SHADOWRUN® 7118

CORPORATE SECURITY™

HANDBOOK

A SHADOWRUN SOURCEBOOK BY MICHAEL E. COLTON AND OTHERS

CORPORATE SECURITY

• A SHADOWRUN Sourcebook •

• IMPORTANT MESSAGE •

FOR _____

DATE _____ TIME _____

M _____

OF _____

MESSAGE _____

FASA CORPORATION

SIGNED _____

STVEECORP FORM 300LZP

TABLE OF CONTENTS

Published by
FASA Corporation
1100 W. Cermak Road
Suite B305
Chicago, Il 60608

FASA Corporation can be reached on the GEnie computer network (E. Mail—FASA.SUPPORT) on SCORPIA'S Roundtable (page 805) and on America OnLine (E. Mail— FASALou (Earthdawn), FASABryan (BattleTech) or FASAMike (Shadowrun and General Harassment) in the Online Gaming area (Keyword "Gaming"). Via InterNet use <AOL Account Name>@AOL>COM, but please, no list or server subscriptions. Thanks!

CORPORATE SECURITY HANDBOOK

Writing
Michael E. Colton
Rob Cruz
Tom Dowd
Diane Piron-Gelman
Sam Lewis
Mike Mulvihill
Sharon Turner Mulvihill

Additional Writing
Rich Osterhout
Jon F. Zeigler

Development
Tom Dowd
Sam Lewis

Editorial Staff
Editorial Director
Donna Ippolito
Managing Editor
Sharon Turner Mulvihill
Associate Editors
Diane Piron-Gelman
Rob Cruz

Production Staff
Art Director
Jim Nelson
Project Manager
Joel Biske
Cover Art
Doug Andersen
Cover Design
Mike Nielsen
Color Section
Karl Waller (Pencils)
Joel Biske (Inks/Colors—Scenes)
Jim Nelson (Inks/Colors—Characters)
Illustration
Peter Bergting
Joel Biske
Liz Danforth
Earl Geier
Mike Jackson
David Martin
Christina Wald
Layout
Steve Bryant

Playtesters
Al Beardsley, Todd Bolling, David H. Hixon, Lyle P. Jaeger, David Wood

INTRODUCTION

The **Corporate Security Handbook** is a sourcebook for the **Shadowrun** game system. The book is designed to help gamemasters use corporate security systems and the personnel who operate them in **Shadowrun** adventures by giving gamemasters and players a feel for how corporate security works in the **Shadowrun** universe and showing how those systems and personnel will affect adventures in game terms. The **Corporate Security Handbook** offers players and gamemasters detailed information on all aspects of corporate security: simple physical measures, sophisticated technical and magical safeguards, internal security and executive protection, and so on. It also includes new weapons and equipment, new rules and game mechanics for many of the security measures described, and new archetypes unique to the corporate security field. No other sourcebooks are required to use the **Corporate Security Handbook.** The **Corporate Security Handbook** is for use with the second-edition **Shadowrun** rules.

Like other **Shadowrun** sourcebooks, the **Corporate Security Handbook** is formatted as an electronic document from that fictional world. Scattered throughout the document are comments and additions from readers anxious to correct, expand, corroborate, or contradict the information it presents. Because this "black" information comes from characters within the game universe, players or characters cannot safely assume that these comments are truthful, accurate, considered, or clearly thought out (though they may be all those things).

The core information about corporate security comes from Knight Errant, a subsidiary of Ares International and a major security provider in the 21st century. This core text is the security handbook Knight Errant provides to new customers to describe what they are getting for their money. As the book is partly a sales pitch, it may exaggerate or even lie about the effectiveness of the security measures described. Individual gamemasters are the final judges of the accuracy of this information. Gamemasters are also encouraged to tailor corporate security measures to fit the needs and capabilities of their individual gaming groups.

WELCOME TO...

SHADOWLAND

"I have taken all knowledge to be my province."
— Francis Bacon, 1592

CATEGORY	*GO TO:*
Message Base/Mail System	OK
Special Category/Topics (SIGS)	OK
Library Archive	OK
Information Base — SPECIAL FEATURES (Limited Duration Posting)	
Knight Errant Corporate Security Handbook	OK
Virtual Realities 2.0 (Faster and More Frightening)	EN ROUTE!
Bug City (Chicago Under Seige)	OK
Lone Star (Cops and their Bad Habits)	OK
Cybertech (More Big Hardware Than Humans Allowed)	EN ROUTE!
Denver Compilation (Treaty City Stuff!)	OK
Prime Runners (Angels and the Baddest of the Bad Guys)	OK
Aztlan (Down and Dirty South of the Border)	EN ROUTE!

CORPORATE SECURITY HANDBOOK

Introduction	OK
History	OK
Physical Security	OK
Technical Security	OK
Magical Security	OK
Matrix Security	OK
Personnel Security	OK
Executive Security	OK
Behind the Curtain	OK
Ares Security Fall 2055 Catalog	OK
Other Information	OK

DOWNLOAD ALL? OK

NOTE FROM CONTROL—Anyone with any knowledge regarding sabotage to this system should contact me ASAP. Censorship will not be tolerated!

HISTORY

Popular opinion marks the *United States vs. Seretech Corporation* Supreme Court decision as the beginning of independent corporate security. In reality, corporate security has a much longer history.

IN THE BEGINNING

Corporate security as we know it began with the private security providers of the mid-nineteenth century. In the early 1850s, public law enforcement agencies failed to develop fast enough to curb the steadily rising crime brought about by an increasingly urban and industrialized society. Independent companies headed by private individuals stepped into the law-enforcement gap, providing the security services the population demanded.

In 1855, Allan Pinkerton established Pinkerton's North West Police Agency. Pinkerton's provided security and conducted investigations of crime on the nation's railroads. In 1857, the agency expanded to include watchman services for various railroads and industries. Pinkerton's eventually became one of the former USA's largest private security companies.

The 1850s also saw the formation of the first protected freight service when Henry Wells and William Fargo formed Wells Fargo and Company in 1852. Wells Fargo provided secure freight transport for routes west of the Mississippi River. In addition to protecting freight they maintained their own detectives and security personnel, commonly known as "shotgun riders." In 1859, Washington Perry Brink founded Brinks, Inc., another freight protection firm. In 1891, Brinks, Inc. transported its first monetary cargo, establishing itself as the first armored car and courier service.

>>>>>(Monetary cargo? Enough cash to fill a wagon? And they just drove the drek from one town to another. Wow!!! Wish I'd lived back then. My life would have been a lot easier.)<<<<<

—Ox (06:06:45/11-29-55)


SECUR
SPECI
OF THE MONT
JANUARY, 2
BOOGIEMEN

In addition to investigation and transport, private security firms soon began providing other services. In 1858, Edwin Holmes offered the first burglar alarm, and in 1874, American District Telegraph (ADT) was founded. These firms installed various security alarms, responded to alarm calls and maintained their own equipment. In 1909, alarm services branched out into another area when Baker Industries introduced the first fire alarms and detectors.

From the 1870s until the early 1940s, private security firms primarily provided services by contract to industry. Though the various firms filled a definite need, their actions were often fraught with controversy. In one spectacular case in 1894, later known as the Battle of Homestead, private security forces physically assaulted and fired on striking workers in Homestead, USA. Throughout the economically depressed 1930s, overzealous private security forces reacted to striking automotive workers with similar extreme tactics.

>>>>>(You mean things like this were happening all the way back then? The more things change, the more they stay the same.)<<<<<

—Slag (07:56:30/11-29-55)

>>>>>(That's a rog. That kind of corporate abuse of workers occurred throughout the late 19th and 20th centuries. During the grand old days of the 1901 Standard Oil, it wasn't uncommon for one oil company to hire thugs to blow up competitors' pipelines.)<<<<<

—The Chromed Accountant (08:09:23/12-01-55)

>>>>>(So great-great-granddad could have been a runner? Wiz!)<<<<<

—Slag (09:11:45/12-01-55)

In general, private security clients did not expand beyond industrial firms until the 1950s. During that decade, private security providers branched out to protect retail establishments, entertainment venues such as restaurants and hotels, and hospitals, to name just a few examples. Security guards and officers were the first line of defense against crime, until security consulting agencies and private investigation firms began to handle fraud, arson, and burglary investigations. In 1954, a new security provider entered the scene when George R. Wackenhut formed the Wackenhut Corporation. Wackenhut soon became the former U.S.A.'s third largest security firm.

As times changed, so did the way private security providers did business. In the 1960s and 1970s security firms created central repositories of security information to decrease losses by networking. This "network" was first used to reduce auto theft, arson, and jewelry theft. Later, it was expanded to include many kinds of fraud, principally insurance and credit card fraud and credit card theft. However, this "network" was not a computerized entity as we now understand the term. For quite some time, various companies shared information by more ordinary means to catch criminals.

>>>>>(Networking without computers and the Matrix? How barbaric. What did they have—rooms full of index cards sorted by name or event? Talk about a lack of efficiency.)<<<<<

—Delunidai (12:54:34/12-03-55)

>>>>>(Actually, for its time it worked quite well. It was the first real attempt to present a unified front against the criminals, and it pretty much succeeded. Imagine Lone Star and Knight Errant sharing information to solve a crime. I don't think so ...)<<<<<

—Dybbuk (13:22:56/12-03-55)

>>>>>(What makes you think Knight Errant needs the Star's help?)<<<<<

—Mindfire (13:26:43/12-03-55)

>>>>>(Attitudes like that keep us in business. Playing the Star off of the Knight is a favorite pastime of mine.)<<<<<

—Doomstar (16:24:41/12-04-55)

THE CONFLICT OVER AUTHORITY

The social breakdown that occurred during the Awakening had its roots in civil disorder stretching as far back as the mid-1960s. Much of the social disruption involved groups of heavily armed private citizens: drug smugglers, street gangs, rogue survivalists, and foreign and domestic terrorists, to name a few. The government reacted to these threats by stiffening existing anti-crime laws, such as increasing restrictions on the availability and legality of paramilitary weapons through gun control legislation.

Governmental authorities soon discovered, however, that weapons were only part of the problem. Training—specifically, the lack of it on the part of law-enforcement and private security personnel—was also a large part of the threat to social order. Until the mid-1990s, most private security personnel did not even get the level of training recommended by the federal government, much less anything beyond that. The accelerating breakdown of civil order made better training and equipment imperative for private security because private forces were often required to take extreme steps to protect assets from marauding mobs. In the government's view, these better-trained and -equipped security forces constituted "private armies" not answerable to governmental authority.

In 1997, the United States Justice Department, in conjunction with the United States Department of Defense, proposed legislation to strictly regulate paramilitary training. Though the legislation targeted the drug lords, organized criminals, and political reactionaries who historically had used paramilitary methods to gain power for nefarious purposes, the proposed law as written would also have prevented private and corporate security forces from effectively training their personnel. For example, live-fire automatic weapons and demolitions training were considered felonies under the proposed bill.

>>>>>(You can read the book but you can't practice. Reaaaal smart. Another example of criminal government stupidity.)<<<<<

—Whisper (09:12:56/12-01-55)

>>>>>(The book said to cut the blue wire, but first ...)<<<<<
—BitRunner (14:46:54/12-02-55)

Civil libertarians fought the proposed law vigorously as an infringement of individual privacy and weapons rights. Corporations fought the law using a more sophisticated argument. They acknowledged that the government had a duty to oppose groups that used paramilitary methods to deprive citizens of their rights, but stated that the government had no compelling reason to prevent corporations from protecting their own assets against the same groups. To do so, they argued, deprived corporations of the legal right to self-defense.

The political and legal battle continued for many months and became a significant issue in the 1998 Congressional elections. The Supreme Court's surprise decision in *The United States vs. Seretech Corporation* in late 1999, however, rendered the question moot. The Court held that Seretech, and by extension all corporations, had the right to maintain and use an effective armed force to protect their assets. The decision implicitly recognized that such a force had to be armed with state-of-the-art weapons and equipment, and also recognized that security personnel required full paramilitary training to be "effective."

Two years later, in 2001, the U.S. Supreme Court rendered the *Shiawase Decision*, which granted qualifying corporations extraterritorial rights. Many other nations followed suit shortly afterward, making it legal for extraterritorial corporations to provide necessary training and weapons to their security forces throughout the world.

>>>>>(Luckily for us the almighty nuyen still drives the corps. Maintaining a well-trained and equipped security force is not a cheap proposition, and so security is one of the first things to get cut when the ol' budget axe swings.)<<<<<
—Bung (13:45:43/12-02-55)

>>>>>(That may be true for a corp's proprietary security force, but what about the contract providers? They bill themselves as state-of-the-art security forces. Those are a force to reckon with.)<<<<<
—BitRunner (13:55:56/12-02-55)

>>>>>(That depends on the corp. Assuming you keep reading this primer, you'll see Knight Errant goes to the extreme to train their employees in the latest corporate security methods. However, plenty of corporate security providers out there skimp on training and equipment to keep costs down. They don't care about the quality of the service, just the nuyen.)<<<<<
—Dybbuk (06:34:23/12-03-55)

>>>>>(So what are you saying? Only go up against a corp that has substandard corporate security? I wish it was that easy. The corps that have poor security don't have the big hauls. How do you bypass them?)<<<<<
—BitRunner (08:45:56/12-03-55)

>>>>>(Simple. Fight fire with fire. Keep up to date on the latest in security. Train continually. If your target gets a new security widget, you need to get one of those widgets, too. Study it. Find out its weaknesses and exploit them. No one said this is an easy life. From what this primer says, running the shadows ain't cookies and milk anymore. You need brains in addition to brawn now.)<<<<<
—Dybbuk (09:00:34/12-03-55)

The breakout of Virally Induced Toxic Allergy Syndrome (VITAS) in 2010 helped solidify the hold that providers of corporate security had on protection of corporate assets. As the VITAS plague spread throughout the world, corporate facilities closed their doors to outsiders in hopes of keeping the virus from spreading to their personnel. On many tragic occasions, security guards were forced to fire upon angry mobs clamoring for the medical supplies hoarded by corporate medical departments.

As chaos and rebellions erupted throughout the world, governments toppled and corporate security personnel were forced to defend corporate facilities as an army would defend a nation. Paramilitary training was stepped up and many corporations became armed camps.

>>>>>(You should have seen it back in those days. CorpSec boys were wearing camo and carrying enough firepower to take out a panzer. In fact, quite a few mercenaries found easy employment as "security consultants.")<<<<<
—Primus (21:02:34/12-01-55)

SECURITY IN THE AWAKENED WORLD

With the advent of goblinization and Unexplained Genetic Expression (UGE) in 2021, corporate security providers faced yet another problem. Each corporation's own personnel began to change in unexpected and often frightening ways, causing riots within corporate boundaries. The experience of firing on co-workers they had formerly protected caused many members of security forces to question the corporate managers who gave the orders, and morale plummeted. The declaration of martial law by the U.S. government in 2022 only made matters worse. Many of the goblinized workers—security guards and officers among them—went into hiding, eventually building communities of their own. Staggering personnel losses only intensified the morale problem among those left behind.

The rise of magic during the Awakening further disrupted old ways of doing business, as the new threat to security forced security-system designers to radically rethink their tried-and-true methods. Magic contradicted many, if not all of the scientific principles previously used to develop security systems. A magician in astral form could easily penetrate even maximum-security installations because no known security countermeasures existed to defend against such a threat. To counter magical security breaches, corporate security executives tasked their security engineers to develop appropriate defenses and began hiring and training as many magicians as they could find. Unfortunately, regular background checks were thrown to the winds during this hiring spree, and more than a few unscrupulous individuals joined the ranks of corporate security providers.

The hiring bonanza ended in early 2029 when a far greater threat to society grabbed center stage. On February 8 of that year, an unknown killer virus struck computer systems across the world. Computer security officers and system administrators scrambled to shut down their systems, but in most cases failed to beat the virus. Corporate losses worldwide were staggering, as gigabytes of vital data was irretrievably corrupted or destroyed. A panicked UCAS government set the Echo Mirage project in motion to combat this new threat.

Echo Mirage consisted of personnel from several government agencies dedicated to the exploration and exploitation of cyberterminals and cyberspace; it became their job to contain and wipe out the virus. Leaders of Echo Mirage drafted the best of the corporate world's computer security personnel and designers, whose departures caused further damage to corporate databases. The new government "super hackers" developed new ways to access corporate data systems in their hunt for the elusive killer virus. These activities sent shudders throughout the corporate security field as the corporations realized how vulnerable their computer systems had become to unauthorized access. Executive officers turned to their research staffs, who came up with various state-of-the-art intrusion countermeasures (IC) programs to counteract penetrations of corporate databases. Unknown to the corporations, Echo Mirage personnel copied these IC codes and modified them to help contain the killer virus. By November of 2031, the last remnants of the virus had vanished from the Matrix.

>>>>>(Along with the head of Echo Mirage, David Gavilan. For those of you who can't see why I bring that up here, check out my 4-14-54 post in the Corporate Shadowfiles entry on Ares.) <<<<<

—Eddie Monster (11:04:55/12-10-55)

The following years saw the complete development of the Matrix, and with it Matrix security. Virtually all corporations beefed up their Matrix security sections and developed computer hardware and software to support them. Corporate security providers also developed effective magical security countermeasures, often hiring the magically talented. In the modern era, most corporations of any significance can defend themselves against physical, magical, and Matrix-based breaches of security.

MODERN SECURITY SERVICES

The grand old dame of modern security services is Lone Star Security, Inc. Founded in 2017 by Clay Wilson, Lone Star began its rise to national prominence when it landed its first metropolitan law enforcement contract in 2020 with the city of Corpus Christi. Specializing in municipal and governmental security contracts, Lone Star now provides police services to most cities throughout the UCAS, CAS and Québec. The massive organization of the Star rests in solid opposition to street crime and unauthorized use of the Matrix.

>>>>>(I thought this was a Knight Errant sell sheet. Why talk about how big and successful the Star is?)<<<<<

—Slag (04:03:20/12-07-55)

>>>>>(My dear little trog, don't you understand the subtle nuances of advertising? The key phrases here are "old dame," "massive," and the emphasis on the Star's multiple municipal contracts. How many wage slaves believe their city streets are safe? Not many. Think hard—who's to blame? That huge, slow, bureaucracy-bloated old woman—Lone Star. So who can protect us poor, defenseless sararimen? The lean, mean Knight Errant machine. A very effective backhanded cut.)<<<<<

—Keynesian Kid (04:35:21/12-07-55)

In recent years, multiple small security organizations have been founded in the hope of emulating Lone Star's success. Undercapitalized and using inadequately trained staff, most of these small providers cannot offer their customers a fully layered security blanket for a corporate site, nor can they adequately protect or screen corporate employees. These organizations have their uses against opportunistic amateur criminals, but greater resources and sophistication are needed to defend against corporate-backed threats and talented freelancers.

>>>>>(Time for the commercial.)<<<<<

—Keynesian Kid (04:44:32/12-07-55)

Knight Errant Security Services

After taking control of Ares Macrotechnology in 2033, Damian Knight created Knight Errant Security Services by buying outright the remnants of ADT Security Providers. Determined to make his new company a market leader in security services, he ordered its executive officers to concentrate on perfecting corporate security procedures and developing top-notch security countermeasures. Dedicated to providing megacorporate-level security to large and mid-sized companies at competitive prices, Knight Errant swiftly emerged as one of the top corporate security providers in the world. The company deservedly retains that distinction to this day.

>>>>>(That's it? No deep background on the Knight's development? No long discourse on the great and wonderful Damian Knight? I feel used and abused. Left wanting at the height of passion!)<<<<<

—Slag (03:45:22/12-12-55)

>>>>>(Oh, get off it. On second thought, don't. If you want deep background on the Knight machine, check out the entry on Ares in the Corporate Shadowfiles post. For you impatient types who want everything right now, I'll do a quick surf through the Knight's formation. So settle down and let your Aunty Neo-A tell you a story.

In 2033, two days after the global stock market reopened, Damian Knight sat down at a cyberterminal in Stockholm, Sweden. He plugged a stock-trading expert system into the Matrix, and one minute later he owned 22 percent of Ares Macrotechnology. That big a chunk gave him control of the megacorp.

Right away, Ares' new owner took steps to establish Knight Errant. Damian Knight combined all of Ares' corporate security forces into his new baby, and plowed the overhead savings into

the buyout of ADT. ADT didn't have much left in the way of assets, but it had a few outstanding corporate security contracts: just enough to start the ball rolling. Ares personnel and equipment plus ADT contracts spelled Knight Errant Security Services.

The first few years of the Knight's existence were deadly for runners who took jobs against the Knight-guarded corps. Knight Errant went to extremes to make its rep. Samurai and chromed bikers who poked a toe onto corp territory got thrown out on their ears, leaving a body part or two behind. The rumor mill claimed the Knight gave a few bothersome magicians a ride on a deep-space probe. Shadow deckers learned the hard way to respect Knight Errant's software; it wasn't state-of-the-art, but its architecture was still far enough on the razor's edge to slit many a Matrix runner's throat.

After a dizzying 18 months of playing with his security toy, Damian Knight started paying attention to the rest of Ares Macrotechnology. He turned Knight Errant's reins over to Roger Soaring Owl, the current ExecVeep and COO. Knight Errant's rep brought flocks of new contracts, as did the fact that KE's main rival—Lone Star—was bogged down in municipal law enforcement. KE started to skim the cream of the corp-security crop, picking and choosing the most lucrative and high-profile contracts. Today's KE is a first-class organization that earns every nuyen it charges.

One interesting side note: Ares has set up a low-cost security supplier, Hard Corps Inc., to take care of mid- to small-sized firms and those that might be bad for KE's rep. Hard Corps is a natural extension of Damian Knight's business strategy; he works his way down from the most profitable markets to the most marginal. No wonder the guy's rolling in green stuff.)<<<<<

—Double Janet (06:35:44/12-12-55)

>>>>>(I've heard some interesting dirt on Hard Corps. They get a lot of seconded personnel from Ares Arms and KE. Scary types; you know, the Desert War vets so chromed you don't know if their hearts pump blood or hydraulic fluid. So corps that KE won't touch for fear of bad PR get visits from Hard Corps salesmen? Looks like Hard Corps is doing KE's dirty laundry.)<<<<<

—BitRunner (08:22:31/12-12-55)

>>>>>(Not what I've heard, friend. Hard Corps is part of an internal power struggle between Damian Knight and Ares' chairman of the board, Nicholas Aurelius. Those seconded vets in Hard Corps are Aurelius' private little army, in case the power struggle gets out of hand.)<<<<<

—Nuyen Nick (10:33:43/12-15-55)

PHYSICAL SECURITY

Physical security is the fine art of keeping uninvited guests out of your corporate site. Fortunately for the security provider (and for the customer), would-be interlopers have a finite number of ways to break in. Whether entering grounds or buildings, bypassing fences or walls, intruders must go under something, over something, or through something to get inside. Therefore, effective physical security must simply block access upward, downward, and from all sides.

