for such samples. DNA records, however, are not nearly as complete as fingerprint records. Furthermore, DNA analysis is much more expensive and time-consuming, making it unsuitable for low-probability checks or eliminative efforts.

- **Dental records** are used in identifying bodies. Ideally, the lab needs the subject’s full dental history as well as the body or at least a cast and x-rays of the teeth. However, it is sometimes possible to make a tentative ID based only on good photographs of the subject taken before and after death (the photos must, of course, show the teeth—at least a wide smile). There are no extensive dental databases—dental records can only be used to confirm a suspected identity. If you have no suspected identity to test, dental remains can give you the approximate age of the victim, a solid estimate of race, and some aspects of personal habits and medical history. Dental evidence can also match a given set of choppers to bite marks on food, pencils, or other people.

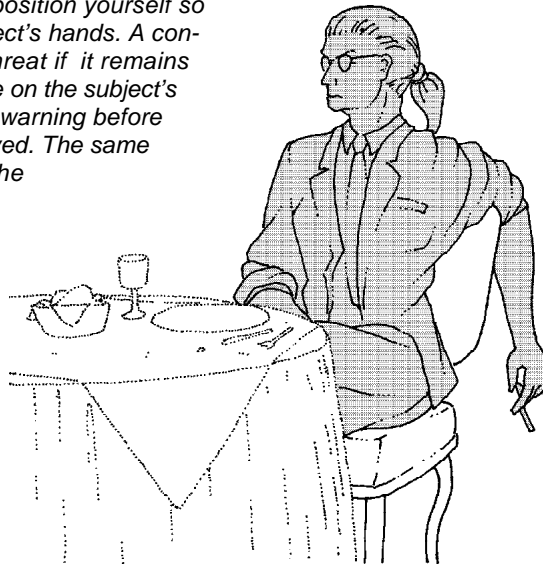
- **Ballistics** analysis yields information on the type of firearm used. The rifling marks on a bullet found on the scene will match those on a test-bullet fired from the same weapon in the lab, giving positive individual characteristics, and may yield class characteristics (make and model, or a limited range of them) of the firearm even if it is not recovered. In addition, powder residue in shell casings or on the victim may provide taggants if the ammunition was legally obtained, and shell casings can

Techniques 7: Detecting Concealed Weapons

Concealed weapons, especially concealed firearms, are commonly encountered in a BlackEagle operative's line of work. It's often critical to know whether someone is armed when you don't have the opportunity to search the subject—or even when you don't want the subject to know that you suspect him or her of being armed.

The first step is to know where to look. Concealed firearms are almost always kept in shoulder-holsters (on the side opposite the subject's primary hand) or the waistband (front or back), with the occasional weapon in an ankle-holster. On rare occasions, individuals will hide weapons in sleeve holsters, but these are generally ineffective and easy to spot. Small handguns hidden in these locations are easily and effectively concealed by loose clothing, but bravado often compels criminals or bodyguards to carry larger, less concealable weapons. Look for bulges in these common locations, for places where the clothing doesn't hang properly, or for the lines of holster straps under the clothing. Also note that all of these require covering clothing—an individual who doesn't take off his jacket when everyone else does, or who is dressed more warmly or formally than the situation requires, may be hiding something.

Often, you won't be able to tell definitively whether someone is carrying a weapon, but if you are suspicious the next thing to observe is the subject's behavior. An inexperienced subject may favor one side, sit oddly, or unconsciously scratch at or fiddle with his or her holster or weapon—but a pro won't give you any of those clues. So instead, position yourself so that you can see the subject's hands. A concealed weapon is little threat if it remains concealed; keeping an eye on the subject's hands will give you some warning before the weapon can be deployed. The same can also be said of the subject's eyes (which will likely begin sizing up the situation and assessing targets in the seconds before guns are drawn), and the positioning taken by individuals in a group. ♦



identify a weapon individually or by class from marks left by the firing pin, extractor, breech face, chamber, or magazine.

- **Tool marks** are left wherever a tool is used as a weapon or in breaking and entering. Class information can be gleaned from the marks left behind, and individual characteristics—based on microscopic scratch marks—can be identified if the tool is recovered. Note that the scratched material must be removed from the event scene and brought to the lab—which isn't always possible if the scratches are on a permanent structure.

- **Soil, glass, and paint** can provide class characteristics, and occasionally individual characteristics. Soil left on a victim's or suspect's clothes, shoes, or vehicle tires and undercarriage can be matched with soil type at the event scene—but soil is never more than a class identifier. Glass and paint are analyzed in the lab for chemical composition, yielding precise class matches. Reassembling broken glass shards can yield individual matches, while looking at paint layers can provide a very tight class match.

- **Cloth, fibers, and rope** always provide class characteristics. Lab analysts look at fiber and strand count and thickness, twist, dye colors, and weave patterns. Fabric weave patterns can leave impressions or prints on bodies or objects.

- **Hair, blood, and excretions** can be used not only to generate DNA traces, but also to provide clues in their own right. All three provide class characteristics about the physical type of the subject. If they originated from an animal, all can also be used to identify the species.

- **Documents** can be examined for the source of the paper and the of writing, printing, or marks on the surface. Inks and toners can be identified, as well as (often) the model printer or typewriter used to produce the document. A glitch in the output from a typewriter or printer will provide an individual characteristic if it can be duplicated. Otherwise, all characteristics will be of the class variety. A document can also be examined for impressions left when someone writes on another sheet of paper on top of it. Computer enhancements can, for example, reveal something written on a typical scratch pad from the impressions on a page ten or twelve sheets down.

- **Photographs and video** can be invaluable—sometimes. Pictures are indeed worth a thousand words, and the right photograph can yield surprising results. Faces can be enhanced and identified, sometimes even if they are unrecognizable to the naked eye. Unidentified objects in the scene can be compared with identified items, yielding precise dimensions. Shadow angles can be measured to tell the season and time of day when the photo was shot. Details unnoticed by eyewitnesses—like the brand of a vehicle's tires (important if you found tracks at the scene)—may be picked up on a photo. However, a photo can't help you if it doesn't have the information you need—no matter how much you enhance it.

Techniques 8: Knowing Illicit Drugs and their Effects

Illicit drugs and their users are often encountered in the course of assignments set in urban environments, or against traffickers or narco-terrorists. An understanding of the types of drugs commonly encountered, and the symptoms of their use, can be helpful. A few of the most common drugs and their general symptoms are presented here—these are by no means comprehensive, and the exact symptoms can vary from individual to individual, and according to the dosage and variant of the drug:

	Amphetamines	Barbituates	Cocaine	Heroin	LSD	Marijuana	Methamphetamine	PCP	Peyote	Stimulants
<i>Drowsiness</i>		•		•		•		•		
<i>Excitation/Hyperactivity</i>	•		•		•	•	•		•	•
<i>Restlessness/Irritability</i>	•	•	•			•	•		•	•
<i>Anxiety</i>	•		•	•	•	•	•	•	•	
<i>Euphoria</i>	•		•	•	•	•	•			•
<i>Depression</i>		•			•	•				
<i>Hallucinations</i>	•		•		•	•	•		•	•
<i>Panic</i>	•				•	•	•	•		
<i>Irrational Behavior</i>		•			•					
<i>Confusion</i>		•						•		
<i>Talkativeness</i>	•		•			•	•			•
<i>Rambling Speech</i>					•				•	
<i>Slurred Speech</i>		•		•						
<i>Laughter</i>		•				•		•		
<i>Trembling</i>	•		•		•		•			•
<i>Staggering</i>		•								
<i>Impaired Coordination</i>		•		•		•		•		
<i>Dizziness</i>	•						•	•		
<i>Slow Reflexes</i>		•		•						
<i>Sweating</i>	•	•			•		•			
<i>Constricted Pupils</i>		•		•						
<i>Dilated Pupils</i>	•		•		•		•		•	•
<i>Nausea/Vomiting</i>									•	



- **Soundprints and audio sources** can also be enhanced. Voices can be identified, and voice-print analyses can indicate whether a recorded speaker is lying, nervous, or drugged. Gunshots and car engines can be analyzed to determine the model of the source, although this is always a class identifier.

Criminal Records

Criminal records contain a great deal of cross-referenced information, and may be useful in identifying suspects even if you have few clues to start with. Fingerprints or DNA samples are obvious file reference points, but you may be able to pull files from photographs, composite sketches, or MO (Modus Operandi).

Criminal record searches, of course, rely on the perpetrator having a criminal record. If the perpetrator has committed no past crimes, or hasn't been caught, a record search will not turn him up—and in fact may give false leads. Of course, a negative result is information in and of itself: it tells you that the suspect is an amateur, is talented enough to have never been arrested (one need not be *convicted* to have fingerprints taken and a basic record file opened), or has the resources to erase records (although the latter is extremely unlikely).

The L&P criminal records databases maintained at the Atlanta and London L&P facilities are fairly comprehensive records on individual criminals as well as criminal and terrorist organization. BlackEagle draws these databases from U.S. and E.C. federal sources, supplemented by Interpol and selected state and private records sources. Information in the L&P records is not as current as the sources from which it is drawn, but is generally accurate and may be sufficient for your needs. When your search request is processed, the results will include the most recent record available, including a field indicating when it was last updated.

If these records do not prove accurate enough, you may be able to do better. The most up-to-date criminal records are kept in state and federal law-enforcement databases. These records are shared with any and all other law-enforcement agencies as needed. If you have connections with your local police, they can get database information from state and federal records.

Informants

Informants are individuals who, for any number of reasons, provide you with direct or background information that applies to your investigation. Although informants may be witnesses also, the two differ in that

Techniques 9: Following up on Gang Crimes

If you investigate crimes in urban settings, sooner or later you'll run into street gangs. Although they're anarchistic, there are a number of patterns to gang crime—understanding them can give you direction when investigating a crime that you know or suspect may have been committed by a gang or gang members.

Gangs generally commit three types of crime: burglary (especially car theft); mayhem (usually as part of an initiation or indoctrination process); and drug distribution. Gangs also fight among themselves—these fights sometimes result from sheer rivalry, but most are related to drug turf and transactions.

Burglary is the first stage of a gangster's career. Most gang thieves are aged thirteen to fifteen—older gangsters rarely participate, except as organizers or mentors. Theft is a way of developing and proving one's skills before moving on to bigger things, and in most gangs only car theft is pursued for real monetary gain (often in conjunction with "chop shops": legitimate auto repair services that deal in stolen cars or parts on the side). Young gangster thieves never work alone (solitary pursuits are discouraged by the gang), but usually operate in groups of three to eight. One gangster commits the theft; the others act as lookouts and can help intimidate or attack victims. Gangs rarely burglarize their own neighborhoods, but travel into other areas (often those of rival gangs) to rob stores and homes and steal cars.

Levels of mayhem vary from gang to gang—some participate in little beyond graffiti and petty vandalism, while others require "littles" to commit violent crimes—even random murders—before being fully initiated into the gang. Mayhem may or may not occur within a gang's home neighborhood. Because of their initiatory nature, most major mayhem crimes are also committed by younger gang members.

Drug dealing, on the other hand, is a more senior activity. Typically, a gangster serves as a runner or mule for a year or two, then moves up to becoming a street dealer. A runner operates alone, carrying drugs from the senior distributors (or "mainheads") in the gang to the street dealers, and carrying cash from sales back. Street dealers operate on open corners or from crack houses, in groups of three or four. One individual sells, while the others stand lookout or provide security. Often, the gangsters hide their drugs near their sales site, and don't bring them out until the deal is concluded. If the police are spotted, the usual response is just to casually walk away, leaving the stash hidden. Dealers often invite customers to partake of their wares on the spot before buying, in order to flush out undercover police officers.

Gangs fight over sales turf, and additional members may be assigned to protect dealers at particularly popular street corners or locations. ♦

informants know more about the event or the perpetrator than what they witnessed at the scene. They are insiders.

There are many reasons why an informant chooses to talk with you. He or she may do it for money, or some other tangible benefit. Informing may be a way to strike at competing criminal organizations—this is especially common in the gambling, fencing, and drug-running underworlds. Spouses or love interests (or ex-spouses or love interests) may inform out of jealousy or as a form of revenge. And of course, the informant may simply think it an act of good citizenship.

Cultivating informants can be difficult, but very rewarding. If you are lucky, you may run across a repeat informant in the normal course of investigation. Generally, however, an informant will contact you after you begin to question people and word of your investigation gets around. Deliberately seeking out an informant is often impossible, and you may end up being fed misinformation. There are a few sources worth looking into, however. Criminals hoping to reduce their sentence are often cooperative in providing evidence, although you won't be in a position to bargain without the help of the prosecuting attorney. Convicts recently released from prison are another likely target—they will often use their underworld knowledge for a source of income until they find another. Of course, such an individual won't do you much good unless his or her background is related to your investigation.

When trying to cultivate informants, start near the focus of the investigation. Remember that an informant is a sort of traitor—someone divulging privileged information. Look for someone who might have that information, and a motive to share it. If your target is a business (licit or illicit), or an individual who runs a business, question the employees, looking for someone who may be dissatisfied with his position or holds a grudge against the organization. Seek out girlfriends, boyfriends, or spouses, or ex's in any of those categories. Find out if the individual or organization has any criminal associations, especially any that have been arrested or convicted, and seek them out.

Remain circumspect when seeking an informant. Remember that criminals hate few things like they hate informants. If they find out that you are looking for that kind of a source, they will compartmentalize their information, making your investigation harder even if you cultivate a dozen informants. They may even plant a false informant, a double-agent to derail your investigation. And they'll certainly put pressure on those they suspect of informing.

For that reason, once you've developed an informant you must do everything possible to protect his or her identity. If your target comes to suspect your informant, his usefulness—and perhaps his very life—will be over. Avoid meeting the informant directly, and never see him or her socially.

Techniques 10: Stakeouts

Surveillance can take two forms: stationary surveillance (stakeouts) intended to monitor activity at a given location, and mobile surveillance (shadowing), intended to keep an eye on a given individual and his activities. Both are labor-intensive and often downright dull, but require skill and attention. It's tempting to foist these jobs off on the least senior member of your cell, but the major decisions on how and where to place surveillance, at least, should be made by experienced operatives.

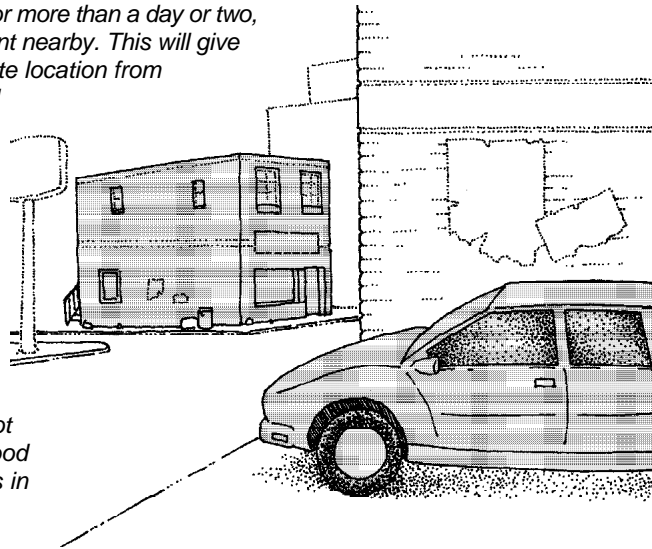
Stakeouts are the easiest form of surveillance, because once a site is selected you need only to wait and watch. Vigilance is required, however, especially in the face of boredom, and you must be discrete. Here are some points to consider when choosing a site:

- **Conspicuousness** is the single most important factor. If you are noticed by the subject, a neighbor, or even a well-intentioned cop, you jeopardize the surveillance and even the entire investigation.
- **View.** Can you see as much as possible, including avenues of approach? It doesn't do much good to have a great view of the street and front door if the subject always uses the back door and rear alley. Also, check conditions for photography if you will be taking pictures or video.
- **Access.** Can you get in and out of your site easily, and without arousing suspicion? If you need to respond or move in, can you do so quickly?

If you are staking out your target for a short time, it may be sufficient to do it from a car, or even on foot. Choose a site that conforms to the criteria above. Park or stand on a side street about half a block away. Never hang around right in front of the target building. Change personnel and locations every couple of hours, or right away if anything or anyone draws attention to you.

If you will be watching for more than a day or two, rent a room or apartment nearby. This will give you a secure and private location from which to work, as well as the increased visibility of height. Use a window a floor up from the subject, if possible, and not directly across. Again, make sure your site meets the above criteria.

Either way, be discrete in choosing your location—the perfect spot won't do you a bit of good if you were too obvious in looking for it. ♦



Surveillance

Surveillance is a time-consuming and basically boring task, and should be left to the final stages of your investigation, when your suspicions are pretty solid and only need be confirmed. Use surveillance to look for something specific—to catch a suspect in the act, get him to lead you to another, or to monitor activity at a given location. You can use surveillance to learn more about the suspect's activities in general, but it is an inefficient investigative tool if the purpose of the surveillance isn't focused.

Your surveillance can take the form of a stationary stake-out (of a specific locale), or a mobile one (of an individual). In either case, the basics—camouflage, stealth, and common sense—are paramount. The sidebars on the previous and opposite pages outline specific surveillance and shadowing techniques. What you most need to keep in mind when using any of these is that a suspicious target will notice anything odd in his environment. For example, a stake-out in an ethnic neighborhood will draw attention from the target (and others) if the investigators, seen going in and out of the stakeout site, do not fit into the community. In short, use common sense, blend into the background, and remember that it is almost always better to lose the subject for a while than to blow your cover and tip the subject to the investigation and your surveillance.

Public Record Sources

When carrying out a background investigation on a person or organization, or looking into such a target as part of an event investigation, you can find a great deal of information in public records. Using public records is easy, free, and totally legal, and public records contain volumes of information on every individual and organization in the country. Birth and death certificates, marriage and divorce records, deeds and home-ownership records, incorporations, bankruptcies, and legal involvements are all recorded at public record sites.

- **Individuals.** Information you can gather on an individual starts with his birth certificate, which will tell you his full name, age, and date and location of birth. Official records from the target's youth are likely to be scarce, but not so from his or her adult life. Court record searches will tell you about any criminal charges the target faced, or any civil litigation in which he or she was involved. Marriage and divorce papers will be recorded, as will birth and death certificates for any children. If the target owned any real estate, deed records will be available, which will include a description and approximate value of the property. Any applications for building permits or rezoning will be recorded. If the target was involved in politics, either as an official or a concerned citizen, his involvement will

Techniques 11: Shadowing

Shadowing is far more difficult than conducting a stakeout, not just because of the increased risk of exposure, but because it can be hard to keep up with an unpredictable subject. Shadowing is always easier with more than one operative, because you can prepare for your subject's movements and shuffle different faces through the high-visibility position. Radio communications are a good idea with a multi-operative mobile surveillance, especially when shadowing cars, but be discrete—nothing is more distinctive or revealing than a person talking into a radio mike.

In general, shadowing only works if the subject doesn't know you are there. If he sees you following, he'll abort his original activity and try to shake you, and you'll never get a chance to see who he meets, where he goes, or what he does. If the subject thinks he's being followed, he will pull a few tricks (see the "Shaking Tails" sidebar, on page 37). It's usually better to let him go than to confirm his suspicions.

Don't rely on disguises unless you are really good. Instead, remain inconspicuous. If you'll be on the tail for a long time, a change of hat, jacket, and/or tie should do the trick—the subject is much more likely to notice these things than your facial features. When on the road, use an inconspicuous car—mid-sized, middle-aged, in blue or earth-tone paint, and with no vanity plates or bumper-stickers. Also, be prepared for contingencies. That means having a map handy, packing a little bit of food and carrying a decent amount of cash and change (so you won't be stuck waiting for change if you have to follow the subject into a restaurant, and then buy something to avoid looking conspicuous). Hit the restroom before you get started. And have some sort of story—nothing elaborate, just something you can say if confronted.

When shadowing alone, hang back almost as far as you can without losing the subject. If he or she enters a store or restaurant, walk past, then find some discrete location from which you can watch the front entrance, and, if possible, one side of the building. The subject may try to lose you by leaving via a rear exit. Following him through will confirm that he's being shadowed, so it's better to hang around outside and take the risk of losing him. If the subject gets on a bus or other public transport, get on as well. Again, he may try to lose you by getting right off, before the bus departs, and if you get off too your cover will be blown. Instead, stay on, get off at the next stop, and board the next bus on the same route. You'll probably lose him, but if you blow your cover he's lost anyway. And he may have really intended to take the bus—in which case you will pick him up again when the next bus comes.

If you think your subject is on to you, play it cool. Stick to your cover, but leave the area. If the subject follows you (not unlikely if he wants to confirm his hunch), stay in public. Enter a shopping mall or a restaurant. Act natural, and don't let him follow you home or see you doing anything that might tip your investigation. Don't use any deliberate techniques to lose him, or he'll know something's up. Chances are (unless you really slipped up) that once his suspicions are allayed, he'll go about his business. If you think he's seen your face, don't tail him again. ♦

show up in official meeting minutes. If the target is dead, there will be a death certificate with place, time, and cause of death, and the county probate court will have his will on record.

- **Businesses.** Businesses leave official paper trails just like individuals. Articles of incorporation—the birth certificate of a corporation—are filed with the Secretary of State (state, not federal) and include the company's business purpose (although this may be stated very vaguely), its registered agent, and the address at which it receives its official (state) mail. The owners may or may not be listed—if they aren't, check other documents, like deeds, permit applications, and litigation records, to see who signed them or appeared in court to represent the company (such a person may or may not be the owner, but will at least give you another lead). All of the same types of documents that apply to individuals—mortgages, property records, building permits, etc., can exist for corporations. Even dissolution papers (corporate death certificates) and bankruptcy filings are left on record.

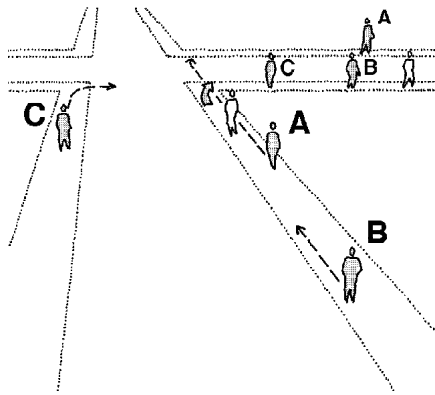
Sole proprietorships and partnerships are non-incorporated businesses. Their records are simply the owners', but under different names. You should be able to obtain a copy of the trade name permit from the Secretary of State.

Obtaining access to local records is very simple—county records are kept at local courthouses and are open to public inspection during regular business hours. In addition, most localities have transferred some or all of their files to electronic databases, accessible by GenNet. Many municipalities, however, have not yet taken that step. If you are looking for records kept somewhere across the country, your choice may be a long trip, or hiring some local organization—like a trust company or private investigator—to search the records for you.

In addition to government records, there are a handful of record sources maintained by private organizations but available to the public. Phone books and neighborhood directories list physical and GenNet addresses, as well as phone numbers. A number of directories available online or on CD-ROM list addresses by street and neighborhood, cross-referencing each address with the resident's name, spouse, and occupation. Following a listing through several of the publications' annual volumes can develop a rough marital, employment, and residential history of the target. The directories, however, are not one-hundred-percent accurate, cover only select urban areas of the U.S., and generally stick to residential neighborhoods. For information on businesses, especially big businesses, look into S&P or Moody's reports on publicly-traded corporations, or any of the several library search services that contain abbreviated information on businesses all over the world. All of these sources contain addresses and phone numbers, a basic description of the company's business, and perhaps the names of corporate officers,

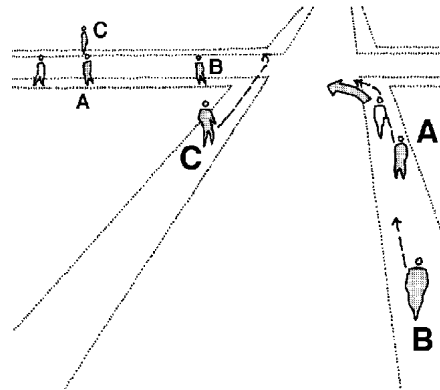
Techniques 12: the ABC Shadowing Method

There are several techniques for multi-person shadowing. The best requires three people, and is known as the "ABC" technique. Two people follow the subject (the "near" the "trail" positions, labelled "A" and "B" in these illustrations), while a third parallels from across the street (the "parallel" position, labelled "C"). You can shuffle the positions of the three as you maneuver through the streets, keeping a fresh face near the subject. Since a shadower is more likely to be noticed following around a corner than simply walking down the street, corners are good places to trade off positions. The two techniques here show how to inconspicuously shuffle your people, while never breaking contact with the subject.



In this first illustration, the subject turns but does not cross the street. The "A" man continues straight, crossing the street, then turns and takes up the "C" position. Meanwhile, the trail, or "B" man, moves up behind the subject. The "C" man crosses at the corner and takes up the trail position.

In the illustration to the right, the subject turns and crosses the street. The "A" and "B" men stay in position, while the "C" man continues straight, then turns on the far side of the cross-street. In this way, nobody draws attention to themselves by changing stride, although you do not get the opportunity to shuffle positions.



If your subject tries one of the tricks mentioned in the previous sidebar, the near follower (the "A" man in the illustrations) can nonchalantly walk on, to watch from a distance, while one of the others follows into a store or onto a bus. If the "A" man is spotted, remove him from the lineup and continue the surveillance with your remaining operatives, or bring in someone else.

This "ABC" technique works well with vehicles, too. The "C" car can parallel a block away, if the street layout allows it. Radio communications, however, are critical for multi-vehicular surveillance. ♦

directors, and major stockholders. All of the above-mentioned sources are commonly available at libraries, or through online information/library services. Also worth looking into are newspaper archives, most of which are not online, or at best only have the last few years' worth available electronically. All, however, are well-indexed, so if your subject has ever been in the public eye you should be able to read about it with a few hours' research.

Private and Restricted-Access Record Sources

If individuals and businesses leave a large trail of public-access records, the trail of private and restricted records is enormous. Tax records, spending habits, credit reports, bank balances, employment data and criminal activities are all recorded in databanks kept by private organizations or by government agencies that do not make them public. Here are a few of the dozens of information sources available commercially or through contacts:

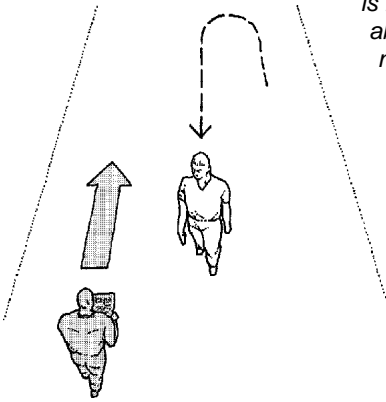
- **Drivers license records** are kept by each state's Department of Motor Vehicles or equivalent, which is usually part of the state revenue agency. Information includes address, weight and height (all three of which may not be up to date), date of birth, hair and eye color, vision-correction requirement, license expiration date, suspension notices, and maybe Social Security number. The record may or may not be available by formal written request, depending on the policies of the state in question. If not, a contact in the local police department, DMV office, county tax assessor's office, or Secretary of State's office may be able to help you. The data is also online, although restricted.

- **Credit bureaus** keep tabs on the credit status of virtually every adult in the country. The information includes credit history, current income and credit sources, current balances on credit cards and other credit sources, monthly payments, and account numbers, as well as supplementary information including current address, known previous addresses, employment, birthdate, and Social Security number. The information is provided, for a fee, to legitimate businesses considering extending credit to the subject. Since BlackEagle is one such business, you can have your L&P coordinator pull a credit record for you. Keep in mind, however, that the data kept on major criminals and other important or wealthy people may be whitewashed.

- **Banks and financial institutions** are notoriously discrete—when dealing with the public. When dealing with one another, however, they are not so cautious. A polite letter of inquiry implying that you represent another financial institution will often be answered with soft information on banking habits and balances. Generally, the data will include account numbers and coded information that translates to ballpark

Techniques 13: Shaking Tails

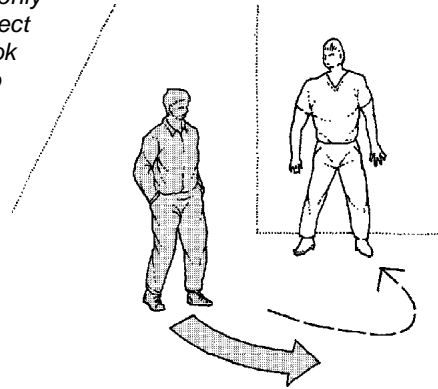
There are several techniques you can use to shake a tail, or force him to reveal himself. A few are discussed here, so you can look out for them or use them yourself, if you think you are being followed. In all of these cases, the subject is likely to notice the tail man, but probably won't notice the "B" or "C" men unless he is both perceptive and skilled. Therefore, you may be able to switch a new person into the tail position and maintain the surveillance, even if one member of your group has been spotted.



A reverse is the most basic tail-shaking maneuver. It forces the tail to either let you go or turn around and follow you, which is extremely obvious. If your subject suddenly reverses direction, walk past and keep on walking. Then, if you are solo, try to pick him up again after circling the block. But be careful—the subject will try to get a look at your face as you pass him. If you're working with a team, split up, circle the block, and pick up the subject with someone else in the "A" position.

If you are being followed, a reverse is a good way to flush the tail and, as mentioned, get a look at his or her face. A reverse will give away your suspicion, however, so if you don't want the tail to know you're on to him, try the next technique.

A less reliable method takes advantage of blind corners. The subject turns the corner, then stops just out of sight. Even an experienced operative finds it difficult not to hesitate or look surprised when he comes around a corner and almost runs right into his subject. The only defense is preparation. Whenever your subject disappears around a corner, be prepared to look extra nonchalant as you follow. If you bump into anyone, mumble an apology and continue on, even if that means passing the subject. Once again, the subject will probably get a good look at your face.



Another good method, for foot or vehicular shadowing, is to speed up or slow down a little above or below the ambient traffic speed. Notice if anyone else seems to be doing the same, and if so, switch to the other extreme. If they also change speeds, you know you have a tail. The best way to combat this as a shadower is to be flexible with the distance between you and the subject. If he speeds up, let the distance grow, then gradually recover it. If he slows down, overtake him a bit, then fall back slowly. ♦

figures on average balances and levels of activity—not actual balances or other exact numbers. You may be able to get this same information from bank databases or connections in bank offices. If you already have account numbers and are willing to impersonate the target, many banks and credit card agencies have over-the-phone services that will give you current balances and even allow you to make changes in service.

- **Freedom of Information Act requests** can be used to dig up government files on virtually any subject. Call the public liaison or FOI officer of any agency that might have the records you want and request everything on your topic. With any luck, they will send you the records within a couple of weeks. If not, write a formal request to the same person, sending it by certified mail. The agency is required by law to respond within ten days, sending you the requested records unless they fall under specific national security or privacy act guidelines.

As mentioned above, many of these sources are only loosely restricted. Much of this information is available for approved uses, or to specific agencies, businesses, or individuals (particularly the subject). A mildly-deceptive phone call is sometimes all that it takes to access many of these information sources, especially if you already have basic information on the subject, such as full name, account numbers, or Social Security number.

Other Leads

There are infinite numbers of other possible leads, depending on the nature and specific circumstances of your investigation. A few are covered here:

- **Stolen property.** Thefts of mundane items do the criminal no good if he or she cannot offload them. If you are dealing with mundane thefts, check out local pawn, resale, and second-hand shops to see if you can locate the goods. Contrary to myth, most shop-owners are very cooperative in this regard. You must, however, be able to positively ID any missing merchandise. Get serial numbers from the victim (if he doesn't have them, try the store where the goods were originally purchased—retailers usually keep good records of major item sales). Also check with merchants, repair shops, and pawn brokers that may have previously handled the merchandise—many will leave hidden marks that a thief will be unable to find—or remove. Once you identify a piece of stolen merchandise, the store's records and the owner's memory should provide leads on the thief's ID.

- **Hospitals.** If a perpetrator was wounded in the act, check with local emergency rooms where he may have sought treatment. Most are required to report shootings and stabbings to local authorities, and even

Techniques 14: Conducting Interrogations

Interrogation differs from the simple questioning of witnesses or informants in that the interrogator is seeking specific information that the subject is concealing. Interrogation is a tricky proposition: done well, it can quickly advance an assignment; done poorly, it can really set you back. When interrogating a prisoner or hostile suspect, keep in mind all of the tips discussed in the “Informants and Witnesses” sidebar earlier in this book (see page 19). Also keep in mind that most effective interrogation techniques don’t yield legally-admissible results when carried out by civilians, and are legally risky at best in many circumstances.

As mentioned in the Informants and Witnesses section, plan your interrogation. Know what information you’re after, and what your subject can likely provide.

Start your interrogation process by building the proper environment. Create an environment that is neutral, private, and isolated—one that avoids distractions, deprives the subject of any interaction except with the questioner, and forces a feeling of isolation and helplessness on the subject. Don’t let anyone but questioner talk to subject, even other members of your cell. Search the subject, and examine anything found on him—even items that aren’t of immediate informational value can provide you clues about the subject’s background and perhaps verification of what he says.

As you start your interrogation, ask direct, simple questions. Keep your manner neutral or even a bit naive—allow the subject to underestimate you. Later, when you have a sense of how your subject responds, you can build towards more sophisticated techniques. A vaguely uncomfortable subject is easy to keep off-guard. If it’s chilly, keep him half-naked, while you dress warmly. If he’s hungry, eat in front of him. If he smokes, deny him tobacco while you smoke.

Ask your questions quickly, so that the subject can’t fabricate a story. Follow up vague answers with questions that elicit details (which are harder to make up quickly). When one line of questioning is finished, quickly change to a new topic to throw the subject off balance. If you can verify any facts while the interrogation is ongoing, do so—and let the subject know that you are.

You want to bully and intimidate the subject as necessary, but you also want to make it easy for him to speak. An excellent method is the “good-cop, bad-cop” trick: work with two questioners, one who bullies and threatens the subject, and another who is sympathetic, who holds back the bully, who acts as the “voice of reason” in the face of an overly-aggressive partner.

Another old tip when dealing with a lying subject is to plant false evidence in his story—the “location trick.” If the subject claims to have been at a certain place at a certain time, recount a phony transient event at that location (a car accident or fire nearby, for example). If the subject accepts it, you’ve proved that he’s lying; if he denies it he may be telling the truth—or you may not have been subtle enough in your implementation.

Torture, in addition to being unethical and inhumane, is generally not a good tool in the hands of the inexperienced. Psychological effects are another matter, and your subject doesn’t have to know that you won’t resort to physical coercion. Put more emphasis on that uncertainty than on any actual physical acts. ♦

if they don't the staff will probably remember them. Sometimes perpetrators will put off medical attention, afraid of being caught at the hospital. This can work against them, though—a person who comes in with a four-day-old wound will be noticed and remembered by medical staff, even if the type of injury is mundane.

■ **Event Investigating**

Event investigations are the most common type of investigative assignment BlackEagle gets. Operatives are commonly called on to solve crimes, to retrieve stolen goods or missing persons, or to track down leaks.

The Event Scene

An event investigation usually begins with an event scene. Sometimes, as with a murder or break-in, the event scene is obvious. When a person is missing, however, the point of abduction may be unknown, and you may have to do some investigating just to find the scene. Some investigations may not really have scenes. If there is one, however, it is generally the first and best source of early leads.

When you get to the scene of the event you are investigating, you want to do everything possible to preserve it. The event scene is the starting point for your preliminary investigation, and may be your biggest source of leads throughout the investigation. You won't know what information the event scene will give you until you go over it again and again. Until then, you want to make every effort not to inadvertently destroy, or let anyone else destroy, the subtle clues left there.

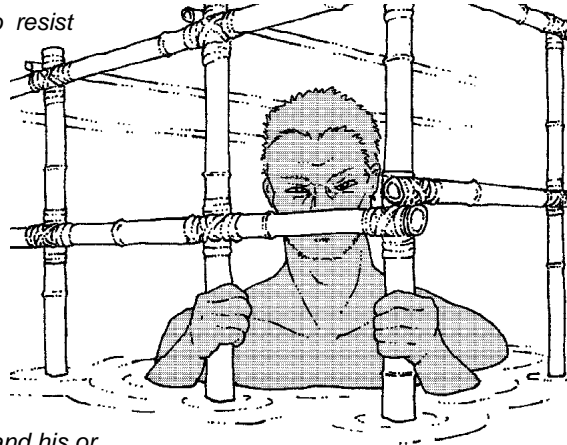
Your event scene includes not just the point of the event itself, but its immediate environs as well. When you identify the center of the action, search the area around it for additional clues or signs of activity. Pay particular attention to the avenues of approach—the perpetrator got in and out somehow. When you isolate the scene, be sure that all relevant areas are protected.

Your biggest concern at the event scene is the collection of evidence, and the preservation of what remains. Since the scene will not remain static forever, do what you can to record it, as soon as possible. Shoot video and take still photographs of everything. Make a sketch of the entire scene, noting details like the position of structures and furniture, the location of entrances and fields of view, and of course the placement of weapons, equipment, and the victim. If your event scene is out-of-doors,

Techniques 15: Holding out under Interrogation

Finding oneself in the hands of a hostile foe—a criminal or terrorist group, a guerilla or enemy military force, or even an antagonistic law enforcement agency—can be one of the most trying experiences of an operative’s career. Clever captors will see you as a valuable information source on the activities of your cell, your client, or allied military or law enforcement groups—and as mentioned in the previous sidebar, there are a number of techniques they’ll use to pry this information out of you.

Fortunately, there are ways to resist those efforts. First and foremost, be familiar with interrogation techniques, such as those discussed in this book. If you see specific tricks being used against you, you’ll find them easy to resist. Remember, though, that a good interrogator will employ such tricks with great subtlety, so you want to make every effort to remain detached. Carry out an ongoing analysis of your situation and your interrogator’s performance in your mind as events unfold—it will help you understand his or her strategy, and perhaps give your mind a much-needed focus if things get unpleasant.



Remain meek, and avoid bravado. If you find yourself among a group of captives, do nothing that points you out as anyone special. When interrogated, be polite—there’s no point in antagonizing your captors, regardless of how much they deserve it or how good it might feel for a moment. Never get into a showdown of toughness or testosterone—there is absolutely nothing to be gained. On the other hand, even when being meek and polite, say nothing that implies that you are going to cooperate—that will only draw out the interrogation session and incite your captors when you fail to do so.

Don’t bother with threats, either—never say, for example, that your fellow operatives know where you are and are coming to rescue you. Even if it’s true, you’re just giving your captors information they want—and you will not succeed in cowing them, or talking them into better treatment.

Don’t let yourself be drawn into conversation, even on harmless topics. Your interrogator doesn’t care to shoot the breeze with you—he’s using casual conversation to loosen you up. It works. Don’t fall for it.

View every session—every exchange—with your interrogator as an individual battle. If you win it, hold onto that victory. If you lose it, don’t lose heart—a war is made of many battles, and some will inevitably be lost.

Finally, always remember that time is on your side. In most situations that BlackEagle operatives face, captivity is short-term—a few hours, days, or perhaps (in extreme cases) weeks. Help is on the way; every minute that you hold out is a minute that your compatriots are working towards your rescue. ♦

in some public place that you cannot close off for long, or is simply likely to be molested or disturbed, focus first on the most fragile evidence—the evidence most likely to disappear or be damaged.

Ideally, you want to be fastidious about your event scene, but we don't live in an ideal world. The assignment may not give you enough time to go through the scene as thoroughly as you would like. The area may be restricted property, and you might not be permitted the access you need. You may run afoul of law-enforcement agencies or criminal organizations, or find yourself in the middle of an ethnic battle (not uncommon at scenes of interracial violence). You may be pressured by the press. Keep your head about you, maintain control of the event scene, and prioritize. If your time at the scene is limited, make the most of it. Be as thorough as you can on your first visit. Never leave the scene until you are satisfied that you've gotten all you can from it.