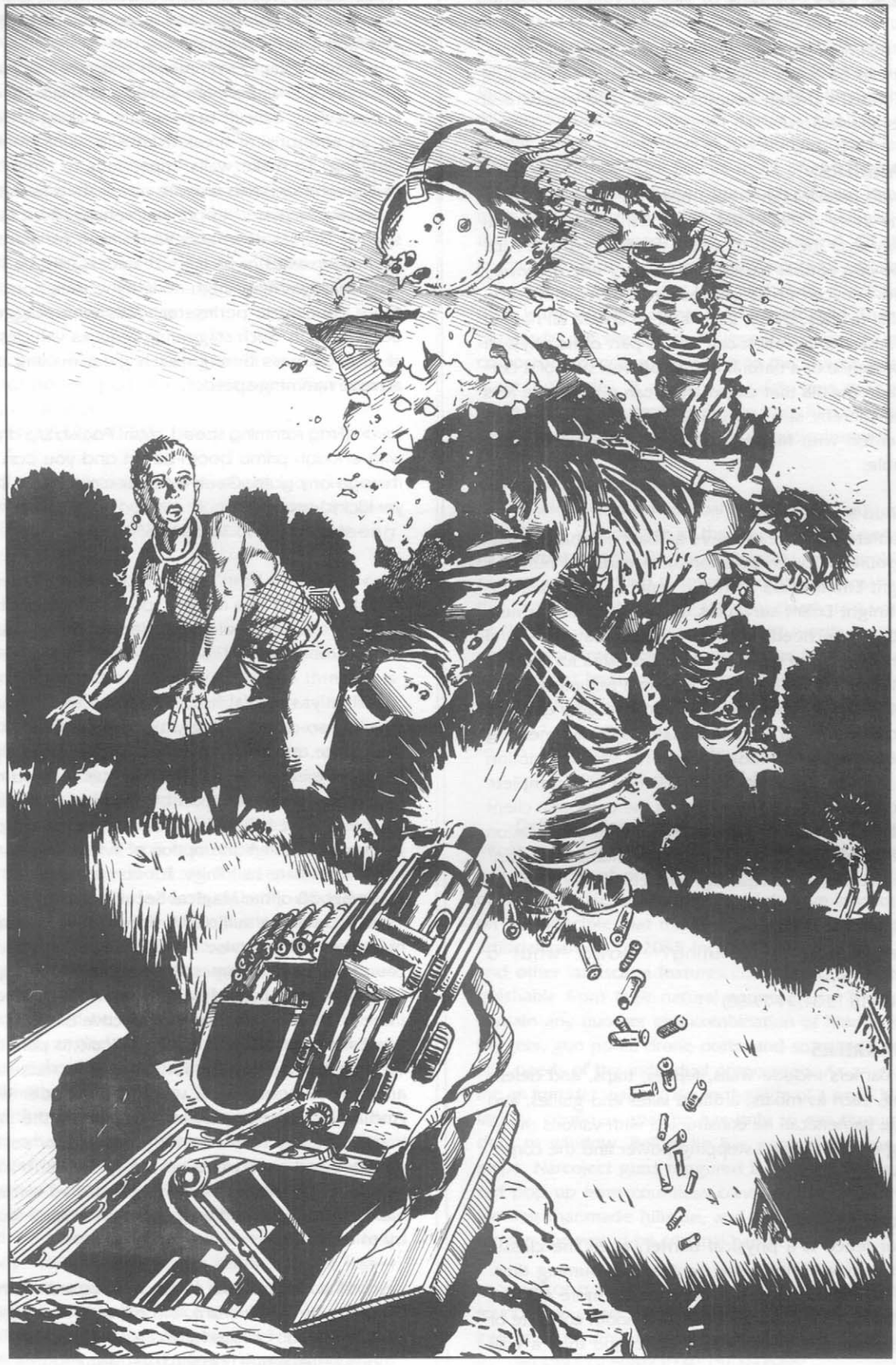
Most uninvited guests are dedicated to whatever act of espionage or theft they intend to commit, and they are also endlessly inventive. No single form of protection can keep a dedicated intruder out of a corporate compound; to be truly effective, security must consist of multiple defensive layers. Perimeter, grounds, individual buildings, and sensitive areas within buildings all need the best protection your hard-earned money can buy. Therefore, Knight Errant Security recommends a varied menu of security options, including both purely defensive and containment measures. Strategically chosen sites for new corporate installations, state-of-the-art manmade physical barriers and strategic lighting, wire and laser traps, sturdy and efficient security drones, and guard patrols equipped with the latest cyberware and topnotch training are just a few of the choices available from Knight Errant.

>>>>>(Fortunately for us dedicated liberators of corporate secrets and other drek, lots of corps can't afford the kind of state-of-the-art package KE's pushing.)<<<<<

—Bashful (16:10:12/12-18-55)

>>>>>(Yeah, but most of the scrimpers don't have anything worth snatching.)<<<<<

—Jesse James (16:15:45/12-18-55)



PERIMETER DEFENSES

Perimeter defenses are the barriers that enclose your corporate site. They can be either natural or manmade, and include walls, fences, traps, lighting, sound barriers, and mechanical devices such as attack drones.

NATURAL BARRIERS

Anyone who recalls high-school history lessons probably remembers the story of Hannibal, the Carthaginian general who led an army over the Alps to attack the Romans. The Alps are an example of a natural barrier: a boundary line drawn by Nature that no one can cross without enormous difficulty. Mountains, cliffs, ravines, rivers, lakes and so on are all natural barriers that a smart corporation can use as part of its physical security. The presence of a natural barrier on one side of a corporate installation means that corporation can put up one less perimeter wall, thereby saving money. A natural barrier can also be augmented with hidden security devices to make it truly impregnable.

Strategic Location Scouting

Many corporate sites already have at least one natural barrier on their grounds. For corporations interested in building new sites, Knight Errant offers a unique service: *strategic location scouting*. Knight Errant surveyors, armed with all the necessary data about the needs of the new installation, travel throughout the corporation's preferred general area for the site and seek out a location with the best possible natural barriers. Through consultation with experts in technical security devices, our surveyors create a list of recommendations for augmenting existing natural barriers with hidden gun ports, sensors, motion detectors, and the like. These recommendations and complete data on the proposed site are presented to the corporate client for a final decision. The modest service fee for strategic location scouting is well below the cost of building the number of manmade barriers necessary to adequately protect sites lacking natural defenses.

>>>>>("Strategic location scouting?" Gawd, what a phrase!)<<<<<

—Jargoneur (15:12:31/11-27-55)

MANMADE BARRIERS

Manmade barriers include walls, fences, traps, and defensive landscaping, such as moats, artificial lakes and gullies, and so on. Manmade barriers can be constructed with various materials, depending on the desired stopping power and the corporate security budget.

Walls and Fences

Any wall or fence is a physical barrier, even the classic white picket fence or an improvised barricade of burning tires. Some kinds of walls and fences, however, are far more efficient at keeping out intruders than other kinds. A smooth concrete or plascrete wall several feet thick does a better job than a wall made out of wood or stone blocks; wood is flimsy enough to ram a vehicle through, and a stone-block wall provides hand- and footholds for scaling.

Knight Errant recommends concrete and plascrete as building materials, as both are sturdy and relatively cheap. Plascrete is particularly difficult to penetrate, making it extremely difficult for an enterprising break-in artist to sink hooks or pitons for climbing. To make walls impervious to ramming attempts by heavy vehicles, walls may be constructed as thick as structurally necessary or placed to prevent vehicles from building ramming speed. The latter option works well for gates and doors in perimeter walls, which must necessarily be light enough to open easily. Many high-security installations feature two or more concentric perimeter walls with staggered gates and doors in each. Such staggering requires vehicles to make several turns to pass through each gate, making it impossible to achieve ramming speeds.

>>>>>(Frag ramming speed, man. Pack a big drone or a vehicle with enough primo boom-boom and you can blow your way through any gate. Geek a few sec-patrols at the same time, if yer lucky.)<<<<<

—Animal (10:15:36/12-11-55)

>>>>>(Like that hasn't occurred to security system designers. You still need a little running space for the car bomb to work—and any decent set of barricades won't give you any.)<<<<<

—Architeck (11:21:36/12-11-55)

Finally, magical intrusions may be discouraged by constructing so-called "living walls" with organic material either on the surface or in the core. The least expensive type of living wall is ivy-covered on both sides, but this method only works well for exterior walls. The recent innovation of so-called "fat" bacteria, developed by a wholly owned subsidiary of Ares Security International, offers the option of living walls to safeguard areas inside corporate buildings. For complete details on "fat" bacteria, see p. 38 of the **Magical Security** section.

Of course, a sufficiently inventive and dedicated criminal may eventually devise a way to scale any wall. One further countermeasure a corporation can take is to top the perimeter wall with wire. Barbed wire, monowire, or electrified wire are three of the most popular and effective choices.

Barbed wire is extremely difficult to penetrate; the twisted X-shapes dotting the longer wire strands can snag clothes and gear, entangling a would-be intruder within seconds. And barbed wire merely inconveniences the intruder. Though it will certainly hold him long enough for security personnel to arrive and escort him off the premises, it does little to no lasting harm. Monowire and electrified wire, on the other hand, will cripple and may even kill anyone foolish enough to try to cross them.

>>>>>(That little piece of KE doublespeak translates as, "Use barbed wire if you want 'em alive. If you want 'em cooked, we'll set that up all nice for ya.")<<<<<

—Masterblaster (17:02:03/10-09-55)

>>>>>(Monowire can be lethal, depending on how high up they set it from the top of the wall. You can hardly see it, and it cuts through just about anything. You step through it to jump down onto the other side of the wall and you may lose a foot, or your whole leg. Then you'll either bleed to death or the thugs with guns'll geek you.)<<<<<

—Reality Czech (12:06:04/10-11-55)

Mildly charged electrified wire does no damage at all to the interloper, but instead triggers an alarm that alerts security personnel to the intruder's presence. Slightly higher levels of current may temporarily stun an intruder, or interfere with his cyberware if he has any augmentation. Very high levels of current, of course, will do permanent damage.

>>>>>(Very permanent. The corp slags'll be oh so sorry to see your cooked meat hanging off the electric wire. They didn't mean to cack you ...)<<<<<

—Jersey City (13:05:57/2-13-56)

>>>>>(I've heard some corps use low-level electric wires and fences to trigger gun ports. The wire don't hurtcha at all—a machine gun chews ya up instead. Snip snip, bang bang!)<<<<<

—Leadboy (10:34:16/3-11-56)

Fences can also be electrified, with the same results. Barbed wire, chain-link, and concertina wire can all be electrified.

Chain-link fencing is the most popular of the three; it is inexpensive, sturdier and more aesthetically pleasing than barbed or concertina wire. Modern-day chain-link is available in either galvanized metal or a high-strength polymer, either of which will conduct electricity. An effective chain-link fence, such as those commonly installed by Knight Errant, should be at least 2 1/2 meters high and no more than 5 centimeters from the ground: tall enough to keep a troll from easily climbing over, and with a gap at the bottom too small for even the smallest (meta)human to wriggle under. In loose or badly eroded soil, the bottom edge of the fence should be sunk below ground level. To make it more difficult to knock down, the fence should be fastened to rigid posts set in concrete, with additional braces where necessary at corners and gate openings. For additional security, the fence should be topped with multiple strands of stretched barbed wire, angled at 45 degrees from the protected area. This overhang should increase the height of the fence by at least 25 centimeters. If buildings, trees, or other vertical objects are within three meters of the fence line on either side, use a Y-shaped overhang; the branches of the Y will prevent a determined climber from using the vertical as a means of ascent or descent. To protect against washouts or channeling underneath, dig culverts at natural drainage points. The openings of culverts should be sized to keep out even the smallest (meta)human body—roughly 625 square centimeters or less—or else should be protected with metal bars to permit proper drainage. The gaps in a chain-link fence should be as small as possible; metahuman races such as dwarfs and elves often have smaller or more slender feet and hands than the average human, and may be able to find hand- and footholds in standard-sized fencing where humans or larger metahumans cannot.

Concertina wire is coiled steel or high-strength polymer wire. Generally, it is sold in lengths that form a barrier 15 meters long and 1 meter high when stretched. Originally used by the military for building perimeter fences quickly and easily, it commonly appears nowadays at low-budget, quick-built or pre-fab sites. Concertina-wire fences most often consist of two coils stacked atop each other or three coils laid out in a pyramid. The ends of each stretched coil are securely fastened together and the base wires staked firmly to the ground. Of all fences, concertina wire is one of the most difficult to penetrate.

One advantage that wire and chain-link fences have over walls is the simple fact that they are not solid. Through the fence, passers-by can see any skullduggery that may be going on inside corporate grounds and report it to the nearest local law enforcement authorities. If an intruder safely gets over a solid wall or fence, the very barrier intended to keep him out shields him from prying eyes as he goes about his nefarious business.

Defensive Landscaping

Traditional manmade barriers such as walls and fences are not always appropriate as the sole means of perimeter defense at a corporate site. They are unsightly and intimidating and can convey an unsettling impression of the corporation to prospective customers. Also, they say very clearly to a would-be intruder that the site contains something worth protecting. For the corporation interested in subtlety, or for whom a relaxed and inviting first impression is vital, Knight Errant offers a valuable service known in the security industry as *defensive landscaping*.

>>>>>(Another jargon gem!)<<<<<

—Jargoneur (16:46:51/11-27-55)

Defensive landscaping refers to the construction of artificial versions of natural barriers. The moats of medieval castles are one example of defensive landscaping, though it is the most obviously artificial. Modern-day defensive landscaping is based on the principle that the best security is the least obvious; the artificial barriers of 2055 include manmade lakes, hills, gullies, and other landscape features constructed so as to be indistinguishable from their natural counterparts. These barriers may contain any number and combination of hidden sensors, alarm triggers, gun ports, drone ports, and so on, tailored to the specific needs of the individual corporation. As an example, imagine an intruder walking down the side of a small hill toward your facility, confident that he has only to get through the nearest door or window. Before he has gone more than two or three steps, Narcoject guns triggered by motion detectors under the turf pop up from countless concealed ports in the innocuous-looking manmade hillside, and a barrage of tranquilizer darts renders the would-be criminal harmless.

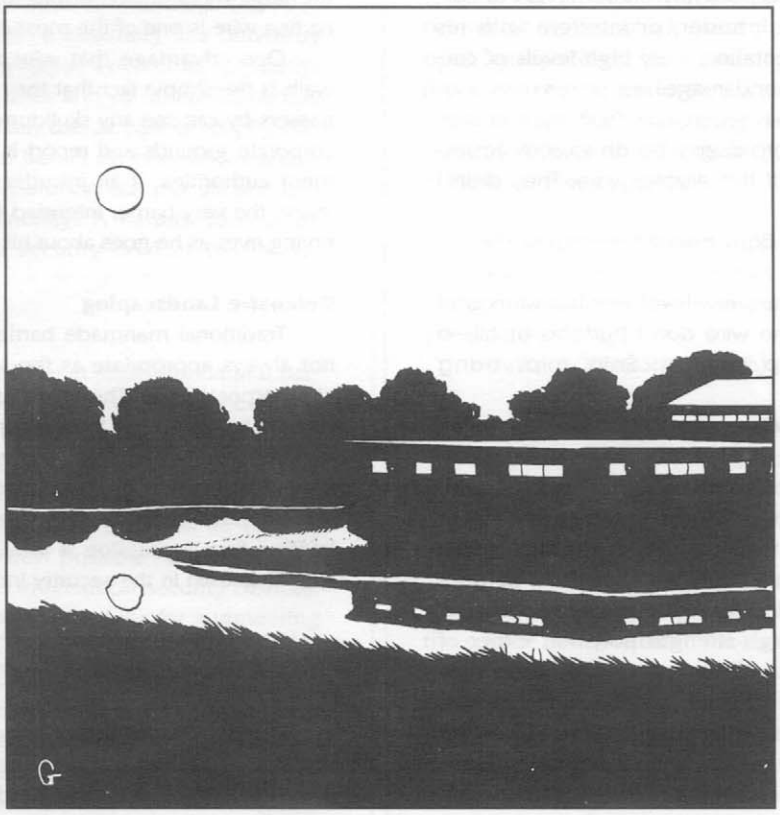
>>>>>(Tranq darts?!! Try cop-killer exploding bullets, or gel rounds—or worse. What's with this pose that the corps are even interested in non-lethal protection?)<<<<<

—Little Cat Feet (10:40:15/09-06-55)

>>>>>(It's a sales brochure, Cat. A surprisingly honest one in some ways, but still a big sales brochure. The corp exec slags who eyeball this can pretty well read between the lines and buy themselves KE's very best killer protection—and I mean that literally—while maintaining the polite fiction among themselves that they're just a bunch of nice businessmen who only want to protect their justly earned profits.)<<<<<

—Libertarian (10:56:31/09-06-55)

>>>>>(Me and a coupla my best bizboys took a line to crack an Ares bopshop, snugged away across a crick and up top of a little hill. They had a fence, electric, that we punched through fine. Few minutes later, our decker sez he's got the central comp dancing to his tune—door's open, walk right in. So we head up the slope and inside—right smack into the empty ends of a coupla dozen SMGs. Lucky me, I was bringin' up the rear—so I bailed back for the fence, fast. On my way down the hill, what do I see but a whole buncha drones that come outta holes in the ground—camera-eye fraggers, not hooked into the main comp. These little buggers felt us walkin' over 'em, popped out and took our mugs after we jandered by, then squealed to the secboyz inside. We never even saw it comin'.)<<<<<



—Uptahere (11:56:10/9-14-55)

>>>>>(I hear there's a few biotech labs out there who've stocked artificial lakes on their grounds with all kinds of weird wildlife. Piranha-flying fish crosses that'll jump out of the water to chomp on you, paracritters that'll curl your hair—you name it, they've probably gengineered it.)<<<<<

—Rifkin II (14:02:04/9-18-55)

Another advantage offered by defensive landscaping is the ability to easily combine physical and magical defenses. An artificial lake, for example, creates a natural home for a water elemental.

Traps and Other Safeguards

Most discussions of manmade barriers begin and end with the wall, fence, moat, and so on, as if nothing more can be done to stop the intruder who successfully breaches the perimeter until he or she attempts to penetrate the facility itself. In truth, the wall is only the first line of perimeter defenses. Various types of traps and additional safeguards, from the primitive to the complex, can contain or temporarily disable an intruder who manages to penetrate the wall. The examples discussed here are only a few of the many possibilities for safeguarding your facility.

The most obvious safeguard, and the one most often used, is the "no man's land." A no man's land is a strip of clear ground between a perimeter barrier and outlying buildings, or between two concentric perimeter barriers, wide enough to permit security forces a clear field of fire. Often, a no man's land also contains obstacles that impede an intruder's movement without being large enough to provide cover: rocks, contoured ground, wire or infrared-beam mazes, and so on.

>>>>>(I hear Ares seeds the no man's land at most of its sites with mines. BOOM!)<<<<<

—Billy Boy (12:16:14/12-10-55)

Mazes of wire or infrared beams can also be used independently of a no man's land. Knight Errant designs and constructs all maze traps to the individual client's specifications. Monowire mazes are relatively inexpensive, though prospective buyers should be aware that these mazes will almost certainly maim or kill any intruder unlucky enough to fall foul of them. Mazes of crisscrossing infrared beams can be designed to trigger alarms or gun ports.

Another type of trap that has gained popularity in recent years is the classic "tiger-pit" trap. Economical and easy to build, a tiger pit consists of a deep hole camouflaged by covering material that will not bear significant weight. The covering material blends in with the surrounding ground, hiding the trap below from the intruder. When the intruder steps onto the covering, his weight breaks through it and he plunges into the hole. He remains trapped until security personnel retrieve him for questioning.

LIGHTING

Security lighting has two purposes: to ensure the swift detection of intruders and to create a psychological deterrent against break-in attempts. Ideal lighting must eliminate shadows in which an interloper can take cover and enable security

personnel to see clearly for considerable distances while blinding the would-be criminal with glare.

Whenever possible, lighting fixtures should be located within the facility's perimeter, shedding their light outward. The farther outside the protected area the lighting extends, the greater chance of detecting an intruder's approach. A fifty-meter range of illumination allows security personnel to see intruders from a reasonable distance and take appropriate action. If a perimeter follows the curve of a river or lake shore, particular care must be taken to eliminate pools of shadow. In shoreline installations, docks and piers offer the best potential hiding places and so must be well lit from several angles.

Perimeter lighting fixtures should be placed to prevent intruders from tampering with or disabling them. A ten-meter gap between the perimeter boundaries and standing lamps or other light fixtures is the minimum standard distance that Knight Errant advises, well out of reach of anyone who might have managed to scale a wall or fence. Needless to say, all perimeter light sources should have a backup power source so that if a blackout occurs, whether natural or otherwise, this vital component of your facility's physical security can continue to function at peak efficiency. Depending on a corporation's specific needs, more than one backup power source may be desirable. Knight Errant will install all backup power sources in spots as inaccessible as possible.

Security lighting can be activated by photoelectric cells, timed switches, or manually. Photoelectric cells, which turn lights on and off automatically when a certain surrounding light threshold is attained, are by far the most desirable because power outages do not affect them. Timed switches also work reasonably well, though they are vulnerable to power cutoffs. If timed switches are connected to an overall computerized security system, they also become vulnerable to tampering by illegal deckers. Manual switches avoid computer access, but can be tampered with more easily than any other type of switch because they must be placed where legitimate personnel can reach them.

>>>>>(I can't believe they're blathering on this much about lights. Bo-ring!)<<<<<

—Slag (18:21:56/12-03-55)

>>>>>(Force yourself to pay attention, cobber. A good runner scopes out every security angle before going in—even the lights. Any piece of info just might come in handy.)<<<<<

—Rodin (18:30:47/12-03-55)

The five standard types of lighting used for security purposes are incandescent lights, fluorescent lights, gaseous-discharge lamps, quartz lamps, and active infrared lights. Incandescent lights are the kind commonly used in the home and light up instantly when turned on. Relatively inexpensive, incandescent light bulbs are available in various wattages and often have interior reflective coating and built-in lenses to focus or diffuse the light. They can also be installed in fixtures that produce the same result. The many types of incandescent lights can suit a wide variety of security needs.

Fluorescent lights and fixtures can also be easily obtained at reasonable prices. Because they are more efficient, however, they cost even less to operate. Both fluorescent and incandescent lights are the best choice wherever instant light is needed for a short time.

Gaseous-discharge lighting refers to mercury vapor or sodium vapor lamps. Both types are more efficient and longer-lived than either incandescent or fluorescent lamps, with low-pressure sodium vapor being the most efficient of all. A mercury vapor bulb gives off a blue- or green-tinged light with a brightness ranging from 30 to 63 lumens per watt; high-pressure sodium vapor lamps shed yellow light with a brightness of 63 to 140 lumens per watt; and a low-pressure sodium vapor lamp sheds a deep gold light with a brightness of 100 to 183 lumens per watt. Sodium vapor lamps are an ideal means of lighting foggy areas, because yellow or gold light penetrates fog better than white light. On the debit side, gaseous-discharge lamps must have high initial voltage to strike an arc. In plain English, this means that they take two to five minutes to light when cold and even longer to re-light when hot—for example, after a power failure. The cost of initial installation is also much higher than for incandescent or fluorescent lamps. However, the longer life of the bulb and the more efficient use of electricity may offset the initial expense. Vapor lamps are best used for exterior lighting that comes on at dusk and remains on all night.

Quartz lamps combine the best of both worlds; they emit an extremely bright white light that provides excellent visibility and turn on as quickly as an incandescent lamp. Quartz lamps of 1,500 watts or better make an excellent choice for lighting around perimeter barriers and in known trouble spots. However, the expense may well be beyond the means of some corporations.

Active infrared lighting is ideal for corporations interested in unobtrusive security measures, where large numbers of security personnel have natural or augmented thermographic vision. To the standard human eye, active infrared light is invisible. However, to a metahuman with heat vision or an individual augmented with thermographic goggles or cybereyes, an active infrared spotlight is as bright as a quartz lamp. An intruder without such vision enhancements can walk right through an area lit by active infrared lamps and be completely unaware of the existence of such a security measure; but security personnel with the right abilities can see well enough to take appropriate action.

>>>>>(Some corps use low-level lighting in the Tir. They cover protected areas with low-watt incandescent lamps, which provide enough light for the elves to see by. Their low-light eyes let them see to shoot, while us poor slots without such vision enhancements are stumbling around in the shadows.)<<<<<

—Lang (13:10:02/10-16-55)

SOUND SYSTEMS

A recent innovation in the security trade, high-amplitude sound is an effective, if costly, method of repelling intruders or rendering them harmless. The home and car alarms of the past century often relied on sound to attract unwanted attention to

would-be interlopers, forcing them to flee to avoid capture. Some modern-day sound alarms still fulfill this function, but newly developed high-amplitude sound systems do far more than that. White-noise generators installed in perimeter walls flood the immediate area with several frequencies of high-amplitude sound, capable of shattering microprocessor crystals in smartguns, cyberware, and various other forms of high-tech equipment commonly carried by the criminal element. His gear and augmentations suddenly rendered useless, the interloper will swiftly depart before security personnel catch up with him—if he can. Sudden jolts of white noise can also incapacitate intruders by overwhelming their hearing; an intense enough barrage of sound can cause acute pain and disorientation, immobilizing the criminal long enough for security guards to reach him. Clients considering the installation of high-amplitude sound systems, however, should be aware that too high a sound level may render intruders permanently deaf.

>>>>>(So what're we gonna do? Sue the corp?)<<<<<
—Slag (14:36:01/11-16-55)

>>>>>(You'd be surprised what you can get away with. There was a case in the 1980s where some joker tried to end it all by leaping onto the elevated train tracks in Chicago. The train ran over him, all right, but it crippled him instead of killing him. He sued the Transit Authority over it and won.)<<<<<
—Legal Beagle (14:48:10/11-16-55)

>>>>>(Nawww ...)<<<<<
—Slag (15:01:16/11-16-55)

Aside from the possibility of inflicting permanent damage, the one remaining drawback to the high-amplitude sound system is its high cost. However, a corporation with a large enough budget—or assets in need of this level of protection—will find the investment more than worth the price.

MECHANICAL DEFENSES

Mechanical defenses include devices such as gun ports and drones. Used in conjunction with natural or artificial perimeter barriers, they are an indispensable part of your overall security blanket. These devices can be combined with various kinds of sensors and detectors; for more information, see **Technical Security**, p. 24.

Gun Ports

The gun port is a simple mechanism, easy to install and conceal. Any one of various guns, a servo motor, and the appropriate type of belt-fed ammunition are all installed in a box or behind a sliding panel in the wall. When an intruder triggers the detector to which the gun port is connected, the box opens (or the panel slides back) and the gun opens fire with rubber bullets or mild tranquilizing darts. To ensure that the target is hit, gun ports can be designed to "sweep" across a wide field of fire.

>>>>>(Funny how lethal those "rubber" slugs can be when they're being spat at you out of a minigun ...)<<<<<
—Brady (03:36:54/11-05-55)

Drones

Drones, automatic or remotely operated by a rigger, can be equipped with cameras for surveillance purposes or with various types of more direct countermeasures.

>>>>>(Guns, chummerboyz 'n' girlz. Think guns. Big, nasty, chew-ya-to-bits guns.)<<<<<
—MamaKnowzBest (04:50:20/11-06-55)

Wheeled, tracked, hovercraft, and rotor-equipped designs are all available, allowing the corporate client to use drones to cover various types of terrain. For additional information on drones and on the function of riggers in your overall security system, see **Technical Security**, p. 32.

BUILDING DEFENSES

Building defenses come into play when and if an intruder breaches the perimeter defenses and actually reaches a building on your corporate site. Building defenses include exterior and interior walls, windows, doors, and locks, as well as containment measures. Properly designed exterior walls, windows, and so on keep criminals from getting in; interior walls, doors, locks, and containment measures keep them from getting too far or reaching sensitive areas if they manage to make it inside.

WINDOWS

Once an easy means of ingress for intruders, today windows can be made virtually impregnable. Ideally, windows should be made of sturdy materials, covered with additional physical barriers wherever possible, equipped with sturdy locks, and integrated into an overall alarm system.

The framework, sashes, and panes of a standard window can be constructed of or reinforced with materials that will make it extremely difficult to break through them. The glass window pane, once the weakest link in any building's security chain, is rapidly becoming a thing of the past. In addition to such reinforced materials as tempered glass, safety glass, reinforced armor glass, and polycarbonate glazing, window panes can be made of fiber-weave plastic composites, polymer composites, and even transparent construction plastic.

The various types of glass are designed to resist heat, flame, cold, and breakage. Safety glass is the least expensive but is also heavy and difficult to install. Wired glass has a wire mesh embedded in it that holds the glass together even if the window is broken, and it is lighter than safety glass. However, an intruder can batter through it given sufficient time. Reinforced armor glass has almost unbeatable stopping power, but is heavier and somewhat more expensive than safety glass. Tempered glass is much lighter, but also less effective; its level of breakage resistance is intended primarily to protect people from flying shards. Of all the types of window glass still in use, polycarbonate glazing is the best value; though considerably lighter than safety or armor glass, it is impervious to the impact of all but the largest rounds of ammunition. Though not inexpensive, polycarbonate glazing is more reasonably priced than the other types of glass that offer similar levels of protection.

Industrial-strength plastics have been used as window material since the latter half of the past century, but only in the last few decades have they come into wider use. The best of the lot, fiber-weave composites, first appeared on the market two to three years ago and have made steady inroads ever since. Increasingly popular alternatives to glass, they offer topnotch breakage resistance and stopping power, but are much lighter and therefore easier to install. They are also much more difficult to cut than most types of glass, and many of them also conduct electricity. When connected to an alarm system sensitive enough to register even the most minute fluctuations in a low-level electric current, these windows are impervious to all attempts to cut through them. Knight Errant also recommends installing windows with frames and sashes built of ballistic composite, which are virtually impervious to break-in attempts.

>>>>>(As usual, KE is overstating the capabilities of its stuff a tad. The actual material can be cut with the right tools; the bitch is how to do that without setting off the alarm. These puppies are almost as sensitive as KE claims, so if you don't have a decker to deactivate the alarm system, you've got to find a way to keep the circuit intact while you're cutting.)<<<<<

—Architeck (09:16:51/01-04-56)

>>>>>(Oh, is that all? Whew. For a minute there, I thought I might have to do something difficult.)<<<<<

—Lysander (10:01:48/01-04-56)

>>>>>(Take note: popular demand for fancy fiber-weaves and the like is driving the price down. Pretty soon any corp bigger than a mom-and-pop operation will be able to afford windows made of this stuff.)<<<<<

—Trendwatcher (10:16:37/01-04-56)

>>>>>(Lots of places are also using ballistic composite to fill in gaps between frame and sash or frame and wall in older buildings. Those old-style wooden window frames warp with age and weather, leaving plenty of space for a handy-dandy crowbar. The smaller corps are getting wise to this and taking precautions.)<<<<<

—Architeck (12:13:51/01-04-56)

Physical barriers across windows are highly effective if integrated into a total security system. Simple grillwork, heavy screening, or chain-link provide some protection, though these measures on their own are hardly adequate. To be truly effective as a barrier, anything covering a window must be combined with additional security measures such as low-level electric current or sensors so that the barrier—or the window itself—functions as part of a complete alarm system. For additional information on alarm systems, see **Technical Security**, p. 26. One-way windows can serve as effective cover against magical attack—a magician has to see the object of his spell before he can cast it.

WALLS, DOORS AND LOCKS

Exterior and interior walls and doors pose similar security challenges. Thick plascrete or concrete makes the most effective exterior walls; interior walls should be built of the most impact-resistant materials possible (within structural limits). Interior doors should be built of hardwood or ballistic composite; options for exterior, emergency, and vault doors include steel, plascrete, or a combination of the two. Door frames should ideally be made of a single piece of 12- or 16-gauge steel, as this material is virtually impossible to pry loose from the rough (structural) frame into which the door frame fits. Every door must fit its frame tightly, leaving a gap of no more than .325 centimeters between the frame and the door lock; anything larger will allow an intruder to force the lock with a prying tool. For customer convenience, Knight Errant offers professional consultations on choosing building materials for sites-in-progress, tailored to the needs of your corporation. For existing facilities, KE recommends reinforcing existing doors and walls with ballistic composite or reinforced-impact plastic.

The number, composition and/or reinforcement of doors also depends in part on how often and for what purpose they are used. Emergency exit doors, for example, are not intended to be used on a daily basis, nor to be opened from the outside. Therefore, removing all exterior hardware from these doors will not interfere with the facility's day-to-day business. Main entrances, on the other hand, must be opened from both outside and inside. They are used frequently, particularly during peak periods such as the beginning and end of the workday and all shift changes. Because these doors need to open easily and often, the only way to properly safeguard them from intrusion is close supervision by trained security personnel (see **Security Guards**, later in this section).

>>>>>(Want to sleaze into a corp site? Buy some solid fake ID and mingle with the grunts slumping into work at 7 a.m. That's the end of the dead shift at lots of places, and the sec-boys at the doors are thinking about going home to bed. That means they're more likely to be careless.)<<<<<

—Dybbuk (14:20:41/12-10-55)

>>>>>(Easier said than done, but Dybbuk's got a point; the weakest link in the security chain is always the (meta)human element.)<<<<<

—Latch (14:31:32/12-10-55)

All doors leading directly outside should be able to withstand physical assault. Emergency exits, however, must be also light enough to be opened quickly by a single person. Special hinges and weighted doors allow even the thickest solid-steel emergency door to serve its intended purpose. Needless to say, any existing doors not needed for the efficient day-to-day operations of a corporate facility should be sealed off with plascrete or concrete.

It is a sad fact of modern life that not all employees are honest. Therefore, interior doors and other physical security measures must protect against employee theft as well as against intruders. In designing optimum interior security, the corporate client must balance the need to protect against dishonest workers with the employees' need to move freely about their assigned tasks. Therefore, any measures taken to reinforce interior walls and

doors must take into account the layout of the building in question and the work to be performed in each area. The last thing a corporation wants is internal security measures that interfere with the running of the company; that kind of protection simply isn't worth the loss of profits. Knight Errant's physical security experts will consult with executives from each client corporation to design optimum interior security.

Of course, topnotch interior security should also swiftly contain or neutralize any intruders who manage to enter the facility. For a complete discussion of available options, see **Containment and Neutralizing**, below.

Locks and Keys

Of course, any door or window is only as secure as its lock. Computer-based systems that function as both locks and identification systems—such as maglocks, keypads, cardreaders, scanners, and voice-recognition systems—are discussed in **Technical Security**, p. 28. The remaining types of locks in widespread use are well-designed pin-tumbler locks and padlocks. Both types cost little, and neither depends on electrical power; therefore, neither can be disabled by power outages. Padlocks are also easy to replace.

The ideal padlock consists of a heavy, corrosion-resistant, solid-steel body with a case-hardened steel shackle at least 1.3 centimeters thick and heel-and-toe locking action. Heel-and-toe locking action means that the lock grabs the shackle internally at both ends, rather than at one end. A good padlock should be key-operable; standard combination locks use simple numeric codes that an alert intruder can far too easily guess. The padlock should attach to a hardened-steel hasp, constructed so that its mounting hardware is completely concealed when closed with the lock in place. Pinless hinges that cannot be removed and a staple as thick or thicker than the padlock's shackle are the finishing touches that make a padlock impervious to all attempts to force it, cut it, or remove it from the door. Smaller versions of padlocks can also be used on windows, either as stand-alone locks or to reinforce standard window locks. The number of padlock keys should be kept small, and access to them strictly controlled. Employers are advised to use distinctive padlocks; certain unscrupulous individuals have been known to destroy a padlock and replace it with one of their own, to facilitate theft at a later date.

>>>>>(Frag. There goes my favorite gambit.)<<<<<
—Houdini (12:16:31/12-12-55)

The pin-tumbler lock, first invented by Linus Yale Jr. in 1861, reigned unchallenged as the unbeatable high-security lock until the development of the maglock in the early 21st century. Even today, a sophisticated pin-tumbler lock poses quite a challenge to the would-be intruder. Many residences and older commercial buildings still use pin-tumbler locks; most people are therefore familiar with them, but few understand exactly how they work.

A pin-tumbler lock consists of five parts: the cylinder, the plug, the pins, the drivers, and the springs. The cylinder contains all the rest of the lock's moving parts. The plug is the piece of metal that fits into the cylinder; a hole milled into the plug, called the keyway, allows the key to be inserted into the cylinder. A series of holes drilled into the cylinder and the plug accommodate the pins, drivers, and springs. The pins—small pieces of brass that are sharp on one end—fit into the holes with their points down. Drivers, similar to pins but with two flat ends, rest on top of the pins. The springs rest atop the drivers and exert pressure on the hardware below them. When there is no key in the lock, the springs push the drivers and pins all the way into the holes, preventing the plug from turning. To open the lock, a key inserted into the keyway must have precisely the right number and size of cuts along its length to raise the top of all the pins flush with the top of the plug, and no higher. If the wrong key is inserted, some of the cuts will be too shallow, and will raise the pins into the cylinder; others will be too deep, and will not raise the pins high enough. Either way, the plug will not turn and the lock will not open.

The difference between an easily picked pin-tumbler lock and one that is virtually impossible to crack is the clearance between plug and cylinder. A large clearance gives the lockpicker a better chance to lift all the pins to the right height at the same time, because it enables him to wedge already-lifted pins in place. With a small clearance, the pins cannot be wedged, and will spring down each time the lockpick moves to another pin. A well-designed pin-tumbler lock, therefore, is practically impossible to open without the right key. As with padlocks, the number of and access to keys should be limited.

Though padlocks and sophisticated pin-tumbler locks are less desirable than maglocks for securing commonly used entrances and exits, they are well-suited for other purposes. Outlying storage facilities can be adequately secured with either type of lock, and padlocks will suffice to secure perimeter gates at lower-security installations. Even emergency doors and windows can be locked with padlocks, though the location of the key should be known to only a few trusted individuals. If the key must be used to open an emergency exit, employers are advised to find a new location for it and ensure that only the most trustworthy employees are informed of the change. Because of the potential for a security breach should the key's location become too widely known, maglocks make a better alternative to secure emergency exits.

>>>>>(So find out who knows where the key is and persuade 'em to tell you. With cred if you can, with pain if necessary. Most folks' honor and integrity doesn't last long if they're gonna die for it—or if you wave a fat credstick under their noses.)<<<<<
—Whisper (03:06:15/10-21-55)

CONTAINMENT AND NEUTRALIZING

Containment and neutralizing measures are the last line of defense against the most determined—or luckiest—trespassers. They stop the intruder in his tracks before he can penetrate the most sensitive areas in a corporate facility, either by trapping him in one place long enough for security personnel to apprehend him or inflicting sufficient bodily harm to incapacitate him.

>>>>>(Riddling the poor slag with minigun fire'll incapacitate him, all right.)<<<<<

—Zeevo (11:08:20/10-6-55)

Containment Measures

Containment measures detain an intruder, but do not harm him or her physically. Steel or ballistic-composite shutters that slam shut over doorways whenever sensors detect an intruder's presence are one popular option; even the best possible cutting tools will not allow the intruder to break through the heavy shutters quickly enough to escape on-site security personnel. Netguns are another common containment measure. Easier to install than shutters, a netgun drops from a concealed port in the ceiling and shoots a light but tough polymer-fiber net around the unsuspecting victim. The criminal lies helplessly entangled in the net, unable to cut or tear through the sturdy fibers while his movements are so sharply restricted.

>>>>>(I've heard some corps use netguns that shoot out monowire. You roll around in a net made of that stuff, you die the death of a thousand cuts in real short order.)<<<<<

—Careful Out There (09:04:45/10-6-55)

Neutralizing the Enemy

Knight Errant offers several neutralizing measures, most of them designed to incapacitate an intruder temporarily without causing any permanent physical harm. For those rare cases in which more stringent measures are needed, Knight Errant provides full security services.

>>>>>(Sure, we'll help you lop 'em off at the knees with monowire or drill holes in their skulls with lasers. For a fee, of course.)<<<<<

—Snake (11:09:56/9-30-55)

>>>>>(Actually, Snake, most corps would rather have you alive than dead—at least for awhile. Dead bodies make lousy informants.)<<<<<

—Reality Czech (12:50:24/10-1-55)

Gun ports and laser mazes are two of the options most often chosen. Gun ports, described earlier in this section, are a particularly effective method of stopping several intruders at once. Laser mazes are generally installed in conjunction with other containment measures such as steel shutters or knockout

gas, so that the breaking of the laser beam triggers these security components.

Monowire mazes can also provide an extremely effective deterrent to break-ins, but should be used judiciously. These devices will permanently injure or kill the criminals they are designed to stop, and so corporations considering them should be aware of the possibility of legal challenge by surviving relatives. The extraterritorial status of most large corporations should be adequate protection, but no court is ever entirely predictable. In several celebrated cases of the past century, burglars and housebreakers won large awards from sympathetic juries. Though these have been rarely referred to since the landmark Shiawase decision, they remain valid precedents.

>>>>>(Oh, like any slag these days can sue a corp and get away with it. Corps do what they fragging want.)<<<<<

—Naderboy (24:00:01/10-23-55)

>>>>>(No lawsuits. Bad for business. No productivity. Bad for business, bad for America. Lawsuits and liberals, and I think Mr. and Mrs. UCAS get that.)<<<<<

—GHW Bush (22:03:05/10-24-55)

Knockout gas is another option for neutralizing the enemy by sedating him while security personnel converge on the compromised area. Gas has several advantages; it inflicts no permanent harm and so avoids possible legal consequences, many gasses are inexpensive, and proper ventilation ensures rapid enough dissipation to prevent it from endangering legitimate personnel who may be nearby (depending on the circumstances of the break-in). For most corporations choosing this alternative, the optimum gas has no odor, acts instantaneously, and will not begin to break down for several years from the installation date. Depending on the needs of the corporation, delivery systems can shunt the gas to a narrowly confined space or over a wide area; in the latter case, Knight Errant guarantees that all intruders in the area specified will be affected virtually simultaneously. Knight Errant specialists can offer corporate clients complete details on the specific knockout agents available, including speed of action, degree of deterioration over time, specific effect on humans and metahumans, and so on.

>>>>>(I love this "no permanent harm" drek. I guess being reduced to a drooling idiot who can't even feed himself isn't considered permanent—though I'm sure my brother would disagree if he had enough of a mind left.)<<<<<

—Naderboy (24:08:11/10-23-55)

>>>>>(Even the "harmless" sleepy gasses can kill you if you're unlucky. A chummer of mine died on a raid when they pumped the hall we were in full of some stuff. Allz it did to most of us was give us dreams like a Salvador Dali painting; but my chummer, he choked on it like it was cyanide. (The corpboys dumped his dead meat into our holding cell to encourage us to talk nice to 'em.) I found out later my chummer had a fatal allergic reaction.)<<<<<

—Ballybeg (20:02:35/9-5-55)

>>>>>(OK, kids get yer allergy shots, now.)<<<<<

—Beavis II (09:20:54/9-15-55)

>>>>>(No joke. Just another reason to do your homework before you go, so you know what kind of gas you might run into and how it's likely to scramble your nerves.)<<<<<

—Careful Out There (12:55:42/9-16-55)

Light and sound also make effective neutralizers when used as part of an overall security blanket. Bright interior lights near hidden cameras, for example, slaved to the cameras so that they light up when an intruder passes or attempts to tamper with one, can blind or disorient the intruder temporarily and cause him to panic. A frightened criminal is a blundering criminal and often proves easy to capture. Bright white lights can also be programmed to flood deliberately dimmed secure areas, blinding the interloper while offering a clear field of vision to security guards equipped with goggles. White-noise generators, previously discussed as a part of perimeter defenses, can also be used inside rooms and corridors; depending on the frequency of the sound generated, they can either disorient the intruder, make him feel physically ill, or even shatter the crystals in every smartgun or cyberware system he possesses. Lethal levels of sound are not recommended for interior defenses, as there is no way to guarantee that legitimate corporate employees may not be within hearing range when the system goes off.

>>>>>(Like that would matter. Dead wageslaves? Who cares? Plenty more where they came from!)<<<<<

—U. Sinclair (00:30:34/11-6-55)

>>>>>(Actually, I wouldn't bet on running across these babies inside—at least, not near the really high-security stuff. After all, the higher the security, the more likely it is that only the top doggies know about it and have access to it. And you don't want to kill those folks off, now do you?)<<<<<

—Rainbo (01:00:20/11-8-55)

GUARDS AND GUARD ANIMALS

Though the ever-changing cutting edge of defensive technology claims most of the spotlight, the (meta)human element is the most vital part of any security operation. The vast majority of alarm systems, perimeter defenses, containment measures, and so on do not stop the criminal all by themselves; instead, they delay him long enough for security personnel to reach him and deal with him. No physical security plan can be considered adequate without trained personnel, from rank-and-file security guards to patrol officers to cybered fast-response teams.

>>>>>(So the computers ain't taking over the world? Awww ... I'm bummin' ...)<<<<<

—Echo Mirage (12:16:11/01-05-56)

All Knight Errant security guards, no matter what their specific duties, receive the best basic training with the latest equipment and combat techniques available. We keep up with the

escalating "arms race" between security providers and the criminal element; nothing that shows up on the mean streets takes KE personnel by surprise. Our operatives do what every good security guard must to be worth his pay; they expect the unexpected and never lose their cool.

>>>>>(Jeez. Don't be so humble.)<<<<<
—Zeevo (06:15:48/12-22-55)

Different levels of ability among security guards, of course, come at different costs. Depending on the needs of the individual corporate client, security forces can be non-augmented or equipped with any kind of cyberware from the basic smartgun to chipped reflexes to tactical-computer implants. Corporations with few on-site assets to protect but a need for a visible guard presence to reassure customers are advised to use non-augmented security officers in large numbers, or those with simple cybertechnologies such as wired reflexes or dermal plating. Heavy dermal plating, however, generally serves to intimidate the public; lighter types are more subtle, and more likely to make prospective customers feel safe. If a site contains large amounts of important data or equipment, augmented guards are a better choice; the extra expense is more than worth the added protection such personnel give to your vital investments.

Against these benefits, the risk of security personnel compromising your facility is relatively small. However, the risk does exist, and all corporate clients should take it into consideration before making a final decision on what kind of (meta)human security force to hire. Even the most loyal guard is still only (meta)human, and may succumb to the temptation to betray his employers if the criminal offers enough incentive. Knight Errant's intensive screening process greatly minimizes the risk of unknowingly hiring potentially anti-social individuals who may choose criminal activity over honest employment, but no screening process is perfect. On balance, the risk is worth it in our judgment; but every client's executive officers must judge that question for themselves. For additional information on KE personnel screening, see **Personnel Security,** p. 51.