In addition to all of that, keep the following in mind when at an event scene:

- **Don't rush in.** The object at the center of the scene—an open vault, a computer terminal, a body—is a tempting distraction. But don't approach it too quickly. You may destroy subtle clues as you rush in—especially if you are coming through the only entrance (the one the perpetrator must have used). You will very likely overlook something in the periphery, and you may inadvertently define your search area too close and too quickly.

- **Document everything.** Don't limit yourself to video and film. Make sketches and take notes. Document the facts, and record the leads that appear to be panning out. But also note your impressions and hunches, and keep track of the leads that go nowhere. You want a record of the bad leads as well as the good, so that you don't repeat mistakes, or in case you want to double-check them later.

- **Include everything.** Take a sample of everything that the perpetrator may have come in contact with—soil, paint, carpet fibres, insulation, you name it. Dust every surface for prints. Take elimination prints from everyone who had access to the scene. Assume that your first visit to the scene is your only chance to gather the evidence—because it might well be.

- **Visualize.** Even with all the time in the world, you can't check everything. Visualizing the scene and the perpetrator's methods will give you clues on where to look for physical evidence, and what to look for first. But keep track of the facts, and keep them separate from your assumptions. The inferences you make are valuable, but don't fixate on them, because they may not be accurate.

Techniques 16: Evidence Collection

Many books could be written on proper evidence-gathering techniques, and many have been. Only a few basics can be covered here. As with so many other things, the key is common sense. Your goal is to preserve the evidentiary value, and sometimes to protect the legal admissibility, of physical objects found at an event scene or over the course of your investigation. Treat your evidence carefully, protect it from contamination, properly mark and record its source, and maintain some level of accountability, and you can't go far wrong. Here are a few specific techniques covering some common and/or particularly delicate types of evidence:

Blood: photograph it first. Then collect about five ccs if it's liquid, or scrape off as much as possible with a clean razor if it's dry. Let it dry before collecting if it's tacky. Liquid blood should be refrigerated, not frozen. Add an anti-coagulant if you have one.

Clothing: photograph it, then gather the pieces carefully and place them in individual garment bags. Bag the hands of bodies so the nails do not scrape up fibres or debris.

Firearms: photograph and sketch them before moving, unless there is a safety concern or weather will affect prints. Collect weapons by the trigger guard, preferably with a stick or pencil. Mark them on the receiver and slide, or on the base of the cylinder in the case of revolvers. Bag or box bullets and shell casings after marking them to correspond with a site map. Mark bullets on the base (the tip may have tissue samples or cloth impressions) and shell casings just inside the mouth.

Impressions and footprints: photograph them first, then carefully clean out debris, spray with shellac or hairspray, and dust with talcum powder. Create a frame about two inches out and above the print, then pour in high-grade, well-mixed plaster.

Soil, glass, paint, hair, rope and other physical items: photograph them, then remove carefully with minimal contact, using tweezers or forceps. Place samples in clean bags, jars, or boxes, and mark the containers to correspond with your site map. ♦

Preliminary Investigation

The preliminary investigation is the set of steps taken at the event scene, to exploit the immediacy of the situation and to provide leads for the main part—the continuing investigation. Conducting a preliminary investigation is simply a matter of exercising common sense—gathering the immediate information (especially transient clues and leads that may vanish) and protecting other information sources. Follow at least the following steps:

- 1. Stop the perpetrator**, if he or she is still around.
- 2. Isolate the event scene.** Remove the victim (unless he or she is dead) and other witnesses from the immediate vicinity. Protect the event scene throughout the remainder of these steps, allowing access only to evidence gatherers.
- 3. Gather eyewitnesses.** Keep them segregated, and get from each their own version of events. Before releasing them, make sure you record their identity and address, and give them some way of reaching you.
- 4. Record the type and method of crime or event**, in so far as you can determine from available evidence. Record the type of injuries and property damage in detail.
- 5. Photograph everything.** Photographs not only provide records of the scene, they may provide their own forensics leads. Some injuries and stains, for example, that might go unnoticed under lighting conditions at the scene, will show up on film. Make a sketch of the scene, complete with dimensions and measurements, because photos alone can be misleading.
- 6. Collect physical evidence.** Begin gathering physical evidence, starting with transient clues: fingerprints, tracks, and samples of liquids or other substances that may evaporate or dry up. Search the area carefully, overlooking nothing. Be sure to handle evidence carefully, so as not to undermine its legal admissibility or forensic value. Some specific things to check right away include garbage cans and dumpsters, the mailbox, GenNet terminal and answering machine (for last use), and doors and lights that might have been left open or on. Also, photograph any crowd that gathers—the perpetrator sometimes returns to have a look.

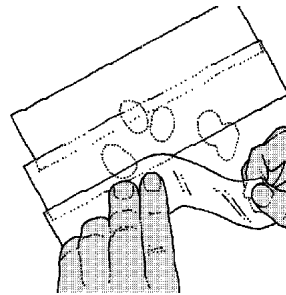
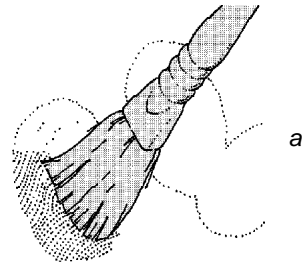
Unless the perpetrator is caught at the scene, a preliminary investigation will not solve your mystery. In fact, it may open up more questions about what happened than you started out with. But it should provide you with a great many leads to follow as you begin the continuing investigation.

Techniques 17: Taking Fingerprints

Fingerprinting is one of the most fundamental methods of identifying people who have been at certain locations or handled specific items. If you don't own or have access to a fingerprint digitizer, you will need to take them the old-fashioned way. In fact, it's a good idea to take fingerprints by hand even if you have a digitizer, to have a permanent, physical back-up record. Here's how to do it:

Step 1

Using a small amount of powder, gently dust the print with soft paint brush. The dust should stick to the print itself, but not to the surrounding surface. It's better to go too light than too heavy, so be conservative with the powder.

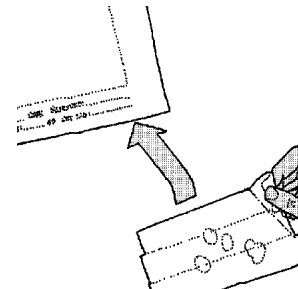


Step 2

Photograph the print, then lay a five or six inch strip of clear tape over it. Lay the tape gently to prevent the formation of bubbles, and if it's too narrow, lay additional strips along-side, overlapping about a quarter inch.

Step 3

If the object in question is portable, send the whole thing to the lab, with the tape still covering the print. If that's not reasonable, peel the tape off carefully and stick it to a card, being sure to notate exactly where it came from.



Once you've got a fingerprint, you'll need a source to compare it to. BlackEagle's criminal databases are pretty accurate, and if you've got connections in local or federal law enforcement, you may be able to send a print through their systems as well. However, such records are limited—an individual with no criminal arrest history may well not be in them. If you suspect a particular person left the prints, meet with him or her. Offer the subject a cup of coffee (or otherwise get the subject to handle an object), then, after the meeting, lift any prints you can from the mug (along with anything else the subject handled in your presence). That'll give you a set of prints for comparison.

Fingerprinting by hand is a simple and quick process if you know how to do it. If you don't, get a fingerprinting kit and practice a little around the house. ♦

Picking up a Cool Trail

BlackEagle is not a law-enforcement agency, and BlackEagle operatives are generally not the first on an event scene. In fact, BlackEagle is most often called in after public-sector investigators have failed, for whatever reason, or set the investigation aside. As often as not, you will be asked to pick up an investigation already started by someone else.

Picking up a cool trail is not necessarily a major handicap, especially if those who handled the preliminary investigation were competent and you have access to their findings. So the first step you should take is to find out who may have already done some investigating, and get ahold of their results. The police may be helpful in this regard, but probably won't be. Nevertheless, you might be able to find the investigation report online, or through a contact in the department. Also check out any private investigation or security firm that was involved, and don't forget journalists.

Regardless of what you learn from someone else's preliminary investigation, visit the event scene yourself. Even if the trail is long cold and all clues have disappeared, you need to see the scene to start building an image of the event in your mind. Follow the steps outlined above as best you can. Canvass the area for witnesses—locals who were around for the investigation (but not necessarily the crime) may remember who the police talked to.

A last resort option is to follow police investigators, to try to second-guess the direction of their investigation. This is an inefficient way to get your investigation going, but if you have been denied any other sources of information it may be your only choice. In any event, remember that the trail gets colder by the day. Don't get hung up on background and getting to the findings of others, or you may find yourself getting further and further behind.

Continuing Investigation

The continuing investigation is the real meat of any investigative assignment. By following up on the findings of the preliminary investigation and looking into the basic leads discussed above, you will develop a more and more accurate and detailed reconstruction of events, and get closer and closer to discovering the perpetrator. If you are putting together a legal case, the continuing investigation is also when you develop your legally-relevant evidence, to assemble into the proof that will be used in trial.

The steps below provide a basic framework for continuing investigations. The circumstances surrounding your particular events may cause you to deviate from these steps, but this list should be useful in most cases.

Techniques 18: Dealing with Kidnappers

BlackEagle operatives become involved in kidnappings because the families of the victims—or their employers, in the case of corporate victims—want assistance but are afraid to involve the authorities. It's critical to remember that in most cases, the priority of the client is the safe return of the victim—catching the kidnappers, or even saving the ransom, is usually a secondary concern at best.

The first step in dealing with kidnappers is to determine their purpose—is the kidnapping criminal (financially-motivated) or political? Most kidnappers will make this intent clear, but because some criminal groups couch themselves in political language—and some terrorist groups rely on kidnapping for income—it's important to determine which goal is primary for the kidnappers. A political victim is in grave danger of being killed by his or her captors when objectives have been met, and the captors are unlikely to maintain a useful dialog with negotiators. A criminal kidnap victim will likely be kept alive, at least until the very last stages of the process, with genuine negotiations running constantly.

When dealing with criminal kidnappers, remember two rules of thumb: time is on your side; and paying the ransom does not mean that the kidnappers will get away. Exercise the first rule with some caution—most criminal kidnappers operate in organized gangs or from mafia ranks; they plan and execute their crimes carefully. Some, however, are less rational or more desperate, and may kill a hostage for little reason. Nevertheless, unless you sense true impending peril for the hostage (beyond the hyperbole and bluff of the first call), use time to your advantage, to investigate the kidnappers and gain a psychological upper hand in negotiations. Excuses for stalling include talking down the ransom amount, gathering the cash without raising the suspicion of authorities or bank officials, converting the cash into low-denomination, non-sequential bills, and finding a volunteer for the drop.

Most criminal kidnappers study their targets well and know what the family or company can pay. Nevertheless, they typically demand more—this is part of the shock tactic of the initial contact. Negotiation is expected, and many ransoms end up being only 20% of the original demand. Again, use this process to stall the kidnappers. Later, when time has worked against the kidnappers' nerves, stand firm on those few demands that you can reasonably make: proof that the victim is alive, and evidence of identification at the drop, so that you know that it's the kidnapers accepting the ransom.

The drop is the point at which the kidnappers are most vulnerable. This is where the second rule of thumb comes into play: the kidnappers are even more vulnerable to identification than they are to capture. There's a certain urge to move against the kidnappers at this point, but it's often better to pay the ransom and recover the victim, all the while using the drop to gather intelligence on the kidnappers. If you're careful and lucky, you may gain enough information to identify and move against the kidnappers later, capturing or killing them and recovering most or all of the ransom. Ensure that the drop volunteer is an operative or a well-briefed civilian. Observe every detail of the drop process, especially vehicles and personnel. If you can safely arrange surveillance of the drop, stay on the kidnappers after the act and learn what you can from their actions.

The same rules of thumb apply to political kidnappings, with this caveat: despite what they say, political kidnappers will probably not release their hostage alive—it's imperative to learn all that can be learned about them before the drop, and to act against them if any reasonable opportunity arises. ♦

1. Follow up the preliminary investigation. Continue following the leads provided by the preliminary, as well as looking into other basic leads.

2. Develop a scheme of events. Create in your mind a rough itinerary of events leading up to, during, and following the event. Use it as a basis for developing leads. Revise it as the investigation unfolds.

3. Continue the search for witnesses. Study the testimony of witnesses. Look for inconsistencies, or unresolved questions. Re-interview witnesses you talked to at the event scheme, going into greater detail to clear up uncertainties in your scheme of events. Canvass for new witnesses.

4. Assess physical evidence. As forensics reports come back from the labs, incorporate their information into your scheme of events. Ask yourself what the evidence in hand does for you, and what other pieces of evidence you need. Look for them.

5. Analyze the legal significance of your evidence. If your evidence must satisfy a client or the court, make sure you have enough admissible evidence to support the case. Remember, it is not always enough to know who did it: in a court, you must prove your knowledge is correct.

6. Identify and locate suspects. Make a list of all possible suspects, and identify those that had the motive, means, and opportunity to commit the crime. With your witness testimony and forensics analyses, identify these suspects. Locate and monitor them. If you have not contacted with them yet, avoid it at this point unless you have a specific reason to speak with them. Otherwise, do not alert them to your investigation.

7. Investigate and surveil the suspects. Learn what you can about the suspects, and see if that knowledge fits in with the circumstances of the event. Watch suspects for behavior associated with the event. Check out any alibis that are keeping potential suspects off your list. Narrow the field and firm up your list.

8. Interrogate the suspects. Contrary to the impression one gets from the movies, you shouldn't interrogate anyone unless you think he is the perpetrator—and you've got good evidence to back you up. The interrogation is often the last step in the investigative process, leading to a confession or at least the demonstrated inability of the suspect to answer to the evidence. It is also, however, the suspect's best opportunity to clear his or her name. If your primary suspect does so during interrogation, you will be set back a few steps. But his or her testimony will probably also fill in some gaps in your understanding of events, which will ultimately benefit the investigation.

The continuing investigation is the bulk of the work in an event investigation assignment. If the case is a simple one, following the steps above with

Techniques 19: Getting Around Locks

A well-rounded cell always has a lockpick gun and an operative capable of using it. Sometimes, however, you don't have the tools or expertise handy, or picking a lock isn't the most expedient way to gain entry to a closed location. In fact, in most common situations it's often easier (or less likely to attract attention) to get around a locked door than it is to deal with the lock.

When attempting to enter a locked location, begin by imagining that you live or work at the location, and that you have locked your keys within. What would you do?

Start by simply checking the doors. Although most businesses are careful and conscientious about locking up, many homeowners are forgetful.

Next, check the obvious hiding places for keys—it's amazing how many people actually hide spare keys under door mats, beneath flower pots, or on top of door frames. Look also for conspicuous stones in gardens—in addition to hiding keys under real stones, some people actually buy fake stones or bricks with easily-found "secret" compartments within. Don't forget to check all of these potential hiding spots at each door—front, back, and sides.

As you move between the doors, give the windows a look. There may be open windows at ground level, or accessible via balconies or trellises. Make sure to eyeball the latches of closed windows—often they're left unlatched.

If there are adjoining buildings or units, check them out. They may have connecting doors, or common attic or crawl spaces. The same is true for attached garages.

If none of these possibilities pan out, and you still don't want to (or can't) pick the lock, you'll have to seek out the building's weakest point. Assess the building thoroughly before choosing a course of action. Any thug can smash a window or pry open poorly-constructed doorframe—and such methods are entirely effective when appropriate—but considerations often preclude such obvious techniques. The college trick of using a credit card (or other thin sheet of flexible plastic) to depress the latch of a doorlock is effective on many low-end or poorly-installed locks; similarly, a wire or strip of sheet-metal can sometimes be used to flick open a window latch, especially one that isn't fully engaged. You may also be able to pick up a few clues from careful observation. For example, if the garage door opener has a numeric keypad with ten digits, the odds of guessing the code are pretty low—but if three of the buttons are heavily smudged with fingerprints, while the others are clean, the number of combinations you'd have to try might be doable in just a few minutes.

If you have time to plan your entry, try to get ahold of a key to make a copy. Your L&P representative should be able to duplicate most mechanical keys, and many electronic ones as well. In the case of electronic proximity locks (for which a passkey is waved in front of a sensor), you may be able to construct or acquire a device for reading the code as the lock is used—you can then use that code in a device to replicate the key. If you've got those skills, you may also be able to "trick" an electronic lock into remaining in the open position even when it registers as locked.

If all else fails and you must break to enter, start with the weakest point—usually a window or the doorframe, as opposed to the lock itself. ♦

a little imagination and insight will lead you directly to a conclusion. Unfortunately, things are rarely that simple. A careful perpetrator will leave few clues and no witnesses. A terrorist group or drug syndicate might have the resources to get the perpetrator out of the country—and your assignment may require you to go after him. You may have trouble with law enforcement agencies that don't want you involved, or with corrupt officials who tamper with records and evidence. You may be requested to keep your investigation a secret, due to the sensitive or even illegal nature of the client's activities.

All of these possibilities, and many more, are complicating factors that make following the above steps difficult or impossible. This book can't possibly cover all contingencies. However, here are a few tips for covering some of those eventualities:

- **Police interference** is one of the worst possible complications, especially if the agency in question feels that your investigation obstructs theirs. You may face criminal prosecution if the agency or public prosecutor gets too uptight. As if that's not bad enough, the high level of police corruption in the late nineties means that harassment may come even if you aren't interfering with an official investigation.

There are a number of routes you can take when you run into police problems. The BlackEagle name is fairly respected (if not appreciated) in most law enforcement circles. If you are troubled by an official you think is corrupt, threaten to expose him. Corrupt officials fear few things more than exposure, and the official probably won't want to tempt the wrath of a highly successful investigative organization like BlackEagle. If you think the police investigator is honest, and you feel safe telling him who you are, try striking a deal—an information trade for the benefit of both parties. If you can't expose yourself like that, or if the investigator is unwilling, your options are limited. One is to simply to work faster. Police investigators are poorly paid public servants, and even the most dedicated generally don't work for more than ten or so hours a day. Beat them to the evidence. A second option is to mislead or cripple their investigation. That route is ethically questionable and downright illegal, but may have to be considered.

- **Taking it on the road.** If your suspect is highly mobile, or if you are investigating events over a wide geographical area, you may find yourself on the move a lot. There is little advice to offer beyond common sense. Try to cover the event scene as thoroughly as possible before moving on. Get as much evidence to the lab as you can. If you have to move before all local leads are exhausted, leave somebody behind to follow up. Stay in contact with one another, your home office, and the lab.

- **Secrecy** is a common complication. Fortunately, it's generally not too crippling, unless one of the above situations is also a factor. The need for secrecy may prevent you from covering the event scene by the book,

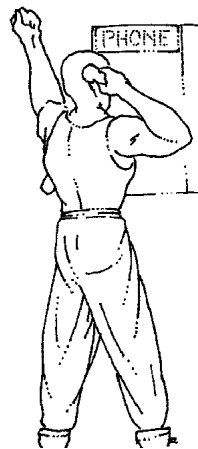
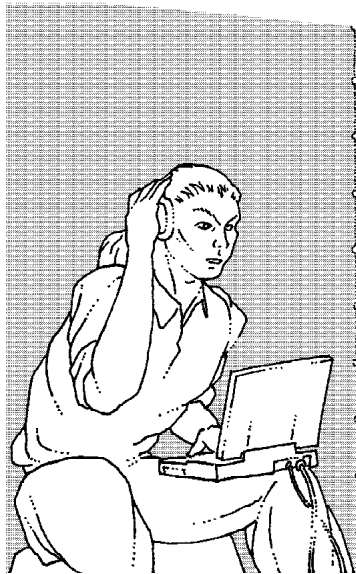
Techniques 20: Cracking Underground Organizations

When dealing with criminal organizations, terrorist groups, gangs or any well-organized opponent, it's common to find yourself seeking an individual who's identity—or just location—is a mystery. Often, success in an assignment hinges on identifying and capturing, neutralizing, or just talking to such a person, but if they're protected by layers of low-level goons or a compartmentalized organization that can be frustrating and difficult.

If at all competent, such organizations are very hard to crack. The thugs and errand-boys that you may interact with will be too disciplined, afraid, or ignorant to give you useful information on the organization, even under intense coercion. Most terrorist or criminal organizations operate in some variant of the cell structure: each individual knows only those personnel he or she works with regularly, and the boss from whom they take their instructions. Further up the chain of command, individuals know the identity only of those directly above and below them. That's the ideal, anyway—in truth criminals often know the identity of other members of their organizations, especially those led by charismatic or powerful bosses.

Such systems of secrecy are effective when events are under control, but they're inefficient under stress. One method for cracking the armor of secrecy is to create a crisis—something immediate, unexpected, and bigger than the low-level goons are able (or have the authority) to handle. Faced with a crisis too critical to deal with through the “proper channels,” a low-level thug will break the rules to call or contact his boss, giving you the opportunity to learn who he deals with. Before instigating such a crisis, be sure you have the means in place to surveil one or more target thugs, so that when they run for help you can find out where they go.

A second method is to trace a leak: send false information into a system, and then observe to see who acts upon it. This rarely identifies a specific individual, but it can narrow the field dramatically. This method is especially effective if you suspect ties between your secret



organization and other criminal—or even legit—ones. Leak some bit of seemingly-critical info to the suspected agency and see if your secret organization reacts. If so, you can usually deduce the sector of contact. This trick is best use to test a hunch, not for random guesswork—and, like the boy crying wolf, it rarely works more than once.

♦

and may make the gathering of evidence difficult. You will need to be circumspect in how you approach witnesses.

How secret you must be depends on the parameters of the assignment. Sometimes it is sufficient to simply mask the source and purpose of the investigation. Carry out your witness interviews with some sort of cover story, and disguise your actions on the event scene to avoid looking like an efficient, well-financed organization. On the other hand, you may have to avoid alerting the target at all—and this can be especially difficult if the target is suspicious, like an underworld or terrorist organization. If that's the case, all of your actions must be covert, and you can count on the assignment taking quite a while. Mask your witness and informant interviews with elaborate and believable covers, and fluff them with bogus lines of questioning to draw attention from your real interests. Gather physical evidence with caution, and secure your communications to defeat possible counter-intelligence.

Evidence Handling

What you do with your physical evidence, is, again, ruled by the parameters of your assignment. If the evidence is being gathered solely for your benefit, your only concern is that it is properly collected and makes it safely from the scene to the lab, so that the forensics results are accurate and complete. If, however, you are collecting evidence for use in legal cases, you also need to provide for accountability and admissibility. See the sidebar article on “Evidence Collection” (page 43) for tips on maintaining maximum forensic value. This section of the text focuses on maximizing the legal value of your evidence.

Legal situations place a substantial burden on the handling of physical evidence, which must be properly obtained and accounted for. Generally, the standards for admissibility are much easier for BlackEagle operatives (or any private-sector investigator) than for sworn law-enforcement officers. Government investigators risk having evidence thrown out of court if it is not obtained in a scrupulously legal manner. BlackEagle operatives face no such restrictions. Be aware, however, of how a judge, jury, and especially the legal opposition will look at your collection methods. Physical evidence gathered by BlackEagle cells has occasionally been disallowed in the past, especially when the legal opposition claimed that the state used BlackEagle to circumvent search-and-seizure laws. Witnesses and suspects have also gone back on statements given to BlackEagle ops, claiming that they were coerced. Juries may or may not be sympathetic.

Even if admissibility is not an issue, the legal significance of physical evidence relies on accountability. Law-enforcement agencies adopt a chain-of-evidence concept to ensure that evidence is not mishandled or

Techniques 21: Police Investigation Reports

Individual law enforcement agencies have their own standard procedures, and there is no specific form or format for police investigation reports. Every police organization, however, produces investigation reports of some sort, and they can all be very valuable sources of information if you can get your hands on them.

All police reports are written to provide a record for judges, attorneys, and other officers involved in the investigation and prosecution of crimes. Ideally, an investigation report is a clear, factual, and complete chronological account of the events, statements, actions, and circumstances of an investigation—but most cops are less than enthusiastic about report writing, and few are talented writers, so the ideal may not be met. As official documents, investigation reports are generally confidential.

There are actually several types of reports: Initial Reports (the immediate write-up of the crime scene or initial facts of the case); Interim (Supplemental, Auxiliary, or Summary) Reports (updating the investigation status for supervisors, district attorneys, or other investigators); Closing Reports (final reports on the investigations' conclusions); and Extract Reports (extracts from Closing Reports, for other, related investigations).

The Initial Report is normally a standard form, with three basic sections. The first covers the crime's circumstances: the type, date, time, and location of the crime, along with information on the victim, witnesses, and reporting party. The second, usually largest, section covers the Modus Operandi: the characteristics of the premises, how the offense was carried out, the weapon used, the apparent motive (or at least what the criminal accomplished); the value of stolen or damaged items; the activities of the criminal and the victim before, during, and after the crime; the vehicle used, and anything distinctive about the criminal. The final section covers information on any suspects, including name, address, and description.

Interim, Closing, and Extract Reports are normally written-out documents, perhaps with a standard form appended. As mentioned above, the format varies, but they are generally objective in tone and chronological in outline. Simple but functional crime-scene sketches are usually included. Proper names are usually fully capitalized, making them easy to scan for.

Interim reports are not particularly common; while an investigation is ongoing, the only source of information may be the investigator's notes. Those may or may not be on the agency's computer system.

A careful read of a police report can tell you as much about an officer—if he is honest, well-trained, and diligent (and whether his investigation was complete or cursory)—as it can about the crime. ♦

tampered with, and to demonstrate that such mishandling could not occur if the integrity of the evidence is later challenged. From the time it is collected until it hits the courtroom, physical evidence is always secure, and a record of its whereabouts is kept. A note is made of every individual that handles it, including investigators, lab technicians, and legal experts, and nobody gets near it that has no express need.

When a well-documented chain-of-evidence exists, the evidence can be admitted as factual during a trial. If not, you can testify that the evidence exists, and even produce it in the courtroom, but the bottom line will be your testimony about the evidence—not the evidence itself. A jury may or may not take your testimony seriously. A suspect goes free on a reasonable doubt, and if your chain-of-evidence is weak or non-existent, then the evidence is doubtful.

Adopt a chain-of-evidence process whenever you are involved in a legal investigation. Collect your evidence carefully, store it safely, and account for its whereabouts at all times.

■ **Background Investigating and Information Searches**

BlackEagle cells are sometimes called upon to conduct background investigations on individuals or organizations. Corporations may want to know something about the doings of a foreign company that is seeking a contract, or the motives of an individual who has suddenly started buying up their stock. Governments may want to know about the ties a company has with overseas insurgent groups, or about assets a corporation may not be listing on its tax returns. There are many reasons a client may ask for background investigations or information searches.

Even when an investigation does not focus on background, it often begins there. You will have to look into individuals and organizations involved in an event investigation. You may even want to check out a potential client. In fact, background checks on individuals, and information searches for plans, weapons purchases, and other information will often precede an otherwise totally tactical operation.

Background Checks

Background investigations on individuals are generally concerned with the target's financial status and income sources, personal holdings, lifestyle, travel, personal contacts, and criminal activities. It is usually to

Techniques 22: Autopsy Reports

Autopsy requirements and reporting methods vary from location to location, but most have several things in common. Autopsies are performed to determine the cause of death to aid in the investigation of crimes, to disclose public health risks, and to aid in civil cases (such as workman's compensation cases).

In most states, the medical examiner takes custody of a body any time a person has died by violence (accidental or deliberate), by unusual, unnatural, or suspicious means, or unexpectedly. Jurisdiction lies in the location where the person died, not where he or she was from. Only the medical examiner, the district attorney, or a judge in a relevant district can order an autopsy, which cannot be blocked by the decedent's (the dead person's) relatives or doctor, or any other outside influence.

A medical examiner will produce a Death Certificate shortly after receiving a body. This certificate lists a cause of death, but this is often preliminary—don't assume that such a document is the last word unless you know that no final report was drafted.

A fully-detailed report (usually entitled something like "Report of Investigation by Medical Examiner") follows an autopsy. Most such reports have several sections: information on the decedent (address, age, gender, etc.); a series of check-boxes for the type of death (suspicious, unusual, violent or unnatural, etc.); info on where and when the victim was last seen alive, where he or she died, and when the police were notified and responded; a section on the condition of the body when found, including the location of blood and wounds; descriptions of fatal wounds and probable cause of death; and, usually near the bottom of the form, a set of check-boxes for the determined manner of death (homicide, suicide, accident, natural, or unknown). A written report may be attached, along with a medical history of the decedent and diagrams of the body, head, and dentistry. Special tables sometimes detail gunshot or stab wounds, listing entry and exit locations for each, as well as sizes, directions, and powder burns or wound characteristics. Photographs are almost always included.

As with police investigation reports, autopsy records can be valuable in pursuing assignments—but, like police reports, they are usually confidential. Some jurisdictions make them available after the close of police investigation into the death, but that's often too late. Data from medical examinations, however, are almost always kept on computer, so access to the medical examiner's office network may yield much of the information included in an autopsy report. ♦

your advantage to keep the fact of your investigation a secret—if the target knows he is being looked into, especially if he knows why, he will probably take steps to guard his information. There are three major sources you can pursue: records, people, and physical evidence.

Record sources are perhaps the most useful of the three. The public and private records sources available to you are covered pretty well under Basic Leads, above. In addition to their availability and ease of use, records are also fairly confidential—the target will probably never learn that you looked after him. A librarian or clerk might remember your face, and your GenNet account will be recorded (and perhaps billed) when you log onto a private database, but in general you are not in danger of alerting the target to your investigation.

Your next source of information is the people around your target. People offer far more information—and insight—about the target than any record could. Most are willing to spill their guts, given a good excuse, unless they have reason to be suspicious or have secrets to guard. On the flip side, people will talk about having talked to you, so you risk the confidentiality of your investigation with every person you question.

Go after people likely to have the information you want, or who can lead you to it. Don't limit yourself to the target's friends or business partners—some of your best informants will be neighbors, doormen, landlords, and maintenance, cleaning, or delivery personnel who regularly visit the target's office or home. People such as these often have more knowledge than you might suspect, and can be quite chatty. They are also low-risk—if your questions aren't too pointed, they are unlikely to report the conversation to the target.

The next echelon of informative people are those more formally involved with the target—friends, relatives, employees, and business associates. Questioning these people entails a far greater risk of blowing the cover of your investigation, so you probably want a clear objective before approaching them. When you do approach, have some sort of cover story. If the person you are questioning has no particular reason to be suspicious, he will be willing to believe a great many things before he suspects something as drastic as an investigation. If, on the other hand, the target has reason to be wary, you must be especially cautious in your approach. In short, if people don't have a reason to suspect they are part of an investigation, they never will. But if the suspicion exists, they will see it everywhere.

In approaching any of the above people, look for openings that will get them talking. Tailor your approach to peak their interest—you may want to pose as a journalist for a publication covering the target's trade or hobby interests, looking for background prior to an interview, or as a prospective employer or landlord looking into the target's character and finances. You may even want to represent yourself as an investigator (not

Techniques 23: Social Security Numbers

The first three digits of an individual's Social Security number indicates the state in which the person entered the Social Security system—usually the state in which he or she was born. Although this is rarely decisive information, it can be used to confirm whether an individual is lying about his or her identity, or using forged paperwork. A particular indicator is any SSN beginning with numbers in the range of 600-699 or 800-999; these numbers have never been issued. The states correspond with the first three SSN digits as follows:

001-003	New Hampshire	449-467	Texas
004-007	Maine	468-477	Minnesota
008-009	Vermont	478-485	Iowa
010-034	Massachusetts	486-500	Missouri
035-039	Rhode Island	501-502	North Dakota
040-049	Connecticut	503-504	South Dakota
050-134	New York	505-508	Nebraska
135-158	New Jersey	509-515	Kansas
159-211	Pennsylvania	516-517	Montana
212-220	Maryland	518-519	Idaho
221-222	Delaware	520	Wyoming
223-231	Virginia	521-524	Colorado
232-236	West Virginia	525, 585	New Mexico
232, 237-246	North Carolina	526-527	Arizona
247-251	South Carolina	528-529	Utah
252-260	Georgia	530	Nevada
261-267	Florida	531-539	Washington
268-302	Ohio	540-544	Oregon
303-317	Indiana	545-573	California
318-361	Illinois	574	Alaska
362-386	Michigan	575-576	Hawaii
387-399	Wisconsin	577-579	District of Columbia
400-407	Kentucky	580-584	U.S. Virgin Islands, Puerto Rico
408-415	Tennessee		American Samoa, Guam, Philippine Islands
416-424	Alabama	586	RR Board
425-428, 587	Mississippi		
429-432	Arkansas		
433-439	Louisiana	700-729	
440-448	Oklahoma		

♦

necessarily a BlackEagle op), if you think the questionee won't spill the beans—people love to feel like they are involved in something important.

The final and most authoritative source on your target is, of course, the target himself. Getting information out of the target is not always as hard as you would think—even if he or she is on guard. Let's face it—people love to talk about themselves, and do it all the time. You just have to figure out how to get them to talk to you.

If the target is hiring employees, or looking for a job himself, you can pose as an applicant or employer to secure an interview. One reliable technique is to pose as a surveyor, asking your questions in person or by letter. Tailor the questions to the target's interests, be they professional or personal. Whatever your course of approach to the target or those around him, mask your real questions with fluff designed to keep the questionee interested and distract him from your line of thought. Word questions so that the answers are lengthy and well thought-out. Do little of the talking. Keep the informant at ease, and maintain real interest in what he or she is telling you. In short, practice the art of conversation to its fullest.

Physical information-gathering can take a number of forms. Sifting the target's garbage is a great way to develop some insight into his or her personality and habits, as well as finding specific sources of information, like discarded documents. Surveillance (covered above) lets you in on the target's day-to-day lifestyle, and possibly on specific activities you are looking for. You may want to have a look around his home or office when nobody is about—but don't get caught. Also, see if you can get into his GenNet account, or home or business records if they are online.

Smokescreens and Hidden Information

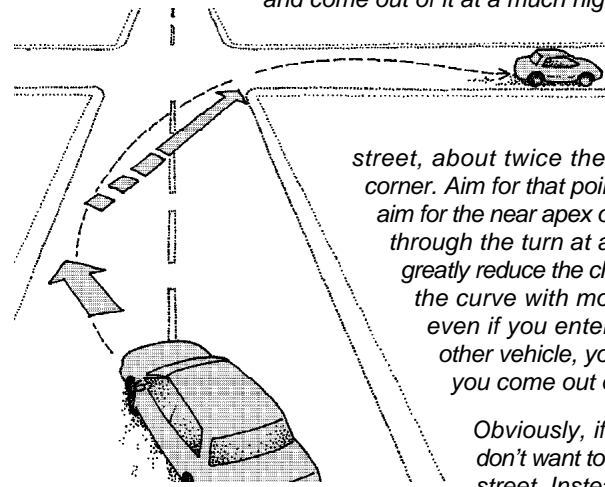
Background checks focus largely on publicly available information. Despite the efforts of public and private record agencies to keep their information current and accurate, it is possible for the records to lie, or at least cover the truth. If you run into inconsistencies, incomplete information, or something that just doesn't make sense, suspect this.

Smokescreens in public records are actually fairly common, and the vast majority of them are totally legit. Businesses often want to protect their information from competitors, or from buyers and sellers who may alter their prices if they know the business's plans and desires. Ownership and transaction records, in particular, are often masked by straw parties. For example, suppose you suspect that your investigative target—XYZ Corporation—owns a particular building. But the recorded deed shows that it belongs to a Mr. Smith, who bought the building from Jones Realty. What the record doesn't show is that at the same time that Smith bought the building from the realty company, XYZ bought it from Smith, with a second deed that was never made public. In short, XYZ fronted the

Techniques 24: High-Speed Pursuit

High-speed chases are an occasional part of a BlackEagle operative's job. One doesn't have to be a trained race driver to chase down fleeing suspects or criminals—a few basic tricks can help.

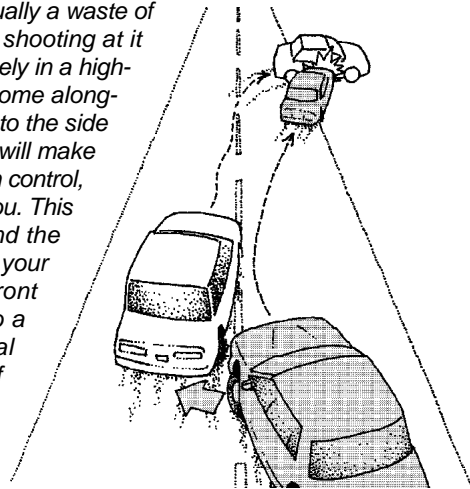
A driver untrained at high-speed maneuvers will likely approach a sharp curve or corner at a high speed, and then slam on the breaks to hug the inside of the corner. In so doing, the driver risks skidding or spinning, and finds himself having to accelerate out of the curve with very little speed. A smarter driver can make it through the same curve with less risk, and come out of it at a much higher speed.



To gain on such a driver as you approach a corner or curve, visualize a point on the opposite side of the street, about twice the width of the street from the corner. Aim for that point. When you reach it, curve to aim for the near apex of the corner, and follow that arc through the turn at a safe speed. In so doing you greatly reduce the chance of a spinout, and you exit the curve with most of your initial velocity—so even if you entered it moving slower than the other vehicle, you'll be catching up with him as you come out of the curve.

Obviously, if there's oncoming traffic, you don't want to aim for the opposite side of the street. Instead, aim for the outside of your lane. This will force you to slow down much more, but you'll probably still gain on a driver that hugs the inside.

When pursuing another vehicle, you have an advantage in being behind it. Don't squander that advantage by attempting to pull alongside like they always do in the movies. A firefight on the move is also usually a waste of time—it's difficult to disable a vehicle by shooting at it from behind, and very hard to aim accurately in a high-speed chase. To stop a fleeing vehicle, come alongside its rear end and give it a solid nudge to the side with the front corner of your vehicle. This will make it very hard for the other driver to remain in control, while taking very little control away from you. This maneuver, when well-executed, will send the other vehicle into a half-spin, whereupon your vehicle will strike it broadside with the front bumper. This will force both vehicles to a stop, leaving you in an excellent tactical position for confronting the occupants of the other vehicle. This bump-and-spin trick is easiest when attempted on the inside of a gentle curve. ♦



money, making Smith a front man, a straw party to hide XYZ's involvement. The deed showing the sale from Smith to XYZ is probably in a safe-deposit box or vault somewhere, ready to be made public if XYZ ever needs to prove its ownership of the building. This type of arrangement is totally legal, and often made for legitimate business reasons.

Business ownership records can be screened the same way. A corporation is founded by one or more individuals, who really use money fronted by others. Immediately after founding, all stock is transferred to those who fronted the money. Since the original incorporators show up on the articles of incorporation, but stock transfers don't, this method hides the true ownership very effectively. Again, it is totally legal and often totally legitimate.

If you suspect a front man, investigate him. Look for connections between the straw party and the suspected actual owner. The front man is often an employee of the company, or a friend—never a stranger. Also find out where tax bills and other official mail is sent—chances are the real owner doesn't rely on the straw man to forward it. Finally, see who signs the checks for the building's upkeep. If there's a management company, approach the agents—but be careful, they may have been instructed to maintain the secret.

Dealing with altered records is another matter. Often there will be nothing to go on, and your only hope may be that the alterer made a mistake. There is a great deal of redundancy in both public and private record archives, and the forger may have missed one or more documents. Dig deeply, look for anything that might have been missed, and, in the case of public documents, request to see original copies. It is unlikely that public or private records could be altered without the assistance or knowledge of somebody at the record site, so you may want to question or look into possible accomplices there.

Any time you think something is fishy, get help from an expert—someone you trust. Your office legal counsel can help you with legal documents and many types of public records. Bankers are also useful contacts, as are trust company researchers and public record keepers. But you must be sure that whoever you deal with is trustworthy—it's a good idea to cultivate contacts for the long haul, make it worth their while to help you, and keep in touch with them.

Techniques 25: Bribery

Throughout the Third World, and increasingly in the developed countries, bribery is an expected aspect of interaction with law enforcement officials. This can work to the benefit of savvy operatives who might find themselves accused of petty (or even severe) crimes—but it is not an end-all solution to lawbreaking. On the contrary, a failure to accurately read the signs or adhere to local customary procedure can land an attempted briber in deep trouble—even in the most corrupt of societies, the penalties for attempting bribery can be very severe.

Customs vary from society to society, and there are often distinct signals a corrupt official might employ to encourage a bribe—and just as often distinct counter-signals that you might not know, or which you might not employ properly if you aren't experienced with the region. One thing remains the same, however: an official seeking a bribe will not immediately write up or arrest his suspect, but will instead spend at least a few moments attempting to resolve the situation on the spot. When that's the case, an appropriate (and defensible, if you've misread the official's intent) response is to express a desire to effect a quick and amicable resolution. The official will then, typically, make an open offer to allow you to pay a fine directly to him, or to give it to him so that he may pay it for you.

If you are not in trouble, but are rather seeking to expedite paperwork, obtain a visa, or encourage the lax observation of a customs official, an effective technique is to ask if the payment of a fee will expedite the process.

Either way, bribery is a subtle process which cannot be carried out under the public eye. Make your initial moves quietly and out of sight of others. Don't expect to take advantage of official corruption if you have already made the evening news or your target is under close scrutiny or pressure regarding your situation. If you have been arrested for a serious offense and think that bribery might be of use—but you don't know how or whom to approach, ask the police to recommend a lawyer. If they're looking for a bribe, they'll set you up with someone who can arrange it.

Typical rates in the Third World run:

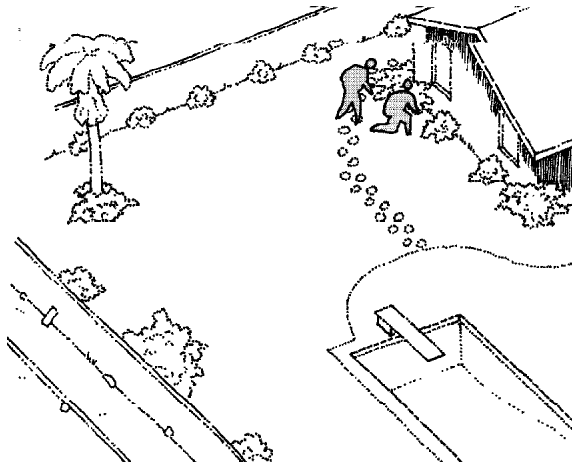
\$10 - \$30 for minor traffic violations (real or imagined); \$50 - \$100 for legitimate or serious infractions; \$500 - \$2,000 for very serious problems (like accidents).

\$10 - \$30 (or a carton of cigarettes or bottle of booze) for an expeditious trip through customs; \$100 - \$500 for oversight of significant smuggling (contraband, questionable items such as electronic surveillance devices); \$1,000 - \$3,000 for customs oversight when major items (firearms, for example) are clearly being moved.

\$10 - \$50 for minor police irregularities (being allowed to leave the scene of a minor crime, for example); \$50 - \$300 for oversight of minor crimes; \$500 - \$5,000 for oversight of significant crimes. If the victim is likely to make a fuss costs can soar—get a lawyer for any crime that's likely to cost more than a few thousand bucks.

Rates in Europe and North America can reach double or triple those listed above, though they can sometimes be surprisingly inexpensive. The risk is much higher, though, as corrupt officials remain the minority. Watch for the signals before making any offers. ♦

Chapter 2: Protecting Yourself and Those Around You



In B/E's first eight years of existence eleven employees were murdered in reprisal for the company's activities, including one senior staff member. Three relatives or spouses were also killed. One uninvolved bystander died. There were forty-three incidents of assaults, and six cases of bombings or booby-trapped cars and homes. All these attacks were aimed at off-duty operatives or their loved ones.

The work we do inevitably makes us targets of violence. Reprisals for the real and imagined harm we do to terrorists, criminal organizations, hostile corporations and foreign governments can be directed at any BlackEagle employee, at any time. Generally, reprisals are aimed not at particular operatives, but at the company as a whole, which means you may be a target regardless of your involvement. Attacks come on assignment, off duty, and against company facilities, operatives, their homes, families, and friends.

Any sort of "normal" existence leaves us vulnerable to these attacks. But there are steps that we can take to afford us some protection without forcing us into lifestyles of paranoia and suspicion. This section covers some of those steps—integrating them into your work and day-to-day life will make you a harder target, and might just save your life.

Home Security

Protecting yourself and your family begins at home. Use your professional experience to assess your home's vulnerability. You don't need to make your home into a literal castle, but you can take some passive security measures. Start with new locks—most builder-installed locks are pretty cheesy, as you probably know. Look into an alarm system, especially if your home is secluded or isolated. After reading the next chapter ([Surveillance and Physical Security](#)), ask yourself if you have a secure perimeter. Check that perimeter—all your doors and windows—twice daily. Be perceptive about your home—your ability to know if something "feels wrong" may be your strongest security asset. A pet can help in this respect—even a very non-aggressive dog will respond noticeably to the presence of intruders. Finally, keep in touch with your neighbors. They can be excellent watchmen, especially if they know you are a target.

Keep a cellular phone in the house, so you have a way to call for help if your lines are cut. Plan an escape route, and practice it if you have a family. If your home is large, choose an interior room as a sanctuary. Give it a decent door with a good lock, and keep a cellular phone inside. If the house is assaulted, your family can hide there and wait for authorities.

Movement and Public Activity

Attacks on BlackEagle offices are pretty rare, presumably due to the security precautions we take. Attacks on operatives on assignment are a little more common, but your unpredictable schedule will make you a difficult target while working. Adopting the advice above will reduce your vulnerability at home. But even though those three areas may account for ninety percent of your time, the remaining ten percent are the most dangerous. The majority of attacks on operatives occur while in public, often on the road between home and the office or at other points in your daily routine.

The big secret, then, is not to have a daily routine. Don't drive to work by the same route every day, or at the same time. Don't always shop at the same places. Own more than one car, or use public transport fairly often. Make your route and vehicle decisions randomly, and at the last minute. Those elements of your daily life that you can't randomize, like when your child gets out of school, don't talk about. You can't prevent a determined attacker from finding out about your life, but you can make it harder.

Travel

International travel can be a hazardous activity for B/E operatives. You are far from the protection and resources of the company. You are in unfamiliar territory. Someone gunning for you has all of the advantages. And in addition to the danger of attacks aimed at you, you face the threat of common terrorism and crime in remote areas where you can't count on the competency of official response.

Protecting yourself while on the move boils down to common sense. While travelling, you have little control over the environment, you can't control the degree of security, and you often—especially when travelling internationally—can't even go armed. Prevention is the best cure.

- **Don't stand out.** Don't do, say, or wear anything that identifies you as a BlackEagle operative. In fact, when travelling overseas, try not to stand out in any way. Wear average clothes—not too nice, but not too shabby, either. Avoid t-shirts with slogans or distinctive artwork, as well as jewelry and jeans or other clothes that might be seen as decadent or desirable.

- **Don't be predictable.** Don't always take a direct flight to your destination, especially if it's public knowledge. In fact, book more than one flight, with close departure times. Reserve hotel rooms in more than one hotel, or don't make reservations at all. If you are staying in one city for more than a couple of days, change hotels once or twice.

Techniques 26: A Home Security Kit

Many operatives keep firearms at their homes, in case their work makes them targets for prowlers, assailants, or even assassins. While that's a good idea (presuming that you store your weapon in a safe manner), there are a number of other items that should be in every operative's home in case of attack or invasion. As mentioned in the text, a cell phone is a bare minimum—any concerted attack on your home will begin with the phone lines being cut. It's better still to maintain a complete kit in a location where it can easily be accessed. Don't use the items in your kit for day-to-day functions—if you do, you'll likely find them scattered or lost when you need them. Instead, set them aside in an easily-accessible place (in your safe room, for example), where you know they'll be when you need them.

Your complete kit should include at least:

- a firearm.
- extra ammunition, pre-loaded into magazines or quick-loaders.
- a cell phone, with 911, the office phone number, and those of the operatives in your cell programmed into speed-dial.
- a good first-aid kit.
- a flashlight and extra batteries.
- a fire extinguisher.
- spare keys to your home and car, and perhaps to a neighbor's if you arrange it beforehand.
- two or three smoke grenades, to aid in escape and evasion.

If you have spares, or can afford to purchase them:

- a light ballistic vest.
- a pair of night-vision goggles, and an IR flashlight.

It's also a good idea to keep a miniature version of this kit in your car, for use not just when under attack but in any unexpected tactical action. Again, keep this kit as a backup—don't use this stuff for regular tactical action, or you'll discover it missing or misplaced when you truly need it:

- extra ammunition, pre-loaded into magazines or quick-loaders.
- a radio, with your cell's standard freqs pre-programmed.
- a good first-aid kit.
- a flashlight and extra batteries.
- a light ballistic vest.
- a pair of night-vision goggles.

For both your home and car kit, keep all of these items in a gym bag or similar tote so that you can grab the entire kit on the run if necessary. ♦

- **Don't be an easy kill.** Some criminals and terrorists, especially amateurs, still have a little compassion. Keep photos of loved ones (real or phony) in your wallet and passport. If taken hostage, talk about your life. Keep the enemy from dehumanizing you, and it will be harder for him or her to kill you.

Protecting Yourself on the Job

Discussion up to this point has been on protecting yourself while off-assignment. But there are a few tips you should know about keeping the job safe, too. Most killings on the job occur in “stand-up” fights—the tactical situations covered elsewhere in this book. But many are assassinations, and most of those occur because something that the operative knows or is doing makes him a target. Adopt the following pointers to keep your job safer:

- **Be circumspect about using your name.** Sometimes you need to identify yourself. Sometimes it's advantageous to tell people who you are and who you work for. But if there's no reason to do so, don't identify yourself. Have a few bogus names for yourself and your cellmates, so you can spontaneously fall back on them. If the enemies know who you are, they can come after you. If not, you hold the cards.

- **Don't let them know what you know.** When questioning an informant or confronting an adversary, don't let him pin down what you know, or even what you are up to. Throw in a few pointless questions, or questions for which you already know the answers. Never leave a conversation having given away more than you learned.

- **Make yourself more valuable alive than dead.** Avoid situations that make your death attractive to the enemy. If you “know too much,” record what you know. Make copies of incriminating photographs, video or other evidence. Put these things in a safe place—someplace where the enemy will never think to look. In fact, make two or three copies, and hide them all over town (it's not a good idea to hide sensitive evidence in the office, although you can let the office know where it is). Then make it known, if possible, that the information will go public on your untimely death.

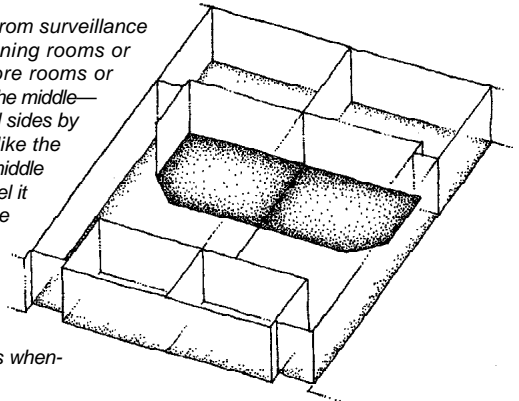
- **Maintain the initiative** when dealing with dangerous individuals and organizations. Don't let them call the shots. Regard any hastily set-up meeting with suspicion. If someone won't let you set the agenda, they may be setting you up. Get to meeting points ahead of time, then observe from a distance until the other party arrives (see the “Hostile Meeting” sidebar, on page 117). Never blindly walk into a disadvantageous tactical situation. Use payphones and untraceable datalines.

Techniques 27: Countersurveillance on the Road

Ops on your home turf are challenging enough, but when you're abroad security becomes even more difficult to maintain. A hotel room or hastily-rented villa doesn't offer the secure base of operations that the office or even your own home provide. Fortunately, there are a few tricks that can minimize the threat to your operational security and help you determine the presence and nature of surveillance against you. These techniques fall into three general categories: building a secure space; camouflaging movement to stymie surveillance; and employing telltales to warn of surveillance efforts. Which of these efforts you employ, and to what extent, depends on the nature of your assignment and the degree of surveillance you suspect might be used against you.

Building a secure space is a fundamental priority: if you don't take this step, your other countersurveillance efforts may well be a waste of time. The most obvious step is to search your space (be that a hotel room, apartment, house, or other locale) for listening and observation devices. A visual search is a necessity, and a sweep with a transistor detector is a good idea if you have one. Don't forget ceilings as well as walls and furnishings; vents, hung ceilings, and false fire sprinkler heads are ideal spots for placing such bugs.

To counteract vulnerability from surveillance that might come from adjoining rooms or apartments, rent two or more rooms or suites, then use the rooms in the middle—those that are bounded on all sides by spaces under your control (like the rooms in this diagram, in the middle of two rented suites). In a hotel it will be difficult if not impossible to control rooms above and below yours (you may be able to rent them, but that doesn't mean you can keep them secure), so pay special attention to ceilings and floors whenever you use this room.



Camouflaging efforts are simply steps to make surveillance difficult. Choosing hotels with multiple entrances (and learning the location of rear or emergency exits), stairwells, and elevators is a good first step—that'll make it hard for an observer to track your comings and goings. Requesting a room adjacent to the ice maker and vending machines can provide the audible and electronic hum that often frustrates eavesdroppers (you can make your own hum by opening the door to the minibar refrigerator, so that the compressor runs continuously). Think of times when you've had difficulty surveilling a target, and choose similar conditions and actions.

Telltales are tricks that can alert you to the surveillance efforts. The old spy-novel technique is a good one: lick a hair and stick it to the door and frame as you exit your hotel room—if it's gone or broken when you return, someone may have been (or may still be) inside. Place items in a particular arrangement or pattern that intruders won't notice—but you will if they're moved. Leave a light coating of dust on your door mat, or spray the doornob with UV-reactive hairspray. ♦

Risk is an inherent and unfortunate hazard in our occupation, and nothing can completely eliminate the threat to yourself and those around you. Common sense and a few simple steps, however, can reduce the danger to you and your friends and family without forcing you into a lifestyle of paranoia and constant worry.

Techniques 28: Office Security Drill

Security at the office is of paramount concern, as recent attacks on BlackEagle operatives have demonstrated. Every operative should be prepared to defend the office and be well-drilled in basic security operations. Know where your safe room is. Walk the shortest route to the safe room from every area of the office. Identify danger areas in each route—areas, such as stairwells or the entrance lobby, that might allow intruders to cut you off. Be aware of who is in the office with you, especially when you're there during off-hours.

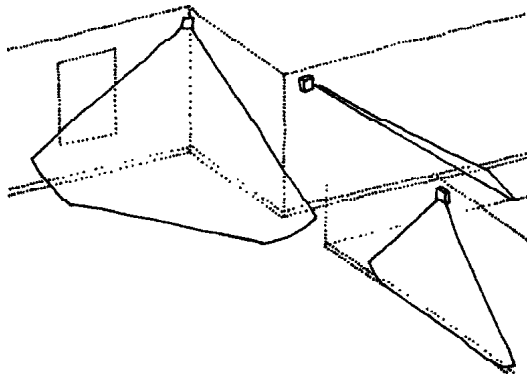
How an attack scenario unfolds can vary wildly depending on your office layout and security measures and the means and objectives of the attackers. Nevertheless, keep these points in mind, and follow them—in the general order of priority listed here—if your office should ever come under attack:

- 1. Take cover. You've just been surprised, but it's a good bet your attackers are well-prepared. Get your head down first; worry about moving or fighting back next.*
- 2. Trip the alarm. If there's an alarm switch near you, hit it.*
- 3. Fight back. If the attackers are in sight, return fire or move to subdue them.*
- 4. Get on the phone. If you can't see the attackers, call for help. Do this even if others are also doing it, or have already done so. Use a cell phone if you have one on you—the office phone lines are probably down.*
- 5. Move to the safe room. Move quickly but carefully. If you are engaged with the attackers, retreat towards the safe room even if you seem to be beating them, until you are certain that they are defeated and that there are no additional attackers.*
- 6. Determine who's in charge. That's your cell leader if he or she is present, or any other cell leader if not. Let that person know that you're there, whether or not you're injured, and whether or not you're armed. Follow that leader's orders.*

If you are the leader at this point, do the following:

- 1. Press the attack or complete the retreat. Decide—quickly—whether to repel the attackers or withdraw to the safe room. If you have any doubt, withdraw. Either way, choose a course and commit to it.*
- 2. Tally your personnel. Get a rough idea of how many people you've got, and how many of them are combat-capable. Try to determine if there are personnel unaccounted for who were likely in the office at the start of the attack, but don't waste too much time on the effort at this point.*
- 3. Get on the phone again. Even if the police have already been called, call them again. Then call the Senior Cell Leader and other cell leaders.*
- 4. Ensure that the vault is locked. Check it. And notice whether the office computers are dumping their files—they should be doing it automatically when the power is cut or the alarm tripped. If not, something is wrong, and that may relate to the attackers' objectives.*
- 5. Finally, identify the attackers. Throughout this process, be observant. Who the attackers are and what they want will be an important issue when the attack is resolved—and might save your lives during the assault. ♦*

Chapter 3: Physical Security and Surveillance Systems



BlackEagle operatives are in a unique position. We have to be experts on physical security—in more than one way. One week we are asked to provide security for an important meeting of international leaders, the next we may be hired to break into the highly-secure office of a mob boss. In either event, it is very important that you know about physical security systems—how they work, and how they can be defeated.

Security Systems

Like everything else, there is a strategy to the composition of physical security systems. A large, well-planned, well-run security system consists of physical detection and deterrence measures, personnel control and access accountability, a force of well-trained guards, and an auditing plan that ensures that no intrusion or leakage will go unnoticed. Such a system is well-balanced, well-tested, and nearly invulnerable. But few such systems exist. Many organizations feel they are too small or poor to invest in a complete system, or don't rate the risk high enough to warrant the effort. Others suffer from poor management. They build unbalanced systems, perhaps relying on minimum-wage guards after spending millions on detection and deterrence, or failing to carry out their own policies on access restriction or protection of goods due to the inconvenience such policies inflict on day-to-day operations. A great many face the inherent difficulties of retro-fitting new systems to old, unsecure buildings.

Despite their relative rarity, this section focuses on well-designed systems. If your assignments require you to defeat a lot of security, you'll be prepared for the worst—anything less will just be easier. And if required to provide security, you'll have the best possible model to emulate.

Most modern security systems are centralized and computerized, often controlled by the same CPU that handles compound or building environment controls, the elevators, and the fire alarm and suppression system. The brain of the operation is the central monitoring console, which in a large office building or hotel is sometimes in the lobby, but is more often in a rear security and engineering center. The central monitoring console controls the intruder detection system, the access control system, the closed-circuit video system, and the radio communication system, as well as the engineering and emergency-management functions of the system. It may also monitor and control telephone and data lines coming into the compound or building.

Security measures are not sprinkled around randomly—they are planned and layered to protect likely targets of intrusion. A large office building, for instance, will have a securable perimeter, some degree of surveillance and traffic control in public areas, and dense security around likely intrusion or burglary targets and avenues of approach to those targets. Security is also attuned to the nature of the threat. For example,

in a warehouse that only stores vehicles and other big items, vents and other small openings will not be as secure as large doors.

There are three different types of security tactics, generally used in concert: perimeter, area, and point security. Perimeter security protects the outer limit of the building, compound, or secure area, and begins with the walls, windows, doors and fences that define the structure. Area security protects a zone—it may include everything defined by the perimeter, or just selected areas within it. Finally, point security protects a specific object or point, like a vault. The sidebar on the next page discusses a typical security layout for a small corporate compound, including the measures that protect a particular office.

Instruments of Security

Security measures can be categorized into two basic sets of measures: deterrents and monitors. Deterrents are measures such as lighting, fences, doors, vaults, and locks that make an intruder's job more challenging, physically or psychologically. Monitors are systems such as alarms, video cameras, and audio sensors, that alert security personnel or the police if an intruder is detected. Guards and security robots function as both monitors and deterrents.

Entire books could be written on security measures, or even on individual devices. There isn't the space here, but below is an overview of some of the many types of security devices you may run across:

- **Fences** are generally exterior deterrents. They can be enhanced with vibration or capacitance sensors. Fences can be cut or climbed over.
- **Mechanical locks** might be keyed or combination. They can be picked, drilled, cut out of the door, or the bolt can be cut. Good ones are case-hardened, and have multiple bolts with internal roller-bearings, which make them almost invulnerable to saws.
- **Electronic locks** are usually tied to the central computer's access-control system. A badge with a magnetic or optical strip unlocks the door for five to fifteen seconds. The central computer records the person's use of the lock, and may be programmed to deny access to certain badges or classes of badges at given locations or times. At their hearts, electronic locks are really just mechanical locks controlled by electronic devices, and the lock mechanism themselves are conventional.
- **IR and photoelectric beams** are run across interior or exterior spaces, generally with no more than thirty yards between sensors. If broken, they trigger an alarm. Outside models are pulsed to resist being triggered by blowing leaves or small animals. If noticed, they can be circumvented by ducking under or stepping over the beam. Mist (from an aerosol can) will make visible-spectrum beams visible, but IR beams can only be seen with IR vision devices.

Techniques 29: Security Strategy

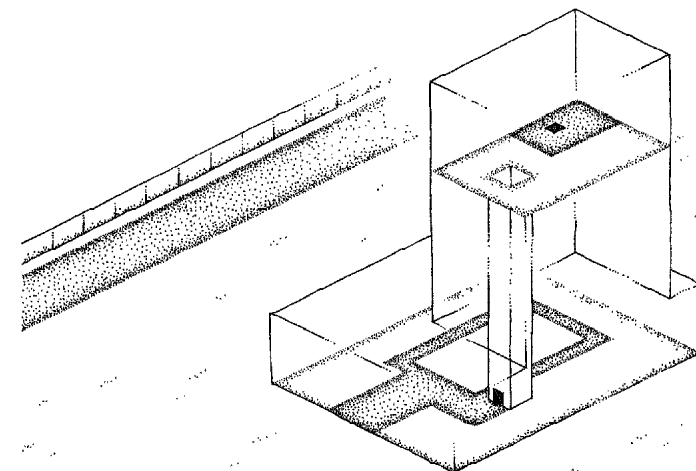
The schematic below shows a section of a corporate compound with an office building, illustrating the use of security tactics. Although there may be many protected points in any given building, this example focuses on a single one, a secure off-line computer in an upper-floor office. Look at the security measures that an intruder would face in getting to the computer:

Outermost is the first security perimeter, a fence supplemented with lighting and, possibly, vibration sensors or photo-electric beams. The next obstacle is the open ground around the building—the dark band inside the fence represents the patrolled area, which may also be surveilled by video. Selective lighting rounds out this layer.

The walls of the building itself form the third layer. The building creates a second perimeter, with restricted access through locked doors and video surveillance. Inside, the lower-floor corridors are patrolled and also watched via video. The elevator is watched by a camera and its use, or the opening of its doors, are reported to the central monitoring console.

The upper-floor office block has additional security. All accessways onto the floor—elevators, stairwells, shafts and ducts—are restricted, monitored, and alarmed, forming a third perimeter. In addition, the right-rear office is video monitored and subject to photoelectric beams and motion detectors, providing area security for the entire office. Lastly, the computer itself is locked and monitored via video.

This instance demonstrates a typical synthesis of perimeter, area, and point security, as well as a mix of deterrent and monitoring security devices. ♦



- **Video cameras** are connected to closed-circuit systems and monitored from the central monitoring console. In systems with many cameras, up to twenty images flash on the screen each minute. That means that a given camera only broadcast a few seconds per minute, so a quick intruder stands a decent chance of not being noticed, especially if the guards are inattentive. In low traffic areas, however, the computer can do the checking, comparing the digitized video output to an image stored in memory. If anything looks different, the alarm is sounded.

- **Motion sensors** are usually infrared. Many models not only detect motion, but even the presence of an immobile object not normally in the area—so they can't always be defeated by slow movement.

- **Pressure mats** are placed under carpet or entry mats, usually near doors or point targets. They sound the alarm if any weight is placed on them. Cheap ones can be defeated by distributing weight over a large area—placing a sheet of plywood over them before walking across.

- **Vibration sensors** pick up vibrations in an object. They vary in sensitivity, and are used on fences, display cases, point targets, and, of course, pinball machines.

- **Proximity sensors** are sensitive to the electrical fields generated by people, and can sense when a person gets within a couple of feet. They are very expensive and touchy, effective only in controlled environments, but impossible to defeat directly.

- **Capacitance sensors** run a very low electrical current through a given object, detecting by change in capacitance when the object is touched. Again, touchy, but good.

- **Ground-surveillance radars** are used outdoors and can pick up man-sized targets for a couple-hundred yards. They can be monitored, or set to sound an alarm any time significant motion is detected.

- **Robots** are usually little more than mobile video platforms. Some models, however, can recognize motion or unusual objects in their patrol area, and sound an alarm. They will follow moving intruders to the limit of their patrol area.

Many of these devices are virtually undefeatable directly. They must be avoided or circumvented to get around them. Never look at a security problem as a bunch of individual challenges—look at it as a system, and find some way to defeat the system as a whole.

Weak Links

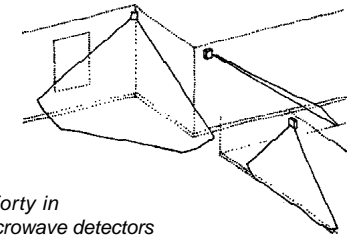
A security system is like a chain—only as good as its weakest link. A cliché, but true none the less. When analyzing a security system, look for aspects that create the weak link. That's where the system is vulnerable. Without going through the millions of possible problems you might find,

Techniques 30: Dealing with Motion Detectors

As with any security device, the first step in defeating a motion detector is to know what you are up against. There are three general types of motion detectors, along with three general deployment strategies for them—to efficiently defeat a detector, you need to know what type it is and how its deployed.

The most common types of detectors are passive infrared (PIR), ultrasonic, and microwave. Of the three, the PIR is by far the most frequently encountered, found in everything from cheap home security kits to impregnable corporate fortresses.

Motion detectors are generally employed for volumetric coverage (covering an entire room or other area), corridor coverage (covering the length of a hallway or other narrow space), or curtain coverage (covering a wall, entrance, or dividing line). PIR detectors can be set for any of these three uses, but their coverage is always flat and fan-shaped (as shown in this diagram). They generally have a range of about twenty meters, or up to forty in



corridor coverage situations. Ultrasonic or microwave detectors are generally only used for volumetric coverage, and they cover three-dimensional volumes roughly elliptical in shape. Ultrasonic units have very short ranges (no more than ten meters), while microwave units can detect out to twenty meters for man-sized targets, and farther for larger movement.

If you know or suspect that a motion detector is in use, do your best to identify its type and, perhaps more importantly, its location. Ultrasonic and microwave detectors are generally much larger than PIR units, and they are rarely used in low-end security arrangements. Most volumetric detectors of all types are placed in corners, where their coverage is generally able to reach the walls (including windows or doors) on either side. Almost all units are less efficient along the edges of their coverage areas, and all have blind areas beneath them and to their sides. Beware, however, that quality high-security setups will have overlapping detectors, each of which covers the blind spots of the others.

Motion detectors have vulnerabilities, even within their areas of coverage. For starters, many have test lights which illuminate when the unit detects motion. In higher-end units these lights are covered, but they are visible in many systems. In situations where animals or pets are present, motion detectors are generally not set up to cover the floor, and their coverage area can be crawled under. PIR systems are less effective at detecting movement directly towards them than they are at detecting motion across their fields of coverage. Almost all detectors attempt to reduce false alarms through a pulse system: a single detection does not cause an alarm; rather, two or more detections within a period of twenty or thirty seconds are needed. Thus a slow-moving intruder can make brief motions without alarm if they are spaced at least thirty seconds apart. Finally, PIR units are susceptible to false alarms from sunlight (on the sensor or a heat-absorbing object in the detection zone), ventilation breezes, and heat sources; ultrasonic and microwave units are susceptible to false alarms from incidental movement caused by winds, breezes, or machinery. Such factors can be used to disguise the cause of an alarm, or to encourage lazy security personnel to disable the alarm. ♦

here are a few possibilities:

- **The computer.** Ideally, the central control computer should be totally off-line—unreachable through the nets. However, since many buildings use the same system to control environment and engineering tasks, sometimes that rule isn't followed. And even when it is, there are often sites within the compound, other than the central monitoring console, that can access the controlling computer. A hacker can surreptitiously command video feeds, access control systems and alarms, or even lock the security personnel out of the system. If intruders control the CPU, the system is compromised in the biggest possible way.

- **Communications.** Most if not all security and monitoring devices are tamper-resistant or self-protecting. In a well-designed system, the communication lines between these devices and the central CPU should also be well-protected, but that is not always the case. The most sensitive device imaginable provides no security if it cannot alert the central monitoring console, or whatever else it is tied to. Of course, most systems monitor the integrity of their communications, but a skilled intruder can break lines without alerting the controlling computer, if he can get to them.

- **Guards.** Ultimately, it is the security staff that reacts to an intrusion, and if the guards are unskilled, their response will be as well. Find out if the company has its own staff, or if the guards are contracted from an outside firm (personnel records will tell you, or the agency name might appear on the guards' badges or uniforms). If you can identify a contract firm, find out how reputable it is. A few provide well-trained personnel—most hire minimum-wage drifters with next to no training. Incidentally, it takes about five full-time personnel to keep one guard position manned twenty-four hours a day, seven days a week. Personnel records can, therefore, indicate roughly how many personnel are on duty at any given time.

- **Access.** It is hard enough to foresee all the possible ways into an area when a security system is designed into a new building. It's even worse when security is retro-fitted into an existing structure. On top of that, changing demands are not always met with changes in the security plan. For instance, in the example quoted a few sections above, small accessways in a warehouse were less secure than large ones because the only stealable merchandise was quite bulky. But if the owners start storing smaller items there, someone has to remember to upgrade security on smaller openings—and that doesn't always happen. Look at the use history of the building, and always check plans for accessways that might be under-secure.

- **Routine.** Good physical security must be backed up by proper use. The most impenetrable vault in the world does no good if someone leaves it standing open. The fact is that most security policies are occasionally forgotten, and sometimes routinely ignored. Learn the habits of the people who work in secure areas, and you will learn a lot about the system's vulnerabilities.

Techniques 31: Dealing with Wires and Beams

Beams and wires are used to protect perimeters and in point security around specific targets. Photoelectric beams are not commonly used in low-end security systems, though they are sometimes found in sophisticated setups and are becoming increasingly common in outdoor perimeter systems. Wires are rarely used in indoor security, but are used in both civilian and (more frequently) tactical outdoor perimeters. Beams are detection devices, generally connected to alarm systems, while wires can be connected to alarms or to physical noisemakers, flares, or even (in tactical applications) mines or grenades.

Beams and wires are both difficult to detect from a distance, and can generally only be located point-blank. When detected, they can be easily avoided by carefully stepping over or under them. An ideal beam system will have too many beams, in too many directions, in too little space, to crawl through or over—but most systems (especially perimeter lines) are not that elaborate.

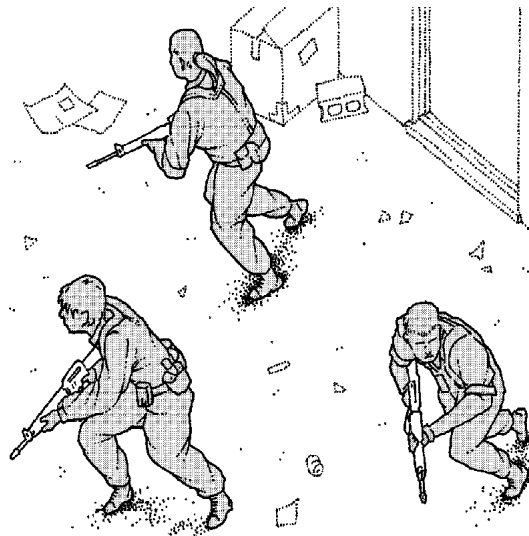
The visible-light beams seen in Pink Panther movies are a thing of the distant past—modern systems rely primarily on infrared lasers, which are not detectible to the naked eye. That doesn't mean that the old trick of spraying a little aerosol into them doesn't work, though—the beams will show up when viewed through night-vision goggles if they pass through smoke, dust, or particulates. Take a spray-bottle of water with you when attempting to penetrate an area guarded by beams. As you move through the area, pause every few steps and spray a light mist into the air before you. Watch through night-vision goggles for beams in the mist cloud.

For wires, the trick is to move slowly and deliberately. Before taking a step, gently extend your hand at head level, then slowly lower it, feeling cautiously through the air all the way down to ground level. Then straighten, lift your foot straight up, and extend it no farther than you felt with your hand before gently bringing it down. Repeat the process before your next step.

Ghost walking like that can take forever, but it's the only way to safely move through an area that you believe to be protected by wire alarms or traps. If you don't have that much time, a quicker though much less reliable method is to carry a lightweight wand—a thin stick or branch—and gently feel for wires with it as you move. That's an iffy method, though—if you know or strongly suspect that there are tripwires around, take the time to ghost walk.

Obviously, with either method you should stop and investigate anything you feel with your hand, foot, or wand. Never cut a wire—most wire systems (even primitive grenade traps) are activated not only by the excess pressure of someone snagging the wire, but also by the lack of pressure of a wire being cut. ♦

Chapter 4: Tactical Operations



Tactical situations are the most dangerous events operatives ever face. Combat is confusing, difficult and deadly. Whereas a bungled investigation will lose you a contract, a bungled tactical op can lose you your life. Study this section, learn from it, and practice its principles in order to succeed—and survive.

■ The Basics

An intensive study of the art of tactics can last a lifetime, especially given the broad scope of BlackEagle activities. But if you forget everything you've ever learned or been told, remember this: combat is a bewildering environment, and the side that can stave off confusion and remain a cohesive unit the longest is generally victorious. The following three points, as general as they are, will help minimize the "fog of war" and keep your cell an effective tactical unit. Remember them and practice them, and all of the tasks and techniques covered in this book will seem easy and natural. Forget these three points, and your tactical operations will be plagued with confusion, difficulty, and failure, no matter how well you know the drills.

- **Planning.** You must be properly prepared for your operations. Gather as much information on your objective and/or the hostile forces as possible. Identify and assess variables. Exploit your advantages. Understand your weaknesses. Prepare for contingencies. Be certain that every member of the cell, and anyone else involved in the operation, understands his or her part, as well as the overall scope of the plan. And whenever possible, set up a drill and practice beforehand. Then fine-tune the plan. There can never be too much planning, but many operatives have died because of too little.

- **Coordination.** A BlackEagle cell, like any good combat unit, is much greater than the sum of its parts—a small cohesive element is far more effective than an uncoordinated mob, even a much larger mob. The minute your cell loses its coordination, you cease to function as a unit and become just such a mob, and a small one at that. Coordination means each cell member knows his or her function, the cell leader is able to keep on top of things, and cell members can communicate with one another as needed. The first step towards good coordination is good comms. The second is practice and experience. Failing those, cell members need to keep cool heads, remember operation priorities, and keep track of one another, the adversary, and events around them.

- **Mobility.** When you are pinned down in combat, you lose initiative and are vulnerable to the full brunt of the adversary's combined resources. Mobility is an advantage that should never be discarded, even

in a defensive situation. Stay on the move, and you force the enemy to constantly react, never allowing him to go on the offensive. The converse is also true—so if you find yourself constantly maneuvering to counter the hostile force's moves, the situation is probably about to turn against you.

Simply drawing up a plan, buying some radios, and trying to stay on the move will not guarantee success in combat. But in small-unit tactical situations, attention to these three elements will give you an advantage even against a larger and better-armed force. It's not the size of your guns that will decide a tactical situation—it's how you use your brains and how you work as a team.

■ Planning Tactical Actions

The types of tactical situations that BlackEagle operatives find themselves in are numerous beyond description. Sometimes, especially when engaged in para-military work or when coordinating with regular military forces, specific planning procedures need to be followed (see the *Operation Order* sidebar). Even when this is not required, the steps outlined here should be considered when preparing for a tactical situation. Whether a cell has weeks to prepare for a jungle patrol, or finds itself setting up an impromptu raid on a hostage scene, these steps should all be followed or at least addressed.

1. Begin with a clear and complete definition of the objective.

You must know exactly what it is you are trying to accomplish before you begin to plan, let alone act. Reduce the objective to its most basic form, stripping away all extraneous elements. Be sure that everyone involved in the operation, and especially in the planning stage, is working from the same sheet of music.

2. Gather Intel. Put together as much information as you can about the adversary, objective, and conditions surrounding the situation. Use as sophisticated an approach as is feasible—whether that means running a full-fledged background investigation, or simply observing the objective for a few moments through a pair of binoculars. Try to put together as complete a picture of what you face as possible, accounting for hostile personnel, weapons, supplies, defensive positions, and surveillance. Also, consolidate all intelligence you have on the adversary's tactics and likely or expected course of action. Finally, look at additional factors like terrain and weather, and try to be aware of how they might affect your plans. If you plan to move at night, find out what the moon stage and cloud cover are going to be like, as well as the time of sunrise. Get good maps and, if possible, building layouts. Good intelligence minimizes the poten-

Techniques 32: Working With an OpOrder

If your cell does a lot of work with mercenary or military forces, you will probably run into an Operation Order (OpOrder for short) or something like it. An OpOrder is the document that orders a military operation, laying out the specifics for how it will be carried out and what it is intended to achieve, as well as background information pertinent to the assignment. The OpOrder described here follows U.S. military standards, but virtually every military and mercenary force around the world uses something more or less the same.

The OpOrder contains several major sections, describing the situation, the scope of the mission, and the planned execution. It may also contain annexes covering insertion and extraction, fire support, and other relevant information.

- **Situation.** This section covers physical conditions and the status of friendly and hostile forces. The opening paragraph describes the terrain, the forecasted weather, and other pertinent facts such as vegetation type and sun- and moon-rise and set times. The second paragraph describes the friendly forces involved or operating in the area, including an overview of fire and logistic support, and attachment and detachment of elements to the units participating in the operation. The final paragraph covers what is known of the enemy, including force size, activities, resources, location, morale, and likely response to contact.

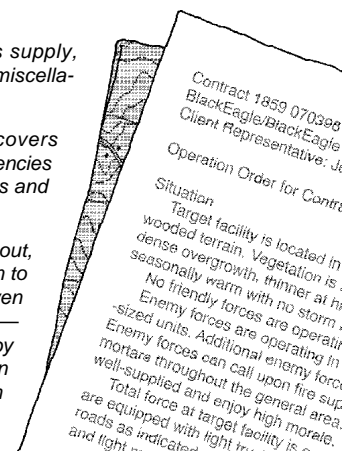
- **Mission.** This section covers the overall scope of the operation. It begins with a scheme of maneuver for the various units involved, goes on to explain the commander's intent in ordering the mission, and finally gives an overview of what tasks each unit will be carrying out during the operation.

- **Execution.** The execution section describes the activities that you will carry out. It begins with an overview of your task, then goes into whatever level of detail is appropriate concerning your activities and coordination with other units. It includes specifics about your insertion point, movement lane, extraction point, objectives, and timetable.

- **Admin and Logistics.** This section covers supply, transportation, medical evacuation plans, and miscellaneous issues.

- **Command and Signal.** The final section covers communications methods, including radio frequencies and call signs, passwords, and the use of flares and smoke for signalling purposes.