GUARD ANIMALS

Guard animals can also offer protection, either alone or in conjunction with (meta)human handlers. Various paranormal animals can be trained to serve as guards; on request, Knight Errant security specialists will provide clients with a comprehensive list of the animals available and their potential uses. Among non-magical animals, geese and guard dogs remain favorites. Geese honk loudly and incessantly at the sight of (meta)humans, making them an effective early-warning alarm. They also have aggressive territorial instincts; they will attack anyone they consider an intruder, inflicting surprisingly painful nips with their bills. Among dog breeds, Doberman pinschers and German shepherds are fast runners that can cover a typical no-man's land in seconds. A brace of mastiffs can take down a troll, and a pit bull's jaw-locking death grip can even bite through light to medium armor. All these breeds are highly intelligent, amenable to training, and even capable of accepting light augmentation. When used together with (meta)humans, guard dogs can often compensate for the guards' innate sensory weaknesses. The presence of a handler guarantees that the animal will not panic or become disoriented under fire, and a magically capable handler can help the guard animal resist spells cast on it.

>>>>>(What's this about augmenting animals? I thought that was impossible.)<<<<<
—Slag (08:15:41/12-14-55)

>>>>>(It is. Several sec providers have tried it; the animals go raving crazy.)<<<<<
—Wraith II (08:25:46/12-14-55)

>>>>>(Plenty of corps might view that as an advantage.)<<<<<
—Dybbuk (08:29:31/12-14-55)

TECHNICAL SECURITY

Technical security was born the moment a group of travelers first decided to train pack animals to warn them of intruders. From that humble beginning, technical security has grown into one of the most important fields of corporate security. No security system can be truly effective unless it integrates the latest security technologies. Knight-Errant's technical security department represents the leading edge of innovation in the field, providing the most reliable and efficient security technology available.

Though almost every well-protected company depends on a security system bolstered with alarms, access controls and active surveillance systems to protect its assets, some private security providers continue to rely on traditional Matrix and computer-based monitoring and control of these systems. At Knight Errant, however, we provide unmatched protection by using state-of-the-art closed-circuit simsense technology, which gives our technical security systems unmatched response times and complete autonomy from the world-spanning web of the Matrix. By using CerebroTech's patented closed-circuit simsense technology, a Knight Errant security rigger "becomes" the building he or she protects. In the same way a vehicle rigger monitors and controls every function and aspect of the machine he pilots—altering speed and reacting to changing conditions with a simple thought—a security rigger can "feel" a door open or "sense" unusual pressure against a fence and respond immediately. Because the system is autonomous from the Matrix, intruders in cyberspace cannot access it.

At Knight Errant, we use the most advanced alarm systems, access-control technologies, and surveillance and control systems together with highly trained personnel to provide unmatched technical security tailored to each client's security needs and budget.


SECURITY SIMNET
YELLOWJACKET 12
NIGHT VISION
INTRUDER ALERT
ATRIX
ARCH
SEVERE
TIRE
DAMAGE

>>>>>(Even the most advanced technologies will never be a match for the human mind. Give me enough time, and I can figure out a way to get around any security measure—and I won't need any shiny toys to do it.)<<<<<

—Luddite (20:18:36/11-29-55)

>>>>>(Trouble is, Luddy boy, you won't have much time when the alarms start beeping and you find yourself surrounded by a swarm of angry drones. Technology is your friend, Ludman, and you'd do well to learn how to use it to your advantage.)<<<<<

—Edi-san (20:32:44/11-29-55)

ALARM SYSTEMS

Though alarm systems generally provide more coverage per nuyen than security personnel, they are not so inexpensive that a company can afford to use such systems without careful consideration. At Knight Errant, our rule of thumb is that no security system should cost more than 10 percent of the total value of the assets the system is designed to safeguard. Knight Errant technical security personnel will help corporate executives analyze their company's security needs and assemble an alarm system that best supplements existing security personnel and perimeter defenses such as walls and defensive landscaping.

To determine whether an area would benefit from an alarm system, our personnel begin by considering the area's security incident records, paying particular attention to unauthorized penetrations. The frequency and type of intrusions dictate the nature and extent of the alarm system needed. For example, if an intruder breaches a boundary fence or wall an average of once each month, that area is identified as a hole in the existing security system to be eliminated through the use of some type of alarm. Depending on the area or asset being protected, KE personnel may suggest a perimeter, area-detection, proximity, or magical alarm for the trouble spot. The different types of alarms are discussed in the following passages—except for magical alarms, which are discussed in the **Magical Security** section, p. 40.

PERIMETER ALARMS

Because perimeter defenses are designed to stop intruders from entering a protected area, these defenses are usually the first level of protection a corporation chooses to reinforce with an alarm system. Perimeter alarms may also substitute for perimeter defenses when physical barriers prove impractical or undesirable. Alarms used to safeguard site perimeters fall into four basic categories: taut-wire detectors, electromechanical devices, pressure devices and photoelectric devices.

Taut-Wire Detectors

A taut-wire detector, also known as capacitance wire, consists of an electrically charged wire stretched around or across a physical barrier. Any (meta)human body or living object that comes within two meters of the barrier produces a disturbance in the electrical field created by the detector, which then alerts a control station to sound an alarm. Anyone who possesses a trideo set can observe the general principle behind this type of system in their own homes by simply approaching the operating set closely. The distortion in the set's image is created by your body disturbing the electrical field generated by the trideo set's imaging components.

The extreme sensitivity of taut-wire detectors is also their one major disadvantage. Such systems sometimes react to mundane animals that wander into detection range, resulting in a potentially high number of false alarms. However, a security rigger monitoring the system can easily use drones to check out alarms, greatly minimizing this drawback.

Taut-wire detectors may be placed on any physical barrier outside the protected site, such as a building roof or any walls or fences marking the border of the site.

Electromechanical Alarms

Electromechanical devices represent the most common and, in some ways, the simplest type of perimeter sensor. Generally used on windows and doors, these devices are electrical switches composed of two magnets or small plates of metal or other conducting material. Normally, the devices are set in closed positions and linked to an electrical circuit connected to a control station. When a window or door is opened, the switch opens and breaks the circuit, alerting the control station. Mechanical switches are also used on both doors and windows. Usually set into the frames, mechanical switches consist of plungers that are depressed when a door or window is shut. Opening the door or window breaks the electrical circuit of the monitoring system. Window foil is a third type of electromechanical alarm. These thin strips of metal are applied to windows in continuous pieces and charged with a constant electrical current. If the window is tampered with or broken, the fragile window foil tears, breaking the circuit and alerting the security system.

Because the security systems in existence by the middle of the twentieth century remain effective even today, most alarm technology has not changed significantly since that time. New materials, however, have largely replaced window glass. These materials provide much greater protection against intruders while allowing natural light into a building's interior and offering views of the outside world. Some of these new materials, more fully described in **Physical Security** (beginning on p. 18), conduct electrical current through their panes and frames, enabling security-conscious companies to create virtually impassable electromechanical alarm systems.

Pressure Devices

Pressure devices represent another type of switch alarm. These devices are basically flat mats constructed of conductive material. When pressure is placed on the device, the switch closes and completes an electrical circuit, alerting the security system to an intruder's presence. Companies can conceal pressure devices under carpeting or other flooring and strategically place them in the areas of a room most likely to appeal to intruders—under windows, in front of doors, around workstations or below closed-circuit surveillance systems. Entire corridors or rooms may be outfitted with pressure devices, though such large-scale coverage can prove prohibitively expensive.

Some manufacturers have begun to design pressure-sensitive mats that resemble natural and common flooring materials. These devices combine maximum protection with minimum obtrusiveness, thus contributing to a pleasant atmosphere that can reduce stress, improve productivity, and raise morale among corporate employees.

Photoelectric Devices

Photoelectric devices offer excellent protection for large spaces. These two-part devices consist of a sending unit that emits a visible or invisible beam of light (or a laser), and a receiving unit that senses the light's presence. If an intruder interrupts the beam of light, the receiver senses the absence of the light and alerts the control station to the presence of unauthorized personnel. Using reflectors to bend the light beam, most photoelectric alarm systems are designed to crisscross an area multiple times, creating an impassable mesh of light.

Additionally, photoelectric sensors may use photo cells designed to receive specific types of light. This feature prevents intruders from defeating the device by "fooling" the photo cells into accepting another light source as the light beam. Until recent years, security theorists had advocated the use of "invisible" light sources such as ultraviolet and infrared light for photoelectric devices. However, the enhanced visual capabilities of metahumans and the invention of inexpensive and easily portable visual enhancers have made this doctrine obsolete. Many corporate security divisions now choose to make use of the cheaper visible laser sensor systems, often color-coordinating the light to complement the surrounding decor, especially in areas frequented by corporate employees.

AREA-DETECTION ALARMS

Area-detection alarms, commonly known as motion detectors, emit specific signal or wave patterns and then monitor these patterns for irregularities caused by the motion of intruders. "Shadows," or blind spots in a protected area can be eliminated by using multiple detectors to provide overlapping coverage.

The three most common types of motion detectors are ultrasonic, microwave, and passive infrared detectors. More recent technological advances have created a fourth type of motion sensor, the air-pressure detector. While perimeter alarms such as electromagnetic and photoelectric devices can be used to defend limited areas as well as borders, area-detection alarms offer additional protection for especially sensitive locations. If positioned properly, motion detectors can offer almost complete coverage of open areas such as rooms, hallways and warehouses.

Ultrasonic Motion Detectors

Ultrasonic motion detectors emit high-frequency sound waves and "listen" for the same wave pattern to return. Any motion, however slight, will alter the wave pattern in the same way that a tossed pebble will alter the pattern of ripples moving across a pond. Anything that disturbs the predetermined wave pattern alerts the control station to sound an alarm. These detectors are easily programmed to ignore such common sounds as doorbells and telecom incoming-message signals.

Microwave Motion Detectors

A microwave motion detector consists of a transmitter and receiver and operates in essentially the same fashion as radar. The transmitter produces high-frequency electromagnetic waves that bounce off objects in the protected area. The receiver reads the echo of the waves and recognizes the pattern created by the objects in the area. Any change in the echo pattern alerts the detector to unauthorized movement in the area.

Unlike ultrasonic waves, microwave signals penetrate walls and windows. This enables microwave detectors to cover larger areas, but also increases the likelihood that incidental moving objects or authorized personnel will trigger a false alarm. Though microwave motion detectors can be adjusted to compensate for extraneous, non-threatening movement, security divisions often restrict the use of such detectors to relatively low-traffic areas. A security rigger can efficiently compensate for potential false alarms by actively monitoring the alarm system via closed-circuit simsense.

Passive-Infrared Detectors

Though technological advances have substantially increased the reliability and accuracy of passive-infrared detectors—for example, they rarely react to sunlight, air conditioning units, or vehicle headlights—the advent of metahumanity has forced the security industry to calibrate infrared units to detect a greater range of body temperatures, which provides greater opportunity for a particularly clever or technologically well-equipped intruder to defeat such detectors. Furthermore, passive-infrared detectors remain more susceptible to false alarms than any other type of motion detector despite improvements in their design. For these reasons, Knight Errant recommends the use of these devices only when no other type of motion detector is suitable for the area to be defended because of the type of work performed in the area, the material stored there, the composition of the surrounding construction, or the personnel or other life forms occupying the space.

Air-Pressure Detectors

Though technically classified as a pressure-detection system rather than a motion-detection system, air-pressure detectors provide more effective area defense than perimeter defense. An air-pressure detector consists of a diaphragm designed to detect changes in the ambient air pressure of an area or room. Movement within the monitored area or a door opening or closing are examples of events that can trigger an air-pressure detector. Air-pressure detectors do not suffer the limitation of blind spots, but must incorporate computers to analyze air pressure and recognize normal barometric fluctuations. A security rigger monitoring the system significantly increases the accuracy of these judgments.

>>>>>(The only way to defeat these sensors is to move real slowly and quietly. If you're lucky, the detector will think you're a draft or slow-flying SST or something.)<<<<<

—Krome Kat (18:31:46/12-11-55)

>>>>>(In other words, you're fragged, right?)<<<<<
—Oke Doke (18:44:21/12-11-55)

>>>>>(Not necessarily. Remember, you're not trying to avoid the detector—it's gonna hear you no matter what. You want to fool the analysis software that decides whether the waveform it's reading is a breeze or a bogie man. And waveform analysis can vary greatly in effectiveness, from almost useless to nearly omniscient.)<<<<<
—Masher (19:01:11/12-11-55)

PROXIMITY ALARMS

Knight-Errant considers proximity alarms an important component of any complete and effective security system. Designed to detect electromagnetic fields and unusual vibrations, proximity alarms efficiently supplement perimeter and area alarms by protecting specific objects in a room or area. Proximity alarms also may be used when other security systems are impractical or undesirable. Most proximity alarms fall into one of two categories: capacitance sensors (also discussed under **Taut Wire Detectors,** p. 26) or vibration-detection devices.

Capacitance Sensors

Capacitance sensors generate electromagnetic fields calibrated to detect the electrical charges produced by (meta)human bodies at specific distances from an object. Generally, these highly sensitive devices consist of discreetly placed wires connected to two balanced circuits. They can be set to detect an intruder approaching within several feet of a protected object or an intruder touching the object. The location of the object, the expected amount of traffic near it, and the acceptable level of false alarms all affect the sensitivity level chosen for the sensor.

In addition to specific objects, capacitance sensors can be used to monitor areas such as storage sites or entire rooms. Capacitance sensors are also often used to turn standard gun emplacements into so-called "smart" gun ports, because they can discriminate between (meta)human intruders and other moving objects.

>>>>>(So what's to keep the smart gun from nailing a wageslave instead of a mean 'n' nasty runner slag? They're both meat, ain't they?)<<<<<
—Witherspoon (12:34:54/12-18-55)

>>>>>(The corp doesn't activate the system until after hours when the only folks who'd be there are runners, you stupid fraghead. Or they make sure the few folks who do need to be in that area know exactly where the gun ports are, and how far away from them to stay in order to keep from tripping the sensor. Why does everybody assume the corps are going to be that stupid about how they use their security toys?)<<<<<
—Dybbuk (13:02:33/12-18-55)

Vibration-Detection Devices

An elegantly simple system, a vibration-detection device uses a contact microphone placed on or near the object to be protected. The microphone is monitored by a central control station that sounds an alarm if the microphone detects any vibrations. These devices are regularly programmed to ignore vibrations common to occupied and unoccupied buildings, such as the sounds of creaking floors, telecom beeps, or the gnawing of a mouse. Vibration-detection devices can also be programmed to ignore vibrations common to the protected environment, such as the sound of thunder, gunfire, and traffic.

>>>>>(Damn, this sounds like some serious drek. With all these alarms and detectors, how can anyone hope to get into any corp facility without tripping something off?)<<<<<
—Tyro (07:22:31/12-08-55)

>>>>>(What's good for the goose is good for the gander, Tyro. There's technology out there designed to counter this drek, too. I've heard there's a fixer outside of Chicago who can provide you with something called a "sneak suit" —a handy little piece of clothing that'll mask your infrared signature. I'm sure if you do some research, you can find other goodies out there.)<<<<<
—Smart Shopper (07:46:12/12-08-55)

>>>>>(Who ever said you need to avoid alarms, boys and girls? Think about it for a minute. Even a small corporate facility probably has a hundred or so alarms and detectors scattered about. Now if all those little bells start ringing at the same time, it's gonna take at least a couple minutes for the security goons to check them out. A lot can happen in a couple minutes ...)<<<<<
—Vox (05:44:13/12-09-55)

ACCESS CONTROL

The single corporate security system most visible to employees—and the one they are most likely to try to circumvent out of sheer annoyance—is the access-control, or identification system. These systems are composed of maglocks, cardreaders and other pass systems, biological recognition systems (biometrics), or any combination of these devices. While Knight Errant recognizes that all corporate employees have a right to personal privacy, the competitive corporate world of the 2050s forces employers to implement ever more vigilant security measures. Though employers can use access-control systems to track the movements of authorized personnel throughout a corporate facility, the primary function of such systems remains identifying and tracking unauthorized persons or activities that might endanger the corporate work force.

To maintain efficient and effective corporate security, Knight Errant requires its corporate clients to maintain at least one form of access-control system on all sites and recommends the use of redundant systems—layered levels of identification procedures—in sensitive areas. Clients may choose from many different styles of maglocks, pass readers, and biometric systems and may also incorporate weapon and cyberware detectors into the access-control system at strategic locations.

>>>>>(Yeah, right. The welfare of employees is always right up there on the list of any corp's priorities. Don't be fooled, chum-

mers. Big Brother's always watching for any sign of waning loyalty among its wage slaves. Anyone in the know will tell you that having someone inside remains the best way of ensuring that a run against a corp will succeed. And the corps never forget it.)<<<<<

—K Dog (13:41:56/12-13-55)

MAGLOCKS

Maglocks offer several advantages over simple padlocks or pin-tumbler locks, which are usually sufficient for low-security installations or installations sufficiently protected by other security measures. Maglocks are available in four levels of sophistication and can be keyed to individual users or groups of users, simplifying access control for areas protected by such devices. Type 3 and 4 maglocks are usually connected to a protected area's technical security system. In such a configuration, any attempt to bypass a maglock will trip the lock's monitoring system and trigger an alarm.

>>>>>(I suppose this means that the good ol' days when maglocks were accessible via a corp's internal matrix are gone forever. No more, "Mister Decker Man, please tell the computer it's wiz to open the maglock on the fourth floor. Better yet, tell it the lock's still closed and no one's messing with it. Thanx!")<<<<<

—Delunidai (10:08:24/12-4-55)

>>>>>(Yup. Most halfway-smart corps now keep their security systems separate from all other systems. And before you figure on cleverly cracking into the separate security system (spirits know how) and fragging with any corp deckers who happen to be lurking about, remember this tidbyte—the big fatcat corps (i.e., the ones with the juiciest pickings) have a rigger running their sec systems instead of a decker. Different protocols, chummer. Totally different game. But go ahead—fry your deck and what passes for your brain angling for a way to bypass the best in the biz. Don't let me stop you.)<<<<<

—Dybbuk (15:30:21/12-10-55)

>>>>>(Fragging know-it-all.)<<<<<

—Delunidai (15: 35:12/12-10-55)

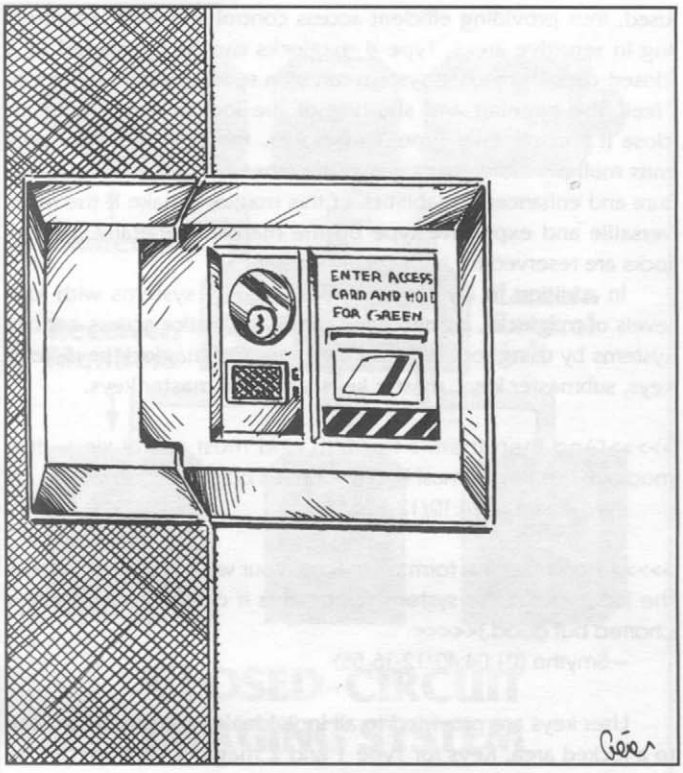
>>>>>(Make that the halfway smart corps who can afford them, Dybbuk. Costs plenty nuyen to completely isolate your security system. But on the ones still controlled via the corp matrix, the maglock itself can give you access to the system—if you've got the right kind of hardware to make the connection between the lock and your deck.)<<<<<

—Latch (00:05: 55/12-11-55)

>>>>>(Never forget, chilluns, that a maglock depends on a physical power source. Snip go the wirecutters!)<<<<<

—Miz Liz (11:43:10/12-17-55)

>>>>>(The trick is finding the source, Lizzie. Do you think a corp's gonna stick it on a post outside the building with a "Danger. High Voltage Electricity" sign to attract your attention? You've also got to get around those old anti-tamper circuits—those



fraggin' things'll start screaming the minute you breathe too hard on that source. And you need the right tools to disable the source once you identify it. Have you ever heard of wireless systems? Can you carry all the special stuff you might need to disable all the possible technology?)<<<<<

—Arthur (16:32:10/12-19-55)

Each of the four types of maglocks available provide a different level of protection. Type 1 maglocks, the least expensive, are essentially electronic padlocks, each containing its own power source. Type 1 maglocks cannot be slaved to an integrated security system nor programmed to respond to multiple individual keys. The Type 1 is roughly comparable to the electronic banking card that served as the precursor to the credstick; an unlimited number of people may carry a Type 1 maglock key that will open the same lock.

Like Type 1 locks, Type 2 maglocks respond to only one key, though any number of people may carry a copy. The most commonly used type of maglock, Type 2 locks can be integrated into a comprehensive security system to enable a security decker or rigger to know when the maglock is open or shut. Type 1 and 2 maglocks employ relatively low-end technology and so are more easily deceived than Type 3 and 4 maglocks. As a result, Type 1 and 2 maglocks are generally used only at minimum-security installations or with low-cost security systems.

High-security installations require Type 3 or 4 maglocks, which provide increased operational flexibility and a greater degree of access control. Type 3 maglocks are fully matrix capable and act as input/output ports. They can be programmed to recognize multiple keys, each assigned to a specific employee and programmed to identify that employee each time the key is

used, thus providing efficient access control and traffic monitoring in sensitive areas. Type 4 maglocks can be connected to a closed-circuit simsense system run by a security rigger, who will "feel" the opening and shutting of the lock and can open or close it himself. Like Type 3 maglocks, the Type 4 model permits multiple individual keying. The closed-circuit simsense feature and enhanced capabilities of this maglock make it the most versatile and expensive type on the market. Generally, Type 4 locks are reserved for high-security areas.

In addition to layering technical security systems with four levels of maglocks, corporations can further tailor access-control systems by using four different categories of maglock keys: user keys, submaster keys, master keys, and root master keys.

>>>>>(And then there's the fifth and most useful kind—the maglock passkey. A must in any runner's bag o' tricks!)<<<<<
—Whisper (22:24:10/12-14-55)

>>>>>(Don't bet the farm on it. Sure, your wiz li'l passkey'll open the lock—but if the system rigger sees it open, your poultry's charred but good.)<<<<<
—Smythe (01:04:40/12-15-55)

User keys are provided to all individuals who require access to a locked area. Keys for Type 1 and 2 maglocks are specific to each lock; keys for Type 3 and 4 maglocks are specific to each user. Submaster keys open all maglocks within a specified area, such as a single wing in a building or a single building on a corporate site. Because they allow access to more areas, submaster keys should be issued only to high-level executives and to on-duty security guards. Master keys open all maglocks in a corporate compound. Usually only one master key exists for a site and is issued to the site's senior security officer. The root master key is a particularly valuable item that must be guarded with great care. This key opens all maglocks in all of a corporation's compounds and facilities. The code of the root master key is programmed into a maglock's firmware, and the security staff must have the root master key in order to reprogram all other keys to the maglocks that it opens. Root master keys are designed for use during security-system installation, re-keying, surprise inspections, and any other situation that requires a single individual have access to all sensitive areas. Only the most senior security executives should possess root master keys.