Depending on the type of operations you carry out, you may some day receive, or even be called on to issue, an OpOrder. Generally, OpOrders are given just prior to the commencement of the operation—usually the same day. They are preceded by warning orders, which cover the same topics in much less detail, but which are issued far enough in advance to give the unit time to prepare. ♦



tial for nasty surprises and increases options in the planning stage, so gather as much as possible.

3. Assess your capabilities and assets. Start with personnel, keeping in mind specialized skills and abilities and where they might be needed. List weapons, ammunition, and special equipment available. Look at the availability of backup, reinforcements, police assistance (if applicable and desired), and, when working with mercenary or regular military forces, the possibility of air and fire support. Don't forget incidental or environmental factors, like defensible terrain or advantageous weather.

4. Establish a course of action. Plan backwards from actions on the objective, or even from the escape or extraction if that will be complex. Backwards planning allows you to account for requirements at the objective, then figure out how to meet those requirements before combat starts, and gives you an accurate idea of your time framework. When planning, keep in mind the optimal use of equipment and heavy or special-use weapons. Decide who will deal with specialized tasks, like countering surveillance or security, placing demolitions, tending wounded, freeing hostages, etc. Make sure that the plan accounts for communication within the cell, and with any outside elements that may be involved. Take maximum advantage of assets, terrain, and environmental conditions. Don't forget to account for insertion and extraction, and for rally points or escape methods if things don't go as planned. Know how you will deal with your own casualties. Have specific back-ups for major contingencies.

5. Prep for combat. Brief personnel that were not involved in planning. Contact other elements involved, particularly if you are relying on outside transportation or fire support. Gather and prepare equipment. Assemble personal kits. Distribute special equipment according to who will be using it. Take care of any additional elements called for, like the preparation of defensive positions or the pre-placement of equipment, demolitions, etc. Use any additional time to go over the plan as much as possible, including dry runs and practice drills.

These five points are the most basic aspects of preparation for a known tactical situation. When your cell has the luxury of weeks to prepare for an operation, you'll want to go through every point mentioned above carefully, repeatedly, and in great detail. Go over your plan, rehearse it, analyze it for weaknesses and unforeseen contingencies, and refine it. You can never be too ready to enter into a tactical situation

But even when a tactical situation arises suddenly, leaving little time to prepare, these basics can and should be employed. Take stock of the situation, know your objectives, assess your capabilities, and put together a quick plan before taking any action, even if you have just a few seconds to do so.

Techniques 33: The Five-Point Contingency Plan

You may notice that many of the tactical techniques discussed in this chapter require the cell to split up. Objective recons, for example, are often carried out with two or more small observation groups, and an advance party is sent out to reconnoiter a patrol base or link-up point. Obviously, when a cell splits up the leader can only be with one element. That's where the five-point contingency plan comes in. It's simply a brief set of instructions for the other element, covering the possibility that something goes wrong.

If you are the cell leader, make a five-point contingency plan any time you will be away from part of your cell. The plan doesn't have to be sophisticated or detailed—it just needs to cover what to do in case you get hit, the other element gets hit, or one of you fails to return. The five points are simply who, what, when, where, and how.

A sample contingency plan might go as follows: "Joe and I are going out to scout the patrol base sight. It's about three-hundred meters south of here, so if we get hit, you'll hear it. If it happens, we'll retreat back to the last rally point. Meet us there. Do the same if you get hit. If nothing goes wrong, we should be back in half an hour. If we're not back in an hour, try to reach us by radio. If we don't answer, get out of the immediate area and keep moving along our current azimuth. We'll catch up if we can." This plan is neither detailed nor sophisticated, but it is enough to prevent confusion and allow the unit to regroup if a simple leader's recon should go awry. It covers the five points for both parties and the more obvious major contingencies. ♦



Being Prepared for that Unplanned Incident

Most of this text discusses tactical situations as though you always have all the time and resources needed to prepare for them. Of course, that's rarely the case. Nine out of ten tactical incidents will be unplanned, often starting with little or no warning. Prepare for these incidents: there are steps you can take to be ready for the unexpected.

- **Know your cell.** This is the most important thing you can do. Practice tactical maneuvers. Establish your own SOP for movement, mutual support, and sectors of security. Have one or more default meeting points in your city, so that you can get back together if separated. Basically, be able to move and act as one cohesive unit when a tactical situation arises, so that you won't have to pause to get organized.

- **Know the terrain.** Know the neighborhoods of your city. Know where the major roads are, and the police stations and especially hospitals. If there are gangs, learn their turfs. If there are bottlenecks—bridges, tunnels or causeways—know how to get around them.

- **Have equipment on hand.** That means carrying a weapon, or having one handy—the dangers of the job can follow you home. Keep a weapon in your car, at least one in your home, and one on your body, preferably with a back-up. Keep a rudimentary tactical kit—maybe a vest, a radio, and some extra ammo—someplace handy, like the trunk of your car (see the sidebar on page 65).

- **Don't disappear.** Make sure your cell members and the office know where you are when you go out on assignment. Keep some means of communication—a radio or portable phone—on hand. Between assignments, check in with the office or your cell leader every couple of days.

There is no end to the efforts you can take to prepare for the unexpected. Use your imagination—many of the steps you take will be geared towards your current assignment, or your local conditions. But never rule out the unexpected, on assignment or off. Expect contingencies, and prepare for them.

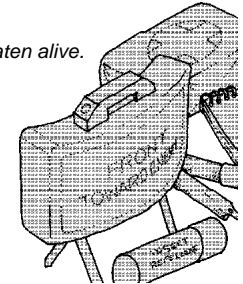
Tactical Principals

A tactics manual can be written as a series of standard procedures for specific circumstances, and many are. But there are basic principals underlying most tactical doctrine, and understanding these principals is often more beneficial than memorizing steps in a few dozen tasks. Besides, BlackEagle operatives face so many very diverse types of

Techniques 34: Field Tactical Kits

Every tactical assignment is different, and requires different equipment. However, certain equipment is almost always good to have along—as you put together a checklist for any tactical assignment that will take you out into the field, start with these basics for each cell member:

- an appropriate personal weapon and sufficient ammunition; a secondary weapon and ammo; grenades as appropriate.
- a good knife, preferably a rugged one with a built-in wire-cutter.
- a pancho and liner or blanket: keeping warm and dry is critical, and these items are also useful for camouflaging positions and carrying casualties.
- a compass and map: a necessary personal backup for your cell's nav gear.
- a basic first aid kit.
- water, and water purification tablets.
- a small flashlight: even with good night-vision gear, there'll be times when you just have to see clearly.
- electrical tape and parachute cord: two basic tools for field-expedient repairs or construction.
- a weapons cleaning kit: get your weapon jammed or gummed up, and you're worse than useless to your cell.
- personal cammo makeup.
- bug repellent: it's hard to remain stealthful when being eaten alive.
- smoke grenades.
- chemical lightsticks.
- a paper pad and pencil.
- zip-lock or waterproof bags.
- personal cammo gear.
- night vision gear.
- changes of socks and underwear: one for every two days in the field.
- food, as needed.



In addition to those items for each individual, your cell should have at least:

- unit weapons (grenade launchers, rockets, etc.) as appropriate, with ammo distributed; explosives (including det cord and claymores) as appropriate.
- a satellite telephone or tactical radio capable of contacting allied units.
- a good medical kit.
- a machete and/or hatchet.
- rope.
- heavy tape (in cammo or a dark color).
- a bolt cutter or heavy wire cutter.
- extra batteries for electronic gear.
- navigation gear (such as a GPS receiver).
- a small field water purifier.

This is basic gear only; specific objectives or environments may demand many additional items. Likewise, you may be able to eliminate some of the items on this list for specific assignments—but have good reason if you're omitting anything as basic as the items listed here. ♦

tactical problems that trying to address them all would be a herculean task. Some specific problems will be addressed later, but we will start here with a few of the basic concepts that take you a long way in dealing with your own tactical problems.

Assault and Support

Before any detailed discussion of small-unit and individual tactics can begin, you should understand one of the most fundamental precepts of modern tactics: Assault and Support. The assault and support concept is an unconventional warfare spinoff of the fire-and-movement doctrine, and is pretty simple conceptually. A combat unit (like a BlackEagle cell) divides itself into two elements, one of which provides suppressive fire to keep the adversary pinned down and unable to counteract, while the other moves towards the enemy, to flank or assault the objective. The division between the support and assault elements can be fixed or informal; the two elements can swap roles as needed (especially when leapfrogging towards an objective), or each can be assigned indefinitely to the respective tasks. The details aren't as important as the basic concept: one part of the unit moves under the protective fire on the other, so that the opponent is constantly suppressed.

This concept is flexible and works well in any environment, from high-intensity warfare to an impromptu engagement with punks on the street. A support element can suppress a sniper, a bunker, a security station, or a handful of gang-bangers while the assault element moves into an advantageous position to take it out and, if necessary, overrun it. The support element can distract a more difficult target (like an armored vehicle), while the assault element does whatever is required to destroy it (like place a mine). And, when necessary, the two elements can support one another in an orderly withdrawal or retreat.

When a firefight begins, the assault element should immediately try to position itself along the flank of the adversary or objective, while the support element rains in suppressive fire, keeping hostile heads down. When in position, the flanking element can signal the support to cease fire (or shift it away from the objective), allowing the assault element to move in, overrun the objective, and subdue the adversary. If overrunning the objective isn't desired, the two teams still have the adversary in a crossfire, minimizing the effect of his cover and forcing him to split his efforts between two fronts.

With the sorts of assignments most BlackEagle cells face, it isn't necessary to formally divide a cell into two distinct elements. Practice and experience will teach you to split your efforts to provide mutually-supporting fire without scattering your assets—you'll get in the habit of splitting into elements as needed. But when preparing for more conven-

Techniques 35: Passwords

Passwords are used to identify friendly individuals or units when they aren't directly recognizable—when you link up with an allied military unit, approach members of your cell in the dark or under cover, or meet a nervous informant at a hotel room. Passwords should be employed any time identification of friendly personnel is hard to verify, but they aren't necessary when you can easily recognize people that you know.

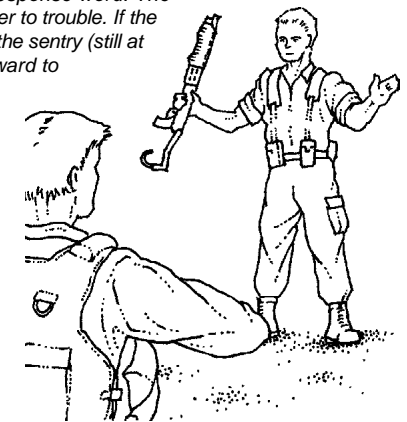
Most military forces rely on two types of passwords: challenge-and-response passwords and running passwords. Challenge-and-response passwords are used most commonly, and generally consist of a two-word phrase. Running passwords are used in emergencies when there isn't time for the normal challenge and response process (for instance, when a military unit is approaching friendly lines with hostile forces hot on its heels), and are usually just a single word.

In both cases, military forces change both passwords daily. That's a good idea for an operative cell that's working with outside forces, clients, or others, but for a cell operating on its own there's probably little need unless the passwords are frequently used and might be overheard. Otherwise, switching passwords every day can lead to unnecessary confusion and forgotten passwords.

Passwords should be random words, unrelated to the assignment and the operatives. Challenge-and-response passwords should consist of two unrelated words, such as "baseball moonscape" (rather than something that might be guessed, such as "baseball homerun"). Make sure that everyone memorizes the passwords (don't write them down), and that if you are switching passwords every day or at some point in the assignment, that everyone is clear on when the new passwords go into effect.

Rely primarily on your challenge and response password. The password is initiated with a challenge from the sentry or individual who detects the approaching person or unit—he orders the approachers to halt and identify themselves. Presuming they identify themselves as friendly, the sentry issues the challenge word, and the approacher responds with the response word. The wrong word from either side alerts the other to trouble. If the challenge and response are both correct, the sentry (still at the ready) has the approacher come forward to be seen, and, assuming that everything is as expected, allows him or his party to pass.

A running password is simpler: the approacher simply hollers out the password as he approaches, and the sentry lets him through. The running password is an alarm call, however, alerting the sentry and all else that hear it that trouble is on its way—so a hostile force using a captured running password gives up the advantage of surprise by using it. ♦



tional-style combat, especially if you will be working with military or mercenary units, consider deliberately dividing the cell into two teams. This will make military-style movement formations and tactics run a little more smoothly.

The two elements created by the assault and support doctrine are sometimes referred to as “fire teams.” In combat, the fire team—not the individual soldier—is the most fundamental unit, and fire teams are rarely split up. Although BlackEagle assignments sometimes demand more flexibility, it’s still a good idea to think of your assault and support elements as individual units. To maintain organization and cohesion, avoid splitting up beyond that point. It’s difficult enough to keep track of two elements in the haze and confusion of a fast-moving tactical action; keeping track of many individuals who have split off on their own is nearly impossible, and robs the cell of your ability to act as a whole.

Security

A tactical environment is, by definition, full of surprises, and there are few good surprises in combat. Do everything possible to minimize them, starting with intelligent security. Security is defined as the actions you take to protect yourself on your flanks and blind sides—the actions you take to prevent surprises.

When on the move, and especially when parked, all eyes must be focused outward, covering every direction and avenue of approach. During some actions, like ambushes or danger-area crossings, specific individuals should be assigned specific security duties—you will want to put one person at your back, facing the rear, and maybe one on each side. But even when that isn’t the case, everybody who is not otherwise occupied should be looking and listening, and ready to respond should a surprise occur.

When a unit is tactical for twenty-four hours or longer, and individuals need to eat and sleep, maintaining total security all the time is impossible. When this is the case, split up security duties. For example, when in a patrol base, half of the individuals may eat and sleep while the other half remain vigilant. Be certain, however, that those on security are evenly spread around the perimeter, leaving no vulnerable sectors.

When carrying out an operation, security elements should have a clear notion of the objectives. Individuals on security are often the first to make contact with hostile forces, especially when the adversary comes from unexpected quarters. In offensive operations, you may want to initiate combat immediately—meaning that the security element should open fire the minute the adversary is spotted. But in many cases, especially covert operations and recons, you never want to be noticed. Then, security should not engage hostiles unless absolutely necessary—

Techniques 36: Radio Prowords and the Phonetic Alphabet

The phonetic alphabet and radio prowords are used to streamline radio communications and prevent confusion in the event of garbled or fuzzy transmission. You may or may not choose to use standard prowords in radio communications within your cell, but it’s a good idea to be familiar with them if you are ever involved with other military or mercenary organizations. The following list covers the phonetic alphabet and some of the more common radio prowords used by NATO and other forces.

Alpha	Hotel	Oscar	Uniform
Bravo	India	Papa	Victor
Charlie	Juliet	Quebec	Whisky
Delta	Kilo	Romeo	Xray
Echo	Lima	Sierra	Yankee
Foxtrot	Mike	Tango	Zulu
Golf	November		

THIS IS: Identifies your station—follow immediately with your call sign.

OVER: Ends your transmission if you expect a reply.

OUT: Ends your transmission if no reply is expected.

ROGER: Indicates that you received and understood the transmission.

SAY AGAIN: Requests repeat of last transmission.

I SAY AGAIN: Indicates you are repeating last transmission.

MESSAGE FOLLOWS: Precedes a message that requires recording.

BREAK: Indicates a pause in your transmission. On any lengthy transmission, it’s a good idea to break every ten or fifteen seconds, to give other, possibly more important traffic a chance to access the frequency.

READ BACK: Requests the message be repeated back.

ALL AFTER/ALL BEFORE: Refers to all that follows/precedes a given point.

FLASH/IMMEDIATE/PRIORITY: Three levels of traffic precedence: Flash is reserved for hostile contact reports or emergencies; Immediate is reserved for important tactical messages; and Priority refers to any other traffic of higher than routine precedence.

RADIO CHECK: Requests feedback on signal strength and clarity.

ANY STATION: Addresses any station on the net.

UNKNOWN STATION: Addresses a station that you cannot identify.

SPLASH: Indicates the impact or expected impact of a fire or air mission. Typically, the artillery unit radios “Splash, over” at the moment it expects the mission to impact; the unit that called the strike replies “Splash, out” to confirm the impact. ♦

that is, when the adversary is just about to blunder into your position. In any event, the leader must make sure his security elements know what is expected of them, and insure that comms and signals for hostile contact are established and understood.

The function of security cannot be stressed too much. But discussing security is one thing, actually practicing it in the field is another. It is very easy, especially for operatives with little or no combat experience, to become distracted. You stop in the woods to look at a map, or on the street to talk to a local, and everyone wants to participate. When conducting a recon, everyone feels the urge to be the observer. When searching an office, everyone wants to be involved. But keeping your eyes outward is what will keep you alive. Reading a map only takes one or two people. If you're not one of them, resist the distraction and stay on security.

Stealth and Speed

Storming beaches and bunkers while overwhelming an enemy with firepower and numbers is the job for large, conventionally-organized armies. BlackEagle cells have neither large quantities of personnel nor withering firepower at their beck and call, and even when working with military or mercenary units are really only capable of operating in low-intensity, unconventional combat environments. In such conditions the key to success is stealth, speed, and the advantages of surprise that those two factors give. A BlackEagle cell cannot muscle its way through a battle, in the field or on the street.

Maintaining stealth means being silent and invisible. Believe it or not, that's not as impossible as it seems, with a little planning and common sense.

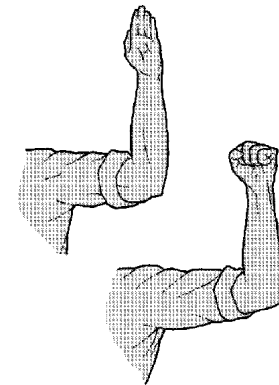
- **Don't talk.** Hand-and-arm signals work great when all members of the group can see one another. When you can't, use radios with headsets. Any good one will have enough mike sensitivity to pick up a quiet whisper, and the earpiece will prevent incoming transmissions from being audible. Even whispers carry, though, so maintain your discipline and keep unnecessary comments to an absolute minimum.

- **Use no light.** You don't need it, even on the darkest of nights, especially if you use night-vision gear. If you must read a map, use a red light, keeping it low and on for the shortest possible time. Never smoke in a tactical environment.

- **Take your time.** The ability to move quietly isn't restricted to indian scouts or ninja assassins. Silent movement just takes practice and patience. Choose your steps carefully. Step toe-first, to feel for debris that will make noise. And move slowly—painfully slowly if you want to be truly quiet.

Techniques 37: Hand and Arm Signals

Hand and arm signals are a great way of communicating when you don't want to be heard—quieter and often more reliable than whispering into a radio mike. You should have a standardized set for your cell. When on the move, shoot an eye towards your cell members every ten or fifteen seconds, in case they're trying to signal you. Get in the habit of passing the signals on: when one member of the cell uses a hand and arm signal, everyone who sees it should repeat it. That'll let the signaller know that his sign is acknowledged, and increase the chances that the intended recipient (who may be looking away at any given moment) will get the message.



Halt and Freeze

Both of these signals are made with up-raised arms, "halt" with an open hand, and "freeze" with a fist.

A few common signals used by military and SWAT teams are shown here and on the next page. You can use them as-is, modify them for your purposes, or make up your own from scratch. But in any event, have a set that everyone in the cell knows and recognizes. Then use them. ♦



Rally point

Make this signal by circling a hand in the air above your head, then point to your rally point landmark.



Security

This signal is made by jabbing two fingers towards your eyes, Moe-like. Use it to assign security positions.

- **Exploit the environment.** This seems to go without saying, but you can't give this point too much thought. Take advantage of overcast nights and inclement weather—rain will really work to your advantage out in the woods. Look to concealed terrain, and plan a route in advance that exploits it.

Once combat has begun, the advantages of surprise quickly disappear. Firefights invariably draw the attention of reinforcements, police, or even unwanted bystanders. Now speed is your ally—without large numbers and heavy firepower, mobility is your trump card. It is critically important to stay on the move—to remain mobile during a firefight, and to leave the scene as rapidly as possible afterwards.

Talking about mobility is a whole lot easier than maneuvering under fire. When bullets are whizzing over your head, it's hard to get up and run just for the sake of mobility. But a well-organized unit can move under fire with relative safety. Practice these steps:

- **Suppress hostile fire.** Send careful, aimed shots towards the adversary's position, even if you can't see him, to keep his head down. Split your fire so that some members of the cell can move while the enemy is suppressed. Splitting fire will also prevent everyone from having to reload at the same time.

- **Make the most of cover.** Use it constantly to move—even if it's just a few feet—so the enemy never knows where you're going to pop up next. When getting up from cover to maneuver, roll away from it before getting to your feet.

- **Outflank the adversary.** Don't face the adversary's position head-on. Move to his sides, forcing him to adjust his defenses. Spread out, creating several small targets instead of one nice big one. Catch hostiles in a crossfire.

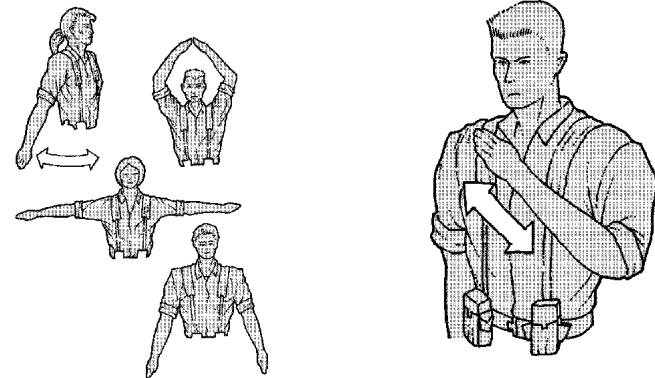
- **Watch your routes.** Be aware of how you got into the situation and how you can get out. Don't let hostile forces cut you off. Be aware of the adversary's routes, too. You may want to cut him off, or on the other hand, you may want to leave him a way out.

Combat is never safe, and moving from a position of relative security (behind a solid wall, for example) can sometimes seem like an insane idea. But no position—not even a concrete bunker—is secure if your opponent can maneuver around you. Following the points above can make it easier to stay mobile, and that's a small unit's key to survival.

Sectors of Fire and Defense

In a tactical situation there is a lot to look out for. If every cell member tries to cover everything, your attention will be too fragmented, and nothing will

Techniques 37: Hand and Arm Signals (continued)

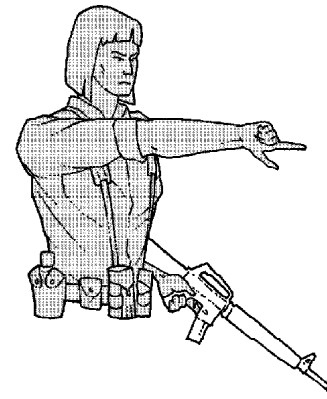


File, diamond, line and wedge

These signals are used to indicate formation changes.

Danger area

This signal is made by slashing an open hand diagonally across your upper chest.



Enemy spotted

This signal looks kind of like a child making a gun with his hand, only inverted. Point to the enemy with it.



Cell leader

This signal is made by tapping your left shoulder with your right hand. Use it to call for the cell or element leader.

be covered effectively. Duties must be split among the cell members, so that everyone has a job to do and nobody is distracted by worrying about someone else's job. That's where sectors of fire and defense come into play.

When on the move you must make certain that you are protected from every angle (as discussed under Security, above). Individuals within your formation should keep their eyes on their sectors. This doesn't just give you all-around protection—it also allows each person to do his job better. The lead man doesn't have to worry about what's going on behind him. He knows that the last man is covering the rear, so he can give the front his undivided attention. Establish an SOP within your cell, so that cell members will fall into this behavior automatically, without having to work things out in each individual action.

If you stop for an extended period, like in a patrol base, think about how your defense works. Deliberately assign each member of the group a sector of fire, so that each sector overlaps those adjacent to it but no individual is having to cover too wide an area. Put your heavier weapons where they will do the most good, or facing the most likely angle of attack. Even if you stop just briefly, set up a simple perimeter (see the sidebar on the herringbone perimeter, on page 107). You don't have to carefully position your forces, but at least arrange yourselves so that everyone is facing outwards.

Once you've set up your sectors, on the move or stationary, stick to them. Don't let the excitement cause anyone to abandon his or her post. A clever adversary, seeing you in a well-laid-out perimeter, will test one side. If you weaken your defenses on the other side in reaction, he will hit you harder there. Likewise, if a few shots are exchanged with your lead personnel while on the move, and everyone rushes up from the rear to get involved, you are vulnerable to attack from behind. Unless the situation is desperate, maintain the all-around integrity of your group. That's not to say you can't be flexible, but if you must shuffle people around, do it carefully and deliberately.

The fire sector concept applies to attacks as well as movement and defense. If you're assaulting a position, for example, every member of the assault element should maintain a lane of movement. Sweep through the enemy position, with every individual sticking to his or her lane. This will ensure that the area is thoroughly covered, that no hostile is bypassed to hit you from behind. Even more importantly, when working in a building or rugged terrain, keeping to lanes will prevent cell members from shooting one another by mistake.

Techniques 38: Deploying Non-Lethal Gasses

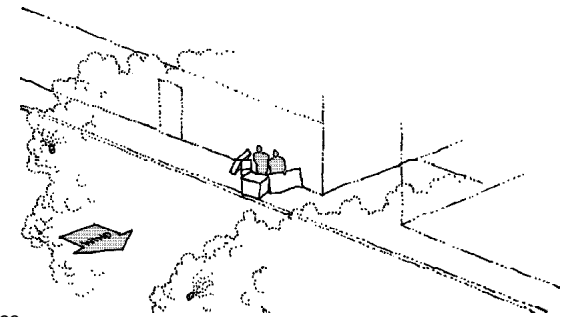
CS gas (also known as tear gas) and other irritant gasses are among the most common nonlethal weapons, often used by riot control and other civil forces. However, they can also be among the trickiest to deploy.

Outdoors, high winds or rain will reduce the effectiveness of gas, and can even blow it back against the user. Use gas outdoors when there is little or no wind or precipitation. Deploy the gas at a moderate density just upwind of the target area, from an upwind location.

Indoors, wind isn't a factor. But you still need to think about your deployment: concentrated exposure can be harmful to the victim and even lead to death for those trapped in the gas.

Indoors or out, a relatively light coverage is enough to deny an area to an undisciplined foe, and moderate coverage will dislodge or disable more determined opposition. How many grenades or other delivery items will give you "light" or "moderate" coverage varies dramatically with conditions and the weapon used.

Ensure that your targets have a lane to escape the gas; ideally, there should only be one lane, it should be obvious to the targets (so that they will not become confused in the gas), and it should lead directly into your preparations to capture them. If there is no escape route, a desperate target may stay in place, possibly suffering injury or death and forcing you to move into the gas to apprehend him. The illustration shows gas being used against insurgents in a street barricade—the gas forms a blocking wall upwind and to their front, leaving them an alleyway down which to flee. Obviously, the other end of the alleyway should already be secured before the gas is deployed (unless the objective is simply to dislodge the insurgents, with no intent to capture them).



CS gas sticks to clothing, so remember a change of clothes for yourself—and your target—for use after exposure. Always have respirator masks available when using irritant gasses, even if you don't plan on entering the gas cloud. Even small traces of the gas can reduce your efficiency, and you never know when you may be forced to expose yourself to more gas than you planned. ♦

Rules of Engagement

Military and police forces normally have tightly-defined rules of engagement, laying forth the conditions under which they use force and the type and severity of force used. Given the broad ranges of actions and objectives BlackEagle operatives face, no such blanket rules apply to our operations.

Normally, common sense will define your choices concerning the appropriate use and lethality of force in your assignments. However, it's always wise to consider the issue before entering into tactical situations, and if there is some uncertainty about appropriate levels, to discuss it with the client.

Non-Lethal Weapons

Because BlackEagle operatives' background training typically emphasizes the use of firearms and other forms of lethal force, many often fail to consider non-lethal alternatives when planning assignments. Non-lethal weapons such as rubber or beanbag rounds for firearms, tear gas, stun grenades, pepper spray, tasers, and restraining foam are often as useful—and sometimes far more useful—than standard firearms loaded with lethal ammunition.

However, just as you need to plan ahead and pick the best firearm for a particular mission, you must likewise put some thought into selecting the right non-lethal weapons. Given the wide variety of non-lethals that are manufactured, clever operatives can often find just the right tool for the job at hand. Some factors that should be taken into account in making the selection include the desired effect, your target, the range at which the weapon will be used, and the degree of lethality that is acceptable. Weapon availability and training are also issues that may color your choice of weapon, or the decision to use non-lethal weapons at all.

Desired effect is your first consideration. Some weapons, such as CS (tear) gas grenades, are best-suited for driving away the opposition—not for disabling or helping to capture them. Restraining foam is ideal for capturing individuals unharmed—if that individual doesn't have a firearm to shoot back in the seconds before the foam takes full effect. Other weapons, such as rubber bullets, can quickly disable adversaries, but risk serious injury. You must determine what non-lethal effect you want before you can seek a weapon well-suited towards attaining it.

You've also got to have a good idea of what your target is, and how effective various non-lethal weapons will be against it. Gas works well against crowds (that aren't equipped with masks), for example, while tasers are effective only against individuals.

Techniques 39: Deploying Non-Lethal and Restraining Weapons

A wide selection of non-lethal weapons is available, with varying effects. New non-lethal weapons are being developed every year—the most exotic of which (blinding lasers and acoustic weapons, for example) are not discussed here—but these more common types are easily obtainable and require little special training to use.

Restraining foams are best used against individual targets, when the target will likely be caught in the open for some seconds (a hallway or corridor down which a target will approach or flee is ideal). Aim the foam at the target's groin area, and then work down the legs. This will restrain the waist and legs and cause the target to fall down. After he has fallen, spray the target's chest and arms if necessary. However, avoid aiming at the head or face, since restraining foam can clog breathing passages and cause suffocation.

Non-lethal firearm rounds, such as rubber bullets and beanbag rounds for shotguns, work well against both individuals and crowds. Fire them low or aim at arms and legs—hits to the extremities are generally as effective as those to the body, causing pain and sufficient incapacitation, and are also less dangerous. When firing into mobs or crowds, target a specific individual rather than firing at random. These weapons are capable of causing harm or death—particularly if aimed at the head or fired from close range.

Personal weapons, such as tasers and pepperspray, don't generally make good offensive weapons as they are limited in range. They are useful against engaged or unsuspecting opponents, however, as they are quite limited in their area of effect, and are generally used at a close enough range that the target can be silenced quickly after their use. Aim irritant sprays directly at the face from short range, and be prepared for the target to become enraged and noisy (though generally blinded and incapacitated). Target tasers center-mass. Tasers and similar weapons that deliver electrical shocks can cause death in the very young, the infirm or elderly, or anyone with a heart condition. And like CS gas, irritant sprays such as peppersprays can injure and possibly even kill through overexposure.

With all restraining weapons, it's important to remember that effects are rarely instantaneous or complete. If your target is carrying a lethal weapon, he or she can still use it, if only for a few seconds. It's not wise to engage a target with restraining foam if he's going to fire back with a submachinegun, unless you ensure that you've got sufficient cover. ♦

Most nonlethal weapons have little if any range—rubber bullets are the major exception, but restraining foams, gas grenades, tasers and pepper sprays are useful only at short or point-blank range. They are appropriate, therefore, only if your plan calls for you to be operating at such short ranges anyway.

Despite their gentle-sounding name, non-lethal weapons are not always safe or even guaranteed not to kill. Adverse reactions to tear gasses and pepper sprays have been blamed for some deaths. Non-lethal rounds may cause serious injuries or death, depending upon the health of the target and the area of the body they strike. Determine what risks you are willing to take with the life and safety of your target, and choose your weapons accordingly.

Finally, of course, is the question of what non-lethal weapons can be obtained, and whether you have the special skills needed to use some types of non-lethal weapons. You probably won't have any trouble using rubber bullets or CS gas grenades, but more exotic non-lethals such as restraining foam, acoustic weapons, or blinding lasers cannot be used right out of the box.

Appropriate Ammunition

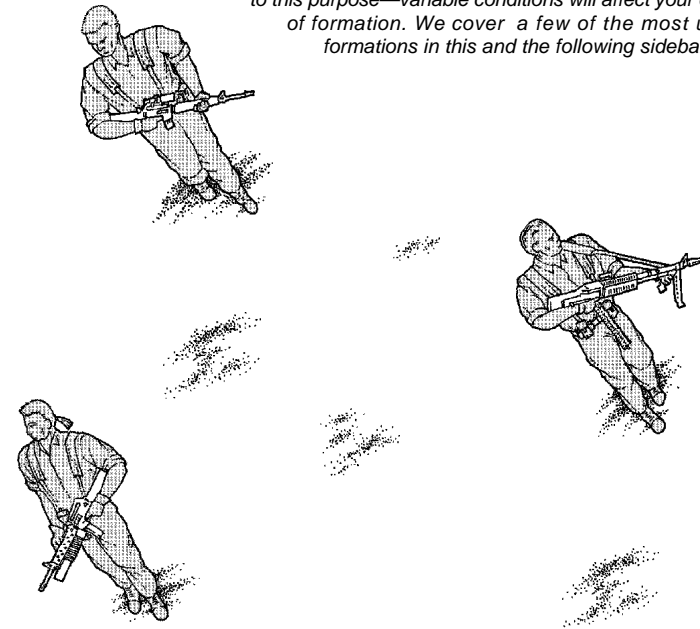
Choosing the right ammunition for the job goes beyond ensuring that you have the right caliber. Good ammo selection and techniques can not only prepare you for your assignment, but can actually aid in your security and combat efficiency.

For starters, assess your requirements. Obviously, your expectations about your adversary need to be accounted for—if you expect to meet opposition wearing body armor, you'll want to pack armor-piercing rounds. It's also important to think about the surroundings—in a crowded urban environment, you don't want your rounds to blow through walls and end up in a school, hospital, or crowded city street, for example. If you are dealing with a hostage situation, or another instance in which it is critical to take down the target with a single shot, you'll want to use the most powerful round available. And finally, if you are on an extended operation that will keep you out of logistical support, it's wise to standardize weapons or at least calibers to some degree within your cell, so that operatives can swap ammo if supplies start to run low. A couple of additional tips:

- When loading your magazines, place a tracer round second to the bottom. In combat, when you see the tracer fire, you'll know that your last round is in the chamber and your magazine is empty. Note, however, that this trick doesn't do much good in an urban or other close environment, as the round may end up stuck in a wall (or a target) before the tracer flare is visible.

Techniques 40: Tactical Movement Formations—the Diamond

Tactical movement formations are designed to defeat the effectiveness of enemy ambushes or attacks, while allowing you to move undetected and react effectively to contact with the enemy. There is no single method best suited to this purpose—variable conditions will affect your choice of formation. We cover a few of the most useful formations in this and the following sidebars.



This cell is moving in a tight diamond formation. The diamond is ideal for small groups—cells or fire teams—operating on their own in medium to dense terrain. The four corners of the diamond give good all-around security. In this layout, the leader is on point. Notice that she positioned her heavier weapons—the machine gun and grenade launcher—on either side, so she can direct their fire in case of enemy contact. If you have more than four personnel and want to use the diamond formation, place the leader in the center and put a rifle on point. If you have more than six or seven people in your group, a wedge formation would probably be better for you. ♦

- If you may be facing a mixed bag of armored and unarmored opponents, alternate ball or hollowpoint rounds with armor-piercing rounds in each magazine. Double-tap each target, to ensure that one of each round type is fired. Even if you choose a single ammo type, take along one magazine of an alternate type. Mark that magazine with colored tape or paint, for easy identification.

- If you're on your belly or crouched in cover, it's easier to drop your empty magazines down your shirt than try to fit them into a pocket or magazine pouch. Of course, your shirt's got to be tucked in for this tip to do you any good.

These tricks will improve your efficiency and help deal with unexpected situations. Remember though that ammunition is like any other tool—it's most effective in the situations for which it was designed. The best ammo tip is simply to know what you're up against, and choose the best ammunition type for the job.

■ Command, Control, and Communication

Combat is a difficult and confusing endeavor, whether it involves a handful of people in an inner-city streetfight or armies of thousands in the jungles of the Third World. Other factors being even, it is safe to say that whatever side is able to manage the confusion and maintain control the longest will be the victor. When a unit succumbs to confusion, its elements are no longer able to function cohesively. At best, its actions stagnate, it is unable to take advantage of its assets, and it is forced into a reactive stance, incapable of initiative. At worst, it is quickly routed and destroyed.

Resisting the fog of war means having a well-synchronized command and control system and maintaining communication within the unit. A BlackEagle cell is too small to have or require a sophisticated command system—generally there is simply the cell leader and other cell members. When moving tactically, the leader should be positioned where he or she can appraise and control the situation should you come under fire. You want heavy weapons close to the leader, so he or she can direct their fire. In some rare instances, it may be better to have the leader at the front of the formation, so that he or she can have a clear picture of what lies ahead.

Most command and control requirements can be met with basic man-to-man radio comms. But when tactical, you want to use your voice as little as possible, even if using VOX headsets. Standardize a set of hand signals within your cell. Some common ones are shown in the

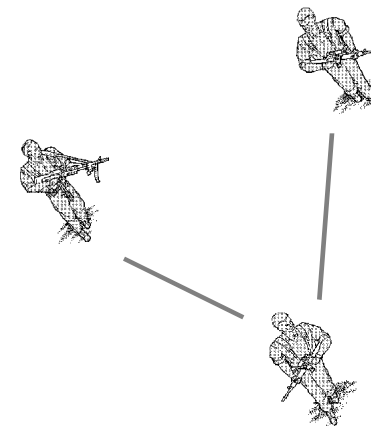
Techniques 41: Tactical Movement Formations—the Wedge

The wedge is the preferred formation for squad-sized and larger elements. If you've got more than six or seven personnel, in two fire teams, use the wedge whenever possible.

It works well in most terrain types, and in all but the worst visibility. Keep your personnel as far apart as vegetation and visibility will allow—about ten meters apart in forests, maybe three times that in open fields.

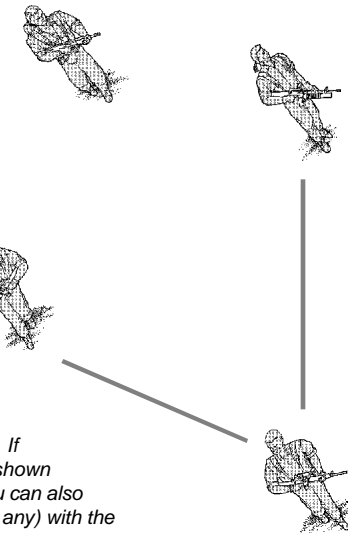
When visibility gets too bad to keep a wedge formation together, move to a file.

Notice how this cell is arranged in two fire teams, each in a V-shaped configuration. The leader is between the two elements. There is good all-



around security, and in case of contact, the two elements can split up to act independently. The heavy and indirect weapons are not convenient to the cell leader's control, but can be controlled by the fire team leaders.

The trail element is the probably assault element—if the cell comes into enemy contact, the lead element can instantly drop and provide supporting fire while the rear element (perhaps still out of sight of the enemy) immediately maneuvers into an assaulting position. The cell leader can go with either element, at his or her discretion. If you have more than the seven personnel shown here, simply extend the arms of the Vs. You can also put one of the heavy weapons (if you have any) with the cell leader. ♦



sidebar on page 91. Adopt them, or develop your own set that better serves your needs.

Good tactical comms sometimes negates the need for some of the procedures described in this text. For example, if every man has a radio, rally points may seem superfluous—you can always make radio contact if you are separated. But keep in mind that comms is not infallible, and things that can go wrong sooner or later will. Radios break. Terrain and weather affect transmission range. You may get a bad box of batteries, or someone may lose their equipment in a firefight. Have a backup plan, and follow good tactical procedure even if it has redundancies.