>>>>>(Senior security executive. Ain't that a pretty name for top hardboy.)<<<<<
—Slag (11:23:45/12-15-55)

Unlike padlocks and pin-tumbler locks, maglocks can be changed easily if a key is lost, stolen, or forged. Re-keying the locks on even one building after a security breach once required many hours of labor and expensive parts. However, re-keying a maglock is as simple as reprogramming a computer. Even if a location remains free from security problems, all maglocks should be re-keyed at least once every six months as a safety precaution. Type 3 and 4 maglocks, of course, can be re-keyed from the central security system. Whenever an employee possessing a user key leaves his position, that key is programmed out of the system. User keys assigned to new employees are programmed on the first day an employee reports for work. If a submaster or master key disappears, corporate security should program a new one and delete the old one as soon as they discover the loss. If a root master key is lost, the locking firmware of all maglocks programmed to accept that key must be replaced.

Maglocks come in two basic styles—keypads and cardreaders. To use a keypad maglock, personnel must enter an identification code that serves as a password on a numeric or alphanumeric keypad. To use a cardreader, personnel insert a card through a slot in the reader. The cardreader identifies the passcard by scanning an identification number encoded on a magnetic strip or microchip in the card. Both styles of maglock can be programmed to log the user's identity and the time he or she opened or closed the lock.

Managing Maglock Security

Maglocks must be incorporated into a total security system with careful consideration to ensure their effectiveness. If their effect on the daily operations of a corporation is ignored, employees may be tempted to circumvent the system. Sign-out systems for user keys allow a corporation to monitor traffic through an area and limit the number of available keys, but such systems may regularly disrupt daily operations and significantly decrease employee productivity. Even requiring employees to constantly unlock doors as they perform their work can produce the same results. For these reasons, maglocks should be limited to high-security or low-traffic areas and should be carefully monitored. Whenever possible, corporations should restrict access to keys to as few employees as possible. These employees should be properly vetted and required to sign the keys in and out. On this smaller scale, the sign-out system represents a reasonable security precaution rather than an unreasonable hindrance. Additionally, maglock keys are normally produced with programs that prevent unauthorized copies from being made. And corporate security personnel can also track the whereabouts of maglock keys through magical means.

A corporation that fails to install maglocks and distribute keys in a carefully considered, judicious manner may as well not install locks at all. Remember, access control is only as effective as the system set up to provide it.

PASS SYSTEMS

For many applications, maglock systems may prove undesirable. The fact that maglock systems require employees to possess physical keys produces its own set of security risks. Employees may lose or forget their keys or even be robbed of them. The unauthorized use of even one key to enter even the lowest-security area of a corporate facility may represent a serious security breach. Maglock systems also prove unsatisfactory as a means of tracking guests. Re-keying locks after every visitor is impractical, and most security divisions generally consider all non-employees significant security risks.

A Knight Errant pass system can help solve many of these problems. In such a system, the corporation issues unique

identification cards to employees and visitors and places proximity readers at strategic points throughout a building or compound. The cards contain tiny microchips that emit low-powered signals, which are read by the proximity readers. If the card carrier has access to the area protected by the reader, the reader accepts the chip's signal and unlocks the door or other barrier for the pass user. If the carrier does not possess clearance for the area in question, the door may simply not respond. More commonly, any attempt by unauthorized personnel to access a restricted area alerts the control center or security rigger to a potential intrusion attempt, and the system or rigger can question the intruder through a closed-circuit television and/or intercom system.

>>>>>(Word is that some corps can't be bothered to deal with what they consider clumsy and outdated i.d. cards—so they install the chip with the signal right into their employees' heads. Naturally, few sane people would agree to this without some serious coercion, but it all looks real reasonable if hidden inside the legit employee health program. The tiniest bit of minor surgery and presto!—the corp has a perfect wageslave it can track even if he's "offered a better life" elsewhere. And the corp doesn't have to worry about lost or stolen passes. The corps are still working on how to eliminate those awkward, unattractive visitor passes they're still forced to issue.)<<<<<

—Whisper (14:22:32/12-16-55)

BIOLOGICAL RECOGNITION SYSTEMS

Maglocks and pass systems are the most inexpensive access-control systems available. However, both types of systems are of limited reliability. For the most effective access control, Knight Errant recommends biological recognition systems. Generally, these systems cost considerably more than maglock or pass systems, but the greater costs are offset by the biological recognition system's greater reliability and convenience.

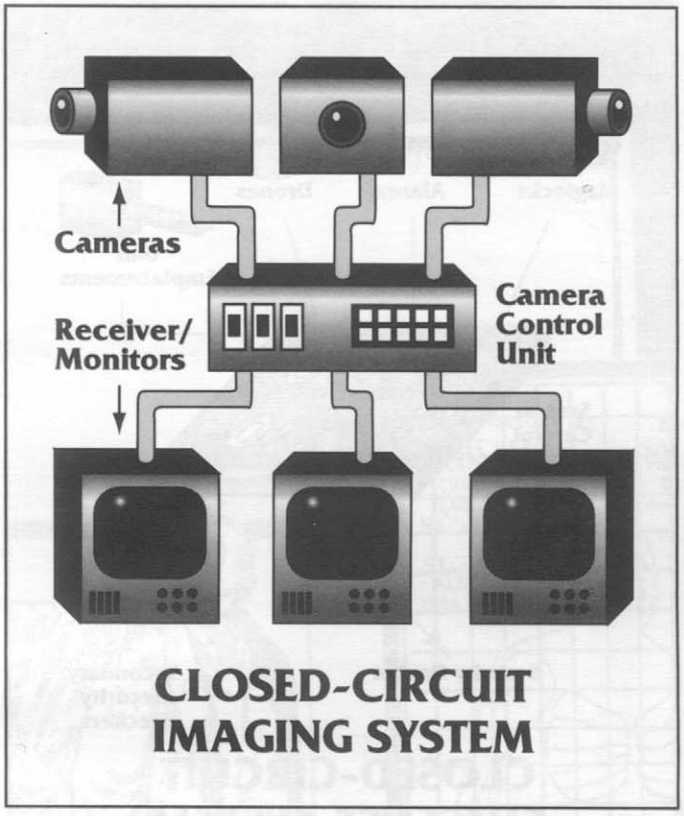
Biological recognition systems identify individuals by their unique traits. The most common type of biological recognition system reads the fingerprints of corporate personnel. Thousands of different prints can be stored in the system computer, enabling a corporation to provide guests with access to restricted areas. Other systems use palm prints, voice-verification, and retinal scans. The most secure bio-recognition systems read two or more indicators. For example, a high-security installation may be fitted with voice-verification and retinal-scan recognition devices. Current bio-recognition systems are also sophisticated enough to detect employee vital signs.

>>>>>(Aw, drek. I guess cutting off the guard's hand to get by the lock don't cut it anymore.)<<<<<

—Slag (11:25:36/12-21-55)

>>>>>(So have your mage whip up a little mind control spell. Suddenly the guard's your long-lost Uncle Bob, thrilled to give you a tour of the wiz new laboratory no one's supposed to know about.)<<<<<

—Cheetah (09:11:34/12-22-55)



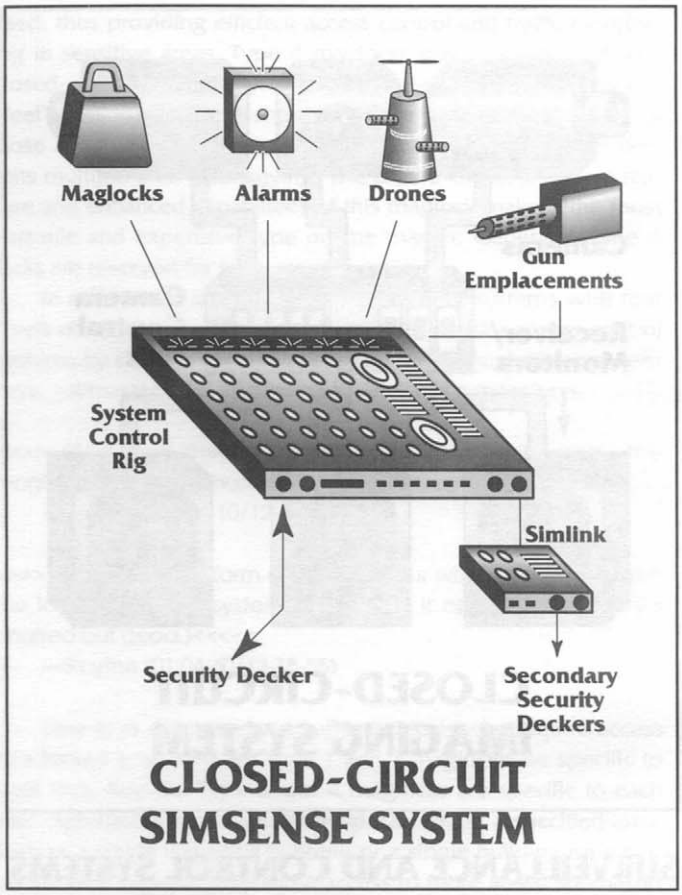
SURVEILLANCE AND CONTROL SYSTEMS

Closed-circuit imaging systems, such as closed-circuit television (CCTV) and closed-circuit trideo (CCT) provide remote visual access to multiple areas of a security site. Closed-circuit simsense (CCSS) systems enable a single security rigger to remotely monitor and control an entire technical security system. Though CCSS systems remain fairly expensive, closed-circuit imaging and simsense systems enable small numbers of personnel to monitor large areas, which makes them economical investments in the long run.

CLOSED-CIRCUIT IMAGING SYSTEMS

At their most basic, CCTV and CCT systems consist of a fixed camera, a receiver/monitor, and a cable link between these two components. Most systems, however, consist of multiple cameras, linked to a bank of receiver/monitors by a camera control unit. Generally, cameras are placed on fixed or movable mounts throughout the security site and monitored from a single location. Today's imaging systems can easily accommodate up to 100 cameras, which means that a single security officer can "watch" an entire complex of buildings. Additionally, modern cameras are sensitive enough to record images in extreme low-light environments and other conditions that would prevent (meta)humans from seeing.

When cable links are not feasible, the cameras, control unit, and receiver/monitors of a system may be linked by microwave transceivers to create a wireless system. These systems provide almost unlimited flexibility for camera placement and coverage.



CLOSED-CIRCUIT SIMSENSE SYSTEM

CLOSED-CIRCUIT SIMSENSE

CCSS systems use simsense and neuromuscular interface technologies, similar to those used in vehicle control rigs, to create system control rigs for running security systems. A CCSS system consists of a number of technical security devices—such as maglocks, alarms, detectors, "smart" gun emplacements, and drones—connected to a special simsense deck known as a security control rig. The security control rig translates the electrical signals from the devices into neuromuscular signals, which are monitored by a security rigger plugged into the rig. The control rig works in reverse as well, translating neuromuscular signals from the rigger into electrical signals that can be transmitted to any number of devices.

The CCSS system enables a security rigger to control a security system just as a vehicle rigger "drives" a vehicle. The security rigger literally "feels" the system components as if they were parts of his own body. The opening of a single maglock, the triggering of an alarm, an intruder stepping on a pressure detector—all these events produce physical sensations in the security rigger. The rigger may then activate system components through simple neuromuscular commands—with a flick of his wrist, for example, a rigger may sweep a room with fire from a gun emplacement.

Simlinks connected to the system control rig enable secondary riggers to monitor the sensory input received by the primary security rigger and aid in the operation of the security system.

SURVEILLANCE AND CONTROL DEVICES

If the security rigger is the "brain" of a CCSS system, then surveillance and control devices may be viewed as the system's eyes, ears, and hands. As described above, these devices enable the rigger to detect activity throughout the site and to act in the physical environment. Surveillance and control devices include maglocks, alarms, and access-control devices (described previously) as well as drones, weapon and chemical detectors, and cyberware scanners.

Drones

Drones are perhaps the most versatile of all surveillance and control devices. They range from simple, remote-control camera platforms no larger than a bread box to complex, programmable machines as large as small cars. The more complex drones may be fitted with diverse arrays of sensors—video, audio, thermal, and motion-detecting types—and nearly any type of weapon—ballistic, nerve gas, net, and taser to name just a few. Drones may be programmed to operate independently of external controls, slaved to a system control rig, or any combination of the two. These machines can be used to quietly patrol a security site, illuminate intruders with spotlights, target intruders with lasers, or even respond with weapons fire. Drones may even be equipped to patrol external areas of a security site. As a result of their unmatched flexibility, drones are well-suited for both access-control and surveillance duties.

Knight Errant uses two main types of drone: semi-mobile and free-ranging. Semi-mobile drones are designed to patrol specific routes within a facility. Generally, these inexpensive machines lack internal guidance mechanisms and independent power supplies. They are commonly designed to follow tracks or wires and must be connected to external electrical power supplies. However, most are fitted with limited backup power systems that enable them to remain functional in the event of a power interruption.

Free-ranging drones are fully mobile and contain independent electrical power supplies. They are the most versatile of all security drones, as well as the most expensive. These machines come in a variety of designs—including airborne, marine, amphibious, and land-based models—and can be programmed to patrol specific areas of a site or wander in random patterns. They can be configured to relay all of their sensory input to a central security system or set up to alert the system operator when they detect specific, discrete events.

Weapon Detectors

Self-contained weapon detectors have been used in the security industry for a number of years, and they are a valuable addition to any CCSS system. Most contemporary weapon-detection systems use magnetic-anomaly detection (MAD) technology. Detection circuitry can be installed into doorways and entryways, or in free-standing frames. When a piece of ferrous metal passes through the loop formed by the circuitry, it induces a current in the circuitry's detection coils. A sophisticated microprocessor in the circuitry then compares the current pattern to patterns caused by various weapons. If it finds a match, the circuit triggers an alarm.

Chemical Detectors

Like the weapon detector, the chemical detector is a security staple that has taken on renewed importance with its integration into CCSS systems. Chemical detectors check for airborne traces of chemicals emitted by explosive compounds. By their very nature, explosives possess relatively unstable and volatile molecular structures. As a result, they emit certain chemicals into the atmosphere around them. Some of these chemicals, namely nitrogenous compounds, produce a distinctive odor that can be detected.

In addition to explosives, today's chemical-detection systems can detect the propellant used in modern, caseless ammunition.

>>>>>(Just get yourself some zipper-loc bags and lock in the freshness.)<<<<<

—Kray (22:31:45/12-22-55)

Cyberware Scanner

Like any other technical security device, cyberware scanners can be integrated into CCSS systems or operated independently. Cyberware scanners consist of sonic/magnetic scanners connected to microprocessors. Whenever an individual passes through the field of the sonic/magnetic scanner, the scanner performs sonic and magnetic imaging on the individual. The resulting images are instantaneously checked against a library of cyberware profiles stored in the microprocessor, which then identifies any cyberware detected. Generally, cyberware scanners can detect and identify all standard and restricted cyberware that contain non-organic components. Organic and vat-grown implants, as well as organically masked Alpha and Beta-level cyberware, may be difficult to detect, however.

>>>>>(Don't be intimidated, my shadowrunning friends. KE's new CCSS system may seem invincible, but it's got some serious weaknesses. First of all, sensors and detectors can be fooled a lot more easily than you'd think, especially if the corporation you're targeting decided to save some money on them—and you'd be surprised at how many corps will cut corners on alarms and such so they can spend a couple million nuyen on a shiny new CCSS system. (Fragging fools're shooting themselves in the hoop, but what do I care?) Second, with a little know-how anyone can tap into the cables that connect the security devices of a CCSS system to its control unit. Do that, and you can feed the control unit whatever signals you want. You can march an elephant into the damn place and the security rigger's never gonna feel a thing. If it's a wireless system, you can get the same results by jamming the microwave signals from the security devices and transmitting your own to the control unit receiver. Drek, with a little practice you can make these new CCSS systems work for you, because nine times out of ten a corporation that lays out the nuyen for one of these systems figures it can lay off most of its old security guards and rely on the system alone.)<<<<<

—The Panther (08:13:22/12-17-55)

>>>>>(You're forgetting the biggest weakness of the CCSS system—the fact that the entire thing rests on one individual, the security rigger. If you can get to him, you can have the run of the place.)<<<<<

—Skeeznik (10:21:55/12-17-55)

>>>>>(Sometimes you don't even have to get to the slot. In a large system the rigger's going to feel all kinds of glitches and false alarms half of the time. Unless he's logged a lot of hours on the system, he's not gonna know which alarms are real until it's too fragging late.)<<<<<

—Kat (18:30:21/12-19-55)

MAGICAL SECURITY

The dawning of the Sixth World and the reemergence of magic presented security specialists with an enormous challenge. Conventional physical and technical security measures had little or no effect against magical forms of breaking and entering. Astral magicians could enter maximum-security sites in a blink of an eye, and magic spells could foil the most sophisticated security procedures with the wave of a mage's hand. As with the rest of the newly Awakened world, security system designers in the early decades of this century lacked experience with magical threats, and had to play a fast and furious game of "catch-up" in order to deal with them.

>>>>>(KE is making more of the problem than it warrants, probably to boost their own fees. Once we all got over the shock of magic's appearance in our mundane world, security firms adapted to it just like everyone else. Nowadays magic is just part of the equation, with its own limitations and advantages. Astral scouting lets you recon a site before going in, but you can't use it to read technical documents or to affect anything you see. Mages can help a team of runners crack into a place with sleep spells, invisibility and the like, but a trank gun and some camo can work just as well. In fact, magic's major impact has been new orders to the security troops: "Geek the mage first.")<<<<<

—Bitrunner (11:23:45/10-12-55)

>>>>>(Glad to be a rigger.)<<<<<

—Hotrod (12:55:32/10-13-55)


MJ 95
FOR NIGEL

At first, security departments reacted to the new magical reality by keeping hired magicians on-call to respond to all magical intrusions detected. These magically trained security specialists were initially assigned to a corporation's physical security department and treated as glorified guards. But as the number of magic-related security incidents increased, it became clear that simply keeping magicians on hand like so much office furniture was doing little to diminish magical security breaches. The regimented operating procedures of the typical physical security department did not sit well with the free-thinking outlook common to most magicians, and these talented individuals were sufficiently rare that demand for them soon outstripped supply. To keep these rare, expensive, and vital security personnel happy, many corporations began setting up independent magical security, or magsec departments run by and for mages.

CONTEMPORARY MAGICAL SECURITY

Contemporary magical security consists of two elements: magically gifted personnel, and technology that takes the properties of magic into account. Knight Errant recognizes the equal importance of both elements, and knows that the most effective magical security requires them to work in tandem. In addition to recruiting topnotch security mages and specialists, Knight Errant makes a point of hiring the best magical security engineers to research, design, and/or acquire cutting-edge security technologies.

TECHNOLOGICAL DEVELOPMENTS

As the number of magic-related security incidents rose throughout the early 21st century, experts in magical security realized that they needed more than on-call mages to handle the threat. Security system designers began learning magical theory and working with mages to design barriers and other technological deterrents that could help keep out or detain astral intruders. The so-called "living wall," genetically engineered ivy force-grown over perimeter walls and the exterior walls of buildings, was the earliest and simplest of these measures, along with barrier spells and wards. More recent technological advances include improved wards and barrier spells, living restraints, fiber-optic networks, and FAB (fat airborne bacteria) zones.

>>>>>(Speaking of tech advances, corps in the Tir and Aztlan use magical lighting. Their security magicians quicken light spells to places inside the protected area. Magical light doesn't give off heat, so it won't "blind" thermographics the way mundane bright light does. Also, the security magician is instantly alerted if one of his quicken light spells goes down. The disadvantage is, an intruder can ground through the spells. That's why the corps tend to leave magical lighting to sorcerer adepts.)<<<<<

—Lady Sally (10:34:48/11-23-55)

Barrier Spells

Barrier spells, either temporary (sustained) or "permanent" (anchored), are an effective means of securing an area against magical intrusion. Temporary barrier spells, most often used by security magicians trying to channel or restrict the travel of astral beings or creatures, are cast as needed and provide a swiftly deployable and flexible means of magical protection. Though effective, the effort of sustaining them preoccupies the casting magician for the duration of these barriers' existence. Some magicians can order elementals to sustain such spells, though this is not the most efficient use of spirit assets.

>>>>>(Barriers are visible astrally. Another use for a watcher—"Oooooh! Boss! Glowing wall over dere!!")<<<<<

—Magister (02:15:33/12-11-55)

>>>>>(I whip up watchers almost like spells. Low-power, really dumb ones. Let them run around screaming—it really confuses things. And of course, when they hit something you know about it.)<<<<<

—Kubit (04:55:44/12-13-55)

>>>>>(Weirdo.)<<<<<

—Jax (05:11:32/12-13-55)

>>>>>(Some of Knight Errant's security teams are known for creative use of barriers and such. It royally frags to be on the tail end of a run, minutes from freedom, when unexpected barriers start cropping up. Unless you want to waste precious time taking them on (and thereby telling the casting magician exactly where you are), you gotta go around them. Trouble is, "around" is usually exactly where they want you to go ...)<<<<<

—Omen (16:41:23/12-30-55)

Anchored barrier spells—especially those with sophisticated links for activation—can be extremely efficient and flexible. Casting them, however, depletes the casting magician's power to some extent and may even reduce his long-term effectiveness. For this reason, anchored barriers and other types of anchored spells are best used to protect only those sites most in need of topnotch magical security.

>>>>>(I've done some anchoring. You've got to be a really tough hombre to create many of those things.)<<<<<
—Suedo King (03:22:41/11-30-55)

>>>>>("Tough hombre," eh? I know Aztechnology uses anchored and quickened spell constructs often. Anyone have any idea why?)<<<<<
—Trevor (06:44: 23/12-01-55)

>>>>>(I suspect they've found some way to transfer the burden of creating the things.)<<<<<
—Divine Fool (07:10:43/12-01-55)

Barrier spells can also be used with mundane physical security measures to keep intruders from entering or leaving an area. At sites with large numbers of magical security personnel, barrier spells are commonly used as obstructions or to reinforce existing walls and doors. Barrier spells can be re-cast when damaged or disrupted, thereby maintaining the integrity of a perimeter. And when containment is a high priority, the ability to quickly erect a formidable barrier to prevent or channel an intruder's retreat is a valuable tool.

>>>>>(Had a rare piece of drek-luck hit me and the boys awhile back. We were making like rabbits for the exit (never you mind from where) when a mage drops a barrier around us! We kept trying to shoot him, and the barrier kept screwing us up. We couldn't get past it, and while we were stuck there they started bringing in the heavy artillery. Used the fragging barrier as a delaying tactic until they got into position around us.)<<<<<
—Lingo Lizard (21:43:12/12-15-55)

>>>>>(Something similar happened to us. Shaman dropped a mana barrier around us, pretty well crippling our mage's abilities (unless he wanted to step out into the line of fire). Rat bastard.)<<<<<
—Hockney Puck (22:00:12/12-15-55)

Wards

Wards block passage by astral forms or spirits and provide a degree of protection against spells cast across them. They are especially well suited to protecting guard positions or weapon and sensor emplacements, as they protect against magical assault without impeding physical counterattacks. Their lack of physical substance, however, can also be a drawback. Because wards also prevent the passage of dual beings such as most paranormal watch animals, security mages must take care to place them where they will not restrict or impede the animals' activity. Clients considering widespread use of wards should be aware that they are expensive to erect.