■ Movement in the Tactical Environment

When the layman pictures a tactical situation, a gunfight is usually what comes to mind. But in most situations, a firefight—especially one in which the adversary gets a chance to shoot back—only happens when something goes wrong. Let's face it: nobody likes getting shot at. Proper tactical movement is a good way to keep the enemy from getting a good shot at you.

Tactical movement has three general goals: to prevent detection; to allow effective reaction to hostile contact; and to protect the unit from hostile fire, all while moving towards or away from an objective. A number of techniques have been devised to meet these goals under specific tactical circumstances. These are covered below. Before we get to specifics, however, there are a number of general points you should know and keep in mind:

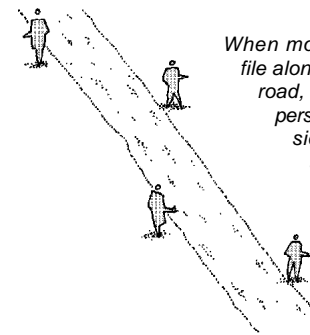
- **Never take the obvious path.** Never walk down a road or path—it may be mined, booby-trapped, or ambushed. Never come in through a front door if there is a side window. Never set up a patrol base in a strategically advantageous location. Never blindly pursue a fleeing adversary, especially in close quarters. Never leave an objective by the same route you approached it. Never poke your head over the top of a wall if you can look around the side.

- **Maintain optimal spacing.** Keep as spread-out as possible, without losing contact or concentration of fire. You want to minimize the number of people that can be taken out by a grenade or an ambush. In the woods, spread out to where each person can see the cell leader, but not necessarily the entire formation. On the street, string out so that you can't all be the target of a single burst of gunfire. But always be careful of

Techniques 42: Tactical Movement Formations—the File



The file formation is used only when visibility prevents other formations, or when you need to move quickly and aren't expecting any enemy contact. A well-spaced file is difficult to ambush, since personnel will be too spread out to fit in a concentrated kill zone, but doesn't allow you to quickly respond to contact. Leaders should stay near the center of the formation, with heavy or indirect-fire weapons nearby.



When moving in a file along a country road, stagger your personnel on either side. This makes ambushes even more difficult, and if you have to scramble for cover, not everyone will be bunched up on the same side. ♦



spreading out too far—you risk being cut apart, unable to maneuver, or unable to control and concentrate your fire effectively.

- **Maintain eye contact.** Every ten or fifteen seconds, look away from your sector and make eye contact with your cell leader. This keeps the group cohesive and insures that hand signals get passed on. What good does it do your rear man to keep perfect watch if nobody notices his warning signal?

- **Remain invisible and silent.** Don't walk along a tree-line—walk parallel to it a few meters inside the woods. Avoid crossing ridgelines, especially bare ones that will leave you silhouetted. Mask your movement with smoke if you must cross open areas and the enemy knows you are there. Never talk unless absolutely necessary—even a whisper into a VOX mike will carry through an empty warehouse or the stillness of the woods.

- **Avoid patterns.** If you are moving within sight, or potential sight, of hostile forces, don't let them predict your movements. Stagger the movements of members of the cell, roll away from cover before getting to your feet, and don't always take the most direct path.

- **Always think defense, especially when stopped.** Form an impromptu perimeter whenever you pause. If you stop to discuss plans, check navigation, observe terrain, etc., anyone not directly involved in the proceedings provides security, watching the flanks and rear. When on the move, people at the rear of the formation need to watch the back, while those on the sides keep their attention on the flanks. If everybody's eyes are forward, the unit is vulnerable. Don't forget trees, rooftops, culverts, etc.

These few points cover some of the basics of tactical movement. Some specific formations are covered in the sidebars. Practice these with your cell—they aren't difficult, but take some getting used to, especially in rough terrain.

Rally Points and Objective Rally Points

Every tactical operation runs some risk of failure or unforeseen difficulties, and you must always be prepared to cope. Establishing RPs (rally points) along paths of movement and near an objective is the most basic precaution you can take—having an RP allows you to regroup and reconsolidate, so that you can continue the operation or withdraw in an orderly and safe manner.

You can plan your rally points prior to the beginning of the operation, or while on the move. In either event, you want to position RPs every few hundred meters, or every major terrain feature (hilltop, ridgeline, city block, etc.), along your path of movement. The RP should be an easily-

Techniques 43: Tactical Movement Formations—the Line

Line formations are used for assaulting enemy positions. Once again, notice that the cell leader is in the center, where she can make contact with her personnel and see what is going on. The heavy weapons are nearby, where she can easily coordinate their fire.

When you move in this formation, maintain your spacing so that you move in a wave over the objective area. The tendency to bunch up as you pass over the objective is strong, especially in uneven terrain or dense vegetation. Resist it. Move forward, maintaining your spacing with the operatives on either side of you. Each individual must stay within his or her lane to ensure a clean sweep of the area. Otherwise, you may pass enemy personnel or positions—and this formation provides little protection against attacks from



the rear or sides. Also, be careful to keep moving at an pace even with your cell. It's easy to get too far ahead or to fall behind in this formation—and that will leave gaps and expose your fellow cell members' flanks to the enemy.

Don't use this formation to approach your objective, to leave it, or to travel in the field. Use it only in direct assaults—it's simply too vulnerable for other situations. Once you're in the line, move quickly and decisively—your speed and the impact of your assault is the only thing that counteracts your lack of security. ♦

identifiable landmark, like a large rock or a funky-shaped tree, so that everyone can find it. Establish the RP by giving a signal (hand-and-arm or radio) as you pass the landmark.

If you break contact with the enemy, always move back to the second-nearest RP, not the nearest. The nearest one may be too close—it doesn't do any good to try to regroup where you may still come under fire. For example, say you establish an RP, and then are hit fifty meters past it. Trying to consolidate fifty meters from the contact point will not give you a chance to break away and get out of hostile fire. But moving to the RP prior to that one will put a few hundred meters and/or a terrain feature between you and the adversary. So make it standard procedure to always move back two RPs before regrouping.

Set up several standing rally points in areas where you often operate, like your home city. That way, you have a consolidation point that everyone knows even if you haven't planned for a tactical situation (if, for instance, you are attacked when off-duty). The advantage of standing RPs is that you do not have to plan for their use—every cell member should know where they are at all times. The disadvantage, however, is that they can be compromised—you can be followed, or one member of the cell can be captured and tortured. When approaching a standing RP, therefore, pause to observe it for a few moments before moving in. You may want to set some sort of visible signal to indicate whether or not it is safe—a signal that would go unnoticed or be meaningless to anyone who didn't know its significance.

The last RP you establish prior to moving against your objective is called the ORP, or objective rally point. Again, place your ORP a few hundred meters or one terrain feature from the objective—but be certain it is out of range or protected from enemy weapons at the objective. The ORP is a great place to pause and make final preparations to move on the objective. If you have equipment that you don't want to carry into combat, it can be cached at the ORP (although if you have any suspicion that it might be tampered with, check carefully for booby traps when you return). If you retreat from the objective, you can pause briefly at the ORP to get everyone together, although you will probably want to move further off before a full reconsolidation.

Remember security when occupying any RP, especially an ORP. You want 360-degree surveillance. Even a group of two or three operatives should sit back-to-back. And an RP is not a patrol base—it's not secure enough to stay there long. Consolidate and move on.

Link-ups

Meeting up with a friendly group in the field doesn't sound too tough, but when it's dark and hostile forces are about, and everyone is trying hard

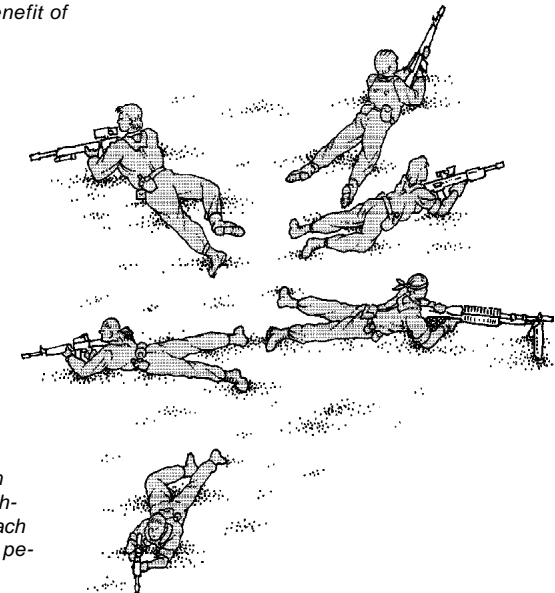
Techniques 44: the Herringbone

Security is one of your principal concerns in a tactical environment—you never know what direction a new threat is going to come from. It's important to keep attention focused outwards, even when dealing with a problem (such as trying to find your location on a map) within the cell.

Believe it or not, maintaining such a focus on security requires coordination. The simplest pattern to adopt is the "herringbone"—a formation that, when practiced, becomes easy to adopt, makes communication and coordination simple, and is highly versatile.

The basics of the herringbone are simple: the lead operative or point man drops prone or to a knee at the twelve-o'clock position. The second operative drops behind and to the right, facing outwards; the third a bit further back and to the left, facing the opposite direction. The remaining operatives alternate sides, except for the last, who takes up a rear-facing direction. If there's cover for individuals (trees, crates, whatever), use it, but don't deform the herringbone shape too much or you'll lose the benefit of easy coordination.

The cell now has security facing all directions. By forming a sort of oval, instead of a circle, communication and movement within the perimeter is simple—but the operatives along the flanks should leave enough space between them to form an unobstructed corridor, so that individuals can move as needed without stepping on each other or exiting the perimeter.



Obviously, it's easiest to drop into the herringbone from a file formation, facing in the original direction of travel. But with a little practice, your cell can drop to a herringbone facing any direction, from any movement formation, almost instantaneously. Use it to create a secure temporary position any time you've got to pause in a tactical environment. ♦

to be silent and invisible, link-ups can be difficult and dangerous. Maneuvering in the woods is often rough, so your problems may begin with simply finding the other group. But properly identifying friend and foe can also be tough, so your link-up procedure must protect you from hostile attack and mistaken friendly fire.

Before two parties can link up, both must know when and where to meet, and what sort of signal will be used at the meeting point. Both requirements can be specified in the operation plan, or you can establish them on the fly, assuming that the parties involved can communicate with one another. Your link-up point should be near—but not at—some sort of minor landmark, like a clearing or fork in a creek. The landmark should be something identifiable on a map, so that both parties can find their way to it, and small enough so that the whole thing can be observed. The signal should be something physical but inconspicuous, like three stacked rocks, or an upright stick, that will indicate the presence of friendly personnel without alerting the adversary.

Link-ups are at their most dangerous point right before the contact is made, when two armed, nervous parties are in close proximity but neither knows where the other is. If your groups consist of more than three or four people, leave most of them parked a few hundred meters from the link-up point, then send an advance party to make contact. After contact is made, one person from the advance party can go back to fetch the remaining personnel.

Whoever goes to make contact should approach the landmark, moving to where it can be observed. If the agreed-upon signal is visible, you know that the other party is already there, and should be somewhere where they can see it. Send one person to the signal, and the other group will see him and send someone to contact him. Once those two have met, both parties can move off to the nearby link-up point to exchange information and send for the remainder of their personnel. If the signal is not present when you get to the landmark, send one person out to set it up, then hide where you can see it. When the other group arrives, they will send one person out into the open, and you can meet him and carry on as just described. In either case, no more than one person from either group is vulnerable at any one time—everyone else is concealed and secure. You are relatively safe from discovery by the enemy and accidental hostile contact with the friendly group.

Approaching the Objective

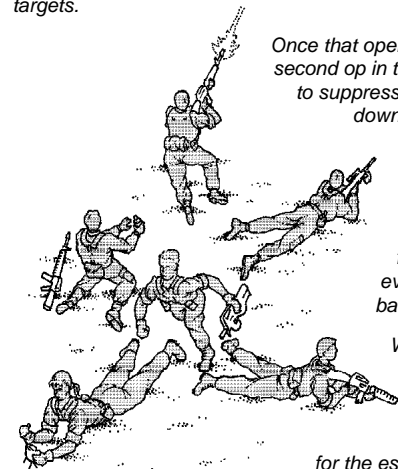
If you employ assault and support tactics when approaching your objective, half your work is done. The two elements can support each other as needed, bounding to get both elements into position. If you think you're

Techniques 45: Breaking Contact

How you choose to handle contact with enemy forces varies dramatically with your assignment objectives. In some cases, you'll be seeking to locate and engage your opponent, but often—especially in areas where your small cell is operating near large hostile military forces—your objective will be to avoid contact. Stealth is the best method, but it isn't always possible or reliable.

When stealth fails—when you've already been spotted, or you won't be able to remain hidden for long—the next resort is speed and firepower. To escape a superior military force, you'll need to move quickly while keeping the enemy's head down long enough to make your escape.

For starters, have a contact signal. This might be a hand signal (see page 91), or you might decide beforehand that whoever spots the opposition opens fire immediately. Whatever the case, drop immediately into a herringbone (see the previous sidebar) with the operative who spotted the enemy at its head. That operative—and that one only—fires up the enemy, blasting off a complete magazine in rapid bursts of autofire. Like all suppressive fire, make it count—put the rounds as close to the enemy as possible, so that they're forced to seek and remain in cover—but don't waste time picking and choosing targets.



Once that operative has emptied his or her magazine, the second op in the herringbone takes up the fire, continuing to suppress the enemy while the first operative dashes down the center and out the rear of the herringbone. The second op empties his or her magazine at the enemy, then dashes out after the first while the third operative picks up the job of suppressing the enemy. This continues, with the forward-most operative firing while the one before him escapes, until everyone has broken contact and is heading back to the designated rally point.

While the first couple of operatives are suppressing and escaping, those towards the rear of the cell might throw smoke or fragmentation grenades to add to the suppression or provide additional cover for the escape—but don't futz with grenades or other weapons instead of shooting; it's critical to maintain the stream of fire. If you've got a claymore with a short timed fuse, the last operative can set it up while the others are suppressing and escaping, then pull the pin as he or she leaves.

Once you've broken from the herringbone, head directly to your rally point (remembering that you always head to the second-closest point, not the nearest one) before attempting to regroup. Keep each other in sight as you run, but don't slow down. You've bought a few seconds of surprise and hesitation in your enemy (which, given the volume of fire you put out, may assume that your unit is much bigger than you actually are), but it won't last. A quick escape is essential, to avoid being outmaneuvered and outgunned by a numerically superior foe. †

undetected, don't open fire until everyone is in optimal position. But you still want to bound—hostiles may be watching, waiting to see the whites of your eyes.

Get the assault element as close as possible before assaulting or opening fire. The support team, however, may not need to be so close. They'll do their job fine at maximum effective range of their weapons, taking aimed shots to suppress hostile fire, spread out to deny the adversary a cohesive return target. Moving closer entails the risk of detection and becoming a target, and increases the chance of being the suppressee rather than the suppressor. But in a fluid or spontaneous situation, it may be better to keep the support element close, where they can respond to changing events, keeping the unit cohesive and cutting down on confusion. The cell leader must decide where to put the support team based on the variables of the situation.

Danger Areas

A danger area is any location or piece of terrain that works to your disadvantage, giving no cover or concealment and making detection or ambush more likely. A danger area might be a road, a creek, a field, an alley, a building lobby, or any other place that makes you uneasy. The best way to deal with a danger area is to go around it, but that is often impossible.

There are dozens of techniques for dealing with danger areas that you must cross. All are based on the same ideas: provide security to prevent surprise attacks while crossing; ensure that the other side is secure before committing to crossing the danger area; and cross carefully (usually one person at a time) to avoid detection in the danger area.

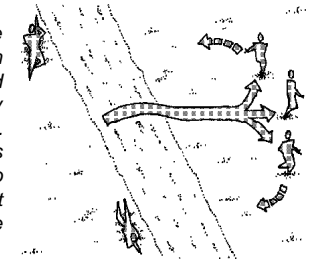
Two methods of danger area crossing are outlined in the sidebar opposite and on the next page. The first is the most cautious, and the slower method, to be used when enemy contact is a real possibility and you can afford the time to do it right. The second is optimal when speed is important, hostile contact is not expected, or the danger area is small. These methods can be easily employed in urban and field settings, and even inside buildings.

Techniques 46: Crossing a Danger Area

There are many different ways to deal with danger areas. The best is to avoid them, but that's not always possible. This method is slow and cautious, and best suited for fairly large units. For ease of illustration, a cell is shown crossing a road, and no cover or vegetation is shown. But everyone should stay well-hidden except when actually crossing, and this technique can be used crossing small fields, alleys, and building lobbies and well as trails and roads.

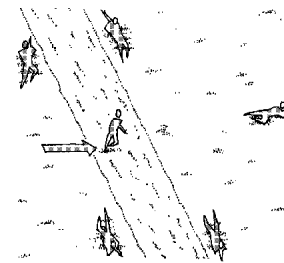
Step 1

Halt your formation a few dozen meters from the danger area, in good cover. Have two personnel from your lead fire team or element take up concealed security positions along the danger area, about fifty meters or so to the left and right of the crossing point. Send three personnel from your trail element across the danger area. They secure an area large enough to hold your formation, with one of them taking point security. The others signal back all-clear, then take security positions along the side of the danger area.



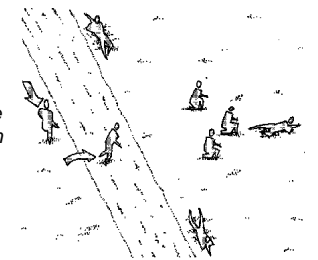
Step 2

Move your remaining personnel across the danger area, one at a time. Reform your original formation in the secure area, with each person taking up his or her position in that formation. In that way, you'll be organized throughout this process, ready to move quickly once across or react if hit while crossing.



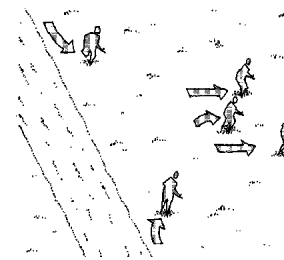
Step 3

Once everyone else is across, the two near-side security people cross. They take up their positions in the lead fire team or element.



Step 4

The lead element begins to move out. As it does so, the three far-side security personnel fall into their positions in the trail element, and the entire formation moves on. ♦



■ Bodyguarding and Personal Security

A unique tactical challenge is that of protecting an individual or group of individuals. Unlike most of the tactical tasks covered in this text, as a bodyguard you cannot always take the initiative—you are at the mercy of the protectee (called the “principal”) and his or her schedule. Keeping the initiative out of the hands of the attacker, then, is a large part of your task.

Types of Jobs and Threats

There are three general categories of personal security jobs: protection against surveillance; protection against the public; and protection against specific threats. The first category occurs when someone is, or believes he is, being watched by some organization. The principal wants a bodyguard to shake tails, find bugs, and generally keep his or her environment free from prying eyes and ears. The second category occurs when the principal, a celebrity or notorious figure, feels that there may be some unknown threat in all of the public attention he or she receives, and wants someone around to ward off crowds, vigilantes or kooks. The third category occurs when the principal has some reason to believe that he or she is a target for attack or kidnapping.

In addition to these three categories, which describe the nature of the threat, there are three general classes of security jobs relating to the level of danger and immediacy the threat poses, and the extent to which the client (who may or may not be the principal) will allow it to affect the principal's activities. These three classes are:

- **Buffer jobs.** Buffer jobs put you between the principal and the public. That may mean protecting a celebrity from crowds or screening all visitors for a major corporate executive. Buffer jobs are not contracted in response to a specific threat.
- **Light Security.** If the client perceives a real threat, but not a specific source of danger—for example, if he is a member of the board of a corporation that has suffered a rash of terrorist killings—handle the case as a light security assignment. Light security provides significant and sustainable protection levels, with minimal impact on the principal's lifestyle.
- **Known Danger.** When the client hires you in response to a specific threat, you face a known danger (that means that you know the danger exists—not necessarily that you know what it is). Known danger assignments require the greatest degree of vigilance and have the most

Techniques 47: Scroll to the Road

Use this faster danger area technique when moving in small groups, when speed is important, and when the chance of enemy contact is not that high.

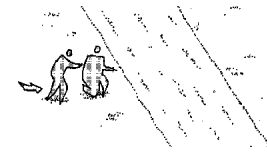
Step 1

When you identify the danger area, halt your formation a few dozen meters away. Send one person up for near-side security. Staying under cover, he puts his left shoulder to the danger area, facing to the right.



Step 2

The next closest person in the formation moves up. He takes over the near-side security, and the first person prepares to move across the danger area, carefully scanning the entire area. It's a good idea to always tap the person on the shoulder to let him or her know that you are ready to take over.



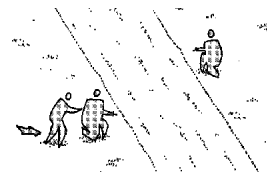
Step 3

The first person crosses the area, and takes up a concealed position on the other side. Again, he puts his left shoulder to the danger area, so that he now faces the other direction. The near- and far-side security elements face opposite directions, completely covering the danger area.



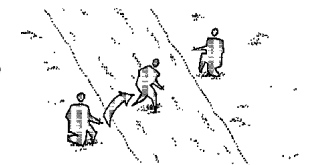
Step 4

The third person in the formation now moves up and takes over near-side security.



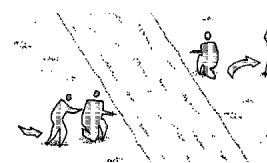
Step 5

The second person crosses and takes over far-side security from the first person.



Step 6

The first person moves out to provide a secure area for the formation to re-form. Meanwhile, a fourth person takes over near-side security, and the third man crosses and takes over far-side. This process continues until everyone is across. ♦



impact on the principal's activities. They are usually short-term and stressful.

Because known danger assignments are the most difficult, and the type of assignment you're most likely to come across (few clients can afford a BlackEagle cell for a long-term buffer job), that's the type that will be focussed on here.

The Rules of Bodyguarding

The tactics of bodyguarding are unlike those of anything else we do. Personal security is an essentially defense-oriented task, and the temptation is often strong to go after a perceived threat. There are times when that is appropriate, but you must always keep your objective in mind. It's not your job to catch terrorists, kidnapers, or mob hit-men. It's just your job to keep them away from your principal. Have the judgement to know when the best defense is a strong offense, and when it isn't. Follow these rules:

1. Never leave the principal. You must stay close to your man. That means within a few feet while in public. Depending on the threat level, you may want to stay that close in private, or it may be fine to stay one or two rooms away.

2. Control the environment. Never let your principal go somewhere you haven't checked. Sweep rooms before the principal arrives, if possible. Always enter a room first and give it a quick look-over before you let the principal in. That includes bathrooms. Maintain a perimeter if you are working as a group, and keep that perimeter secure.

3. Know the routine and the people. Learn your principal's life—his or her routine, habits, and interests, friends, relatives, and business associates. That way, you can more easily identify something out of place while carrying out your task as non-intrusively as possible.

4. Plan for the worst-case scenario. That means looking for tails, bugs, and other signs of a long-term plan against your principal, as well as recognizing the tactical dangers in every room or public area you enter as a matter of routine. You'll be prepared for anything, and your vigilance will discourage potential attackers.

5. Remain unpredictable. Make an attacker's job as difficult as possible by not giving him a routine to exploit.

6. Take command. The client has hired you to protect the principal. Do it, and don't take any guff. You must accommodate the principal's activities and lifestyles, but don't let him or her tell you how to do your job. If he or she will have to make compromises in the face of a real threat, don't make any bones about it.

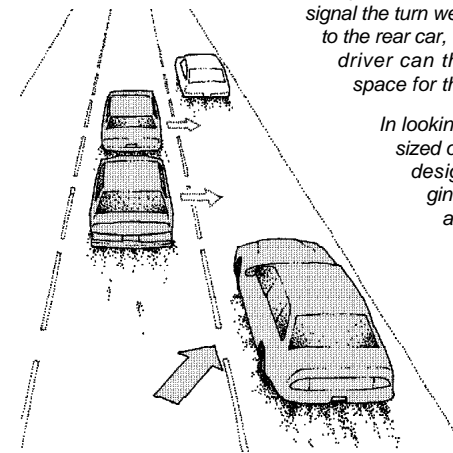
Techniques 48: Personal Security on the Road

Evasive driving like you see in the movies is a last-resort measure—if the situation is that severe, an accident becomes as much a threat to your principal's life as the assailant's attack. But good defensive driving skills can prevent such chases from becoming necessary.

You can use one or more vehicles to move your principal. One vehicle is often more convenient, and sufficient for light-security duties. The wrangler can even double as a chauffeur, although two people are recommended so that the wrangler can keep his attention focused without worrying about traffic.

If you are using two cars, put the runner and perimeter people in the lead car, where they can run interference and disembark first to secure the destination area. If you have a third car, load it with perimeter people. In case of attack, it will be their job to stall the assailants as the first two cars get away.

With a clear view of the road ahead, the runner is responsible for making the convoy's tactical decisions. Keep close together, so that another car cannot get between you, and drive a little faster than the ambient traffic speed—that forces anyone tailing you to do the same, which will make them stand out. It is the lead driver's responsibility to keep traffic and streetlights from splitting up the convoy.



When maneuvering in traffic, the lead driver has the responsibility of deciding when and where to move. Use this technique: When approaching a corner or off-ramp, signal the turn well in advance. Pass the signal back to the rear car, which actually moves first. The rear driver can then hold the lane open, making space for the other cars to move over in turn.

In looking for transportation, go with a mid-sized or larger four-door in an unobtrusive design and color. Get the biggest engine available for the model. You want auto-lock doors controllable from the driver's seat, and a big enough rear floor area to hide or protect the principal if necessary. If you have the budget, get the factory locks changed for something better, have an alarm system and self-sealing tires installed, and store the vehicle in a locked, alarmed garage. ♦

These six points encompass your objective as a bodyguard. Follow them, and you can't go too far wrong.

Personal Security Tactics

There are two ways you can operate when protecting an individual: solo or as a team. Both have advantages and disadvantages. In general, solo protection is better suited to long-term, relatively low-threat assignments. One or two people stay with the principal, while the other cell members rest or carry out counter-threat investigations or operations. You can trade off duties, ensuring that the "wrangler" (the person with the principal) faces reasonable shifts and is well rested. Team security is manpower-intensive, better suited for short-term jobs, but necessary in high-threat cases.

When running a job solo, the basic tactics are covered in the six points above. Stay with the principal and keep your eyes open. Examine every room, every face, and every object, asking yourself whether or not it is unusual or doesn't belong. If the answer is yes, keep track of it. Every time you enter a new room or situation, map out a rough escape plan in your head. Keep at least one other member of your cell on standby, within easy communication.

Team tactics are a bit more complex. It does little good to have more than one wrangler, but a well-coordinated team can add a lot to your security. Organize your cell into three components—a wrangler, a runner, and two or more perimeter people. The wrangler will have tactical control in an incident, so you may want the cell leader to take that post. The perimeter people will be tasked with defining and maintaining your secure area, under the runner's direction. The runner will also be the link between the perimeter and the wrangler. And the wrangler will, as in a solo job, always stay with the principal.

When stationary, cover the immediate area with your perimeter people. Put them where they can control the environment physically, and restrict access to the principal. If you're in a public area where that can't be done, put them where they can observe as much as possible, but not so far away that they can't protect the principal in an attack. Put the runner someplace where he can carry out his job—coordinating the perimeter and keeping the wrangler up to date. The wrangler needs to keep his attention close to the principal, and may not be able to see the big picture without the runner's help. Put together an impromptu escape plan for every new situation ("if we get hit, head out the back door to the car"), and make sure everyone knows it.

On the move, you don't need many people with the principal. With the wrangler close, the runner and perimeter people can move ahead to secure the destination. Don't waste time, however. If the destination will

Techniques 49: The Hostile Meeting

Not all meetings occur in the comfort of the home office—meetings with criminals, suspects, hostage takers, and sometimes even suspicious clients are generally on neutral or unknown turf. Such meetings can be uneasy or downright dangerous. There are ways, however, to maximize security in arranging such meetings, and to give the cell the upper hand should things go wrong.

For starters, insist on an agreeable site—if you can't choose the location yourself, at least demand a site that doesn't work against you. A public location (if your business can be handled in public) will probably keep the proceedings civil—only the craziest of criminals will pull a gun in a busy restaurant, for example. Public sites that have built-in security can provide protection and a sense of security for both sides—for example, both parties can be relatively certain that the opposition is unarmed if you meet in an airport gate waiting area.

If possible, recon the site ahead of time—far enough ahead of time that you won't run into the opposition doing the same thing. Check out the site for cover, all routes in and out, and places where you can position an overwatch or security element—or where the opposition might position theirs.

Never go to such a meeting without notifying the office—or a friend or family member, at least—of where you are going and when you expect to be done. Never go alone—always have other members of your cell follow, or pre-position them where they can overwatch the meeting. Establish an innocuous signal—such as scratching your head in a certain way—that will warn the overwatch element of trouble or have them take action. If you think the opposition is organized enough to have an overwatch element of its own, you may want to decide ahead of time whether you want your overwatch element to watch for and suppress theirs, or ignore it and focus on events at the meeting.

All of these preparations will be moot if the meeting arrangements are a bait-and-switch—if, when you arrive, the opposition insists on moving directly to another location (possibly forcing you to travel with them in their car). Whether or not you should go along with such a situation is your call, but keep in mind that it is tantamount to giving yourself to the opposition as a hostage. Decide beforehand if you want your overwatch element to follow you to the new site (your adversary will probably be prepared to observe any following vehicles) or lose contact with you.

If you have the upper hand—if you're in a position to call the shots—you can of course pull the bait-and-switch on your adversary, forcing him to travel with you to a site which he's unprepared for. That'll put you in control over the meeting's security, but your opponent won't go along with it unless you have the leverage to demand it. ♦

only take a few minutes to sweep and secure, stay near the principal until the last moment.

If an attack occurs, remember your priorities. You may want some of your perimeter people to stage a delaying action, if it looks like the attackers might pursue, but the wrangler should never engage the attackers when fleeing is an option. Get the principal out of trouble. You should always have some sort of escape plan in mind, and the wrangler should act accordingly, immediately and without hesitation, if an incident occurs. Everyone else covers the escape, withdrawing after the principal and wrangler. If for some reason the wrangler doesn't follow the plan, everyone else must follow his or her lead.

One more thing worth mentioning: the "taking a bullet" principle. The most professional of bodyguards won't hesitate to put themselves between their principals and an assailant's weapon. That isn't sheer pigheaded loyalty—it's actually smart security work. An assailant is after the principal, and has no interest in killing the bodyguard. He's looking for a clear shot at his target, and he won't pull the trigger if there are people in the way. Make no mistake—getting shot is a real risk in serious personal security work. But putting yourself between your principal and a gun is more likely to prevent a shot from being fired in the first place than it is to result in you taking a bullet for the principal.

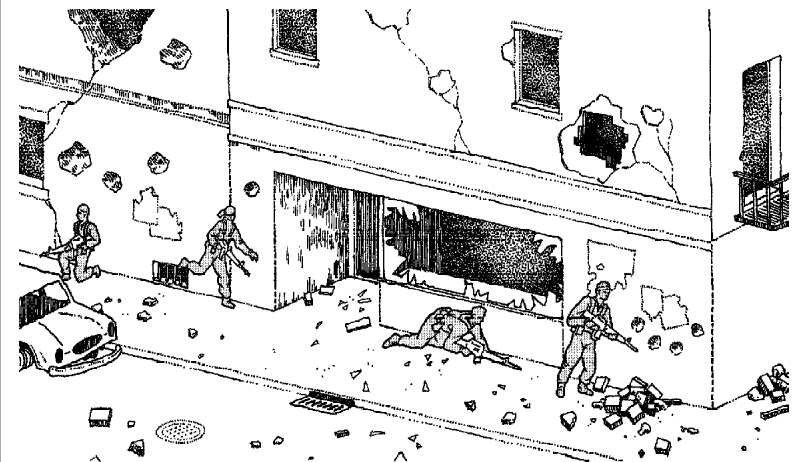
Urban Problems

Tactical problems can be divided up into three basic categories, based on the settings in which they occur: on the street, in the wilderness, or inside buildings and structures. Each of these types of terrain presents a different set of problems, and lends itself to a different set of solutions, even though the basic tactical premises discussed above hold true for them all. For the purposes of this manual, we have divided the discussion along those lines, into this and the following two sections.

Urban terrain is one of the most difficult in which to conduct successful operations, and yet it is the one in which BlackEagle operatives most often find themselves. Urban terrain gives every advantage to the defender, and in conventional warfare is far and away the most casualty-intensive setting for combat. All operatives, and especially cell leaders, should take every chance hone their urban tactical skills.

Techniques 50: Urban Movement Hazards

This illustration shows a small cell moving through very tough urban terrain. Notice a few of the hazards present: windows, doors, and holes in walls, grates, manholes, and basement openings, wrecked vehicles, debris, alleys and blind corners, and fire escapes. This limited list of tactical hazards illustrates the need for attention while operating in an urban environment: the enemy can surprise you at almost any time, often from just a meter or two away.



How do you cope with that? Be careful and organized. The cell above is moving in a file along the side of the street. That minimizes (but does not eliminate) threats from their side of the street—an attacker will have to lean well out of an opening, exposing himself, to draw a bead on them. Their spacing keeps them operating as a cohesive unit, but does not make them a target for a single burst of gunfire. Finally, they have split up security duties. The front man watches ahead, the second man (although occupied at the moment) watches high, the third man watches the flanks, and the last man keeps an eye on the rear. With each person knowing his or her duty, each can pay close attention to his task, and the cell is well-protected.

Notice how these operatives respond to the threats around them. The third man has just hopped over a basement opening, while the second crawls under a window. When he gets out from under it, he'll cover the open doorway while the third man dashes past it. The first man has paused before a pile of rubble—an ideal place for a booby-trap, he will step over or around it. While in other terrain types you generally want to position the cell leader towards the middle of the formation, in terrain like this he or she should be at the front—this cell is about to come to a corner, and the leader will have to make a decision about how to proceed. If he or she isn't in the lead, the cell will have to shuffle around in order for the leader to see what's going on. ♦

Movement in the Urban Environment

Because of the advantages urban terrain gives to static or defending units (and this includes gang-bangers holed up in gig houses as well as organized military units), a cell on the move needs to take special care. Urban terrain gives the adversary a million places to hide—some of which, like rooftops, have no equivalent in other terrain types. Furthermore, buildings give the adversary the ability to maneuver very close to you without your knowing it.

The basics of street maneuvering are the same as those in the field: keep yourself concealed, minimize the adversary's ability to get a good shot at you, and be able to react effectively to hostile contact. Here are some specifics:

- **Keep your back to the wall.** When moving along a street or alley, keep your entire unit along one side, moving in a file along the wall. If you stay in the middle you are vulnerable to fire from both sides, and if you split up one or both elements can be pinned down, unable to help the other or maneuver effectively. But don't assume that your back is safe, just because there's a wall behind it. Rooftops, windows, doors and loopholes are all a threat, even on your side of the street.

- **Keep your eyes open.** As with any type of tactical operation you must assign sectors of security, so that nobody has to watch everything and every angle is being covered. Generally, you want your first man to keep his eyes forward, while the second watches windows and rooftops above, the third looks out into the street, and the last watches the rear. If you've got more than the four personnel in that list, have the additional people watch the hazards above.

- **Always go low.** Look around the end of a wall—not over the top. When you get to the corner of a building, get down on your stomach, ease to the corner, and peer around with your head just inches above the ground. If you have to go over a wall, shimmy over it, keeping your body as flat as possible. The same technique can be used in going through windows.

- **Know where you are going.** Plan your route from cover to cover, several steps ahead. Never move unless you know exactly where you are going. Screen movement across open areas with smoke grenades if you are under hostile eyes.

Urban Tactical Hazards

A list of urban hazards could go on page after page, but just a few are listed here.

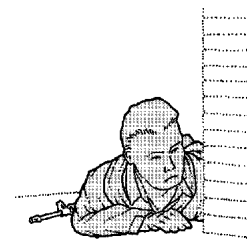
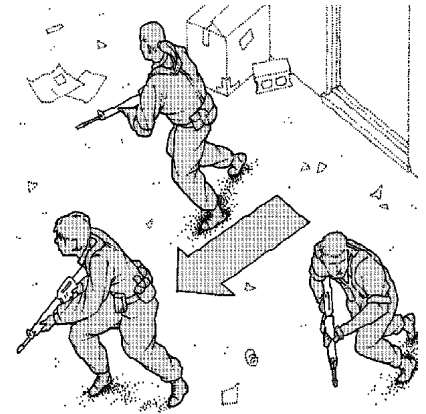
- **Windows, loopholes, and holes in buildings** give hostile elements the ability to shoot at you while almost totally covered and

Techniques 51: Urban Movement Techniques

The cell in the previous sidebar is shown moving in the open. Presumably, they're making their way between one area of cover and the next. That's a cardinal rule of movement in a hostile urban environment: always move from cover to cover. Pick a covered position ahead and move to it, then pause and plan your next move—never simply wander in the open, as you might out in the field.

Cover and concealment are critical in the urban environment. If you don't have it, make it: mask your movement with smoke grenades if you come under fire or get caught out in the open. Don't forget that your opposition has the same advantages, though—if you're forced to dash for cover, be careful. You never know what's inside a building until you get there yourself. The enemy may even use a burst of fire to herd you towards a specific building, in which an ambush is lying. Don't stay in the open if you're being shot at, but be careful about cover that isn't secure.

Treat large open areas in urban terrain like normal danger areas—use the techniques for crossing such areas as described earlier in this chapter. But for small areas, like alleyways, bunch up into a tight formation and cross all at once. This rapid crossing method makes detection much less likely than the slower techniques used in other terrain types.



When you get to a corner, don't look around at head level. Get down on your belly and ease up to the corner, exposing no more of yourself than you have to. Keep your weapon handy, but back where it won't be seen. ♦

concealed. A clever sniper will stay well inside the building, away from his window or loophole, so you won't see his muzzle flash or weapon sticking out. This can lead to some confusion as to the source of incoming fire. If your opposition is in a prepared military defense, buildings that are occupied may have grenade screens in the windows—check, or you may be surprised when your live grenade bounces back into your lap.

- **Rooftops** offer visibility and control over the streets below. In cities, especially low- and mid-rise areas, movement from rooftop to rooftop may be possible, making it difficult to trap an adversary.

- **Doors** are an obvious point of entry and exit. Cover them, and expect them to be covered. Find some other way in or out if you are in a firefight.

- **Rubble and debris** gives the adversary convenient cover and an excellent place for booby-traps. It also makes stealthy movement difficult. Piles of rubble are not restricted to war-torn city shells in high-intensity conflicts. Demolished and dilapidated buildings are common in Third World cities and American urban centers. Even construction sites in upscale neighborhoods can give you trouble with debris.

- **Sewers, storm drains, and culverts** provide instant bunkers and, in some cases, undetectable mobility. Watch for fire from open manholes, gutter drains, and other small openings at low level. Be careful entering manholes and culverts, as they are easily booby-trapped.

- **Abandoned vehicles** are easy to ignore, but make excellent hiding places and mini-bunkers. Keep your eye on them, and check them out when you get close.

Clearing a Zone

Whenever a force wants to dislodge an enemy from an urban area, it begins by segmenting the area into specific zones, then clearing them one-by-one while maintaining the security of the already-cleared zones. This type of fighting is slow and casualty-intensive, but it is the only way to clear a hostile force from an easily-defended town or city. Heavy block-by-block fighting in urban terrain is a job for a regular military unit, and is almost always too much for a BlackEagle cell. Sometimes, however, BlackEagle personnel are called on to assist in clearing specific zones, especially in cases of riot, gang and terrorist activities, or low-intensity combat.