>>>>>(Expensive to erect? This joker's a real king, *neh*? Yeah, just drop a couple of grand worth of ritual materials every time you want a piffling little ward, and do it again a few days later to keep it strong. Get actual.)<<<<<
—Abandano (20:11:21/12-14-55)

>>>>>(So wards are one more thing used only by the people who can afford them.)<<<<<
—Hawkeye (23:01:34/12-14-55)

Living Walls

Sheets of ivy, moss, and/or various clinging or creeping plants are examples of so-called living walls. Enough of these plants covering a wall can prevent an astral form or spirit from passing through it. Living barriers of this nature are relatively inexpensive in comparison to many alternatives, and also are aesthetically pleasing. Some plants, however, may be difficult to maintain or undesirably intrusive indoors. Living walls may be produced through natural or induced growth.

>>>>>("Induced?" Such a pleasant term.)<<<<<
—Whisperwoman (19:21:33/12-17-55)

>>>>>(I'm sure marketing preferred it to "forced.")<<<<<
—Conroy (19:36:45/12-17-55)

>>>>>("You know Mrs. Devlin, I really like what you've done with the office remodeling, but I think the wall fungus is a bit cliché ... ")<<<<<
—Wobble (22:31:54/12-17-55)

Induced living walls are often genetically engineered for density, enhanced rates of growth, and other desirable characteristics. Induced living walls are often used deep inside protected sites, where sheets of genetically engineered fungus or similar minimal-light plants are built into walls or doors. At somewhat prohibitive expense, living walls can be built into movable panels for emergency deployment across a hallway or passage to prevent the escape of an astral being.

>>>>>(Yow! I know one astral-happy mage who's gonna be real unhappy.)<<<<<
—Xanos The Great (14:21:37/12-18-55)

>>>>>(Only one?)<<<<<
—Spammer (15:35:16/12-18-55)

Cost is the primary disadvantage to induced living walls. Expensive to engineer and maintain (many gengineered plants require specific lighting and/or nutrients), induced living walls are recommended only for sites in need of the very best magical protection.

Living Restraints

Recent advances in induced biotechnology have enabled major security providers to offer corporate clients two types of living restraints to contain astral intruders: living nets and living mesh. Both consist of woven of strands of induced biomatter and are becoming increasingly popular despite their expense.

>>>>>(Oh wiz, this barfs.)<<<<<
—Mr. Mysterio (16:22:34/12-20-55)

Living nets are propelled from launchers that double as storage vessels for the biomatter. The launched net surrounds the astral form or spirit; its mass drags the target to the ground and renders him or her immobile. Such devices are difficult to aim and use, and almost always require a wielder who is astrally perceiving (and thereby at risk of attack) or the presence of ultra-violet fat bacteria and the proper UV detection equipment. The biomatter woven into the net lives for only a few hours once removed from its storage container.

>>>>>(A few hours?? How long is a few hours? Less than six??)<<<<<
—Amberus VI (18:56:34/12-20-55)

>>>>>(Depends where you are, the temperature, if Mars is in retrograde, and so on ...)<<<<<
—Weiner Velt (19:12:43/12-20-55)

Living mesh behaves much like a living net, but usually covers a larger area such as an entire room. It can be deployed to block hallways and passages, or used outdoors in combination with traditional camouflage material to isolate an area. Like living nets, living mesh dies quickly once removed from storage.

>>>>>(I can attest to the fact that the drek burns well.)<<<<<
—Winter (13:22:43/12-19-55)

Fiber-Optic Networks

Fiber-optic technology has existed since the 20th century, but it wasn't until the late 2040s that magical security engineers began using it in magical protection applications. Knight Errant was among the first security providers to use intricate fiber-optic systems to enable security magicians to "see" remote locations from a secure command center. Because a mage needs to see the object of his spell in order to cast it, these fiber-optic links greatly extended a mage's reach.

>>>>>(Fiber-optic cables run all over the world. Does this mean you can cut into the phone network and cast a spell?)<<<<<
—Slag (12:56:50/12-14-55)

>>>>>(No, no, no—and again, NO. When used in magical applications, fiber-optics cannot use any type of image-boosting or enhancement. These systems can only use natural lighting and so are limited to a cable length of only 2,500 meters. The KE system uses prisms to shift from one camera to another. It's not a super weapon, but it sure lets a mage extend his "line of fire.")<<<<<
—TechWiz (13:01:53/12-14-55)

FAB Zones

It is common knowledge among students of magic that astral beings, such as astrally projecting magicians or spirits, cannot coexist in the same relative space as a living object in the real world. This law of nature allows living walls to work. The plant life is alive, and so the astral being cannot pass through it.

>>>>>(Not ever?)<<<<<
—Rather (02:11:32/12-22-55)

>>>>>(Nope. Not unless the living material can be bypassed physically with no effort—none whatsoever. Only if that's true can the astral form pass through.)<<<<<
—Magister (02:35:42/12-22-55)

>>>>>(So you can't get through an ivy curtain because a living body that tried to shove through would have to exert some effort, however minimal, to do it?)<<<<<
—Palo Alto (03:01:31/12-22-55)

>>>>>(Exactly.)<<<<<
—Magister (03:07:52/12-22-55)

>>>>>(How big an opening does an astral body need to get through?)<<<<<
—Iopus (04:21:45/12-22-55)

>>>>>(Same size as the magician's physical body. Sorry, chummer, no sliding under doors.)<<<<<
—Magister (04:28:33/12-22-55)

Knight Errant has recently acquired a new and effective magical security device that takes this principle to new heights. Engineers at BacteriTech, a wholly owned subsidiary of Ares Security International, have created astrally active, or "fat" bacteria that allows non-magical security specialists to detain or even capture an astral intruder. Genetically engineered to be denser than normal bacteria, these airborne organisms can be pumped into an area in sufficient density to restrict the movement of an astral being and reduce its perception to some degree.

The primary fat airborne bacteria (FAB) strain is ideal for filling enclosed spaces, such as double-thick walls and ceilings surrounding a protected area, thereby turning entire rooms into holding pens for astral intruders. As effective as ivy at stopping an astral being's movement, FAB is more portable, less conspicuous, and easily deployable.

>>>>>(Ain't this grand. So much for sending in your astral scout. Does anybody know how to detect this drek from the outside?)<<<<<
—Wraith II (01:02:33/12-21-55)

>>>>>(Research, chummer. The corps ain't gonna post little stickers that say, "WARNING—THIS AREA PROTECTED BY ACTIVE BACTERIA. ASTRAL TRAVEL WITHIN THESE PREMISES IS STRICTLY FORBIDDEN." Know your enemy before entering.)<<<<<
—BitRunner (01:05:45/12-21-55)

>>>>>(Fortunately, this drek is expensive and difficult to maintain. Cost alone should keep it from becoming commonplace.)<<<<<
—Dybbuk (04:11:45/12-21-55)

>>>>>(Expect the unexpected.)<<<<<
—Mindfire (05:56:35/12-21-55)

FAB are stored in large, pressurized tanks with built-in "feeding vats" designed to keep them alive. Once released, FAB has a relatively short life expectancy and dies within a few hours.

>>>>>(And oh does it stink. You can smell it for miles. I've breathed the drek, too—not pleasant. Wear an air filter mask for prolonged exposure.)<<<<<
—Weiner Velt (21:13:45/12-15-55)

>>>>>(BacteriTech has been the target of several recent runs (gosh, wonder what they were after?). As far as I know, none of them succeeded.)<<<<<
—Orlando (23:00:32/12-16-55)

>>>>>(Let me guess—their mages couldn't take an astral stroll inside.)<<<<<
—Slag (23:05:56/12-16-55)

>>>>>(Worse: they check in, but they don't check out.)<<<<<
—Orlando (23:07:57/12-16-55)

An alternative strain of FAB, called FAB-UV, is highly sensitive to ultraviolet light. When subjected to UV light (usually projected from hand-held or wall-mounted lighting units), the bacteria "glows." The relatively weightless bacteria move aside in the presence of an astral form, allowing observers to perceive and track the motion of an astral being by watching the displacement. Simply flood an area with FAB-UV and hit the UV lights. If security personnel see an astral intruder, they can seal off the area until security guards arrive to apprehend the intruder.

>>>>>(Oh, peachy.)<<<<<
—Turner (12:16:31/12-18-55)

>>>>>(Wanna hear scary? A mage's astral form's gotta return to his meat body within six hours or he geeks. So guess what? If the sec-slags trap you in one of their FAB-filled rooms for long enough ...)<<<<<
—Leeza (11:56:33/12-24-55)

Unfortunately, both strains of FAB have proven less than 100 percent reliable when fielded in mobile containers and sprayers. The bacteria works best in controlled environments with little or no air motion. Additionally, care and maintenance of both strains of FAB are prohibitively expensive; all but the best-financed clients may not find it worth the cost, except for the highest-security sites.

>>>>>(Sounds to me like FAB is a dual-natured organic substance, so it must exist simultaneously on the physical and astral planes. That would mean a magician in astral form could not pass through it, move it, harm it, or destroy it.)<<<<<
—Slag (12:10:35/12-26-55)

>>>>>(Is this stuff dual-natured? Is that how it works?)<<<<<
—Wraith II (12:30:22/12-27-55)

>>>>>(I don't think FAB is dual-natured. KE's just saying that as a smoke screen. I think BacteriTech bred this stuff by pure luck; I bet they don't even know why it does what it does.)<<<<<
—BitRunner (12:34:55/12-27-55)

>>>>>(Wait a minute! I thought an astral being cannot affect a physical being?)<<<<<
—Wraith II (23:34:15/12-28-55)

>>>>>(Don't forget, an astral being cannot pass through living material. The FABs are physical, but tiny; they act like a fluid, displacing around the astral magician the way water displaces around your foot when you stomp in a puddle.)<<<<<
—Grendel (23:39:34/12-28-55)

>>>>>(Yeah, but aren't bacterial structures too small to block astral forms? Ivy and moss work because they have a structure.)<<<<<
—BitRunner (23:45:12/12-28-55)

>>>>>(The air's full of normal bacteria. Why doesn't it work like FAB-UV? It's physical, isn't it? If somebody astral can't move or pass through something with physical mass, how can an astral being travel through air filled with any bacteria?)<<<<<
—Dybbuk (00:23:12/12-29-55)

>>>>>(Good point. Maybe BacteriTech™ ain't telling all it knows. I know I'm not buying the official explanation (dual nature, my hoop!). Bitrunner's right, though; normal airborne bacteria is too small to affect astral beings. What the critical mass is, no one can say. But FAB works, so it must have some kind of large inter-bacterial structure. I'm betting on superlong molecules of amino acids, produced by the bacteria as a waste product and creating large clumps. That would also explain the short life span.)<<<<<
—Mindfire (00:29:24/12-29-55)

The latest addition to the FAB arsenal, the astral containment net, is made of interconnected, hollow polymer tubes filled with FAB and loaded into a modified netgun. An astrally perceiving magician, an adept, or even a mundane security guard armed with the netgun physically patrols a protected area; upon detecting an astral intruder, the security operative fires the net and captures the intruder within an astrally active barrier that also has physical mass. Mundane individuals lacking the innate ability to detect astral intruders can use the BacteriTech™ Netgun in conjunction with a FAB–UV aerosol and a portable ultraviolet light.

>>>>>(Idea time. Why not get a gel gun to fire pellets of FAB at an astral form that's been spotted using FAB-UV? Geek the mage real good.)<<<<<
—Slag (02:23:45/12-31-55)

>>>>>(No go, Slag old friend. Explaining the metaphysics of the thing would take forever, but essentially an astral mage has no "mass" and thus no resistance to the slug. At best, your bullets can only push him back. Note, however, that the same can be said for the netgun. The net has to totally surround the mage, or it'll just displace him through the wall, or floor, or what have you.)<<<<<
—Mindfire (02:29:36/12-31-55)

>>>>>(Not if the wall or floor is filled with FAB.)<<<<<
—Whisper (03:05:45/12-31-55)

Magical Alarms and Countermeasures

Though not "technological" in the strictest sense of the word, increasingly sophisticated arrangements of anchored spells are becoming more and more common as alarms and intrusion countermeasures. Many different combinations of such spells exist, limited only by the imagination and abilities of the spellcasters. All such spell-based magical protection, however, consists of at least two anchored spells connected by at least one spell link.

Most magical alarms and countermeasures use detection spells anchored to given places, and linked to secondary spells that alert security personnel to an intruder's presence, physically detains the intruder, or otherwise renders him immobile until security personnel can arrive on the scene. The detection spell activates as soon as it senses the intruder's presence, triggering the secondary spell (or spells). Secondary spells can either strike a specific target or affect all targets within a given area. Among the most popular spells used for this purpose are barrier spells, which throw a barrier of magical energy across an intruder's path; thunderclap spells, which make a loud noise that activates conventional sensors; and area-effect stun spells such as stunball and stunblast that can knock out several intruders in a localized area.

>>>>>(Some chummers of mine went on a run once and got caught by one of these "magical countermeasures." Some secmage had anchored a detect person spell to a certain room through which you had to pass to get to the good stuff and linked it to a stink spell. My chummers triggered the detection spell, wandered into the center of the stink spell's radius and got hit with a mega-explosion of a stench that one of them described as "eau de rotting skunk carcass, blended with vintage thousand-year-old eggs." It was so sudden and so awful that they couldn't do anything for several minutes except double over and empty their stomachs. Of course, that several minutes was all the corp secboys needed to get to 'em.)<<<<<
—Mr. Wizard (23:04:56/11-07-55)

>>>>>(Your chummers got off easy. I've heard rumors about corps using anchored detection spells linked to little gems like flame bomb spells. "Somebody's here who shouldn't be—BOOM!!")<<<<<
—Gadfly (23:10:09/11-07-55)

>>>>>(Rumors is all they are, Gadfly. Think about it; any corp stupid enough to use that kind of security measure runs far too high a risk of crisping their own staff. "Oops—looks like Johnson forgot

about the flame bomb spell covering the research lab. Shouldn't have worked after hours, poor slot!")<<<<<

—Magicker (23:22:01/11-07-55)

MAGICAL SECURITY FUNCTIONS AND PERSONNEL

The typical contemporary magsec department consists of the following subdivisions: guards and wards, physical defenses, research, and special assignments.

Guards and Wards

Guards and wards personnel patrol astral space within protected areas, create and maintain astral wards, summon and control beings such as watchers and elemental spirits, and keep protected areas under surveillance via fiber-optic observation networks. Mages assigned to the latter task are often sorcerer adepts, capable of casting spells but not of astral projection.

>>>>>(Don't be fooled. Plenty of these guys are full-fledged mages capable of anything.)<<<<<

—Dybbuk (12:09:56/11-12-55)

>>>>>(Fiber-optic systems are so alien to the world of the shaman that almost all the mages manning such operations are hermetics.)<<<<<

—Whisper (15:09:32/11-16-55)

Patrol mages inspect protected areas, customarily once or twice a shift in less secure sites and more or less constantly in high-security areas. Because astral projection is draining for a mage, at least two should be assigned to patrol duty in each shift. Most Knight Errant guard mages work in teams of three or four, depending on the needs of the client.

Security mages often use watchers, elementals, nature spirits or ally spirits to help them patrol the astral plane. Such helpers can be instructed to tell the on-duty mage when an intruder is present, alert physical security personnel, or trigger astral traps or detaining devices to catch an astral interloper. In general, other spirits perform these functions better than watchers or elementals; elementals are harder to summon, and both elementals and watchers can provide only a limited number of services before they dissipate. Nature spirits, by contrast, can protect a site astrally from sundown to sunup. Also, a nature spirit in tune with a facility as a whole can protect it without aid from other sources, notifying its shaman of both physical and astral intruders anywhere in the facility.

>>>>>(Nature spirits might be best for the job, but they're not commonly used. The first reason is cost; security shamans who can summon them are rare birds and can charge quite a lot for their services. Also, the instructions given to a spirit are critical. They can't memorize the faces of all authorized personnel at a

facility, so some type of pass is needed to show the spirit that the person is a friendly. And of course, any ID system is vulnerable to counterfeiting.)<<<<<

—Mindfire (15:31:18/11-16-55)

Because the number of security mages is relatively small, they can and do command a high price for the valuable skill of creating wards. The cost, coupled with the fact that individual wards can only cover relatively small areas, may make them prohibitively expensive for many corporations. Knight Errant recommends reserving a portion of your total security budget for warding around the most sensitive areas in your corporate site and adding other layers of physical and/or technical protection around the wards.

Physical Defenses

Personnel assigned to physical defenses install, inspect, and repeatedly test astral barriers and all security measures put in place to deter or detain astral intruders. Physical adepts in this subdivision astrally scan the perimeters of protected areas in search of any flaws and are often called on to help deploy astral barriers quickly in the event of a security breach. Other personnel install and test various types of living walls.

>>>>>(And you thought all those pretty, ivy-covered R&D sites just proved that the big, bad corps have a green side!)<<<<<

—Whisper (12:54:21/11-02-55)

>>>>>(Ivy and moss cannot cover windows or doors, and don't completely cover roofs either. A well-executed site security system uses such natural growth to channel the movement of astral beings to areas patrolled by watchers, paranormals, and the like. So if you go through a hole in the ivy, be sure a hellhound isn't waiting on the other side to take your head off.)<<<<<

—Wraith II (13:34:32/11-04-55)

Research

The research subdivision has the vital responsibility of keeping corporate magical security on the cutting edge. Most research personnel provided by reputable security firms work with mundane scientists trained in magical theory as well as the hard sciences to develop new magical security technologies and techniques. Knight Errant security mages assigned to research are career thaumaturgists with advanced degrees from the best-known institutions, and also have considerable field experience testing new magical security systems—a rarity among magical security providers.

>>>>>(Hermetics love this kind of post, but I've yet to see a shaman working in the magical-research straitjacket.)<<<<<

—Wraith II (06:50:20/11-23-55)

Special Assignments

As all corporate executives know, the responsibilities of different departments occasionally overlap. Magical security is no different; magically gifted personnel may be needed to fulfill a variety of special assignments outside the standard magsec duties in the interests of giving the corporate client the most effective, efficient, and comprehensive security blanket. Personnel security often requires magical support for investigations, interviews and interrogations; topnotch physical security requires magical support for its fast-response teams or may use mages to screen guests at important functions; executive protection teams usually include a magician and a physical adept. Knight Errant security mages can fill these and many other roles, depending on a client's needs.

>>>>>(Ever had an investigator ask you questions in the presence of an "assistant" who sits there and stares off into space? Mr. Blank-Screen's a mage checking the truth of your statements. It's a scary thing to go through.)<<<<<

—Suit (10:56:32/11-05-55)

>>>>>(Most special-assignment mages are the best of the best; KE and others can afford them by tacking on mega-premiums for "Extended Personnel Security.")<<<<<

—Mindfire (12:03:58/11-27-55)

USING SECURITY SHAMANS

Because security as a whole is a regimented field whose procedures and responses are pre-planned and coordinated whenever possible, the majority of security mages are hermetic magicians rather than shamans. The structured demands of the job appeal to the hermetic's orderly mindset, while many of the more freewheeling shamans find that same structure unappealing.

>>>>>("Freewheeling," of course, being a corpspeak euphemism for "festering pain in the hoop.")<<<<<

—Toni (10:22:56/11-23-55)

>>>>>(If shamans are such a royal pain, why do corps hire them?)<<<<<

—Slag (11:32:44/11-23-55)

>>>>>(Primarily because they can use nature spirits. Nature spirits can guard both astral and physical boundaries. Personally, I'd rather deal with an elemental than a nature spirit; nature spirits are sapient, so they get ideas of their own.)<<<<<

—Mindfire (12:00:02/11-23-55)

Of the shamans working in the field, those with certain totems tend to have certain predispositions that suit them for particular areas. For example, shamans who follow Wolf and Dog totems—as do most in this field, in fact—often see their fellow security personnel as their "pack" and the corporate site as their "territory." These attitudes make them extraordinarily protective of the facility and its occupants, much more so than the hermetic mage who may regard his work as an ordinary job. In general, Wolf shamans prefer working at rural or remote sites while Dog shamans are more comfortable in suburbs and cities.

Security shamans who follow Snake and Bear—the next most common totems in the security field—do not share the

territorial imperative of the Wolf and Dog totems and so are better suited for protecting individuals than corporate facilities. These shamans make excellent members of executive protection teams.

>>>>>(What about biomedical research sites?)<<<<<
—Roving Rover (23:02:34/11-31-55)

>>>>>(Any Dog or Bear shaman in his right mind would abhor those places—unless, of course, we're talking toxic magic.)<<<<<
—Whisper (24:10:30/11-31-55)

In general, shamans who follow the totems equivalent to animals that can be trained for guard duty are more likely to be interested in security work.

>>>>>(Hey, the drek about guard animals in **Physical Security** talks about using geese to protect a site. Does that mean Goose shamans do security work?)<<<<<
—Roving Rover (00:22:39/11-15-55)

>>>>>(Goose shamans only live on the islands of Hawai'i.)<<<<<
—BitRunner (01:12:58 /11-15-55)

>>>>>(Different Goose, chummer. The Hawai'ian Goose is the Anglo name for Nene. The Goose totem followed by a Goose security shaman is as different from Nene as Wolf is from Dog.)<<<<<
—Dybbuk (03:46:10/11-15-55)

>>>>>(Okay—following that logic, what about barghests or hell hounds? They are used for security work. Do they have equivalent security shamans?)<<<<<
—Roving Rover (03:55:12/11-15-55)

>>>>>(Rover, you're talking about a shaman following a paranormal animal totem. That doesn't happen. It's impossible.)<<<<<
—Dybbuk (04:33:43/11-15-55)

>>>>>(Are you sure about that, Dybbuk?)<<<<<
—Mindfire (11:13:22/11-15-55)

>>>>>(Huh?)<<<<<
—Dybbuk (11:15:22 /11-16-55)

Corporate executives are advised to keep these predilections in mind when contracting security shamans. Knight Errant will make these decisions before assigning shamans to your corporation, after full consultation regarding your site's security needs.

>>>>>(Pay attention to this, folks. Before you go into a facility, find out what kind of magician is guarding the place. Lots of high-tech and fiber-optics means you'll probably face hermetics. Low-tech/enviro-friendly is a sure sign that a shaman's waiting for you. Each type of magicker has different weaknesses to exploit and requires a different approach to handle. For example, if the place is guarded by a shaman, make your move just at sunup. The spirits he's had with him all night will be gone at sunrise, and he'll be busy summoning new ones.)<<<<<
—Whisper (14:44:32/11-17-55)

MATRIX SECURITY

Matrix security, more commonly known as "matsec," is one of the most vital components of a comprehensive and effective corporate security system. Information—whether a corporation's financial records or its latest industrial designs—remains perhaps the most valuable commodity of our time. And given the increasing use of computer matrices for data storage and manipulation, the need for complete and efficient matrix security systems grows more important each day.

Knight Errant has long been a leader in the field of matrix security, with expertise that no other security firm can offer. We can provide highly trained security deckers, state-of-the-art intrusion countermeasure programs, and the latest hardware to create an effective, efficient matrix security system tailored to your needs. The following overview of matrix security development will enable you, our customer, to better understand matsec in general as well as Knight Errant's available matrix security systems.

>>>>>(Who do they think they're foolin'? They can't stop us from breaking into their matrices. Sure, their security deckers may nab the occasional amateur or their IC may geek the careless slag who gets into a corporate matrix that's over his head. But KE's security deckers—or anyone else's, for that matter—have never been able to stop a real professional decker determined to get into a system. It's just not possible. For every new security program or new piece of hardware they come up with, a hundred people will be devising ways to get around it. It's like a game.)<<<<<

—Ivanhoe (03:16:28/11-09-55)

>>>>>(Yeah, right Ivan—some game. For anyone else out there getting ideas, think about this—of those hundred people devising ways to defeat the latest IC, about ninety-nine will die trying or get their brains so badly fried they'll wish they were dead. The first time you see someone's eyes turn up into their sockets and the drool start coming out of their mouth as the black IC does its work, you'll realize that people play for keeps in the Matrix. It's true we seldom hear about successful datasnatches and Matrix runs, but no one likes to talk about the countless deckers who get geeked either.)

—Lola T. (06:12:18/11-10-55)

A HISTORY OF MATRIX SECURITY

The origins of today 's matrix security systems and technology can be traced directly to the computer security departments common to corporations and government agencies during the late 20th and early 21st centuries. These departments existed to protect an organization's computer hardware, software, firmware and data.

>>>>>(And there were deckers back then, too. They called 'em "hackers," and some of them were quite accomplished. They used primitive home computers to hack into national defense systems, bank records, you name it.)<<<<<

—Brainiac (07:13:19/11-11-55)

To perform these tasks, the departments employed computer scientists and security specialists who designed and implemented procedures, programs and hardware to protect an organization's electronic assets. The mission of contemporary matrix security differs little from these aims; today's security deckers protect much the same assets as did their twentieth-century counterparts. However, the tools and techniques used by the matsec practitioner have changed drastically as a result of several important events.

The first of those events occurred on February 8, 2029, when a computer virus of unprecedented power and unknown origins struck computer systems across the world. Computer security officers and system administrators scrambled to shut down their systems. In most cases, they failed; the virus crashed innumerable systems, wiping them clean of their data and even burning out their hardware. As the virus spread, governments toppled and the world economy nearly collapsed. Within the first quarter of the year, the virus had shattered the Grid, the data network that connected computer systems worldwide. In response, the president of the UCAS ordered the creation of a multi-agency task force to contain and destroy the virus. The members of the resulting Echo Mirage project soon found themselves overwhelmed by the psychological demands of psycho-physiological combat in cyberspace, and so the project leaders began recruiting the most brilliant data-processing mavericks private corporations had to offer.

>>>>>(Kinda interesting how the authors of this account don't even speculate about the origins of the virus. Could it be that the anarchist hackers created the virus that crashed the Grid? I guess admitting that would mean admitting that all the computer or matrix security in the world is kinda limited.)<<<<<

—Geekster (12:03:50/10-06-55)

>>>>>(Or perhaps they don't want people thinking about the origins of the virus because someone might bring up that nasty old rumor about the virus being a corporate computer-security project that went outta control. Frag, some people even claim that the corporate talent recruited to contain the virus were the same slots who created it in the first place.)<<<<<

—Brainiac (12:15:45/10-06-55)

By August of 2029, the team used improved cybertechnology to begin a coordinated attack on the virus. Eighteen minutes after engaging the virus in cyberspace, four Echo Mirage members had died, victims of lethal biofeedback induced by the virus. During the continuing assault on the killer virus, the remaining Echo Mirage members learned they could easily defeat existing computer security measures by using their cyberterminals. As a result, several corporations began to develop new security software designed to repel intruders using matrix interfaces and to aid in the containment of any future viruses These new programs were the first generation of intrusion countermeasures, more commonly known as "IC."

>>>>>(It just warms my little heart to think of those selfless corps, protecting us all from future viruses. The truth is, the slots were drekking in their pants when they realized that anyone with a cyberdeck could get into their systems. And

of course, our KE friends don't mention that black IC was one of the first types of intrusion countermeasure developed.)<<<<<

—Einstein (13:24:26/10-05-55)

Meanwhile, the members of Echo Mirage developed new combat programs and more powerful cyberterminals, as well as new techniques to combat the virus. By late 2031, the team had finally destroyed the last remaining concentration of the virus code. The task had cost billions of dollars and claimed the lives of twenty-five of the original thirty-two members of the Echo Mirage team. Four Echo Mirage veterans returned to the corporate employers who had so generously loaned them to the project. Within five years cyberdecks had become commercially available. The appearance of these cyberdecks, as well as the IC, hardware, and firmware developed by Echo Mirage designers, represents the birth of matrix security as we know it today.

>>>>>(Can you believe this bulldrek! This makes it sound like the corps saved the world from the dreaded killer virus. Don't get me wrong, I'm indebted to the men and women who died fighting the virus just as much as the next slag, but it was Echo Mirage who did it—not the corps!)<<<<<

—Hairball (13:34:29/10-11-55)

>>>>>(No drek, HB. Check this out—I was browsing through Corporate Shadowfiles elsewhere on this system and found something interesting about Knight Errant's boss, Damian Knight. Seems his real name is Major David Gavilan, USAF, commander of—you guessed it—the Echo Mirage project. Seems Gavilan bugged out soon after Echo Mirage closed down and was never heard from again. Now this thing we're reading is a Knight Errant manual, and Gavilan/Knight runs the KE show. So it seems pretty obvious that this whole "corps saved us all" drek is just a smokescreen designed to hide what really happened to him.)<<<<<

—BitRunner (03:14:36/10-12-55)

>>>>>(Soundz great, but that wuz more than twenty years ago. If this Knight/Gavilan thing is true, what duz he still have to hide? If he is still creating propaganda to cover his tracks it must be something really heavy.)<<<<<

—D. (04:20:21/10-12-55)

>>>>>(Or it could be a red herring to keep us guessing about Damian's true background.)<<<<<

—Doomstar (06:10:12/10-13-55)

LATER EVOLUTION

Initially, matrix security divisions concerned themselves solely with protecting their corporation's computer assets, such as data, software, hardware and firmware. But as security technologies such as closed-circuit video and trideo, access controls, maglocks, and alarm systems became increasingly networked and complex, matrix security personnel found themselves spending larger amounts of time operating these systems—while still shouldering full responsibility for computer security. This development overtaxed matrix security workers and forced personnel trained as computer scientists and technicians to handle "traditional" security problems and incidents. As a result, intruders found it increasingly easy to defeat technical security systems.

To help alleviate this problem, security system designers developed matrix-accessible security systems and hardware. These enabled matsec personnel to control maglocks, alarm systems and the like without having to leave their firms' matrices. Unfortunately, the new hardware also enabled any intruder who gained access to a company's matrix to control these systems. And so matsec personnel ended up monitoring an increased number of matrix nodes—the new technology intended to decrease their work load actually increased it. System designers created intricate program frames and IC to ease the burden, but this additional software severely slowed and occasionally overloaded corporate matrices. Unauthorized intrusions continued to increase, forcing matrix security personnel to spend even more time monitoring non-matrix security systems.

Advent of Security Riggers

In the late 2040s, designers at CerebroTech, a wholly owned subsidiary of Ares Security International, began experimenting with Artificial Sensory Induction System Technology (ASIST) in an attempt to create a more efficient means of controlling matrix-accessible external security systems. Unfortunately, the layers of programming required for the user interface on an ASIST-equipped cyberdeck slowed the system to unacceptable levels. The CerebroTech team solved the problem by combining Muscular Signal Transference (MST) technology and Vehicle Control Rigs (VCRs) used by riggers with ASIST technology. This breakthrough resulted in the first closed-circuit simsense (CCSS) system.

By 2050, the first CCSS systems were operational. These systems enabled riggers to "drive" a security system in much the same manner they control a vehicle. The new "security riggers" enabled matrix security personnel to again devote themselves exclusively to patrolling the matrix. The development also enabled corporations to remove all non-matrix-related security functions from their matrices, making these functions less vulnerable to intruders. As the work of security riggers has become increasingly important in recent years, many firms have begun creating separate technical security divisions to oversee these tasks. For more information on security riggers, see **Technical Security**, p. 32.

>>>>>(Removing non-matrix-related systems from matrices may have made them less vulnerable to matrix intruders—but not invulnerable by any means. In fact, in a way it makes defeating such systems easier. All you have to do is take out or pay off the security rigger controlling the systems.)<<<<<

—Sutton (17:16:32/09-15-55)

>>>>>(You gotta be fraggin' whacked to trust some corp security rigger. I had some chummers who made that mistake. They were doing a run on a Mitsuhama facility—shoulda been a milk run. They paid off the security rigger scheduled to be working that night and got into the place, null perspiration. While they were inside, he raises the fraggin' alarm. The entire team got geeked as they conveniently "disobeyed" the security warnings. Apparently, the fragger figured everyone who knew about the run was inside the facility at the time. Course, he didn't realize that I knew. The following week he died in a tragic accident when his home simsense rig malfunctioned and fried his brains.)<<<<<

—Mad Doggy D. (05:10:26/09-18-55)

DESIGNING A MATSEC SYSTEM

All modern matrix security systems are composed of three components—security deckers, intrusion countermeasures, and hardware. All Knight Errant matrix security systems provide the highest quality components available. Many of our highly trained, experienced security deckers, for example, have backgrounds in military, intelligence, or law-enforcement matrix work. Knight Errant also works

closely with the most highly respected software and computer firms to provide you with state-of-the-art intrusion countermeasures and the latest hardware and firmware—all custom tailored by our specialists to meet your matrix security needs.

Before designing any system, members of our matrix security technology division will visit your work site to evaluate your existing matrix system and meet with you to discuss your security needs. Within a few days, they will return with several recommended security configurations. Our experts will recommend security decker staffing arrangements, intrusion countermeasure configurations, and any modifications or additions to your hardware needed to provide the best matrix security available. You are free to choose from any of the recommended systems or consult with our experts to modify any of the recommended designs to best fulfill your requirements.

Once you have approved a system, we will assemble all the necessary components and install them within days. Knight Errant will provide dedicated security deckers who perform matrix security work exclusively. Depending on your needs, these deckers will perform matrix watch duties themselves or train your own deckers to carry out security operations. Once your system is in place, our deckers will run mock-intrusion drills to thoroughly test the entire system and keep it running at optimal effectiveness.

HOW IT ALL WORKS

Once your matrix security system is in place, roaming security deckers and certain forms of intrusion countermeasure programs (IC)—white and access—will "patrol" your matrix constantly. If a decker or IC program detects any persona that lacks the proper identification codes, the decker or IC triggers a passive alert. If further attempts to identify the persona fail, the decker or IC triggers an active alert. The decker may then attempt to detain the persona himself or call for additional security deckers. If an IC program triggers the alert, the decker monitoring the system will dispatch at least one security decker to investigate. In addition, any variety of aggressive IC programs—the so-called gray, blaster, killer, and trap IC—may be activated to confront the intruder.

>>>>>(Those "aggressive" IC programs are the least of your worries if you're running in a KE-protected matrix. What the little book here doesn't mention is the infamous "Black Knight" IC the KE boys employ. Don't get me wrong. They'll try to detain you if possible. It only makes sense, because the customer is gonna wanna find out who sent you snooping around their matrix and why. But if the KE matrix cowboys can't catch you, they won't hesitate to loose Black Knight against you. And that drek'll geek you right nicely.)<<<<<

—The Professor (15:35:22/12-01-55)

>>>>>(They don't restrict it to a last-resort measure, either. The KE matsec folks regularly recommend that their clients protect the most sensitive nodes of their systems with black IC.)<<<<<

—Brainiac (20:31:22/12-01-55)

If these measures fail to detain or repel the intruder, the decker controlling the system may institute a partial or complete shutdown of the system, depending on the configuration of your matrix security system and the security rating of the node where the intruder is detected. A shutdown dumps the intruder from the affected nodes or system. Any legitimate users in a node or system about to be shut down receive a warning of the impending event and the system automatically backs up their work. Of course, the backup feature may be disabled for the most sensitive nodes to allow for more rapid shutdown.

In addition to these measures, Knight Errant's matrix security team can outfit particular nodes of your matrix with access IC, barrier IC, or scramble IC to provide additional security.

PERSONNEL SECURITY

No corporation can afford to be without the very best personnel security. This portion of your overall security blanket allows you to discover and deal with potential security breaches involving the one group of people who has a legitimate right to enter the corporate premises every working day: your employees. Personnel security, or persec, lets you determine which employees are or may become a risk to themselves or to the corporation. Persec also handles security intelligence and counterintelligence operations, through which it protects the employees that are every corporation's most valuable asset.

>>>>>(How noble.)<<<<<
—Slag (09:06:45/11-29-55)

>>>>>(I think the trog misunderstood the statement. Persec protects the employees for the corporation's benefit.)<<<<<
—Papa (09:10:34/11-29-55)

>>>>>(Sarcasm, Papa dearest. Sarcasm.)<<<<<
—Slag (09:16:24/11-29-55)

INVESTIGATIONS

Unfortunately, virtually every corporation suffers losses from the "internal threat"—employees who steal from their employer, harm the corporation or help others to do so. To minimize this ever-present danger, personnel security operatives conduct background investigations of a corporations' potential employees and periodic re-investigations of its current employees, as well as conducting loyalty checks and special investigations on known or suspected troublemakers.

>>>>>(Ever wonder how some corps define troublemakers? It's a scary list, folks. People who ask for personal time or take sick leave, or—horror of horrors—take a vacation are seen as a real threat by some corps. I've seen KE start investigations on a poor sap who organized the company picnic while on company time.)<<<<<

—Suit (22:01:40/10-24-55)

>>>>>(Most corps don't go to that extreme, simply because their sec providers (KE or whoever) have already vetted the corp workforce to make sure they're all nice, obedient sheep. The investigation of a potential employee is a critical part of personnel security; being ruthless at this early stage minimizes the number of "troublemakers" and potential security risks who get into the organization.)<<<<<

—Neuron Surfer (23:08:55/10-24-55)

>>>>>(But once you're in, you've signed your life away. Persec monitors your every move. They watch who you meet, who you talk to and for how long. They monitor your fragging bank account. They track your movements in the office through the key card that lets you into your cubicle. They reduce your entire life to statistical norms: how many times you go to the bathroom, how many lunches you take at that Chinese place down the street. You bounce out of your norm just once and a visit from persec is on the agenda.)<<<<<

—Suit (23:13:56/10-24-55)

There is, of course, no foolproof way to single out potentially dishonest employees. Effective screening procedures such as those offered by Knight Errant, however, can eliminate applicants with unsavory pasts or those who may be unstable and therefore untrustworthy. Tests that measure a job applicant's honesty index are among the initial, basic screening measures offered by KE and other security providers. Of course, honesty tests and other screening procedures are only the tip of the personnel-security iceberg. They can eliminate obvious risks and point out potential difficulties, but they can never completely guarantee the performance of prospective or current employees under changes that may occur on the job or in their private lives. The only way to completely guard against security risks is through constant surveillance and periodic reinvestigations of previously vetted employees. Knight Errant keeps these investigations as subtle as possible without compromising thoroughness, in order to avoid causing resentment that might turn an honest employee into a dishonest one.

>>>>>(Oh, lovely. How do you "subtly but thoroughly" investigate Joe Wageslave—who's actually bought into the idea that The Almighty Corp is his mommy and daddy and grandparents all put together and would never do anything to harm it—without provoking resentment because the corp he loves so much doesn't trust him a centimeter?)<<<<<

—BizWatcher (20:57:03/11-11-55)

>>>>>(Does anybody love the corps that much?)<<<<<

—Slag (21:02:23/11-11-55)

>>>>>(You'd be surprised.)<<<<<

—BizWatcher (21:06:34/11-11-55)

>>>>>(Whether Joe Wageslave loves the corp or not is immaterial. By investigating him "just because," the corp lets him know he's guilty until proven innocent.)<<<<<

—Dark Justice (22:09:22:/11-11-55)

>>>>>(And that surprises you? What century are you living in?)<<<<<

—Reality Czech (22:13:45/11-11-55)

Another problem can arise when corporate clients whose operations require high degrees of technical skill undercut the effectiveness of their own screening programs. At times, personnel security teams find it necessary to turn away applicants with unique qualifications because they pose a security risk. Corporate executives should think twice before resisting the recommendations of the personnel security team in these cases; overlooking security risks for any reason inevitably turns out to be a bad bargain. To ensure such conflicting needs are balanced, Knight Errant works with its individual clients to develop selective procedures. Such programs add a little extra cost, but ultimately pay for themselves in reduced losses, more loyal employees, and lower turnover.

>>>>>(I've heard about one place that gets around this problem—at least among its mid-level technocrats—by fitting them with high-level skillsofts. As long as the job in question doesn't require creative thinking, the savings in security are enough to recoup the cost of fitting everybody. It also gives the corp a workforce with a uniform set of skills that can be quickly updated without incurring education expenses or paying for lost working time. The biggest advantage, though, is the fact that the workers check their skills at the door before they go home. It's easier to guard a vault full of skillsoft chips than 300 microcircuit engineers who might want to go and work across the street.)<<<<<

—The Chromed Accountant (10:34:56/12-01-55)

>>>>>(You want to trash that corp? Sneak a little virus into the next skillsoft update. All the wageslaves plug in the next day, and zing, they spend the day playing connect-the-dots on a microcircuit.)<<<<<

—Waki (11:56:43/12-01-55)

Effective investigation of applicants and/or current employees includes thoroughly checking each individual's employment history and references. Knight Errant's personnel investigators check employment, financial, and educational records by interviewing former supervisors, co-workers, neighbors, and friends. References in particular are thoroughly explored to uncover other associates of the subject. Interviews with these associates often prove invaluable in establishing an accurate picture; individuals used as references, after all, are most often good friends or favored fellow employees and are therefore disposed to be biased in the subject's favor.

>>>>>(All you runner wannabes, key in on this last paragraph. If you're looking to slip your most excellent self into a corp, make sure your background data and funny SIN are airtight. And make sure the security witchhunters can't get to any of your louder-mouthed friends.)<<<<<

—Papa (10:57:23/11-29-55)

>>>>>(Bogus SIN and background chatter's easy if you got the nuyen!)<<<<<

—Slag (11:00:30/11-29-55)

>>>>>(Yes, but quality costs. Buying that sure-thing background might well cost you more than the job's worth. That's why most runners don't use the insider approach—the economics don't work out.)<<<<<

—The Chromed Accountant (11:16:45/11-29-55)

Signs of instability in personal relationships, frequent shifts from job to job, a history of declining salaries, or unexplained gaps in employment history may indicate a security risk. Applicants who are overqualified for the position in question or have difficulty recalling the names of supervisors in the recent past, or who cannot give accurate recent addresses may also be risks.

>>>>>(So think twice about dumping your no-longer-significant others, boys and girls. Wouldn't want to look like we had "unstable personal relationships," now would we?)<<<<<

—Socio Pat (18:32:09/11-28-55)

INTELLIGENCE/COUNTER-INTELLIGENCE OPERATIONS

An old saying describes the difference between intelligence, counterintelligence, and law enforcement: "Intelligence is the art of reading someone else's mail, counterintelligence is the art of keeping someone from reading your mail, and law enforcement is the art of catching those who are reading your mail." Intelligence and counterintelligence operations that fall under the purview of personnel security providers cover the first two of those functions. Persec conducts intelligence operations as they pertain to the corporate client's security, such as determining when a hostile corporation may attempt a clandestine operation and running defensive operations designed to protect the client's work force from hostile intelligence activities. Reputable personnel security providers do not generally initiate offensive intelligence operations against hostile corporations.

>>>>>(Right, and shadowrunners never steal for their own personal profit. This last statement is corpspeak. Translated into English, it reads, "Knight Errant (or whoever) will take any action against your enemies that you care to order, as long as we all pretend to know nothing about it if it goes bust.")<<<<<

—Orwell (20:18:29/11-02-55)

Intelligence operations most often involve gathering information about rival corporations and/or governments. The data gathered enables the personnel security team to plan effective responses to any operations these rivals may attempt. Intelligence investigators also debrief personnel who have been targeted by the opposition, to determine where the security department failed in protecting the asset and to discover how the opposition works.

Counterintelligence investigators handle briefings on possible threats and the procedures in place to neutralize them for any employees at risk: those believed to be targets of hostile operations, those assigned to temporary duty away from the corporation's holdings, attendees at multi-corporation conferences, corporate officers working on joint ventures, and so on. Counterintelligence investigators also interview employees whose periodic reinvestigation reveal unusual circumstances. Such occurrences often indicate willing or unwilling contact with persons hostile to the corporation's interests—in either case, a security breach waiting to happen.

>>>>>(So the guy who's forced to talk secrets with a rival corp so their goons won't kill his family gets treated the same as the slag who spills his guts for a nice fat credstick. And the corps wonder why so many wageslaves are so cynical ...)<<<<<

—Plus Ça Change (18:38:32/11-06-55)

>>>>>(In corps that make their money with lots of wet assets (brain power), counterintelligence is a critical part of the job. Pre-hiring investigations have to be less intrusive for top talent; you don't want to make Dr. IQ think the work environment is "unfriendly." So right off the bat, the corp's more likely to find itself stuck with a disloyal employee who might tell secrets to hostile corps (and every corp is hostile). Can't use heavy security around a valuable wet asset; being surrounded by goons or constantly watched by cameras bugs them and reduces their productivity, so upper management doesn't let you play Big Brother with them. And of course, unguarded wet assets are ripe targets for friendly or unfriendly extraction. So the security team has only one option left—the preemptive strike—and pulling that off requires knowledge. First, find out whether Herr Dr. IQ is feeding the latest formula for Stuffer Shack Nuke-and-Serve Burritos to Nerps R Us. Then keep an eye on runners and other unsavories who specialize in delivering disgruntled employees to new work environments. Once you've identified the threat and the method, call in the heavy artillery and smash them into paste before they can work their little operation. Herr Dr. IQ is not inconvenienced, his productivity for the corp in question continues undisturbed, and the profit margin for Nuke-and-Serve Burritos stays where it oughta.)<<<<<

—Neuron Surfer (15:58:34/11-13-55)

>>>>>(Need to eliminate a wet asset? Feed a paranoid security spook a line about how much of the candy store the poor slot is giving away. There's no method quite like the old tried-and-true.)<<<<<

—Papa (16:25:46/11-30-55)

SECURITY AWARENESS

Security awareness programs are designed to educate your work force on specific security measures, how to avoid compromising situations, how to handle incidents in which security is compromised, and so on.

>>>>>(Education my left foot! Try brainwashing. I've seen some of the security awareness programs the benevolent corps have produced. They program the wageslaves to follow corp management's directives like lemmings.)<<<<<

—Whisper (11:03:20/11-30-55)

Through seminars, films, programs, and briefings, security awareness specialists educate the employee on the nature of potential threats to them and to their workplace, as well as teaching various strategies for coping with whatever situations may arise. Keeping the average employee involved in the security of the corporation gives them a sense of self-worth and also keeps lines of communication open between employees and security personnel. Knight Errant designs all security awareness programs in consultation with our corporate clients, tailoring each program to the client's specifications.