Zone clearing is hard work, and almost always requires the cell to operate in conjunction with a larger force—be it local police, a military or mercenary unit, or additional cells. In order to effectively keep a zone clear, you must have the security of a larger force at your rear to prevent any hostiles that you dislodge from simply infiltrating back behind you. As an attacking force in an urban environment, you are at a clear disadvan-

Techniques 52: Diversions

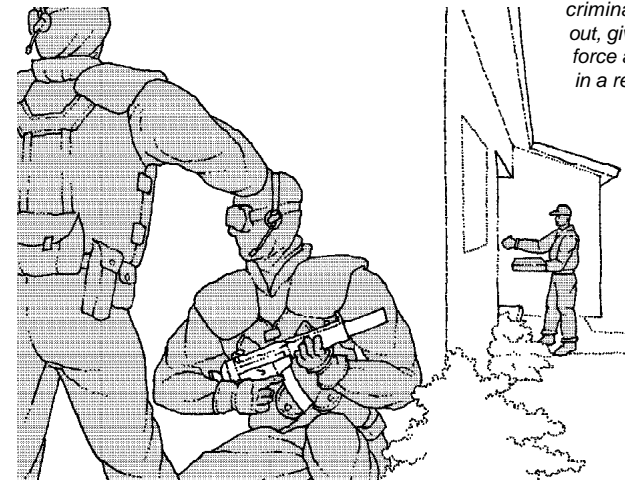
Many of the tactical problems discussed in this manual can be augmented by the careful use of diversion. Diversions distract an adversary, screening your intent and causing him to misappropriate resources. You can use a diversion to make an adversary weaken his defenses in key areas, maneuver into a trap or ambush, or open up a lane of movement for you.

There are pros and cons to using diversions. A diversion may ruin the element of surprise, or put the adversary in a heightened state of alertness. It may not have the effect you desire, or may simply not work at all. A diversion requires some of your personnel and firepower that may be needed elsewhere, and it may put those resources at risk.

Nevertheless, diversion is an important tactical tool. If you think that a diversion might help you, consider the following: First, what effect do you intend? In what other ways might the adversary react? What will you do if the diversion doesn't have the desired effect? Next, consider your resources. Can you spare the necessary personnel? Will they be at too great a risk? How will they disengage from the diversion, and how will you link up with them after? Finally, when you have a good idea of how you will use your diversion, compare your plan with a non-diversionary one. Does the diversion really offer that big an advantage, as compared to the risks involved?

Once your diversionary plan passes those tests, figure out how you will implement it. A diversion should captivate, or at least split, the adversary's attention. That may mean something big and dramatic, especially in a firefight. Pyrotechnics and gunfire work well, but they must be used in a convincing attack or a clever adversary will see through it. On the other hand, if a firefight has not begun, you may want to go with something more subtle, especially to maintain the element of surprise. A simple knock on the door may

divert the attention of criminals in their hide-out, giving your assault force a moment to slip in a rear window. ♦



tage. Your goal, then, should not be to assault the adversary, but to dislodge him and force him out of the zone, or at least into a less advantageous defensive position.

Your zone should be delineated by easily-controlled open areas like major roads or parks, and should be small—certainly no bigger than a city block. In smaller towns, Third World cities, cities built on rugged terrain, or urban areas hard-hit by heavy combat, such delineations can be hard to make as there won't be many wide, straight streets. In any event, do your best to find clear boundaries for the zone, and position elements from your backup force to cover as much of the side lanes as possible.

You will have to clear buildings one by one. Start with the dominant building—the one that overlooks all of those around it—unless it requires you to cross too much terrain to get to it. Ideally, you want to get to the roof. Leave one or two people on security and work your way down through the building, clearing it room by room. Make liberal use of grenades and automatic fire, before you see the adversary (keep in mind that fragments easily penetrate flimsy interior walls). Don't move in a predictable pattern of rooms, and, if possible, blast or pound your way through interior walls rather than moving through easily-defended and booby-trapped corridors. Be thorough, making sure you cover every room.

When the building is clear, move back to the roof and climb over to the next one. Or, blast a hole through an adjoining wall in an upper floor. If you can't get to or maneuver on the roofs, you can work from the ground up, but that's a little more hazardous.

Storming a Building

Having to dislodge a hostile force from an occupied building is one of the most dangerous actions a BlackEagle cell can undertake, although careful planning and execution can reduce the risks greatly. As with all tactical tasks, the key is stealth and surprise. Even if the adversary knows you are out there and ready to come in after him (as is typical in hostage situations), you can still use surprise to your advantage.

How you handle the action depends on whether or not the adversary knows you are coming. If not, you want to do everything possible to avoid alerting him. Even if he does know you are there, and you have a standoff, you want to remain as low-key as possible. The following instructions assume that the adversary knows you are coming, but there are variant steps below, in case you have the advantage of complete surprise.

Throughout your preparations, build towards the element of surprise by never letting the enemy size you up. Pinned down in a building, the adversary is at a distinct disadvantage. Increase it by not letting him know which sector to defend. Don't do it like the movies, with a ring of assault-rifle-wielding men encircling the building from twenty meters out.

Techniques 53: Dealing with Hostage Situations

Hostages can be taken by criminals or terrorists, and this differentiation is critical. Criminals generally take hostages more-or-less by mistake—they are caught at the scene of a crime, and grab a bystander in an attempt to force authorities to let them go. Terrorists take hostages by design, to use them as leverage against specific goals (actual demands or public attention). Due to the scope and implications of their acts, negotiations with such terrorists are almost always best handled by governmental authorities, and aren't covered here. On the other hand, BlackEagle operatives on assignment might easily run into opponents who take impromptu hostages as acts of desperation or for bargaining chips, and find themselves having to respond to or bargain with such hostage-takers.

A hostage in your opponent's hand forces you to stop and negotiate. It doesn't, however, give that opponent any negotiating advantages—and certainly no tactical ones. The first thing to consider when faced with such hostage takers is their situation. The penalties for kidnapping or murder are stiff—how do they compare with the consequences for giving up? If giving up is clearly a better option, a cornered hostage-taker can usually be talked into it, especially if there's a sufficient show of force to convince him or her that escape simply isn't an option. A more desperate hostage-taker—one who has already killed several people, for instance—may not see surrender as a more attractive option. Find a way to make it attractive.

The second consideration is the hostage—or rather, the number of hostages. With multiple hostages, a criminal may feel that he or she can kill or hurt one or two, as proof of resolve. That option does not exist if the hostage-taker has only one victim, a single bargaining chip that must be conserved. Sometimes a hostage-taker can be convinced to give up some of his or her victims, especially women, children, the elderly, or the wounded. Use every ploy you can think of to reduce the number of hostages, getting it down to one if at all possible.

Finally, keep this in mind: sane or insane, rational or irrational, a criminal who has taken a single hostage is very unlikely to kill that hostage if any other option exists. Sane criminals know that they gain nothing—and lose their only bargaining chip—if they do; suicidally-inclined criminals are more likely to use their last act to kill themselves—or take a shot at you—than to kill a hostage that means nothing to them. With that in mind, be firm in negotiations with such hostage-takers—never make a concession unless you get something for it. And don't make the mistake that we see all the time in the movies: never, ever, give up your weapon because of a criminal's threat to kill a hostage—you gain nothing, and end up in the same situation with even less leverage than you started with.

Most hostage situations are settled by negotiation, but sometimes action is required. Throughout the negotiation process, make every preparation for tactical action. But only act if one of three conditions occurs: the hostages appear to be in grave, immediate danger; negotiations have broken down; or an excellent opportunity (such as the hostage getting free) arises. ♦

Instead, keep your forces under cover and hidden. Keep all movements concealed.

1. Clear the area. Get as many innocents and uninvolved people as possible out of range of the inevitable gunfire. This is not just a civic duty—civilians running around will create chaos, hinder your actions, and give the enemy potential hostages.

2. Isolate the enemy. Deny him communications and anything else that might work to his advantage. Cut his power, cable, and phone and data lines right away, to hinder his defense preparations. Then, even if you are ready, wait a while before making your move—he'll be on guard after you cut the lines.

3. Gather intelligence. Figure out what you're up against. Get building plans. Determine how many bad guys are in there, how many hostages, and where they all are. Learn all of the entrances, and try to guess where bolt-holes or escape routes are located.

4. Plan your assault. Cover all entrances and possible escape routes with snipers or support elements. Look to enter the building by unexpected routes—rear or upper-floor windows, basements, openings blasted through from an adjoining office, apartment or townhouse, or from the exterior if no adjoining building exists (make sure you know where the hole will lead, and that you aren't taking down a structural wall). Plan to move in with two or more assault elements, if possible, attacking from different parts of the building. Make sure each element knows its lane, and which rooms it is responsible for—you don't want to shoot each other.

5. Move in. Stagger your assaults by five or ten seconds. This will give the enemy just enough time to fix his attention on the first assault before being hit from behind by the second. Immediately proceed the assault with a flash-bang grenade or CS gas (be sure to protect yourself from the effects of these devices). Move quickly through your lanes. As you clear each room, report the number of hostiles and hostages seen and killed, and the direction taken by any that fled. Don't hesitate—the force and momentum of your assault should prevent the adversary from regrouping or even reacting.

6. Mop up. Re-secure all rooms and search the building for bolt-holes or stray hostiles. Outprocess hostages to make certain the adversary doesn't slip out among them.

If the adversary doesn't know you are moving in, handle things a little differently. Follow the above steps, but in a slightly different order.

1. Gather intelligence, as described above.

2. Plan your assault, using the same tactics discussed above. One difference will be that you may want to start the assault with a distraction, like having a someone disguised as a delivery person knock on the front door. This is a risky move, but will draw hostile attention away from the assault points.

Techniques 54: Searching Prisoners and Bodies

It's easy to think that the fight is over when an operative cell has met its tactical objectives and all hostiles have been driven off or captured. But for an injured or captured opponent, especially a criminal, terrorist, or fanatical guerilla, the fight is never over—and the searching and handling of such personnel can be as dangerous as combat against them if you aren't careful.

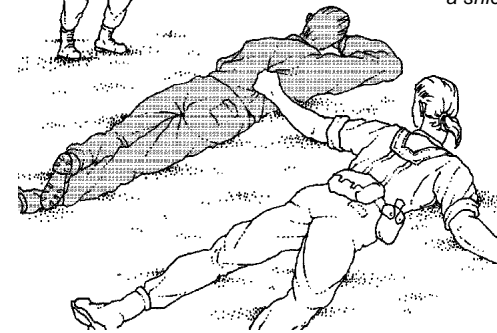
In handling prisoners the key is to keep them in positions from which it is impossible to make quick or dangerous moves, and from which they can be easily observed and covered by one or two operatives. There are many such positions, but the best is to have the prisoner lean against a wall at a 45° angle, with both hands and feet spread wide. From such a position sudden moves are difficult, and the prisoner will not be able to easily observe his captors. While one operative searches this prisoner, a second operative covers from a few paces away. The covering operative should hold onto the searching operative's weapons, to keep them out of reach of the prisoner; when moving about the searching operative should always loop behind the covering operative, so as to never block his line of sight and fire on the prisoner.

Keep prisoners waiting to be searched kneeling or laying face-down on the ground, with hands behind their heads and ankles crossed. Face kneeling prisoners away from you, where their hands and ankles can be easily watched and they cannot observe their captors' activities. Stagger their positions so that all are easily seen and none block line of fire or sight to the others.

Bodies can be just as dangerous as captured prisoners, in part because a corpse may in fact be a live hostile playing dead, and in part because real bodies are often booby-trapped by withdrawing combatants. Thus, in searching a body, it's most important to keep it well-covered until it is clearly established as dead, and to move the body in a careful manner to minimize the threat of booby traps.



A face-down body is a particular challenge, as it must be rolled over to be thoroughly searched (and even to confirm that it is, in fact, dead). Safely rolling a body requires two people. One lays down beside the body and gently rolls it over, keeping it facing away from himself and using the body as a shield against any booby-traps that might be set beneath the corpse.



The second operative covers the body from a short distance away, from which he can see beneath the body as it rolls up. He'll be in a position to spot any booby-trap or suspicious movement in time to warn the other person or shoot the hostile. ♦

3. Clear the area. Quietly removing civilians from the building and its surroundings will be a difficult and delicate process, and you will want the help of local authorities if the nature of your assignment allows it. Be as discrete as possible, to avoid alerting the enemy, but be aware that civilians will not always cooperate, and the situation can blow open at any moment.

4. Move in. Cut power and other lines just as you make the assault, to maximize enemy confusion. Otherwise, carry out the assault exactly as described above.

5. Mop up, as above.

Fighting in either of these scenarios will be intense and brutal. Every member of the assault team should be well armed and armored. Make certain you have excellent comms, and that everyone uses it. It's generally fairly easy to avoid hitting hostages—innocents react rather differently than hostiles when you burst into the room—but your cellmates can be easily mistaken for hostiles. The section on [Clearing a Room](#), below, talks in more detail about actions within the building.

Suppressing a Sniper

Dealing with a sniper in an urban situation is very different from dealing with one in the woods. In a combat situation, where the enemy is well-trained in military tactics, your chances of eliminating a careful sniper are pretty low. However, in riots, insurgencies, and criminal activities, snipers are not generally so well-trained or mobile.

A civilian or criminal sniper will almost always act from high ground, giving him a wide field of view and range of targets (this is generally not true for a military sniper, who will look for a well-concealed, inobvious position from which he can easily escape). This will make approaching him difficult, but it has disadvantages as well.

In dealing with a sniper, you want to surround and isolate him, deny him any targets, and then move in on his position. Follow these steps:

1. Clear and surround the area. As in any other urban operation, you must get civilians out of the way so that you can act unhindered. While doing that, set up a cordon to prevent the sniper from slipping out of the area. Remain low-key—don't give the sniper any intelligence on your size or movements.

2. Set up counter-snipers. Chances are, the sniper will be well-emplaced, in the most controlling terrain in the area. Covering his position will be difficult. Set up two or three counter-snipers anyway, so that if he gives you the opportunity you can take him out.

3. Move in. If your counter-snipers don't do the trick, move in on his position. Try to infiltrate the area on a blind side, getting into his or a

Techniques 55: Trauma in Combat

Every BlackEagle cell should have a qualified medic, or at least someone who's emergency medicine skills are strong enough to deal with the immediate priorities of combat trauma. But that cell member won't always be available when an operative goes down—he or she might even be the casualty. For that reason, every operative should know how to handle casualties in the field—if not first aid, then at least the tactical priorities that will help keep a casualty alive for a few moments and keep everyone else from becoming casualties as well.

Follow these five steps when one of your cell members is wounded in an ongoing tactical confrontation:

1. Assess the situation. Before doing anything—before even approaching the victim—assess your tactical situation. If combat is heavy and ongoing, you must continue to press the opposition—you cannot divert your momentum over a casualty, no matter how much noise he or she is making or how close you are personally. Chances are, even with the worst injuries, if your casualty is alive he will survive another few seconds without aid. If you do give up your momentum and lose the fight as a result, your casualty will die anyway—perhaps along with the rest of the cell.

2. Approach the casualty. If you're in tactical control and can get to the casualty, do so. Assess his status quickly. If you're under fire, move yourself and the casualty to safety immediately, regardless of how badly wounded he is. Otherwise, wait until after dealing with the four Bs (the next step), or until your medic says it's OK before moving.

3. The "Four Bs." Now you're ready to actually address your casualty's condition. Keep your head about you and deal with the four Bs: Breathing, Bleeding, Broken bones, and Burns. Even if you have little medical training, addressing these four major points (in order) can make the difference between life and death for your casualty.

4. Treat wounds. Having addressed the four major points that can kill your casualty outright, you can begin to actually treat his or her wounds in detail, or move him or her to an aid station or trauma center. If you are in the field, you may need to sedate your casualty; in either event, work to reassure him or her.

5. Distribute mission-critical equipment. Finally, regardless of what you do with your casualty, be sure to take any special equipment (including extra ammo) that he was carrying which you will need to complete your assignment.

Once you've addressed these five steps, you can then assess your situation: whether you can continue with your assignment as planned, make changes to your tactical plan, or withdraw. ♦

neighboring building. Then assault his position in the same way you would storm a building (covered above).

Obviously, these instructions simplify the task and don't consider the sniper's mobility, the possibility that he is barricaded in an inaccessible structure (like a tower), or that he is protected by a security force. You must tailor your plan of action to the circumstances on the scene, using these three steps as a framework.

Interior Problems

Interior actions are often just an extension of urban actions. But because of the specialized nature of our work, which often calls for tactical actions largely or entirely indoors, this section is dedicated solely to indoor tactics.

Moving Indoors

How you move indoors depends on your conditions and objectives. In all-out combat, the ideal tactic is to blast your way through buildings, making your own doors to avoid booby-traps and ambushes and to keep the adversary on the defensive. But in a "civilized" environment, like an office or apartment building—or any situation where stealth is preferred—that's not an option.

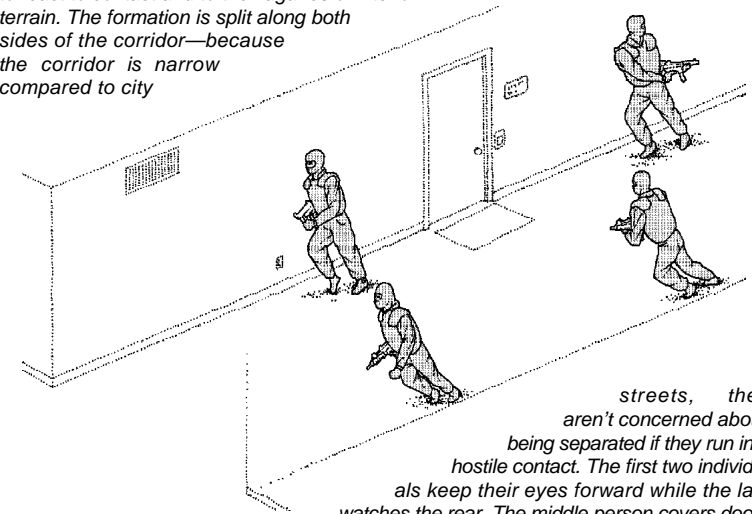
Indoor movement during all-out combat is covered pretty well above, so this section will stick to the more "civilized" setting. However, just because the environment may be a clean corridor instead of a shelled ruin, the goals of tactical movement still hold: to avoid detection, to mitigate attack, and to prepare to react to contact. Here are some specific tips for moving indoors:

- **Know the terrain.** Buildings have limited numbers of exits, and they restrict movement inside, so it is more important to know the terrain here than in any other environment. Your opponent will probably know the layout—if you don't, you're at a distinct disadvantage. Look at the layout of corridors and suites, the locations of elevator shafts, service ducts, stairwells and fire doors. Don't restrict your thinking to two-dimensions—look for crawl spaces, catwalks and gantries, wiring vaults and ducts, and maintenance areas that run vertically or between floors.
- **Know the security.** Know what you will likely face in terms of physical security and personnel. Be prepared to circumvent or bypass it.
- **Find some other way in.** Security precautions are generally focused on entrances. Enter the building by some unexpected route—

Techniques 56: Interior Movement Hazards

When infiltrating or assaulting buildings, you want to avoid movement in corridors and other open, public passageways as much as possible. Move from room to room by connecting doorways, false ceilings, and other less-surveilled and trafficked routes whenever practical.

Of course, it isn't always practical. When you must move in the open—when time does not allow a more circuitous route, or there simply is no other route and you cannot make your own, smart movement can maintain your cover and keep you alive. The cell shown here is moving carefully down a corridor during an infiltration (a situation in which they do not expect a hostile response). Their formation gives them good security and allows them to react to contact and to the vagaries of interior terrain. The formation is split along both sides of the corridor—because the corridor is narrow compared to city



streets, they aren't concerned about being separated if they run into hostile contact. The first two individuals keep their eyes forward while the last watches the rear. The middle person covers doors and other hazards as the formation passes them. The formation is moving quickly, at a quiet jog, to minimize the amount of time spent in the open, vulnerable hallway.

This sort of formation is well-suited for covert infiltrations, in which rapid movement and sharp eyes are priorities, but hostile contact is not expected without warning. If an armed threat is more likely—and especially when making assaults—it's often better to bunch your cell together, putting the leader at the head of the formation with each cell member lined up behind. That presents the minimum possible target area to an enemy confronting your cell from the front. Of course, each cell member still maintains the same sectors of security.

It may not look like there is much going on in these illustrations, but every visible object represents a hazard. Hostiles may be around the corner or behind the door—they'll appear at very short range when they do turn up. Vents, electrical sockets, and floor mats might each contain surveillance or alarm devices. Every cell member must remain on his or her toes at all times—even more so than in any other tactical terrain. ♦

ventilation gratings, the roof, an upper-floor window, or through an adjoining wall. Don't expect these to be unsecure, however—just less secure.

- **Avoid corridors.** Use interior connecting doors as much as possible. Climb over partitions. Sometimes you can get over a wall by going through the crawl space between the hung ceiling and structural ceiling above, although structural walls and security barriers will go all the way up through the crawl space. Use maintenance passageways, air spaces, and service accessways instead of major corridors whenever possible.

- **Be small and agile.** You don't need crew-served weapons indoors. In fact, pistols and submachineguns generally provide all the firepower you need at interior ranges. Small weapons won't give you trouble in doorways, elevator shafts, and other restricted spaces. Go light on gear, as well, and wear soft-soled shoes.

Interior Tactical Hazards

The nature of tactical hazards indoors varies greatly with conditions. You might expect booby-traps, for example, in an abandoned house in war-torn Central America—but not in the lobby of a gleaming corporate center. What you will run into are hidden security and surveillance devices and a completely different set of tactical hazards than any found elsewhere. What sets these hazards apart is their proximity—indoor actions take place at very close ranges. Here are a few things to look out for.

- **Corridors, lobbies and doorways** funnel your movement through predictable areas. They are primo spots for security devices like IR beams, pressure-sensitive mats, motion and heat detectors, audio sensors and cameras. They are also good for ambushes. You can rarely avoid these areas altogether, but check them out, and be very careful moving into or through them. Treat lobbies and large entranceways as danger areas.

- **Walls and ceilings** may or may not be solid. Hung ceilings and drywall partitions are particularly flimsy. That means they can be breached—by you or the adversary. Always think in three dimensions, and never assume you're safe just because you've got your back to the wall. Remember, an assault team will try to come in by an unexpected direction.

- **Balconies, catwalks, and gentries** create a three-dimensional tactical environment. Any time you move into an area with a large overhead space, be aware of what's above—how it can be used against you, and how you can use it to your advantage.

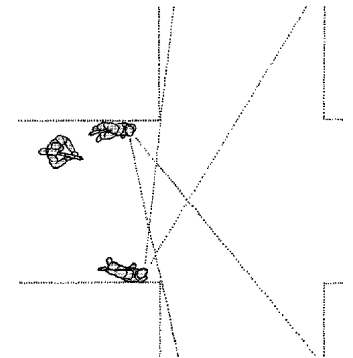
- **Stairwells** can be particularly treacherous. They are excellent locations for audio and visual surveillance, and they offer little cover. Fire

Techniques 57: Interior Movement Techniques

The principals of interior movement are similar to those of urban terrain: move point to point, planning each movement ahead of time before breaking from cover; maintain vigilance against attacks that may come from point-blank range; and keep relatively close together in open areas. But there are special considerations to interior tactical movement as well. The movement of your opposition, like your own, is regulated by corridors, stairwells, and elevators—so know where those are, and keep an eye on them whenever possible. Know the habits of the people (opposition or bystanders) who use the building you're infiltrating, so you'll know whether you're likely to run into anyone—and what to expect if you do.

When entering a room, check every blind spot before walking in—behind the door, behind any corners, behind large furnishings. Have the first person in scan the room, while the second man covers the blind spaces nearby, such as behind the door. Never turn your back on a blind spot until the room is secure.

When approaching a corridor intersection, slow down and ease up to it with your lead people against opposite walls. As the illustration shows, this arrangement gives you good visual coverage of the side hallways without exposing yourselves. Notice that the third man is covering the corridor ahead.



Stairwells are a particular challenge—with their tight turns and terrible visibility, surprises lurk around every corner. Avoid them when you can, especially when the opposition knows or expects that you're around. Always move slowly and cautiously in stairwells. Stick to the outside wall, with your lead man keeping his eyes on the next landing. Have the second man watch up the stairwell as far as possible, and the tail man watch the rear.

Be circumspect about the use of lights, especially when they can be seen from other locations (through windows, for example). You can be seen from without if you turn on lights when you enter a room, and it looks even more suspicious if you wave flashlights around in the dark. If you need light to work but can't risk turning on the overhead lights, use the smallest flashlights you can. Keep the light masked as much as possible, and don't walk with them or wave them around—turn them off as you move, using them only when standing still. ♦

codes require that stairwell doors remain unlocked, at least from inside the building. That means you can always get into the stairwell, but not always back into the building. Furthermore, the doors are often wired to the fire alarm. Keep this in mind, watch out for security, and stay close to the walls as you use stairwells.

- **Elevators** are easily monitored and even controlled remotely. Don't use them unless your movement won't arouse suspicion. Elevator shafts, on the other hand, are generally unmonitored and contain little security, and make great movement routes. In large buildings, there are often many elevators in one large shaft. Keep in mind, however, that elevator doors may have sensors that report their opening if the elevator car isn't present. Also, if a security breach is discovered, elevator shafts will be one of the first areas secured.

- **Ducts and airvents** criss-cross every modern building. Contrary to what you see in the movies, however, few buildings have extensive networks of navigable ducts. Even when you can move through or on them, metal ducts are incredibly noisy. Squeezing through a vent or short section of ducting can be a good way of getting from one room to another, however, but watch out for security measures, especially if you are using a duct to get into a secure area.

- **Furnishings** provide visual cover and some physical protection. Security desks and other key points are also often armored, to give security personnel a solid defensive position. Most other furniture does not make effective armor, but provides visual clutter and concealment for the adversary. Scan the area at floor level when entering a heavily-furnished room, to see if anyone is hiding under furniture.

- **Windows** let you see out and others see in. Stay away from them—if you are in a lit room after dark, outsiders will be able to see in much better than you will be able to see out. You can be noticed by an outdoor patrolman even after penetrating layers of indoor security measures. Also, an outside assault force will position snipers on the windows, and you become a target if you get where they can see you.

Infiltration

Infiltration is the act of getting into and out of a building without alerting anyone to your presence. It can be quite a challenge in a well-secured building staffed by competent security personnel.

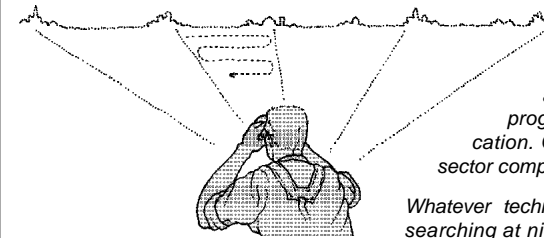
There are as many ways to infiltrate a secure building or compound as there are to get around a locked door. You can pound your way in, or pick the lock, take apart the hinges, or wait until someone comes along and opens it, then follow him through. When planning an infiltration, you must start with good intelligence. You want to know not just what physical

Techniques 58: Area Search Techniques

There are two sets of search techniques, depending on whether you are searching a broad area visually (attempting to find a boat adrift on the ocean, for example), or a small area in person (looking for an item dropped by a suspect at a tactical scene, for instance).

Broad search techniques vary according to whether you are on the move, or visually searching from a specific location. When on the move (for example, when searching from an aircraft), travel along a specific grid or spiral out from the spot you think you'll most likely find your target. If scanning from a specific location, break your area of search down into sectors (use landmarks on the horizon to define them). Then scan horizontally along the

horizon in one sector, then back just below the horizon, and so on, searching back and forth as you focus your attention progressively closer to your location. Once you've searched one sector completely, move on to the next.



Whatever technique you use, if you are searching at night (even with night-vision gear), move your gaze in constant small loops

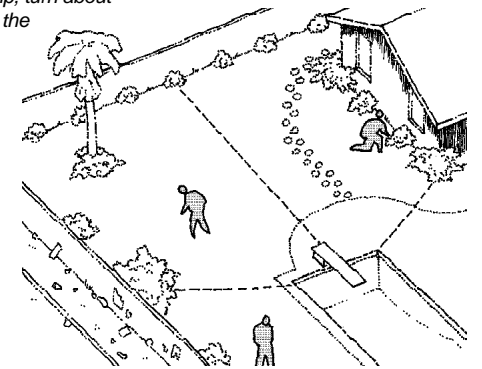
or figure-eights as you scan. In low light, your eyes have a blind spot dead-center—by moving in constant small loops, you increase the chance that you'll spot something in your near-peripheral vision and not miss it in your blind spot.

A close search is a search of a specific area—a crime scene, a tactical objective, or a room, office, or home—for items lost or hidden there. There are a number of methods that can help ensure an organized and thorough search—which to use depends on the area, the number of people involved in the search, and the amount of time available.

In an open area, where the items being searched for might be anywhere, the easiest method is the strip search. Divide your area into imaginary strips, and have your searchers walk them slowly. If you have only one searcher, walk the length of one strip, turn about at the far end and walk back along the next strip, etc.

If you are searching around a specific spot or item, have a single searcher walk in a slow spiral out from that epicenter.

In a room or enclosed space (or even broken-up outdoor area, such as the yard around a house), divide the area into imaginary zones of manageable size. Then search each area one at a time; if you have more than one searcher, assign one to each zone. ♦



security exists, but also how skilled the security personnel are, and what procedures are followed.

Start by looking for flaws in the physical security system (see [Chapter 3: Physical Security and Surveillance Systems](#)). You must have the skills to defeat the individual security measures you will encounter, or the system as a whole, or some method of getting around what you can't defeat. If you can find no flaws in the physical system, look for holes in the routine, bad procedures, or good procedures that are regularly ignored. Don't be afraid to get radical—often some sectors of security are left unattended to because the designers figured “nobody'll ever try to get in that way.” On the other hand, keep your plan as simple as possible—every complication increases the chance of failure geometrically.

If you find little information on security, or no exploitable flaws, you can try to wing it. Make sure you're getting paid well, though, because the risks are high. Bring along the skills and tools you will need for any foreseeable security or surveillance hazard, move carefully and take your time, and always think about how you are going to get out. You may want to make one or two recon trips, to probe the security and see what is there. But remember that if you are detected, the adversary is warned.

For any infiltration, use two parties—one to do the actual infiltrating, and the other to overwatch from the exterior. If possible, have the overwatch party isolate the building, intercepting the phone, data, and dedicated alarm lines from at least the security station. If you are hacking the building's security and/or engineering computers, the overwatch party should handle that too (even if you have to get someone inside to get on the system, you should then connect him or her to the overwatch party via cellular modem—that way, your inside people can concentrate on their job, not on working the computer). The overwatch element can keep the infiltrating party apprised of the situation, especially of the activity of visible security personnel or police. And finally, the outside element can provide a diversion if needed to help the infiltrating group escape.

Surveillance equipment generates records, so wear a balaclava or a mask. Wear gloves, too, and long-sleeve clothes, so that you minimize the fingerprints and blood and DNA samples left behind.

Clearing a Room

The key to taking a room is overwhelming surprise and force. Like an ambush, you never want to give hostiles a chance to fire back. Unlike an ambush, the adversary has many advantages when you enter a room. So even if you are restricted to non-lethal force, make as much impact as possible to overwhelm the room's hostile occupants.

Techniques 59: Shaking Trackers

There are two types of trackers that you might find on your trail: human trackers and dog trackers. The former are pretty few and far between; you are likely to encounter skilled human trackers only among the elite of competent guerilla or counter-insurgency forces. Dog trackers are much more common, and might be employed by security, police, or co-in forces anywhere in the world. Dogs are generally only useful when the scent they follow is fairly recent, but they can make good time, allowing their handlers to close on their quarry quickly. Human trackers, which rely on visible signs rather than scent, can follow a much older track (if the weather is in their favor) but tend to move much slower.

In general, only good tactics, woodcraft and speed defeat human trackers. Even among elite woodsman, there are few who can effectively cover their tracks for more than a few dozen yards—not nearly enough to throw off a competent tracker. But basic habits can deny the tracker the information he seeks: avoid building fires and leave no garbage, brass, or other materials behind at encampments or rally points (even buried garbage will be found). Avoid direct routes to objectives or extraction points to prevent the tracker from surmising your destination. And don't dwaddle—tracking is a slow process; if you can widen the gap between you and your pursuers you might make their efforts moot.

If fooling a human tracker is difficult, fooling a dog is impossible. There are only two options: disable the dog; or confuse its handler. If you know that you will be dealing with tracking dogs ahead of time, come prepared with some sort of disabling material. Don't bother with poisoned food—a well-trained dog will not eat without its handler's permission. Eucalyptus oil (available at health food stores) will numb a dog's nose, reducing its efficiency—dribble or spray a swath of it across your track. If you're lucky, this may gain you a couple hours' time. A more permanent, though riskier, solution is dried blood meal mixed liberally with cocaine. The dog, sniffing the blood meal, can take in enough of the cocaine to kill it. The powder must remain loose, however—not be blown away by wind or soaked up by ground moisture—and it must be spread out in a manner unnoticeable by the handlers.

If you can't disable the dog, go after the handler. Running through streams and other hollywood techniques rarely fools the dog—but they can, if used properly, fool the master. After crossing an obstacle such as a stream, run a random pattern, zig-zagging, doubling back, and making large leaps, for a few dozen yards. Given enough time, the dog will find your trail again—but in the mean time its erratic behavior may convince the handlers that it has lost your trail. ♦

Clearing a room properly requires three people. One will act as security, remaining in the corridor or adjoining room to watch your back. If the way behind you is secure, you can do without him. The remaining two operatives actually storm the room. Do not look into the room or do anything that will alert the occupants to your presence—you need the element of surprise to make up for the occupants' inherent defensive advantage. Follow these steps:

1. Start with a grenade. If you don't want to use lethal force or cause that much property damage, or if you are worried about hostages or innocents, use a flash-bang grenade. If the door is closed, kick or blast it open—don't turn the handle and alert the occupants—and throw your grenade. If you don't have to kick open a door, cook off the grenade, so that the occupants have no time to react.

2. Rush the room. As soon as the grenade blows, the first person should spring through the door, spraying the room with automatic fire (don't hit your hostages), and put his back to the wall beside the door. The second operative moves into the opening, staying low, also spraying the room. If anyone is returning fire after the initial onslaught, move quickly to cover while hitting him with maximum firepower.

If you do not wish to use lethal force, you must maximize the suddenness of the attack to totally intimidate the adversary. Rush in with more than two people if a lot of opponents are expected. Instead of pausing inside the door, rush headlong into the room and get your weapons in the adversary's face. Shout "freeze!" Shoot over his head if practical. Control the room before anyone can react.

3. Secure the room. Check hiding places. Make certain all hostiles are incapacitated, and not within reach of weapons. Get hostages out of the area, but check each to make sure that no hostiles are slipping out with them.

Field Problems

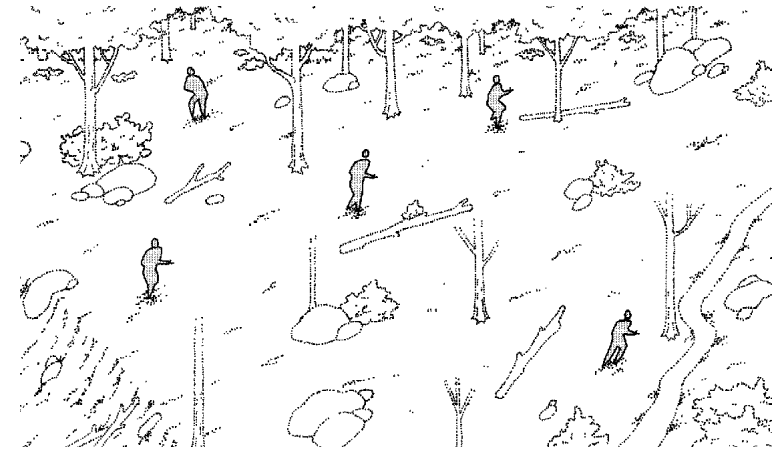
BlackEagle/BlackEagle is not a mercenary organization, but it is when our assignments take us into the field that we most resemble one. The tactics described below are derived from standard military doctrine on light infantry and guerilla operations, modified for use by cell-sized units.

Tactical Travel in the Field

The U.S. Army specifies three major types of movement for squad- and platoon-level elements moving in the vicinity of the enemy: Travelling,

Techniques 60: Field Movement Hazards

The illustration above shows a cell moving through light woods, towards the lower right (foliage in the foreground has been omitted for clarity). Tactical movement in the field differs from that in other terrain types because of the different nature of the threat. Danger is more dispersed, and hostiles are probably not going to appear right on top of you. Your concern in the woods is to avoid detection and tactically disadvantageous terrain, while minimizing the effectiveness of surprise attacks.



This cell's diamond formation and loose spacing makes it a difficult target in an ambush kill zone, and lessens the likelihood that a single grenade, mine, or booby-trap could take out the entire cell. They have good security in all directions, and the formation allows them to act in a coordinated fashion when hostile contact is made.

There are as many hazards in the field as there are in any other environment, although they are not as dense. Trees provide cover for attackers at ground level and up high. Rocks, logs, bushes, tall grass and undergrowth conceal booby-traps, noisemakers, and attackers. Open terrain makes you an easy target, while dense cover bunches you up and denies you maneuvering room. The footpath in the lower right may or may not be a danger area, but is definitely a more likely spot for mines and booby-traps. Holes, ditches, and gullies create dead space that gives attackers cover—a good reason to have a grenade launcher along. The right flank man in the illustration has moved to where he can see into the ditch on the lower left. That's a good move, but avoid silhouetting yourself along the edge of a deep ravine or on a ridge. ♦

Travelling Overwatch, and Bounding Overwatch. All three are based on the assault-and-support concept that is fundamental to modern infantry tactics.

Travelling movement is used when hostile contact is not likely. Support and assault elements move in line, with about double the distance between the two elements as between individuals within them. If hostile contact occurs, the trail element can move up beside the lead, or fall back to move around to a flanking position. Travelling movement is the easiest formation to maintain while moving through the brush, and for that reason is the fastest of these three techniques.

Travelling Overwatch is used when hostile contact is more likely. The trail element remains in the rear, but moves to the side on which the enemy is most likely to appear, and chokes up a little on the lead element. This allows the entire unit to bring fire on the enemy at the point of contact, while maintaining flexibility of movement. Because it is a slightly more complex formation than Travelling, Travelling Overwatch tends to be a bit slower.

Bounding Overwatch is used when hostile contact is imminent. Lead and trail elements continually trade places, with one element remaining in a supporting position, ready to open fire on any hostiles that might appear, while the other element bounds forward a short distance. Then the moving element halts and assumes the supporting role while the other moves past it. The two elements leapfrog forward, with one always being covered by the other. Because only half the unit is moving at any given time, Bounding Overwatch is a slow form of movement.

These three types of movement are not the only options in the field, just the best ones when someone gunning for you might be around. File movement (see the sidebar on pages 103) is good for speed, and essential in limited visibility.

Field Tactical Hazards

Tactical hazards in the field are not as dense as those in urban or interior environments, but they are diverse and just as dangerous. Look out for terrain or vegetation that will conceal attackers or traps, limit your ability to maneuver and respond, or funnel your movement. Here are some specifics:

- **Trees, rocks, undergrowth, and debris** give hostile forces concealment, allowing you to walk right up on them before they attack. They may also conceal traps or noisemakers. Watch everything, including the foliage of trees. Step over or around logs, debris, and rocks, especially if you are approaching a known or suspected hostile position, where trip-wires and other traps are likely.

Techniques 61: Field Movement Techniques

When moving in the field, take your time. Keep your formation loose. As you walk, always be aware of the nearest tree, rock, or other cover, so that you can dive towards it if suddenly attacked. Step over logs and small rocks, rather than on them. Move your feet slowly, and plant them toe-first, so that you can feel the ground—especially when near a suspected enemy position, where traps are more likely. Give obstacles—like ponds, ditches, cliffs, open areas, or areas of dense bracken—a wide berth. Never walk along paths—if you want to follow them, stay a few meters to the side. As quiet as you try to be, your movement inevitably makes some noise, which can mask the sounds of others, so pause occasionally to listen. Any time you stop for more than a few seconds, get down prone, facing out.



This six-person cell is moving in a wedge, in what's called the "travelling" movement mode. The assault and support elements are one behind the other. This makes for easy movement in bad visibility or thick vegetation, while maintaining flexibility in case of contact. If you are expecting contact however, the "travelling overwatch" or "bounding overwatch" are more cautious movement techniques.



The cell to the right is using the "travelling overwatch" movement technique. It is similar to the travelling technique above, except that the rear element has moved up and to the side on which enemy contact is most likely. Notice that both elements still maintain their wedge shapes.



The final movement technique is the "bounding overwatch." The two elements leapfrog forward, each covering the other in turn. This is the slowest but most cautious movement technique, used when enemy contact is imminent. ♦

- **Draws, gorges, ravines and hills** create dead space—areas into which you cannot see. Steer wide of them, or check them out. Carry a grenade launcher or other indirect-fire weapon in your cell, so you can flush out attackers if they use dead space against you.

- **Open terrain** with little vegetation leaves you too exposed, not just to direct attack but also to artillery and other fire support. Avoid it if you can, move carefully and quickly through it if you can't. Always spread your formation way out when crossing open terrain.

- **Close terrain or dense vegetation** limits your visibility and movement options. If you cannot avoid dense or difficult areas, at least be cognizant of possible attack and keep an escape route in mind. Do not let yourself be funneled into an area where the terrain totally dictates your movement.

- **Streams, paths and roads** are natural movement routes—which means that they will be watched, patrolled, or trapped. Never use roads or trails. If you want to follow them, stay parallel at least ten or twenty meters off to the side.

Patrols and Patrol Bases

One of the most basic tasks in field operations is the patrol. Patrols may be assigned to gather recon, secure a region, or intercept hostile units. They may require days in the field, or just hours. Movement on patrol is highly tactical—a patrol never wants to be detected first, if at all.

How you carry out your patrol will vary with the situation and objective. Generally, the purpose of a patrol is to maintain a presence, preventing the enemy from acting in the area with impunity, to totally exclude the enemy from the area, or simply to keep tabs on enemy activities and positions. Patrols in the wilderness may follow careful patterns of movement, designed to efficiently cover the entire zone, or they may wander at random. In either event, you need to plan your patrol route to hit likely enemy avenues of movement or activity. That means checking roads and trails that hostile forces may use and investigating terrain features that they may find useful. Remember, whereas in some tactical operations, like infiltrations and recons, you want to avoid contact at all costs, when on patrol you want to find the adversary. You still don't want him to find you first—even on a search and destroy operation you want the element of surprise. In fact, sometimes you simply want to observe the adversary, preferably without his knowing you were around. So despite the fact that you want to move through likely areas of contact, you should still be as careful and quiet as on a recon or infiltration.

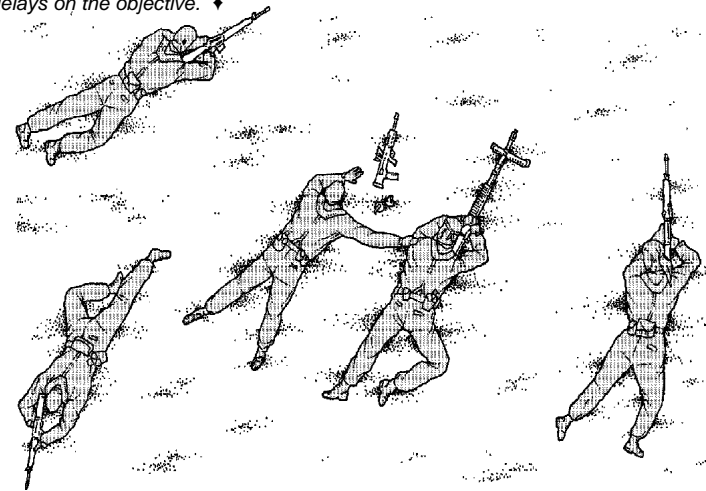
Whenever your patrol needs to stop—to rest, eat, or send out smaller recon elements—set up a patrol base. A patrol base is just a

Techniques 62: The Near Ambush

The illustration below shows a typical cell-sized element prepared to conduct a near ambush. For clarity, no vegetation or cover has been shown, but of course everyone should be well-concealed. In this example, one individual has been assigned to security (he's the one facing away from the kill zone). If you have a larger element, place additional security on either flank. Everyone else above may look like they're asleep, but they are just keeping their heads down for maximum concealment—only the ambush leader looks up into the kill zone. He's going to start the ambush with his most casualty-producing weapon—in this case, the machine gun. He's got his hand on the machine-gunner's shoulder so that he can silently signal him when the time is right. When the machine gun opens up, everyone else will open fire as they look up and into the kill zone. Notice that the leader has a couple grenades handy.

Although this illustration does not show it, you want to position your ambush along the side of the target's likely route, not across it. First, you don't want to hit the target from the front, since the formation will probably be strung out and the leaders and heavy weapons that you want to take out first will probably be in the middle (the exception is vehicle convoys: you want to hit the lead and tail vehicles first, to trap the others in the kill zone). Second, if you block the target's path, you cannot avoid an engagement if something goes wrong (like the hostile unit turns out to be much larger than you thought). By positioning yourself along the side of the route, you can strike whichever part of the formation you like as it passes through the kill zone, or hold your fire and let the target pass if something is amiss.

Once the initial attack has had its effect, the assault element will get up and move through the kill zone, engaging any survivors. In a unit this size, the assault team should probably be the two rifles on the ends. That would leave the leader and the machinegun on overwatch, ready to provide supporting fire for the assault element and alert for counterattack. You may prefer to have the leader in the assault team, but whatever you do, make sure the assault and support teams are decided beforehand, to avoid confusion or delays on the objective. ♦



glorified objective rally point, with a little more attention paid to defensibility. Follow these steps:

1. Select a site based on a map recon. The site should be off the beaten path, someplace where you are unlikely to be stumbled upon. A marsh or similarly inhospitable point is ideal (you aren't in this for the sake of comfort). Never choose a strategically important point, like a hilltop, as the enemy will likely check it out (the exception is cover—if you are in an area that offers little concealment, take what you can get).

2. Move up to the site, but don't move in. Set up an ORP a few hundred meters away and send a two or three man recon team to check it out. If it looks suitable and there are no hostiles about, leave part of the recon team there to keep the site secure while one person goes back to fetch the rest of the group.

3. Occupy the site and set up security. Make sure your security covers all angles and avenues of approach. If you have heavy or crew-served weapons, place them facing the most likely approach angle, or towards suspected hostile positions. When everyone is in place, send out recon teams to quickly check out the area within a hundred meters or so, especially blind spots. Place leaders in the center of the perimeter, where they can keep an eye on everything. Keep movement to a minimum.

4. Establish watch schedules and orders of work. Generally, you don't want to fall below fifty-percent security—that means that no more than half the personnel are sleeping, eating, cleaning weapons, or resting at once. If there are specific tasks that need to be accomplished (like navigation, satellite comms, equipment or weapon repair, etc.), take care of them as soon as possible, so that you can move on if necessary. Personal hygiene, eating, and sleeping (in that order) are the last things you attend to.

The patrol base offers a relatively secure point from which you can launch other operations, like smaller patrols or objective recons. If you leave it unoccupied, however, consider it unsecure, and do not re-occupy it without going through the above steps (in fact, it's generally a good idea not to re-occupy it at all—find another spot). If an element leaves the patrol base, especially if it includes the leader, establish a contingency plan covering what to do if the departing element is attacked or fails to return, or if the patrol base is attacked. The leader must insure that all separated elements know what to do in case of the unexpected.

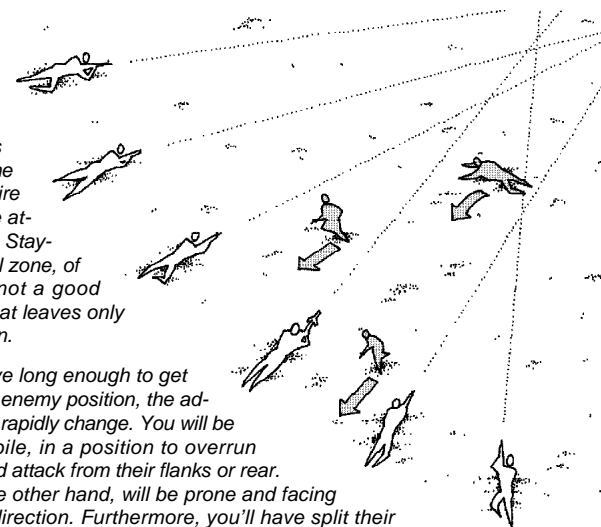
Ambushes

The concept behind an ambush is simple: hit the adversary before he knows what's going on, and hit him hard enough so that he won't hit back. Despite the simplicity of the concept, however, there are a number of

Techniques 63: Surviving an Ambush

If you're in the kill zone of a near ambush and are lucky enough to survive the initial attack, there's only one thing to do: get up and run towards the attackers. This seems pretty counter-intuitive, but it actually moves you into decreasingly intense fire—whereas if you run away

from the kill zone, as this illustration shows, you will stay in the attacker's sights and the combined fire of the entire attacking unit. Staying in the kill zone, of course, is not a good idea, and that leaves only one direction.



If you survive long enough to get close to the enemy position, the advantage will rapidly change. You will be up and mobile, in a position to overrun their line and attack from their flanks or rear.

They, on the other hand, will be prone and facing the wrong direction. Furthermore, you'll have split their formation, breaking their ability to effectively act as a unit. Exploit that confusion to the maximum.

Smart movement techniques should result in some of your cell not being caught in the kill zone. If you're one of those lucky individuals, don't hesitate. Move immediately to flank the enemy's position—but look out, because the enemy should have positioned one or two personnel on security, to protect from just such a move.

Far ambushes are a completely different story—there's very little chance that you can close the distance between the kill zone and the ambushers before they hit you or displace to a new location. On the other hand, your chances of being able to get into cover are much better, as the enemy won't be able to pour quite as much devastation into the kill zone as during a near ambush. So when hit from a distance, drop immediately, then move for cover and return fire. ♦

things you should know when setting up an ambush, in the field or elsewhere.

Military doctrine classifies ambushes as either near or far, and this is an important distinction. A near ambush is designed to annihilate the adversary, while a far ambush is usually intended to harass. Conversely, a near ambush will put you so close to the adversary that if he can react, you will have little room to maneuver. With the far ambush, you will be far enough from the kill zone that escape will be fairly easy. Don't go the middle route: if you cannot (or don't want to) totally destroy your adversary in a near ambush, stay far away enough to make a clean getaway.

When setting up either type of ambush choose a point along an adversary's expected route. It should offer cover for you and a kill zone that causes the adversary to tighten his formation (so that you can concentrate your fire) and denies him cover. Remember, however, that a smart adversary will maneuver around an obvious ambush site—and you don't want to be flanked while lying immobile in the bush. Place your ambush along the side of the adversary's route—not across it—a couple hundred meters away for a far ambush, or as close as a few dozen for a near one.

Once you've chosen your site, set up your people. First and foremost, position security around the ambush site. The ambushers will all be looking into the kill zone, so you will need at least one person watching your back, and, if the unit is big enough, one on each side (see the sidebar on page 143). Security is especially important in an ambush, because you are immobile and your attention is focused tightly on one area. Everyone should be totally concealed. Only the leader should observe the kill zone—everyone else (other than security) should keep their heads down. Since you will want to start the ambush with your most casualty-producing weapon (be it a mine or a crew-served weapon), you want the leader to have control over it. If this is a near ambush, assign assault and support elements, and position them on either side of the leader.

The leader must watch his kill zone carefully, and be patient when the enemy appears. A careful foe will space out his personnel, so that the entire unit will probably not fit in your kill zone. Wait until you get the maximum number of personnel in your sights, trying especially to get enemy leaders and heavy weapons (probably in the middle of the enemy unit) into the kill zone. Then open up with the claymore or machinegun. The other members of the ambush team, who should have had their heads down for maximum concealment, can now look up and open fire. Pour as much concentrated firepower into the kill zone as possible—the object is to never let the adversary fire back.

At this point, the difference between a near and far ambush becomes important. In a near ambush, you should be able to destroy the enemy unit in the initial volley. That is not so likely in a far ambush.

Techniques 64: Field LZs

Helicopters and VTOL aircraft have wonderful mobility, but they cannot go everywhere. If you are relying on helicopter extraction or medivac in the field, you must know the basics of landing operations. Because air ops often use a separate radio net than ground ops, you cannot rely on being able to communicate by radio with a helicopter as it approaches—and that makes proper technique in choosing and setting up field LZs especially important.

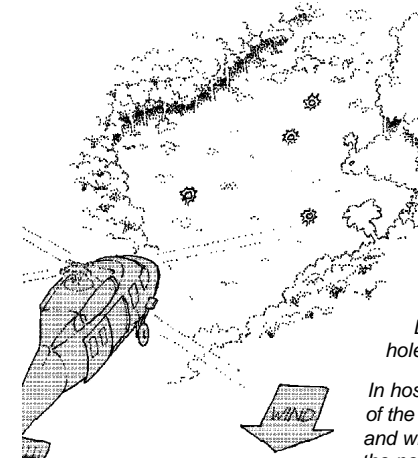
First, a helicopter requires a sufficient landing space, with plenty of clearance for its rotors. In daylight operations in favorable weather, a helicopter can put down on a plot of land only slightly larger than its landing gear, provided there is nothing taller than a man within the sweep of its rotors. At night, or in windy weather, a helicopter requires a space of at least 75—and preferably 90—meters in diameter, the center 50 meters of which must be clear of any significant obstacles or brush. High altitudes or temperatures make helicopter operations more difficult—increase each dimension by 10% for every 300 meters in altitude or ten degrees above 90°.

Most helicopters can land in water up to half a meter deep if the bottom is firm—but good luck getting the pilot to try it.

Optimally, helicopters require a 75-meter wide approach with a slope not greater than 1:5—that is, a 75-meter wide lane in which there is no obstacle over 20 meters tall within 100 meters of the LZ, or 60 meters tall within 300 meters. A helicopter can exit by the same lane, but a second lane, in the opposite direction, will allow a faster and safer withdrawal. If possible, both lanes should face into the wind.

As the helicopter approaches you'll need to mark the LZ, not only to identify the location but also to tell the pilot that you're there and ready for him. If you have time to set up, place

four markers in an inverted "Y," forming a triangle around the zone with the leg pointing in the direction of the approach lane. If there isn't that much time, place a single marker at the head of the LZ. Green or yellow are common LZ marking colors (if you're working with a military force and have an OpOrder, the marking color should be specified)—use smoke or a flare, chemlight, panel, or other marker. If you don't have an established signal, use colored smoke (anything but red) or wave the pilot in. Use red markers or smoke only to designate hazards in the LZ—obstacles that couldn't be cleared, holes in the ground, etc.



In hostile territory, set security around the rim of the LZ. Make sure that everyone knows how and where they'll be boarding the aircraft (see the next sidebar) before it arrives. ♦

In the near ambush, when the adversary appears to be subdued, call for a shift fire. The support element moves its fire out of the kill zone, but may continue to fire over the adversary's head if it will help suppress survivors. The assault element then rushes the kill zone, engaging any hostiles that may have found cover or otherwise survived the initial onslaught. Once the assault element has secured the kill zone, carry out any secondary tasks, such as first aid, search of enemy bodies and equipment, and prisoner processing. Keep at least some of the support element in an overwatch position. Wrap up as quickly as possible, then get away from the area.

In a far ambush, you are unlikely to totally destroy the adversary. He may be able to regroup and maneuver against your position. As soon as the initial volley has had its effect, use the confusion to withdraw. If you were properly positioned, you should be able to get clear before the enemy even knows where you are.

If you are ambushing vehicles, you will need some sort of obstacle to keep the target from simply driving away. Cratering the road may work, although it will have to be an awfully big crater to stop tracked vehicles. Felling a tree over the road is another good method, as is destroying the lead and tail vehicles at the outset of the attack, thereby trapping those in the middle. Since most vehicle convoys will put out a forward scouting party, you want to create the obstacle after the advance guard passes. For example, attach a mine to a tree in such a way that detonating the mine will fell it across the road. Blow the mine after the advance guard passes, just as the main body of vehicles gets into the kill zone. Make certain before you start the attack that you have the weapons needed to destroy all of the vehicles, especially armored vehicles, and don't send in the assault team until all vehicles are disabled.

Turnabout is fair play, and ambushes can be used against you. When on the move, watch out for terrain that forces your group to bunch up, especially if there is little cover. When moving on a road, stay well strung-out (twenty meters or so between personnel) so that the entire group won't fit into a kill zone.

If you are hit by an ambush, drop immediately to the ground, returning fire (this will probably be an involuntary reaction anyway). The enemy should have opened with his most casualty-producing weapon, so it is likely that your formation will be cut in half at best, or annihilated at worst. Don't stay down for more than a couple of seconds. If it is a far ambush, move quickly to cover. If it is a near ambush, get up and charge through the hostile position, firing like mad. That may seem suicidal, but if you are in the kill zone and still alive your seconds are numbered anyway, and moving in any other direction keeps you in the enemy's concentrated fire. Ideally, you want your entire cell to get up and charge at once, but there will probably be too much confusion and too little time to organize a concerted effort.

Techniques 65: Helicopter Insertions and Extractions

Helicopter operations in hostile areas are vulnerable to enemy action, and the noise and dust made by helicopters can draw the attention of the opposition—making ground forces vulnerable as well. Keeping insertions and extractions by helicopter efficient and quick improves everyone's chance of survival in a hostile environment.

The first thing to remember in dealing with helicopters is that you are coordinating your efforts with the flight crew. You will probably have little chance for verbal communications with the crew due to the noise of the aircraft and the fact that the crew may be on a separate radio net than your tactical communications, so it's critical that you pay attention to them and behave in a way that they expect. On military helicopters or large civilian craft, the crew chief will be your primary contact and your liaison with the pilot. Be sure to keep the crew chief (or the pilot) within your sight as you operate around a landed or landing aircraft, in case he or she needs to signal you.

In addition to difficulties in communicating with the flight crew, you will also have difficulty communicating with your cell when around noisy aircraft. Again, stay alert and keep an eye on your cell leader.

As aircraft approach your LZ, either on extraction in the field or prior to taking off for insertion, it's critical to be prepared. Airlifts are organized into "flights" and "chalks"; a flight is a group of aircraft making a single trip, while a chalk is a single aircraft within the flight. An insertion for one cell will probably only require a single chalk in a single flight; a large military airlift may involve several flights of dozens of chalks each.

Determine before your lift who will travel in each chalk, and assign a chalk leader to oversee boarding and coordinate with the flight crew. For each aircraft, split the assigned personnel into two groups and station them on either side of the LZ, so that when the aircraft lands the passengers can approach the side doors quickly and board in an efficient, orderly manner. If the LZ is hot and you're engaged in security as the aircraft approaches, make sure each person knows which side to approach as he or she disengages from security to board. If you must move around the outside of the aircraft, go around the front to avoid the rear rotors and keep yourself within the pilots' field of view. Keep weapons pointed away from the aircraft at all times, and, when aboard, point them at the floor.

Your aircraft will want to stay on the ground for the minimum amount of time possible—in fact, the aircraft may not even land at all, choosing instead to hover half a meter off the ground. When that's the case, be cautious—helicopters generate a great deal of static electricity, and you can be severely shocked touching both the aircraft and the ground at the same time.

On insertion in a hot region, disembark quickly and move straight out away from the aircraft, to the edge of the LZ. As passengers on either side reach the LZ edge, spread out to provide security. As soon as the aircraft departs, regroup at the head of the LZ and move out immediately—the noise of the helicopter may bring danger within moments. ♦

Those individuals who survive the kill zone and charge through the enemy's position can now engage the hostile force from behind, or withdraw to a rally point.

Recons

The recon is the one type of conventional warfare action to which BlackEagle operatives are most often assigned. There are several types of recons, but most are beyond the scope of BlackEagle operations. For example, recons-in-force, sometimes carried out in conventional warfare, involve probing an enemy's positions with combat units. This text focuses on the type of recon that our assignments most often call on us to do: the objective recon. An objective recon targets a specific known or suspected hostile position or other objective. When properly carried out, an objective recon should never involve direct hostile contact or combat.

In concept, an objective recon is a simple operation. One or more elements approaches a known or suspected position, observe it from one or more locations, and then withdraw. But if the target wants to avoid observation, it will take steps to foil reconnaissance activities. Actually carrying out a recon can be a difficult and complex operation.

Start by establishing the number of recon elements that will observe the site. A recon element should consist of at least three people: an observer, a recorder, and at least one security person. The presence of three personnel means that each can focus completely on his job—the observer, for example, can keep his eyes on the target without having to look away to scribble notes or watch for hostile patrols, while the security man can observe the surroundings without being distracted by the target. If you will be watching the target for an extended period, you may want to double up on the tasks, having up to six or eight personnel in the team. In planning, weigh the requirement for extra people against the added possibility of discovery that a large team creates.

A careful adversary will have his site spread out and camouflaged, making it difficult to observe the entire target from one angle. Because of this, and for the sake of expediency, you will often want to have more than one recon element to observe from several angles at once. If this is the case, you will need to establish an ORP or patrol base from which the elements can operate, and at which they can link up when they are finished with their observations. If you didn't want to occupy and maintain an ORP, at least establish a rally point at which the elements can meet when they are done.

When the elements leave the ORP move them out in different directions, so that they can approach the target from different sides. Maneuver as necessary when away from the target, but when you get within a couple hundred meters, head straight towards it (you don't want

Techniques 66: The Objective Recon

An objective recon is simply an excursion to look at something. Usually, however, it's something that someone doesn't want seen, and you don't want to be seen looking at it. The trick, then, is getting close without getting caught. This section covers planning for an objective recon, and movement in the area of the objective, to make that trick work.

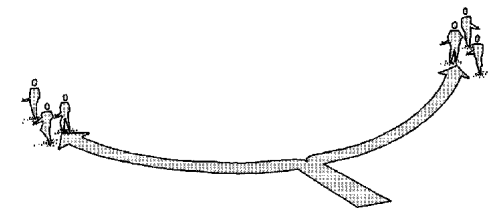
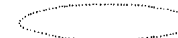
In this example, your cell is tasked to recon an uplink site that is the telecommunications center for an insurgent group. The client government has located the dish on a satellite photo, so you know its location to within a hundred meters or so. The recon is to determine the nature of the equipment at the site, as well as the status of the defenses and the unit manning the location. The site is in dense jungle, so you will have to get pretty close, but there may be hostile patrols.

Step 1

Before you leave, decide how many observation parties you will be using. For this example, assume you have a six-person cell. That will give you enough for two parties, which will allow you to finish the job in half the time with consequently less likelihood of running into a patrol. Assign observation, recording, and security duties for each element. Do a map recon, to get a feel for the best avenues of approach and observation. Remember, you want to avoid contact, so choose a route that is unlikely to be heavily patrolled or monitored, but that offers you good cover and concealment.

Step 2

When you get roughly a kilometer from the objective, establish an ORP. Plan a return time and a contingency plan. Split up from the ORP, with each observation element swinging wide around the objective to get to opposite sides. Do not get closer than half a kilometer to the suspected site (indicated by the circle in the background). The closer you get to the site, the more likely you will be to encounter surveillance measures and patrols, or to be seen or heard from the site itself.



to move at an angle to it, because your flank will be open if you are detected). Set up your observation point as close as you can get without being detected. If you want to move to another point, pull straight out until you are a couple hundred meters away, maneuver as necessary, then head straight in again (see the sidebar).

Make as many observations as you need. Look for the following: type and layout of buildings, structures, and defenses on the site, including possible minefields and electronic security measures and the enemy's unit size, activity, weaponry, and special equipment. Try to observe the enemy's communications methods, and if possible, to identify command posts and individuals of importance. Of course, make whatever specific observations you may have come for (like the presence of a drug lab, uplink, or special military hardware, or the possibility of hostages or POWs being kept there, etc.).

Other types of recons that BlackEagle cells sometimes carry out are area and route recons. They are a little less complicated than the objective recon, and in fact closely resemble patrols. Area recons cover geographical zones, looking for signs of hostile activity, but avoiding contact. Route recons explore terrain for potential movement routes. Both should be carried out just like patrols, but with special attention to avoiding hostile contact.

Raids

Raids are attacks on specific objectives, usually designed to harass or to secure a particular goal rather than totally overrun the site. Raids differ from assaults in that they rely on stealth in approaching the objective, and generally attempt to circumvent security at the objective rather than overwhelm it. Finally, raids are not intended to seize and hold ground—when a raid is complete, the raiding force leaves the area.

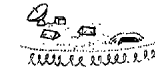
Raids are based entirely upon tactical principles and tasks already covered. They use two elements—an assault element and a supporting element—supplemented with a security force. The two elements generally operate from different positions near the objective, and maneuvering in the area is handled just like an objective recon. Follow these steps:

1. Plan and assign tasks. Your final maneuvering will be very close to the objective, so you cannot risk being disorganized at that point. Know which avenues of approach each element will be using. Divide your force into assault, support, and security elements. Put all crew-served and heavy weapons in the support element. If you need to conduct a recon to know what you are facing, do so.

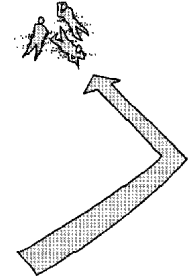
2. Move into position. Handle this just like an objective recon, using the techniques discussed above to get your assault element and support/security element into position. Discovery at this point compro-

Techniques 66: The Objective Recon (continued)

Step 3

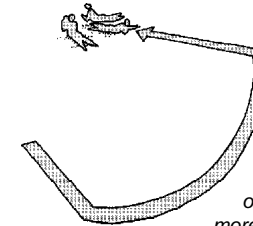


When your first observation point is directly between you and the site, move cautiously towards it. Be mindful of booby traps, noisemakers, and observation or listening posts. Move slowly and surreptitiously—crawl if you have to. Stop when you get to a point where you can observe freely. Keep one person on security, watching your back, while another observes and the third records what is seen. Stay at the observation point for as short a period as you feel you can, but record everything you can see.



Step 4

When you've seen all you think you will from your first point, back directly away from the site until you are five hundred or so meters away. Then move around until you are straight out from your second point. Move in and observe some more.



Step 5

Once you've finished, back out again and head back to the ORP, by a different route than the one you took getting to the objective. Link up with the other observation party, which should have been doing the same thing from the other side of the objective, and get out of the area.

Of course, you aren't restricted to two parties observing from two points each. One observation may be sufficient, or you may need several parties watching from several points. It depends on the size, camouflage, and security of the site, as well as the type of information you are looking for. You may need to come back several times, to make observations at different times of day, or to see how activity at the site changes over time. This example, however, gives you a good idea of how to move around and approach the objective.

If you do run into trouble on a recon, remember that you are split up, at a disadvantage tactically if not numerically. Plan to withdraw on contact, moving back to the ORP. Make sure that your contingency plan accounts for what to do if one element is attacked. ♦

mises your only advantage—surprise—so take your time and be careful. Position the assault element where it can move quickly to the objective, facing a minimum of open ground or obstacles. Put the support element where it can overwatch the entire objective, or as much of it as possible, preferably about ninety degrees from the assault element's path. Protect the support element with the security team.

3. Begin the raid by moving in the assault element. If there is little or no security at the objective, do not open fire until necessary, to maximize surprise. If the site is well-secured, especially if it is surrounded by open areas or obstacles that the assault team will have to breach, suppress hostile security with fire from the support element as the assault element moves. Use smoke to mask the assault element's activities and to confuse the adversary. Don't use so much, however, that the support element can't see what's going on.

4. Bring in the support element if necessary. If the objective is small, or the assault element is capable of carrying out whatever tasks are necessary, leave the support element on overwatch. If you need them on the objective, however, bring them in through the breach that the assault team made. Leave your security at the breach point, to keep your escape route clear.

5. Finish your business and get out. Do whatever it is you came to do—rescue hostages, destroy equipment, steal records, or whatever. Then get off the objective as quickly as possible. Move to your ORP, reconsolidate, and move out.

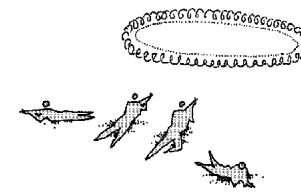
Actions on and After the Objective

When combat starts your presence is announced, and you have lost the advantage of stealth. Even in a silent mission, the moment you capture, kill, or disable an adversary you create evidence of your presence. It is wise to assume that discovery can't be far behind. For this reason, you always want to minimize the time you spend on an objective or at the scene of combat. Shortly after your discovery, or after an open firefight begins, you will draw attention. Reinforcements for the enemy may show up, or the police, or innocent bystanders who may become targets—or witnesses. Worse than that, if your adversary has the backing of indirect fire you can expect his position to be pre-referenced with fire support, and incoming rounds will land within minutes, or even seconds, if you overrun the position.

Techniques 67: Conducting a Raid

A raid, in its simplest form, is a basic assault-and-support attack. A support element overwatches the objective while an assault element moves into it and conducts the business of the raid. If two fire teams are needed on the objective, the support team can move in as well, leaving a security element to keep the escape route clear. Or, if you have enough personnel, you can split the assault element into two teams once on the objective. In any event, it is advantageous to keep the support team off the objective if you can, where they can provide fire support, keep an eye on things, and split hostile attention between two fronts.

This example shows a seven-person cell conducting a raid on a small compound, with the objective of destroying equipment and disrupting hostile activities. The cell leader has decided beforehand that the support element will go into the objective, and the cell has been divided into an assault element, support element, and security team. Because the compound is surrounded by a wire obstacle, two members of the assault element have been assigned breaching duties.

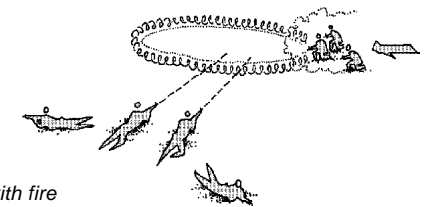


Step 1

Move all elements into position. Place the assault element at a point along the perimeter where they face a minimum of hostile fire getting to the wire and onto the objective. Put the support element at an angle to the assault team's path, but not too far off, because they will have to follow the assault team in. Using movement techniques discussed in the previous sidebar, get the assault element as close to the wire as possible. The support team can be farther off, as long as they can observe the objective. Have the security element watch the support team's back.

Step 2

This compound is surrounded by a wide open space (not shown), and it's unlikely that the assault team will get to and through the wire without being detected and attacked. Therefore, protecting the assault team is more important than maintaining surprise. When everyone is ready, open the attack with fire into the compound from the support element. Meanwhile, the assault team, under cover of smoke grenades, moves to the obstacle. The two breachers make an opening while the third person provides security and suppressive fire.



The lesson: get off the objective. This should be on the top of your mind from the moment the objective is taken. To minimize time on the objective, know beforehand what you will be doing there. Some common tasks you may face include:

- **First aid** for your casualties and, possibly, the adversary. You must be prepared to move badly-wounded personnel.
- **Searches** of bodies or the area. Even if you did not come looking for specific items or information, you may want to search bodies and equipment for incidental intelligence.
- **Prisoner handling.** If there are surviving hostiles to be taken prisoner, you will need to secure, search, and segregate them.
- **Hostage processing.** Hostages will be bound or locked up—you will need to free them. Even then, you cannot simply tell a rescued hostage to run along—they must be escorted to safety and debriefed. They may need medical attention.
- **Demolitions.** Your goal may be to demolish an enemy target, or you may simply want to destroy the equipment and weapons that the hostiles were carrying.
- **Recording.** You may need to record your findings on the objective, like photographing hostile casualties and equipment.
- **Reporting in.** If your action was part of a coordinated effort, you will need to report your success to your superior or coordinator.

You need to know who will be handling these tasks beforehand, so there will be no time-consuming confusion on the objective. Cross-assign these task, also, so that if one member of the cell is wounded another can pick up for him.

While these tasks are being carried out, remember security. If everyone is busy, you are vulnerable. Leave at least two people on overwatch. If a counterattack is a real possibility, move into a defensive position just beyond the objective before beginning your actions on the objective. Secure and reload. Then send small groups back to the objective to carry out their tasks.

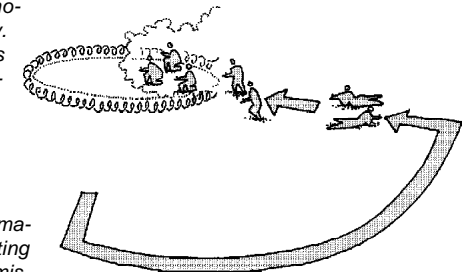
Your total time on the objective should be measured in seconds, not minutes. It is important to remember that you are most vulnerable while on the objective, having not only advertised your presence, but also given up stealth and mobility, your two principle assets. Don't hang around.

Once off the objective, there are a few things you want to attend to before wrapping up and heading out for a beer. The first is reconsolidation. Each individual needs to assess his ammunition, equipment, and casualty status, and report that status to the cell leader. That way, everyone knows the cell's situation, and you can make adjustments accordingly. Reconsolidate as soon as possible once off the objective—either on return to your ORP, if applicable, or at another hasty stopping point a few hundred meters beyond the objective. Stay alert during the reconsolidation, because you are still close to the objective, and don't waste time.

Techniques 67: Conducting a Raid (continued)

Step 3

The assault team moves through the obstacle and onto the objective. Again, they use smoke to mask their movement and create confusion. Meanwhile, the support team moves to the breach. You cannot take your time at this point—if the assault team has to wait around, they will be pinned down and momentum will shift to the adversary. When the support element reaches the breach point, they enter, leaving the security team outside.



Step 4

The assault and support teams maneuver on the objective, supporting one another, and carry out their mission as quickly as possible. Stay mobile, and take advantage of the confusion you have created at this point.

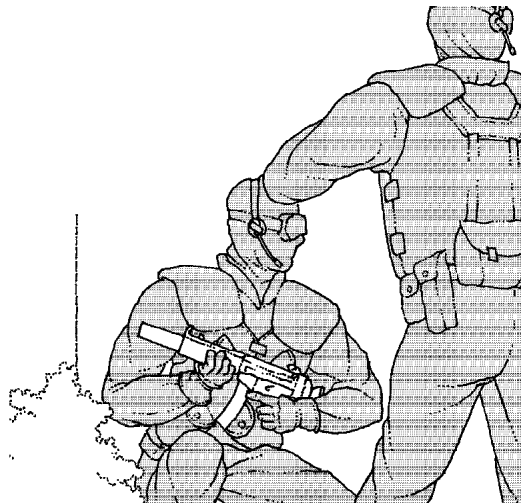


Step 5

With the security team providing suppressive fire to keep the breach clear, the assault and support elements exit the compound. It is possible that the enemy will move to close the breach, or cut you off from it. If this is the case, create another breach and exit from there (make sure that your security element is warned). In any event, move quickly back to your ORP and reconsolidate. Then move out of the area—you can count on being pursued, no matter how much confusion you created. ♦



Chapter 5: BlackEagle/ BlackEagle: Company Methods and Policies



BlackEagle/BlackEagle is quite a company. Just a two-man operation ten years ago, we now have hundreds of employees on four continents. We're one of the biggest companies providing security, certainly the biggest providing investigations, and probably the only one in the world that takes on the whole range of other services our operatives carry out.

Having covered the tricks that you help you, a BlackEagle operative, succeed out in the field, this chapter covers the company itself—who we are, how we do things, and how we can support you when you're on assignment.

■ Part 1: The Company

As just noted, BlackEagle/BlackEagle has come quite a ways in just a few years. There's no doubt that we've been in the right place at the right time to prosper from a changing—some would say declining—society. But there's more to our story than that—it's the personalities behind the company that have made us what we are today.

History and Scope

BlackEagle/BlackEagle is a fairly young company, but we've enjoyed unparalleled success and enviable growth. Although we are now a global firm employing hundreds of personnel, things were not always so grand. What follows is a brief history of the company and an overview of our activities.

BlackEagle/BlackEagle was founded almost a decade ago as a two-man firm providing security and investigative services in the Atlanta, Georgia region. For Clifton and Sheppard BlackEagle, working in the early days from their own apartment, work was slow initially. But by the end of their first year in business, things began to pick up, and they were expanding. They moved to a larger office, added new employees, and expanded their clientele. Two years later, the company incorporated and added its second office, located in Washington, D.C. Operations in this office and in Atlanta skyrocketed, as a changing society opened new business opportunities in an untapped market. The company continuously reinvested its profits, and during its third year opened offices in New York and Los Angeles. By this time, it was becoming apparent that the informal "team" approach used by the company in assigning missions to its employees was very successful, and the system of "cells" now used was formalized. In the fourth year, BlackEagle opened a "buying service," which allowed employees to purchase arms and other expensive pieces

of gear at wholesale prices. Originally run by a group of operatives in their spare time, this service was later expanded into the Logistics and Procurement Branch. Later, L&P would be further expanded to provide forensics and database support, as well as all types of inexpensive and rapidly-delivered supplies.

Four years ago, with further expansion of operations and a greater demand for services, the corporate structure currently used was put in place. This established the Administrative, Legal, and Logistics and Procurement Branches as well as the Operations Branch. By now, the company had offices in six U.S. cities, with an average of four cells in each. Shortly after this point, the company revised its policy (which to this point had been to decline assignments outside of the United States) and accepted its first overseas assignment. A year later, the first foreign office was established in London, overseeing operations in the European Community.

Today, BlackEagle/BlackEagle has sixteen offices in seven countries worldwide, and we are still getting bigger. Forensics support is being expanded by L&P Branch, and a training program has been instituted to accommodate the increasing demand for new operatives. Our Legal Branch is legendary, having set important precedent in a number of landmark cases. And of course, little needs to be said about the reputation of our operatives.

The scope of our operations has broadened with the expansion of the company. While we once investigated stolen cars and provided security for bank transfers, we now investigate international terrorism and provide security for heads of state. Corporate and governmental work, often involving multiple cells, now accounts for over \$30 million annually. We still accept and even encourage small contracts (contracts with private individuals, valued at \$20,000 or less), and they make up almost thirty percent of our business.

Organization

BlackEagle/BlackEagle is organized into four Branches—Administrative, Legal, Logistics and Procurement, and Operations. Of these, the Operations Branch is most central to the fulfillment of the company's assignments and its purpose. The Administrative, Legal, and L&P Branches exist to serve the Operations Branch, and one another, in the fulfillment of operational assignments.

The Administrative Branch regulates the day-to-day functioning of the company, insuring smooth communications between distant offices and the company's Branches. The Legal Branch provides advice in the negotiation and settlement of contracts, and provides services and aid when assignments bring operatives into conflict with the law. The L&P

Branch has, next to the Operations Branch, the broadest scope of activities. L&P provides materiel and forensics required by field operatives, operates safe-houses, and trains new and experienced operatives in basic and advanced operations techniques. The Operations Branch, of course, does the work that is the purpose and meaning of this company.

While other Branches are divided into Departments, the Operations Branch is divided into the geographical regions its offices serve. These are called Theatres, and there are four of them: the Atlantic and Pacific Operations Theatres in the United States, and the European and Far Eastern Operations Theatres abroad. There are several regional offices in each Theatre, and though each office has representatives from some or all of the other Branches, all regional offices belong to and are run by the Operations Branch. There are three offices that are not run by the Operations Branch: the Atlanta corporate office and the L&P facilities located in Atlanta and London.

BlackEagle/BlackEagle is run by its Senior Staff, which includes the Vice-Presidents for the Administrative, Legal, L&P, and Operations Branches, and the Executive Vice-President, and which is headed up by the President. This body sets the company's policies and strategies, and resolves any issues too large or important to be handled on the managerial level. In general, however, BlackEagle's leadership is intentionally decentralized, leaving a lot of authority at the office and cell level.

Beneath the senior staff is the company's management. As just mentioned, each Branch is headed by a Vice-President, who is a Senior Staff member. Directly below him or her are the Department Heads, or, in the case of the Operations Branch, the Theatre Heads. Department and Theatre Heads are the seniormost of the management, and are in charge of the specific functions performed by each Branch. The Legal Branch, for instance, is divided into the Operations Assistance Department, which provides aid to Operations Branch cells and individual operatives, and the much smaller Administrative and Public Relations Departments. Department heads command a skeleton of managerial staff that supports the functions of the departments. Theatre heads preside over the Senior Cell Leaders, who in turn manage the regional offices. Some Theatre Heads may also serve as Senior Cell Leaders for cells operating out of the main office for their theatre.

Each regional office contains a number of operations cells, headed up by their Cell Leaders. The Senior Cell Leader is always an ex-operative of considerable experience. He assigns incoming jobs to cells with the appropriate skills and experience, monitors ongoing assignments, deals with security and public-relations concerns, and is generally responsible for the successful operation of the office.

Senior Staff

BlackEagle's policy and future are set by a group of six Senior Staff members: the BlackEagle brothers and the heads of each Branch. In years past, this company was small enough for every employee to have easy access to the Senior Staff. Because the company has grown so much in the past few years, many operatives nowadays may not even have had the chance to meet some of the company's leaders. What follows is a brief bio on each, to give you an idea of the background of the BlackEagle/BlackEagle leadership.

President: Clifton BlackEagle

A native of the southeast, Clifton BlackEagle grew up in Atlanta, Georgia. After studying law at Auburn University under scholarship, Clifton pursued a variety of interests before setting up a private investigations firm in his hometown. Business being slow, Clifton expanded his firm into a partnership with his brother Sheppard and took on security work in addition to investigations. One of only two initial operatives, Clifton continued in that capacity for two years until the company incorporated, at which time he left operations to become the company's president.

Executive Vice-President: Sheppard BlackEagle

Sheppard BlackEagle also grew up in Atlanta, where, throughout his youth, he excelled in athletics. This physical prowess served him well throughout a heated career in the security industry. Sheppard joined his brother to found BlackEagle/BlackEagle in 1990 and was a full-time operative for two years. The incorporation process made him Executive Vice-President, but Sheppard still continues to participate in an occasional field operation.

Operations Vice-President: Alex O'Grange

Alex was one of the first five operatives to join BlackEagle/BlackEagle. He became a team leader after just one year with the company, and two years later he headed the newly-opened New York office. In 1996 Alex became the head of the Atlantic Operations Theatre, and he became the Operations V.P. a year later with the retirement of his predecessor Charlie Doyle. Alex was born in Washington, D.C. and was raised in Washington, Rome, and Vienna. He received a degree in Sociology with a Police Science

minor from the University of Virginia, and was highly decorated for his service as a police officer in his home town.

Legal Vice-President: Trieste Montieth

Born and raised in New York City, Trieste received both her undergraduate and Law degrees from Columbia. A relative latecomer, Trieste joined BlackEagle in 1996 as head of the Operations Assistance Department of the newly-formed Legal Branch. In 1998, Trieste ascended to Legal Vice-President after the former Legal V.P., Ben Morilla, was assassinated in Paris. Trieste is the only Senior Staff member with no operations experience.

L&P Vice-President: Ramsey Clayton

The idea for a BlackEagle buying service was originated in 1994 by Ramsey Clayton, then a field operative. Originally, Ramsey took on the task of obtaining hardware for his fellow operatives at wholesale prices in his spare time. The overwhelming response, however, convinced Ramsey as well as Clifton and Sheppard BlackEagle that some sort of full-time logistic support system was necessary. The buying service was formalized, and in 1996, under Ramsey's direction, was expanded into the Logistics and Procurement Branch. Ramsey now oversees procurement, forensics, and training support for operatives all over the world.

Administrative Vice-President: Kimball Marsh

Kimball was BlackEagle/BlackEagle's first employee, having started with the company in 1990. Although she has never officially been an operative, Kimball has been directly involved in many assignments, especially in the early days when the line between office personnel and field operatives was thin at best. Like the BlackEagles, Kimball is a native of Atlanta. She attended Georgia State University.

■ **Part 2: Operations Policy**

When you're out in the field struggling through some killer assignment, you're going to be making most of your own rules. That's as it should be—no two assignments are the same, and no set of regulations could

possibly deal with all of them. The company does, however, have a number of processes and policies that can streamline your routine assignments, and make even the toughest of them run a little easier. This section covers the most basic of these standard operating procedures.

Following Policy

Given the scope and nature of BlackEagle operations, it is clear that no policy book, no matter how thick, could cover every eventuality. As just mentioned, that's not our intent. These are minimal guidelines designed to explain the company's structure and keep operatives and the company out of trouble. Follow them when possible, and to use your best judgment at all times.

Sometimes the circumstances of an assignment make it impossible, or at least unduly dangerous, to complete the operation while following company policy. Do not knowingly enter into assignments that require you to break these rules. However, when you find yourselves in that situation, it is up to you and your Cell Leader to make the call. If a policy guideline is broken, the Cell Leader or individual operative will be held accountable for the repercussions. If it appears that sound judgment was used, the company will back you up as necessary (in our line of work, after all, these things are sometimes unavoidable). If, however, it appears that policy was recklessly or negligently disregarded, those responsible may face company punishment in addition to any other fallout from their actions.

Cell Organization

Operatives of BlackEagle/BlackEagle are organized into functional units referred to as "cells." The cell is the smallest operational unit for services provided by the company, and a cell may not be subdivided for operational purposes unless under extreme circumstances and with the approval of the Senior Cell Leader.

A cell may consist of as little as two or as many as seven individual operatives, but generally has three to five. One individual serves as Cell Leader, and is ultimately responsible for cell contracts and the successful completion of the cell's assignments. Cell leaders are elected by the individual members, according to the following guidelines:

- **Status.** The Cell Leader must be of Veteran 1 or higher status. Only cell members of Operative or higher status may participate in choosing the Cell Leader (operative status is explained below).
- **Senior Cell Leader Approval.** The Senior Cell Leader has the authority to veto the Cell Leader choice. This authority is rarely exercised,

however.

- **Timing.** Cell Leaders may only be elected between assignments.

Cell leadership shouldn't change during the course of an ongoing assignment, except as described below.

The elected Cell Leader must designate an alternate to fill in if he or she becomes disabled or killed, or suffers a no-confidence vote. If an assignment is ongoing, the alternate will fulfill the duties of the Cell Leader until the assignment is completed. If the cell is between assignments, then the alternate will fulfill the duties of Cell Leader only until a new Cell Leader can be elected.

A "no-confidence" vote is a means for changing cell leadership during an ongoing assignment. No-confidence votes should only be called for under extreme circumstances, when one or more cell members feel that the Cell Leader's decisions are likely to result in death or unwarranted danger for cell members. If the cell votes no-confidence, leadership of the cell passes to the alternate. No-confidence votes should not be taken lightly, as leadership changes during assignments can sometimes be as dangerous to a cell as its leader's poor judgement. In addition, no-confidence votes can have an adverse effect on client relations.

Whenever there is a change in cell leadership or membership, the Senior Cell Leader must be notified and the operations roster updated. Of course, the circumstances of an ongoing assignment may make it unreasonably difficult to contact the Senior Cell Leader. As with all company policies, this rule may be bent as individual operatives and Cell Leaders see fit.

Whenever possible, new operatives will be placed in existing cells with veteran operatives. When this cannot be achieved without disrupting successful veteran cells, or when demand for additional personnel is high in a particular office, cells may be created of entirely new operatives if and only if a Cell Leader of Veteran Operative 3 or higher status is assigned.

All cells operate from regional offices. The highest authority assigned to any regional office is the Senior Cell Leader. The Senior Cell Leader does not regularly participate in active assignments, but is required to be an operative of Veteran 3 or higher status. It is the duty of the Senior Cell Leader to assign incoming contracts to cells within the office based on the difficulty of the assignments, availability and experience of the cells, and the reasonable distribution of contract value amongst operatives from the regional office. Additionally, it is the Senior Cell Leader's duty to coordinate the activities of the Operations Branch at his office with the Legal, Administrative, and L&P Branches and with the Home Office through the Theatre Head.

The Operations Roster

The Senior Cell Leader for each office maintains an Operations Roster, used in divvying out incoming jobs and to maintain a record of each cell's activities. A cell's position on the roster is a key factor considered by the Senior Cell Leader when assigning contracts. However, a cell that appears at the top of the Operations Roster is not guaranteed the next available contract. The difficulty and nature of an assignment, experience of a cell, and fair distribution of contract value weigh heavily in the Senior Cell Leader's decision.

The roster contains general information regarding each cell's current activities. A cell may appear as "on-assignment", "on-call", "available" or "off-duty". A cell listed as on-assignment is currently under contract and will not be awarded further contracts until the current one is completed. Only in very rare circumstances will the Senior Cell Leader assign more than one contract to a single cell. This helps minimize possible conflicts of interest and helps assure the highest quality service to the client.

A cell listed as "on-call" is currently in the office and under contract to be ready to respond on short notice for a client. The pool of available cells is usually rotated through the on-call status, with more shifts allocated to cells lower on the roster. A cell listed as "off-duty" is only called upon under extreme or life threatening circumstances. BlackEagle operatives take their vacations as seriously as they do their assignments.

A cell listed as "available" may be called in on reasonable notice to take a contract assignment as it becomes available. However, it is often the case that contracts become available unexpectedly, and must be assigned on very short notice. So, in reality, any cell that appears on the roster as available is really considered on call. If an available cell turns down a contract offered to them by the Senior Cell Leader, they may be moved down the roster at the Senior Cell Leader's discretion.

The Operations Roster for an office also lists information about the current status of all the operatives assigned to that office. The names and status of the operatives, as well as any other duties such as Cell Leader or Alternate Cell Leader are listed for each cell.

In the event a Senior Cell Leader is unable to maintain the Operations Roster or to make contract assignments, he or she must designate an operative as Acting Senior Cell Leader to perform these duties. The designated operative must be of Veteran 3 or higher status and must be approved by the Theatre Head.

Often, cells are given numerical titles within an office to sort of designate their general level of seniority. This is an informal system, and cell numbers or titles do not indicate any official benefits or responsibilities. In offices where this system is used, the alternate Senior Cell Leader is often the Cell Leader for Cell 1, but that's simply because the title "Cell 1" is usually given to the cell with the most experienced operatives and

Cell Leader. As a matter of company policy, the alternate Senior Cell Leader can actually be any appropriate operative, or even an employee from another Branch, if he or she is qualified through past operations experience.

Operative Status

Another task of the Senior Cell Leader is the awarding of operative promotions. Operatives are ranked according to their experience with an loose status system. This rank reflects the number of assignments a operative has participated in, and is used whenever seniority is an issue. BlackEagle/BlackEagle tries to minimize the importance of status in terms of responsibility and leadership—all operatives are expected to make sound decisions and to account for their actions. However, status is useful when decisions must be made on access to resources or assistance, and for making sure that experienced veteran cells are rewarded for their past service with access to lucrative contract opportunities.

Status promotions are based on the number of assignments in which an operative participates. In general, every contract assignment counts towards status promotion. Particularly long, dangerous, or protracted operations may occasionally be counted as two assignments for promotional purposes—however, these cases are the exception, not the rule. Likewise, particularly short or easy assignments, or those in which a given operative did not really participate, might not be counted towards promotion. The Senior Cell Leader, under the advice of the Cell Leader, must decide how to apply each assignment towards promotion.

Status promotions are awarded according to the following guidelines:

Number of Assignments	Operative Status
0-4	Rookie
5-11	Operative
12-19	Veteran
20-29	Veteran 2
30-39	Veteran 3
40-49	Veteran 4
each add'l 10	one add'l level

Status promotions are used to determine seniority, mainly for matters of contract assignment and logistics support. When a Senior Cell Leader speaks with a client about a contract, he refers to the Operations Roster

to determine which cells are available, which have the most appropriate skills and experience, and how contract value has been distributed in the past. Once these factors have been accounted for, he may use seniority to determine which of the candidate cells gets the assignment. Similarly, seniority may be used by L&P personnel when they have conflicting requests for logistic or forensic support. Generally, factors such as need, waiting period, and the nature of the requests come first, but with other factors even, seniority may decide which cell gets the support it wants first.

Outside of these and similar considerations, status has little effect on an operative's standing. Status does not directly lead to an increase in pay or benefits, except that high-status cells are more likely to be awarded high-value contracts.

Operations Restrictions

BlackEagle/BlackEagle tries to place as little restriction as possible on the operational activities of its cells. That doesn't mean we'll take on any and every assignment that comes our way. You may set your own standards for what sorts of assignments are acceptable to your cell (noting, of course, that passing up assignments may bump you down the assignment roster). The following restrictions are the company's bottom line for unacceptable assignments:

- **Terrorism.** BlackEagle/BlackEagle does not contract for or carry out deliberate acts of terrorism. Deliberate terrorism is any violent act against civilian targets designed to intimidate the populace.
- **Assassination.** Contracts obviously intended to target individuals for assassination may not be carried out within the United States or the European Community unless that target is clearly criminal and the approval of the Senior Cell Leader is obtained. This rule may also apply in other nations as defined by regional office policy.
- **Obstructing justice.** Counter-law-enforcement assignments (assignments designed solely to deliberately foil the efforts of law-enforcement officials) may not be carried out in the United States or the European Community. Take on other assignments which might bring you into violent conflict with law-enforcement agencies only with caution. In such cases, the client may be comfortable with an "escape or surrender" clause, which would allow you to avoid violence with the law (see Contracts, below).
- **Out-of-region assignments.** Assignments must take place predominantly within the region served by your office. In other words, an assignment taking place in San Francisco, California should be handled by a cell from the Los Angeles regional office, not by one from Atlanta. There may be some exceptions to this rule, but at the very least, a cell

operating in another office's region must notify the Senior Cell Leader of that office.

Use your discretion, and talk with your Senior Cell Leader, if you think a proposed assignment is questionable. There are also a few other policies covering our activities. One of these is non-disclosure. Operatives are prohibited from speaking publicly about the details of their assignments, or about the activities of the company or the company's facilities or resources. This is discussed further under Security, later in this chapter.

Contracts

An assignment contract defines exactly what services a cell will carry out for a client, and what the rights and obligations for each are. The contract is an agreement between the two parties, and BlackEagle/BlackEagle expects full compliance from both clients and operatives.

No assignment, or part of an assignment, may be carried out without a contract. The exception to this is a preliminary investigation to determine the feasibility of an assignment, done without the expectation of direct payment. Any time operatives do any work for payment, even if it is preliminary to an actual assignment, a contract must be written up. This prevents confusion, and is for your protection and that of the company. Contracts distribute liability between the company and the client—the lack of a contract may make BlackEagle totally liable in the event something goes wrong with the assignment. If you do work for payment without a contract, you and your cell will not, of course, be entitled to legal, medical, or L&P support.

Operations contracts are typically negotiated by the cell which will carry out the assignment, assisted by a Legal Branch representative and sometimes the Senior Cell Leader. Negotiations are ultimately the responsibility of the Cell Leader, but all cell members are entitled to participate in the process, and contract adoption is only done with the approval of the majority of the cell members. If a cell cannot come to terms with a client, the Senior Cell Leader may pass the assignment to another available cell.

There are several factors to consider when you negotiate a contract. These include:

- **The scope of the work.** Make sure the contract addresses the specific objectives of the assignment as well as the maximum amount of time committed.
- **Value.** Specify the overall payment and whether it is a lump sum or per diem. Determine and spell out the payment method as well as which party is responsible for expenses.

- **Limiting factors.** The cell or the client may wish to specify factors which would limit the cell's activities. Many of these factors are covered by the standard clauses described below.

Company policy requires that the office Legal Counsel be present for final stages of contract negotiations, and that no contract be finalized without the consent of the Senior Cell Leader. Of course, no contract may be finalized that violates operations policy.

BlackEagle rarely makes the contents of its contracts public. However, some clients still have concerns about a written record of the services they are requesting. In these cases, it may be acceptable for contract language to be vague or non-specific. It is important that the Senior Cell Leader and office Legal Counsel carefully examine all contracts, however, to ensure that the company's position is defensible. And it is especially crucial that an explicit understanding of the contract's scope is shared by all parties, even if all of the details are not written out.

There are a number of standard clauses frequently included in BlackEagle contracts. These are described below. You may wish to include some variation of one or more of these clauses in your contracts as you negotiate them. Have your office Legal Counsel determine their exact wording.

- **"Partial Fulfillment," or "Incompleteness."** This basic clause requires partial or complete payment by the client even if the cell is unable to complete the assignment, or if the assignment expands well beyond the scope of the original contract. For example, if a contract called for the return of a missing person, and that person was discovered to be held in a maximum-security government installation, partial payment may be in order if the contract assumed less difficult conditions. This clause protects a cell from having to complete an assignment that ends up going way beyond its original scope.

- **"Drop-Dead Dates."** Drop-deads allow a cell to back out of an assignment if, at a certain point, it appears that the assignment will be impossible to carry out. For instance, imagine a client wants a burglary investigated. Very few leads exist, and the police have already given up. The cell could specify a drop-dead date. If that date is reached, and the cell's best effort has led to no new leads, it could then drop the assignment with no contract penalty. Usually, some sort of partial payment is associated with a drop-dead.

- **"Escape or Surrender."** In some cases, contracts may have the potential for causing violence between operatives and law-enforcement agencies. An escape or surrender clause will prevent the cell from having to fight, even if that means the assignment can't be completed. For example, if a cell on assignment were caught trespassing on restricted property, they may be allowed to give themselves up rather than battle armed security personnel or police. This clause can be very handy if a cell

is looking for evidence or information and secrecy is not a factor. On the other hand, an escape or surrender clause may not be appropriate for a covert operation, or when a cell is handling sensitive merchandise or evidence which must not fall into the wrong hands.

- **“Rules of Engagement.”** When a BlackEagle cell is hired for a tactical engagement, it is wise to include the Rules of Engagement in the contract. For example, if the client is a foreign government, it may require that the cell adheres to the Geneva Conventions to which it is a signatory. The cell may have rules of its own. When working for a less scrupulous client, for instance, the cell may wish to specify the types of activities it will not engage in—like killing prisoners or conducting terrorist actions. “Escape or Surrender” clauses are often part of the Rules of Engagement.

- **“Non-Disclosure.”** BlackEagle/BlackEagle makes it policy not to disclose the details of its assignments. Sometimes clients like this to be spelled out in the contract. Additionally, operatives may desire for their own protection that the client be obligated not to disclose any assignment details. Assignments against organized crime or terrorism often invite reprisal attempts against the company. These can be avoided if the client is required to keep quiet about our involvement.

- **“Right to Extend.”** This clause gives the client the right to extend a contract at more or less the same rates of payment, if an assignment may lead to additional, related objectives. This may be beneficial to both the client and the cell if it appears that a successful assignment will lead to additional work. The cell may specify that, if available, it gets the rights to additional assignments before other cells.

You are expected to complete assignments for which you contract, even in the face of great adversity. It is important for the company’s reputation and for business that assignments are not abandoned, that clients are satisfied, and that a high success rate is enjoyed. That’s why the above clauses can be so important—they help protect you from getting tangled up in assignments that become impossible to complete.

It is equally important that you are forward with clients concerning the difficulty and chance of success of a given assignment. If a client understands what factors make an assignment dangerous or difficult, he or she will understand why clauses are added, fees are high, and success may not be certain.

On some occasions, especially when cells are contracted to retrieve stolen merchandise, track down bail-jumpers, or repossess goods, contracts are paid by a third party such as an insurance company or bank. In these instances, it is especially important that the contract be finalized by the office Legal Counsel. Frequently, insurance companies require a number of clauses restricting the scope of work and limiting total payment.

Contract Payment

BlackEagle operatives are paid according to the value of the contracts for assignments they complete, as opposed to wage or salary. Contracts are paid by the client to the BlackEagle/BlackEagle, and each participating operative is then paid a share by the company. The payment of contracts and of operatives follows this schedule:

1. **Payment is made.** Contract payments, including retainers and partial payments, are made directly to the company. If the company or individual operatives picked up the costs of expenses that should, by contract, be the responsibility of the client, those are also paid to the company. Under no circumstance is any money paid directly to operatives.

2. **Expenses are deducted.** All expenses charged to the company (for items purchased through L&P Branch, for example) during the assignment, or paid by operatives, are taken out. Operatives claiming expenses must do so within three days of the close of the assignment (of course, exceptions can be made in the case of injury, imprisonment, or other incapacity).

3. **Shares are cut.** The remainder after the deduction of expenses is halved. One half is kept by the company, and the other half is paid to the operatives. That half is split into even shares—one for each cell member, with an additional share for the Cell Leader. All shares are awarded, with shares going to stated beneficiaries in the case of operative deaths. If cell leadership changed over the course of the assignment, the bonus share is split between the leaders.

4. **Paychecks are issued.** BlackEagle/BlackEagle issues a check to each participating operative, accounting for his or her share and any expenses that came out of his or her pocket, minus federal and state taxes. Checks are generally cut within ten days of the close of the assignment.

Take, for example, a cell with four members that completes a contract valued at \$50,000 plus expenses. Along the way, one cell member spent \$2,000 out-of-pocket on travel. The cell also charged \$4,000 for equipment purchases to the company. The cell provides the company with proof of the out-of-pocket expenses, and BlackEagle invoices the client for the total of \$56,000. The client pays the company. The expenses, totalling \$6000, are deducted from that total (the \$4,000 charged to the company goes to L&P, to pay for the purchased equipment). \$25,000 is kept by the company. The remaining \$25,000 is split into five shares—one for each of the cell’s four members, with an extra for the Cell Leader. Finally, checks are issued. Two of the cell members get \$5,000 each. A third gets \$7,000—his \$5,000 share plus the \$2,000 reimbursement for

his out-of-pocket expense. The Cell Leader gets a double share—\$10,000. All applicable payroll taxes are deducted.

Multi-Cell Operations

In addition to the single-cell operations most frequently carried out by operative cells, BlackEagle/BlackEagle also contracts for long-term, generally multi-cell operations. Occasionally, you may be asked to participate in multi-cell operations for which you did not contract. As with any other assignment, you aren't obligated to participate. However, if you are asked to participate in a multi-cell operation but do not, you may forfeit position on the operations roster—meaning that you might not have immediate access to alternative contracts.

There are two primary kinds of multi-cell operations:

- “On-Call” Assignments. Sometimes a client requires BlackEagle services to be continuously available on very short notice. In these instances, rather than tie up a single cell in waiting around for an assignment that may or may not materialize (thus preventing it from doing any other work), several cells are rotated through the “on-call” status. Any cell on-call needs to be in the office for the entire on-call period (usually rotated every twenty-four hours). Whichever cell happens to be on call when the assignment comes through gets the job. Depending on the contract, there may be some nominal payment for on-call service, or the cell might only get paid if it happens to be the one on-call when services are needed.

- “MPI” Assignments. MPI (abbreviated from Man-Power Intensive) assignments are those in which a relatively large number of personnel are required. Security and para-military are probably the most common type of MPI assignments. Although BlackEagle shies away from large-scale mercenary assignments (except in a leadership or training role), security operations are fairly common. When practical, the Senior Cell Leader will consult with all cells required for an MPI assignment before finalizing a contract.

In addition to these types of assignments, there is also internal work which occasionally requires the help of operatives from one or many cells. BlackEagle/BlackEagle will often, for example, run background investigations on new clients or businesses which adjoin BlackEagle offices. Operations such as these are designed to help protect company employees and facilities from attack (see the Security section, below), and rarely produce revenue. As with on-call assignments, the type of work required and the compensation given operatives who participate varies according to the nature of the situation.

From time to time, cells may be asked to participate in office security. In general, there will be at least one cell in the office at any given time (manpower permitting), either in an on-call status or simply providing a security presence.

Safehouses and Relocation

The Logistics and Procurement Branch operates a number of safehouses for the protection of operatives involved in dangerous assignments. These are always available for use, although their locations are only disclosed to operatives on a need-to-know basis. Additionally, a cell's activities may be so dangerous that the cell will have to be broken up and its operatives relocated for their own protection.

Safehouses are maintained in order to provide a secure and protected haven for cells, operatives, or operatives' families when their lives are threatened. Safehouses may only be used after or between assignments, or during a long lull in the middle of an ongoing assignment. Under no circumstance should you carry out an assignment from the shelter of a safehouse. Security is paramount with safehouses, and the dangerous activities of one operative or cell will not be allowed to threaten the safety of other operatives also relying on the safehouse.

Several L&P safehouses are operated in the United States and Europe. The exact number and their location are never revealed for security reasons, but any time you or your cell needs access to one, simply contact your Senior Cell Leader. In some instances, when the use of a safehouse is pre-planned, you may be told of its location before carrying out your assignment. In general, however, locations are only disclosed when needed.

Even if you know the location of a safehouse, do not drop in unexpectedly. Instead, have your Cell Leader or Senior Cell Leader arrange your arrival. Unexpected operatives attempting to enter a safehouse will probably be treated as hostile by the house's security force.

A safehouse is only a temporary refuge, and sometimes the threats against an operative are too serious to allow return to his or her original location. In these extreme cases, BlackEagle will relocate operatives or cells, to remove them from the proximity of the threat. When an entire cell must be relocated, it is broken up, with individuals moved to different locations. Relocations are rare, and the circumstances of each are handled on a case-by-case basis by the Senior Cell Leader, Theatre Head, and Operations Vice-President.

■ Part 3: Support

Given the broad nature of BlackEagle assignments—from counterterrorism to criminal investigation to corporate espionage—BlackEagle operatives need to be able to call upon a broad spectrum of support services. The company offers a surprising range of services given the company's size and the fact that we are a private (non-governmental) organization.

Office Representatives

BlackEagle regional offices vary in size and scope from as many as ten cells to as few as three. Support staffs vary from a single administrative secretary to a legal, L&P, and administrative cadre of eight or ten people. In offices supporting large numbers of cells, or located overseas where local assistance is impractical and travel times are an issue, the company provides additional staff to assist operatives in their work. These Legal, Administrative, and L&P personnel act as liaisons between their respective branches and individual operatives.

BlackEagle/BlackEagle provides a wide range of support services for its Operations Branch. L&P Branch provides equipment, forensics, and training, Legal Branch provides assistance with contracts and other legal difficulties, and Administrative Branch provides medical and insurance benefits.

Equipment

The L&P Branch is capable of purchasing, usually at well below retail price, virtually any product required for operative assignments. Some items in common demand, such as popular models of smallarms and basic surveillance equipment, are kept in stock at the Atlanta and London facilities, and can generally be shipped to any regional office in twenty-four hours or less. Items which must be ordered from a manufacturer or distributor take longer. Company policy states that items restricted for sale by government regulation will only be provided to operatives properly licensed to receive them. However, L&P Branch offers licensing programs as part of the training process.

BlackEagle operatives are encouraged to purchase the equipment needed for an assignment. If, however, an item is prohibitively expensive, or unlikely to be used more than once, it may be possible for L&P to loan it to the cell for the duration of the assignment. A fee will be charged to the cell which will be deducted from the expense account for the contract (this

may be paid by the client, or deducted from the contract value, depending on how the contract was settled). Loaned items must be returned at the end of the loan period, and the cost of damage will be deducted from the contract value. L&P discourages loans.

The L&P catalog lists items in stock for purchase or loan, with prices, fees, and shipping times listed. L&P can generally obtain any piece of equipment, even if it isn't listed in the catalog, given sufficient time. Although L&P tries to keep equipment availability high and costs low, try to remember that exotic or expensive equipment may be time-consuming and costly to obtain. If you need to buy or borrow equipment, talk to the L&P representative at their office, if there is one. If there isn't, contact the nearest L&P facility (Atlanta for offices in the Atlantic or Pacific Operations Theatres, or London for the European and Far Eastern Theatres) by telephone or GenNet.

Forensics

In addition to equipment, Logistics and Procurement Branch also provides forensics support for operations cells. Available forensics support includes but is not limited to national and international law-enforcement database searches; ballistic analysis; fingerprint and DNA identification; photo-imaging and audio analysis; and limited lab processing and access to international intelligence bulletins. Because the legal considerations can rarely be surmounted, BlackEagle/BlackEagle cannot provide full medical forensics, but L&P can arrange for limited medical testing through contract labs.

How you go about requesting forensics support depends on whether or not your office has an in-house L&P representative. If so, you need only speak to him or her. If not, contact the nearest L&P center (Atlanta or London) by phone or GenNet. Sometimes delays in service are unavoidable. When there are conflicting requests made for L&P services, preference is given to the requesting operative of the highest status level, taking into consideration the urgency of individual cases and the delay each party has experienced.

Legal Aid

The Legal Branch provides legal assistance to cells and individual operatives. As previously discussed, office legal counsels help settle assignment contracts. Additionally, the Legal Branch is available to help operative cells and individual operatives if, through their work, they get into trouble with the law.

If you are arrested or otherwise jailed, make every effort to contact your Cell Leader or Senior Cell Leader back at your office (see the sidebar earlier in this book, on page 15). Since most municipalities in the U.S. and abroad allow an arrestee to make only limited phone calls, a call to your Cell Leader gives you someone outside working on your behalf, who can then get in contact with legal help as well as family or friends if appropriate.

If you are wounded in the course of an assignment and require emergency medical care or hospitalization, contact your Cell Leader if at all possible. Your Cell Leader should in turn contact your office legal representative. In most locations inside the United States hospitals and clinics are required to report to law enforcement agencies wounds that could be the result of illegal activities, such as gunshot and stabbing wounds. It's in the best interest of the company and of the operatives involved to have legal counsel present at the hospital or clinic to prevent unnecessary administrative or legal entanglements. Of course, as mentioned below, don't allow these considerations to endanger your life—if you need medical help, get it, regardless of whether or not you can get word to the office.

Medical Support

Medical support is provided by the Logistics & Procurement Branch—that is to say, L&P makes the necessary arrangements for operatives to get the medical care they need through local hospitals and trauma centers. Getting adequate emergency medical support services in some remote locations in the U.S. or abroad, however, may be difficult. If your cell plans to carry out a dangerous assignment in a remote area, your Cell Leader should make prior arrangements with the local L&P Branch representative—he or she can provide information on medical facilities in the area, and coordinate as necessary with those facilities or arrange for medivac backup if they aren't adequate.

Even the safest looking assignments and the best crafted plans can take a wrong turn, leaving operatives in dire medical circumstances. When the difference between life and death is a matter of minutes or even seconds, the best doctors in the world can't help if they aren't there in time. Consequently the first line of support for operatives needing emergency medical attention is in the cell itself. Keep your EMT skills up to date—every operative should have or develop basic first aid skills, and every cell should include at least one operative with more advanced training. Ultimately, it is your Cell Leader's responsibility to be adequately prepared and equipped for medical emergencies.

MPI operations that are particularly risky sometimes warrant the contracting of well-trained emergency medical professionals. Your Senior Cell Leader may request that the L&P Branch provide for medivac

services and medical field personnel over the duration of an assignment. In operations where BlackEagle is working with a government agency, there may be "mercenary rights" laws that requires the agency to provide adequate medical support. In the absence of such a requirement, the L&P Branch may try to work with the agency to coordinate medical support. MPI security operations, although usually not as risky as paramilitary operations, may justify having full time medical services contracted during the operation. It is the Senior Cell Leader's responsibility to arrange adequate medical support for multi-cell operations.

The L&P Branch arranges to maintain medical support services and trained medical personnel in safehouses on an as-needed basis. A safehouse's medical facilities are not comprehensive, though—do not rely upon them in lieu of hospital facilities.

■ Part 4: Security

Our work is dangerous enough when we deal with our own assignments. Unfortunately, sometimes those assignments bring us additional trouble, when their targets put up active defenses, or they or their allies or successors seek revenge at a later date. Maintaining basic security is the first defense against such trouble.

Physical Security

Our company pursues many activities, and often makes enemies. Some of these enemies—terrorist groups, criminal organizations, and even foreign regimes—are powerful, have many resources, and can act at random anywhere on the globe. For this reason it's critical that BlackEagle facilities everywhere have adequate security to protect the company's personnel and property. A few of the measures taken to protect our offices, and the security responsibilities of individual operatives, are outlined here. Not every BlackEagle office has implemented these measures. Offices that find themselves lacking in some areas should seek to incorporate these guidelines into future retrofitting plans. Future offices should include these guidelines as a critical component of their initial design.

To begin with, all BlackEagle offices have alarms and some sort of physical barriers. Most are wired with silent alarms to local police stations. Many have bullet-proof windows or blast-proof doors. First floor offices usually have reinforced walls.

All BlackEagle offices have one room designated as a “safe room.” This room is usually centrally located, where it’s isolated from exterior walls and can be easily and quickly reached by all office personnel in the event of an attack. Most office safe rooms have reinforced walls and doors and are stocked with food, water, backup weapons, and medical and other supplies. Safe rooms are also equipped with cellular phones/modems and portable GenNet terminals, in case communications lines are severed.

BlackEagle personnel are also part of any facility’s defense system. While some of our facilities, namely the training areas, L&P warehouses, and corporate offices, have full-time security staffs, most regional offices do not. In a typical regional office, the administrative staff is the first line of defense. The office receptionist sits at or near the office entry. From there he or she can monitor people entering or leaving the office and trip an alarm if anything untoward happens. In some offices, the receptionist can monitor video of other office areas or even the exterior of the office. Receptionists’ desks are frequently armored. Administrative staff members are trained to deal with emergencies by alerting operatives or other authorities, but not to actually defend the premises.

During times of increased threat, cells or individual operatives may be called upon to maintain a security presence in the office. Normally, available cells low on the Operations Roster are called in first.

Clients and their representatives frequently visit BlackEagle offices. While it is certainly all right for non-employees to come into company facilities on business, their movements within the office should be controlled. Keep non-business visits to a minimum. Certain areas within all BlackEagle offices are designated “secure.” These areas are off-limits to all non-employees under all circumstances. Secure areas usually include vaults, forensics labs, and locker and storage rooms. On occasion, when a situation warrants, an office’s Senior Cell Leader may authorize a non-employee to enter a secure area.

The sidebar on page 69 covers security drill procedures, for dealing with outright assaults of company offices.

Operational Security

Security—that is, the protection of company facilities and information—is of utmost importance to all BlackEagle personnel. It is the company’s experience that most thefts, kidnappings, assassinations, and attacks, as well as many client grievances, can be traced to indiscriminate talk—loose lips—on the part of operatives and other employees. For these reasons, it is imperative to discrete, and to never discuss any BlackEagle assignments or capabilities with outsiders or in locations where they might be overheard.

BlackEagle’s reputation for discretion and integrity is of primary importance to us. Many clients require secrecy concerning our employment, for reasons of public relations, honor, or even legality. BlackEagle honors such requests, and follows a policy of confidentiality even when secrecy is not required.

The safety of operatives also requires secrecy. Carelessness with assignment information can lead to a failed assignment at best, and possibly to the injury or death of operatives involved. Due to the sensitive nature of the information contained in the Operations Roster, it can only be called up on a secure office terminal, or remotely over a secure phone or data connection.

Because BlackEagle’s activities often bring its operatives into conflict with the criminal or terrorist element, it is of paramount importance that offices and safehouses remain secure. Again, don’t discuss any information concerning offices or safehouses publicly.

Security extends to the protection of information stored electronically as well. Standard backup procedures are executed regularly. In addition, an automated back-up system has been installed in every BlackEagle office, in the event that an office is assaulted. If an assault occurs, all office electronic records are immediately dumped via high speed secure satellite link to two other BlackEagle offices. An additional copy is dumped to a storage device in the office’s main vault. Once the information is secure off site, and in the vault, all remaining copies are destroyed. The vault is automatically locked, and any tampering with the vault will cause the storage device to self destruct. Lost information can be recovered from backups off site, but leaked information is gone forever.

Counter-Surveillance Measures

The locations of BlackEagle offices are publicly-known—we’re in the yellow pages in every city where we’ve got an office. Consequently, we must be particularly concerned about surveillance attempts against our facilities. All BlackEagle offices are equipped with a few basic counter-surveillance measures. Many exterior windows are made of one-way tinted or opaqued glass, providing visual privacy. Multiple-pane glass with additional vibration damping is installed to foil laser mikes and other eavesdropping devices. Even with these precautions, however, it’s always a good idea to avoid discussing sensitive information near windows.

BlackEagle offices should be relatively EM clean, with little or no signals leaking from electronics in the office. Any signals broadcast within the office or between the office and an outside location (such as an operatives home via laser-data-link), should be multi-way encrypted.

Some offices have metal and EM detectors at their entrances to scan guests before the receptionist buzzes them in.

All offices have secure phone lines, allowing voice conversations to enter and leave the premises encrypted, to be decrypted off site before entering the phone network. It's still wise to exercise caution when speaking over phone lines with clients—despite all our security their phones may still be bugged. The best method of communicating sensitive information is in person in a secure place, such as the office's conference rooms.

Weapons Policy

BlackEagle/BlackEagle operatives pursue dangerous careers, and most own firearms and other weapons. In order to protect employees from accidents and to make BlackEagle offices less inviting for thieves, there are a few basic guidelines concerning the use and storage of weapons in company offices.

Keep any weapon stored on the premises of a BlackEagle office or facility shall be kept in a gun locker, vault, or other secure area. Stored firearms should always be kept unloaded, with cylinder, slide, or bolt removed. The Senior Cell Leader may authorize a small number of loaded back-up weapons to be kept in a non-secure (but hidden) location, for use if the office comes under attack. Know where these weapons are located, in case they are needed in an emergency.

You may carry loaded weapons in the office. Obviously, however, all weapons should be kept on safe unless they are being cleaned or maintained. Weapons undergoing maintenance should, of course, be unloaded.

It is important to observe all common-sense rules regarding firearms. Careless handling of weapons is not only dangerous to office personnel, but also to innocent civilians nearby. Most BlackEagle offices are located in urban areas, and they often share buildings with other businesses.

done our best to preserve this camaraderie. Our benefits structure reflects this attitude of cooperative support.

General Benefits

BlackEagle/BlackEagle provides a spectrum of benefits comparable to those offered by most professional employers: medical coverage, leave, insurance, etc. For full details, talk to your office Administrative representative. A few particular issues are worth mentioning here:

- **Medical coverage.** BlackEagle covers unconditionally all medical expenses incurred by an operative during the course of an assignment, or directly as the result of an assignment. The company extends this unconditional support to the families of its operatives: if your family ever comes to harm as the result of an assignment or your on-duty activities, they are covered in full. For more mundane health concerns, Administrative Branch can provide you and your family with low cost comprehensive group medical and dental coverage.

- **Leave.** The lifestyle of an operative can be very demanding, both physically and mentally, and the peace of mind of our operatives is critical to our success. For these and other reasons BlackEagle enforces a minimum leave policy. Operatives are required to take a minimum of twelve weeks per year vacation—this reduces burnout and affords operatives time off without worrying about maintaining status among their peers. Some operatives take advantage of the minimum leave policy by working on the legendary and well-earned "BlackEagle lifestyle." If you function better under extreme pressure, take advantage of free training opportunities offered by the Logistics and Procurement Branch.

- **Insurance.** In the event of your death, dismemberment, or serious injury, BlackEagle provides Life and Disability insurance. This coverage is extended at all times. Family members and loved ones who are affected as a direct result of an assignment are similarly covered.

■ Part 5: Employee Policies and Benefits

The same commitment and support for one another that makes our system of cells so successful is present at every level of BlackEagle/BlackEagle. Although the company has grown over the years, we have