>>>>>(Sounds like a bunch of elves and norms with perfect teeth trying to make everyone feel good about themselves and the corp. Gaaagh.)<<<<<

—Slag (17:23:46/11-30-55)

>>>>>(These guys look like fluff, but they aren't. They run the "squeal on your mom" side of the op. The cute little thing with the bubbly personality in the next cubicle more often than not is looking for workers who are "at risk"—the folks who grumble and grouse about the corp, their hours, their pay, you name it. These moles prowl the corridors, sit in a bathroom stall and eavesdrop on the gossip and generally act like busybodies. They're less intimidating than the Gestapo-like goon of popular fiction, and a lot more effective.)<<<<<

—Papa (19:10:45/12-01-55)

>>>>>(Notice that the writers of this lovely little KE sales pitch don't say anything about what else a personnel security specialist does. I know—I used to be one. In between running our little seminars about How the Wonderful Corp is Making Sure You Survive to Slave Here Another Day, we did lots of other little things—like check out all the people on the daily deviants list. They'd give me one at the start of each day, and I'd spend the bulk of my time asking rude, intrusive, bullying, or just plain idiotic questions of co-workers who'd done absolutely nothing to merit them. Why are you going to the bathroom so much these days, Mrs. Smith? Because being eight months pregnant is hell on the bladder—ah, yes. Of course. Mr. Jones, are you aware that you are using 15.25 percent more paper clips than normal, and would you like to explain that? Is that a bundle of pencils in your pocket, Mr. Doe, or are you just glad to see me?)<<<<<

—Suit (20:01:06/12-01-55)

>>>>>>>(So why'd you do it, then?)<<<<<

—Slag (20:11:08/12-01-55)

>>>>>(Because if I'd refused or even hesitated a little bit, I'd have been on the deviants list.)<<<<<

—Suit (20:13:45/12-01-55)

EXECUTIVE PROTECTION

Personnel—executives in particular—are perhaps the most valuable and vulnerable asset of a corporation. In today's high-stakes corporate world, a myriad of assailants—rival corporations, radical terrorists, organized crime and professional criminals—routinely target executives and their families. Unfriendly extraction, kidnapping, assassination, blackmail, and physical threats are all real dangers faced by today's corporate executive. Even the mere threat of these dangers can seriously impede an executive's efficiency; and if one of your executives falls victim to such a threat, your firm's performance and stock price as well as your ability to recruit first-rate personnel may all suffer severely.

However, a well-designed and effective executive protection program can shield your employees from danger and foster a sense of security, enabling them to concentrate fully on their work and ensuring maximum productivity.

>>>>>(This makes it sound like the corps contracting with KE don't really give two dreks about their employees beyond what their deaths or injuries may cost.)<<<<<

—Dreyfus (04:26:13/11-11-55)

>>>>>(Very observant, D-boy. You're one quick learner. What the hell's wrong with you? Did you grow up in a cave or something? Corps only care about their people as far as they affect the bottom line. They don't give a frag personally if an assassin splatters Joe Executive's brains, but news of something like that might really shake the confidence of the shareholders. And those skittish stockholders are likely to get rid of their stake in the corp and invest elsewhere. Likewise, if a corp is repeatedly hit by wet jobs or extractions, word's going to get out among prospective employees. And who the hell wants to work at a place where you don't know if you'll be heading home at the end of the day with all of your limbs?)<<<<<

—Bill B. (02:16:54/11-12-55)

>>>>>(You'd be surprised how jumpy people can get when it becomes clear that a corp can't protect its own. I'm not saying I've ever done it myself, but I've heard of corps hiring terrorists and criminals to wage harassment campaigns against rival corps.)<<<<<

—Ratboy (13:35:56/11-12-55)

>>>>>(Wouldn't that lead to outright warfare between the corps?)<<<<<

—Dreyfus (12:23:43/11-13-55)

>>>>>(Only in a few extreme circumstances, Drey. The corps contract independents to carry out their drek work—it's virtually impossible to track down who's behind a terror campaign. And usually a targeted corp does not want to draw any extra attention to the fact that it cannot protect its employees.)<<<<<

—Ratboy (12:40:32/11-13-55)

UNMATCHED PROTECTION

The wide range of threats faced by today's corporate executive makes executive protection one of the most demanding areas of corporate security. Each and every potential attacker can hone his skills and plan of attack—and so the executive protection provider must devise a flexible program that effectively protects against a variety of attacks, including those the provider has not predicted. Few, if any, other security providers in today's market can match the vast resources of Knight Errant or our firm commitment to using the most sophisticated technology available to ensure the safety of your executives. For example, Knight Errant maintains a massive database of criminal offenders that rivals those of many national law-enforcement and intelligence agencies.

>>>>>(That database makes a great business directory if you ever need a little dirty work done. The "whereabouts" entries for most of the people in the database are usually outdated, but the entries provide nice little rundowns of everyone's particular "talents.")<<<<<

—Brainiac (14:02:06/11-25-55)

But perhaps the most important resource Knight Errant possesses is our group of skilled executive-protection personnel. After all, effective security first and foremost requires judgment and training. All Knight Errant execsec personnel receive extensive training in armed and unarmed combat, emergency medical techniques, countersurveillance techniques, piloting and driving, and communications technology. In addition, many of our execsec specialists have worked for the top state, corporate and military security agencies in the world, providing them with the expert judgment that only years of experience can instill. In addition, all KE personnel receive training in social skills and cultural literacy that enables them to operate unobtrusively in any social setting. Finally, Knight Errant assumes all liability for the actions of its security personnel.

>>>>>(Knight Errant assumes liability? That's supposed to be a selling point? I'd think that would kinda frighten off clients.)<<<<<

—Dreyfus (12:16:23/11-16-55)

>>>>>(Most would-be clients understand that execsec can be a messy business, and sometimes people make mistakes. Didn't you ever hear of the Unicom affair? I'll clue you in. It happened a few years ago. Seems that Unicom, a small software firm, had been negotiating a deal with a larger manufacturer to share research and facilities. Anyway, they reached a deal, and several of the head execs from the two firms were sharing a celebration dinner when disaster struck. Apparently, Unicom's security people hadn't been notified that one of the larger firm's vice-presidents would be arriving late. Unfortunately, the veep in question bore an uncanny resemblance to Rory O'Callahan, the international terrorist. Anyway, the veep came in unannounced, and being quite full of himself—as these corp types so often are—expected the security people to recognize him. Well, they didn't, and when he refused to stop and identify himself, they let him have it. The larger firm sued Unicom, which ended up paying millions of nuyen in a settlement.)<<<<<

—Emma Li (12:20:24/11-16-55)

>>>>>(Just goes to show you—always be polite to the nice security man and answer all his questions.)<<<<<

—Banacek (16:23:10/11-18-55)

BASIC PRINCIPLES OF EXECUTIVE PROTECTION

Any reputable execsec provider knows that the best way to provide effective executive protection is to outthink attackers rather than outshoot them. An execsec program based on this philosophy produces the safest, most effective protection while reducing the likelihood that unprofessional, trigger-happy execsec personnel will create unwanted publicity for your firm.

At Knight Errant, we incorporate this philosophy by following two basic precepts when designing and operating all our executive protection programs. We identify and anticipate threats before they happen, then carefully design measures to reduce the subject's vulnerability to these threats.

By following these precepts, our executive protection teams can minimize the risks faced by your executives. At the same time, they can allocate the available resources to guard against those threats most efficiently. This eliminates the need to waste precious security resources on unneeded procedures and produces a program that does not overly restrict your employees' activities or impede their performance of their duties.

IDENTIFYING THREATS

Identifying potential threats, or threat analysis, is the first step in designing any executive security program. Our execsec specialists begin this analysis by researching the subject's physical environment—his work place, residence, and other locations where he spends time—as well as the nature of his work and his

lifestyle. After investigating these areas, our specialists use this information to pinpoint potential attackers and the form potential threats may take.

Keep in mind that researching a subject's threat environment often requires our personnel to conduct extensive interviews with the subject, his employer, co-workers, family, and friends. Occasionally subjects do not understand this necessity and protest against what they see as an unwarranted intrusion into their work and private lives. To avoid such misunderstandings, Knight Errant recommends that you discuss your firm's security needs with any employee designated as the subject of an executive protection program before the program's implementation.

Analyzing the Work Place

The nature of a subject's work remains one of the simplest yet most effective indicators of potential threats. For example, any high-ranking executive or technical staffer involved in sensitive research may be targeted for an unfriendly extraction. Rival corporations, groups or individuals whose businesses may be hurt by the work of the executive or researcher are naturally potential threats. If the researcher or executive also works as a mage, he may face attacks from astral space.

Analyzing work place threats includes extensive background checks and monitoring of all employees. In this instance, Knight Errant's personnel security division will prove invaluable. By carefully monitoring employees, our specialists can spot undercover operatives who may be targeting subjects. Knight Errant specialists also provide a convenient means to perform checks on your own security divisions, which often prove a favored bolt-hole for undercover operatives. Our specialists also monitor all telecom links in your offices for evidence of operatives within your work place.

>>>>>(Too bad Knight Errant hasn't always been that thorough with its own people. I know for a fact that the extraction of Dr. Martin Wankov from Mitsuhama Computer Technologies was pulled off by a group of shadowrunners posing as a small security firm. They grabbed Wankov while he was on holiday in Honolulu. Apparently, the KE execsec team protecting Wankov got a little lazy when they contracted out the security for his trip.)<<<<<

—BeBop (14:10:56/11-16-55)

>>>>>(I've heard of that job too. It seems the group had a drek-hot decker who planted an entire fictional background for the firm in the Knight Errant database. The KE drekbrains guarding Wankov literally handed him over to the runners!)<<<<<

—Bettina (03:06:10/11-18-55)

Analyzing the Residence and Private Life

The subject's activities outside of work may also yield valuable information when performing threat analysis. Researching the threat environment of the subject's life outside the workplace usually begins with extensive background checks and/or interviews of any household staff the subject employs. Kidnappers or extortionists may infiltrate the household of a high-ranking executive by posing as household workers; more frequently, household workers may sell or unknowingly reveal information about a subject that aids an attacker. The telecom links of a subject's residence are also routinely monitored, and Knight Errant execsec teams also inspect the physical security measures in place at the subject's residence.

With regard to the subject's private life, KE security personnel routinely conduct background checks of the subject's friends, acquaintances and other contacts to ensure that they do not include potential attackers. Our specialists also investigate the private life of the subject and conduct an extensive interview with him. This area of threat analysis is often overlooked by less professional execsec providers, even though several aspects of a subject's private life—such as political affiliations, excessive drinking, drug or chip abuse, gambling, or deviant sexual practices—may leave the subject vulnerable to blackmail or other dangers.

>>>>>(Wow, I've been leaving myself vulnerable to blackmail for all these years without knowing it!)<<<<<

—Depraved in Des Moines (05:15:36/11-22-55)

>>>>>(I don't think it matters what kinda sordid drek rings your little bell, Depraved. From what my sources tell me, people already know you're a deviant anyway, and no one really cares.)<<<<<

—Vesparius (06:17:23/11-22-55)

>>>>>(Joke all you want. I know a slot who amassed a small fortune by blackmailing a certain former high-ranking exec over at Fuchi. Seems this exec liked to pop a few bottles of vintage Scotch, get wrecked and play hide the credstick with a certain joygirl. Well, the exec's playmate happened to work for my blackmailing friend.)<<<<<

—S. (10:17:30/11-22-55)

>>>>>(That kinda scam's getting harder to pull, cuz lots of corps have begun supplying their execs with corp-approved joygirls and joyboys. These arrangements help protect the execs—and they also provide the corporation with a little leverage come salary review time.)<<<<<

—Krusader (08:12:14/11-23-55)

Today's corporate executive must travel frequently, which places him in an entirely new threat environment. Knight Errant execsec specialists collect and analyze information on all of a subject's travel destinations for potential threats. The political climates and security agencies of each destination, local corporations, the subject's transportation providers, hotels, and other potential sources of danger all come under extensive review.

>>>>>(If you're gonna try to grab an exec, vacations and business jaunts are probably the best times. Travel always throws a lot of "unknowns" at an execsec team, and they usually overlook at least one or two. Also, they may tend to get careless (as in BeBop's earlier post).)<<<<<

—Bettina (04:17:21/11-20-55)

Identifying Potential Attackers

No threat analysis would be complete without a thorough investigation of all potential attackers. This type of research is particularly important today, as an executive may face a variety of assailants, including corporate or government-backed agents, terrorists, organized-crime figures, professional criminals, opportunists, and common street thugs. The nature of the subject's work and his physical environment largely determine the type of assailant likely to target the subject. In addition to identifying potential attackers, Knight Errant execsec providers investigate the motivations and methods of attack that potential attackers favor and create psychological profiles of all individual, institutional, or corporate threats. During this stage of designing a protection program, Knight Errant execsec providers create a watch list in our extensive database specifically for the client corporation's use.

>>>>>(These folks are always on the lookout for shadowrunners, so it's a good idea to mix up your modus operandi. Keep 'em guessing about how, when, and where you're going to strike—as well as how many runners will be on your squad and what kind of firepower you'll be bringing. Believe me, eventually these slots will pick up on even the vaguest pattern in your way of doing things. And when they do, they'll be ready for you.)<<<<<

—Arbeghast (06:15:52/10-30-55)

Identifying Potential Forms of Attack

Finally, Knight Errant specialists identify potential forms of attack. These generally fall into four different categories: blackmail, unfriendly extraction/kidnapping, assassination, and physical threats.

Blackmail is the extortion of money or valuable information from the subject by threatening to expose a past criminal act perpetrated by the subject or discreditable information about him. Unfriendly extractions and kidnappings are slightly more difficult to prevent than blackmail; unfriendly extraction involves forcibly removing the subject to a location where he can be debriefed and persuaded to abandon his ties to his employer, and kidnapping involves seizing and detaining the subject for a ransom (usually of money or information). Assassinations are even more difficult to prevent. The most difficult danger to guard against, however, are physical threats directed at the subject and/or his family. Attackers usually resort to such threats to extract information from an executive or to influence his business decisions. From the subject's viewpoint, assassination is undoubtedly the most dangerous form of attack. In truth, however, a successful blackmail attempt, extraction or kidnapping may prove the most damaging to the subject's employer.

>>>>>(I don't understand. How can blackmail or kidnapping be more damaging than having one of your execs get geeked?)<<<<<

—Dreyfus (03:16:33/11-02-55)

>>>>>(Think about it. One of your execs gets geeked, you replace him and carry on. It's a setback, but nothing you can't recover from in a couple of weeks. But say someone—a rival

corp, for instance—is blackmailing that same executive. He may end up supplying them with specs on your latest software before it hits the market, or filling them in on that big surprise acquisition set for the next quarter. He might be coerced into doing any number of things that will increase your rival's profits and probably cost your firm millions—maybe even billions—of nuyen. Hell, I've heard of instances where an exec gets so frightened by his blackmailers that he won't cooperate with his own employer's security personnel, so they're forced to geek the guy themselves.)<<<<<

—Kommando (03:24:36/10-02-55)

>>>>>(That's cold.)<<<<<

—Dreyfus (03:31:10/11-02-55)

>>>>>(That's business as usual.)<<<<<

—Lenny (03:33:22/11-02-55)

REDUCING VULNERABILITY

Once Knight Errant's execsec specialists have conducted a thorough threat analysis for the subject, they use that information to design an executive security program aimed at reducing the subject's vulnerability to the identified threats. Because every subject differs, each execsec program also differs. However, all KE programs use the same methods to reduce a subject's vulnerability. These methods include security awareness and lifestyle modification, physical and technical security measures, transportation security measures, magical security measures, information control, and aggressive intelligence gathering.

SECURITY AWARENESS AND LIFESTYLE MODIFICATION

Security awareness, an often-overlooked aspect of security, simply means keeping the subject and his family informed of security measures implemented by the execsec team. Subjects can aid in their own protection by cooperating with their security providers and following those providers' advice and instructions. Occasionally a security specialist may request that a subject alter his lifestyle to reduce his vulnerability to threats. For example, a subject who engages in excessive drinking, illegal drug or chip use, gambling, or deviant sexual practices may make a tempting blackmail target. By changing such behavior, the subject can greatly reduce his vulnerability.

PHYSICAL AND TECHNICAL SECURITY MEASURES

Physical and technical security measures are the most visible means of reducing a subject's vulnerability. Knight Errant physec and techsec procedures are described in detail in separate sections of this handbook. Typical measures associated with executive protection include full sweeps of the subject's work place and residence for electronic surveillance devices, the installation of signal scramblers on the telecom lines in the subject's work place and residence, and the assignment of executive protection specialists to accompany the subject at all times. Initially, the execsec team leader will

recommend physical and technical security measures for the subject's home and work place after the first round of threat-analysis interviews. Then the team leader will meet regularly with the subject to fine-tune these measures and discuss events and changes in the subject's schedule that may require new measures.

TRANSPORTATION SECURITY MEASURES

Work places and residences present static environments that can be fitted with numerous security systems. Providing security for a subject and his family as they travel to and from work or school, or simply leave their home for any reason, is much more difficult. As a result, the subject may be most vulnerable at these times. To reduce this vulnerability, the Knight Errant security team includes riggers trained in aggressive driving and piloting maneuvers, as well as emergency medical techniques, armed and unarmed combat, and countersurveillance. Or, if the subject prefers, the Knight Errant team will personally train a driver supplied by the subject. The team also provides an armored vehicle for the subject's use or will fit armor to a vehicle supplied by the subject. In addition, the team provides secure storage for the vehicle when it is not in use, to safeguard against vehicle bombs or sabotage.

The Knight Errant execsec team also performs advance planning for security on any trips taken by the subject and his family. Our personnel collect and analyze data about the subject's destination to identify potential threats, map out travel routes, obtain secure vehicles for the subject, and make other logistical preparations. At least one executive protection specialist accompanies the subject on every trip.

MAGICAL SECURITY MEASURES

Even the most thorough physical protection cannot protect a subject against an attack from astral space, and so magical security measures are an important part of any executive protection program. In addition to providing protection against magical threats, magical defenses can indirectly aid in defending a subject against physical attacks. Spell defenses, protective wards and elemental spirits, and magical combat expertise are all necessary for complete protection, and every Knight Errant execsec team contains a highly trained security mage who can provide these measures.

INFORMATION CONTROL

Subjects can be particularly vulnerable during activities outside of work, vacation or business trips, and public appearances. In these situations, even the most extensive security measures can be defeated by an assailant who is familiar with the precautions and has time to carefully plan his assault. To guard against such an occurrence, the execsec team maintains strict secrecy concerning a subject's security precautions and strictly controls all information concerning the subject's daily schedule, travel itineraries, and the like. By controlling such information, the execsec team can greatly reduce a determined assailant's opportunity to plan an attack.

>>>>>(These guys'll spread disinformation when it suits their purposes. I had a couple of friends who planned to grab a Renraku researcher and sell him back to the corp. Well, the researcher's protection detail got wind of the plot and let slip the guy's itinerary for a trip to a conference. My friends thought they'd scored big time when they got ahold of the itinerary. They carefully planned the grab, but ran into a team of KE security men when they went in to snatch the guy. No one's heard from my friends since.)<<<<<

—Macfly (07:24:16/11-05-55)

AGGRESSIVE INTELLIGENCE GATHERING

An aggressive intelligence-gathering program is one of the most effective means of reducing a subject's vulnerability. By carefully tracking potential threats and continually reassessing the threat environment, a Knight Errant execsec team can defuse potential threats before they endanger the subject. Using the previously compiled watch list, Knight Errant specialists continually gather intelligence on all potential threats and assess the degree of danger they represent. Our specialists also watch for any signs of surveillance directed at the subject, because periods of surveillance precede almost all serious attacks.

In extreme cases, the team may pre-emptively eliminate a potential threat.

>>>>>(Yes, boys and girls, "pre-emptively eliminate a potential threat" means just what it sounds like. If a KE execsec team hears you're planning to take stab at their subject and they know where to find you, they're likely to come after you—and not just in "extreme cases," either. Killing a would-be attacker before he strikes is a lot more convenient for them than waiting for the attack and trying to defend against it. So don't go bragging about your upcoming extraction run to the local joygirls in the corner bar. Come to think of it, don't go bragging after the fact, either—cuz the KE execsec boys don't like being shown up and they certainly don't like people jawing about it.)<<<<<

—King E. (09:25:10/11-19-55)

EXECSEC TEAM PERSONNEL

Every Knight Errant executive protection team consists of highly trained, carefully screened, seasoned professionals. Many team members have security or intelligence backgrounds, and all have proved themselves on assignments protecting corporate executives, heads of state, and other public figures. All possess high levels of skill and expertise, and all are dedicated to the safety of the subject. The exact composition of your team will vary depending on your needs, but every Knight Errant team includes a team leader, security magician, physical adept, decker, riggers, and executive protection specialists.

TEAM LEADER

The team leader oversees the team, ensuring that its members work together to provide the best security they can. The leader also acts as the team's liaison with the subject and with

other security providers. The team leader is always available to answer any questions the subject may have regarding his execsec program.

SECURITY MAGICIAN

The security magician is primarily responsible for providing the customer with spell defenses. The magician also oversees all magical security measures called for in the subject's comprehensive protection program.

PHYSICAL ADEPT

Every Knight Errant execsec team includes a physical adept with astral perception, who works closely with the security magician and acts as the team's "eyes" in astral space. The adept also works as an "advance man" to examine locations the subject will be visiting and to aid in coordinating security measures with other security providers.

DECKER

The decker acts as the team's information specialist. He or she checks and double-checks the customer's reservations and itineraries and monitors local police, fire/rescue, and air-traffic control communications. The decker also conducts all background checks and oversees all communications/surveillance components of the execsec program. All execsec team deckers are equipped with state-of-the-art cranial decks.

RIGGERS

Every execsec team includes three riggers trained in evasive and aggressive driving and piloting techniques. Most of these riggers have a fixed- or rotating-wing aircraft, an armored limousine or other passenger vehicle, and a cargo vehicle at their disposal. They also receive advanced mechanical training that enables them to personally perform repairs on these vehicles. All Knight Errant execsec riggers are equipped with state-of-the-art cranial remote-control decks.

EXECUTIVE PROTECTION SPECIALISTS

The average Knight Errant execsec team includes three executive-protection specialists (EPSs). These personnel form the foundation of the execsec team and perform many of the minor duties involved in creating and maintaining a viable executive security program. Many of them possess expertise in specific areas such as countersurveillance or intelligence gathering. All are equipped with the latest cyber enhancements and undergo extensive training in the use of the most advanced communications and combat equipment.

>>>>>(Take note, people. These slags are not your usual "hey, he's a big guy—let's strap a gun on him" bodyguards. They're as deadly an adversary as you're likely to meet.)<<<<<

—Mako (11:12:31/11-29-55)

BEHIND THE CURTAIN

>>>>>(OK—I just know every slag reading this board has missed a whole bunch of jazz that might save your sorry hoops someday. And I'll tell you why, chummerinskis—because nowhere in this lovely little chunk of scammed tidbytes do the KE folks show you how all this wiz security works in action. So I've taken it on my little self to do just that. Read the following and learn, my friends. (I stole it from the personal diary files of a security jobber at a major corp, never you mind which. Doesn't matter. I got it, it's genuine, and it'll teach you something if you pay attention.))<<<<<

—Mindfire (21:23:45/12-31-55)

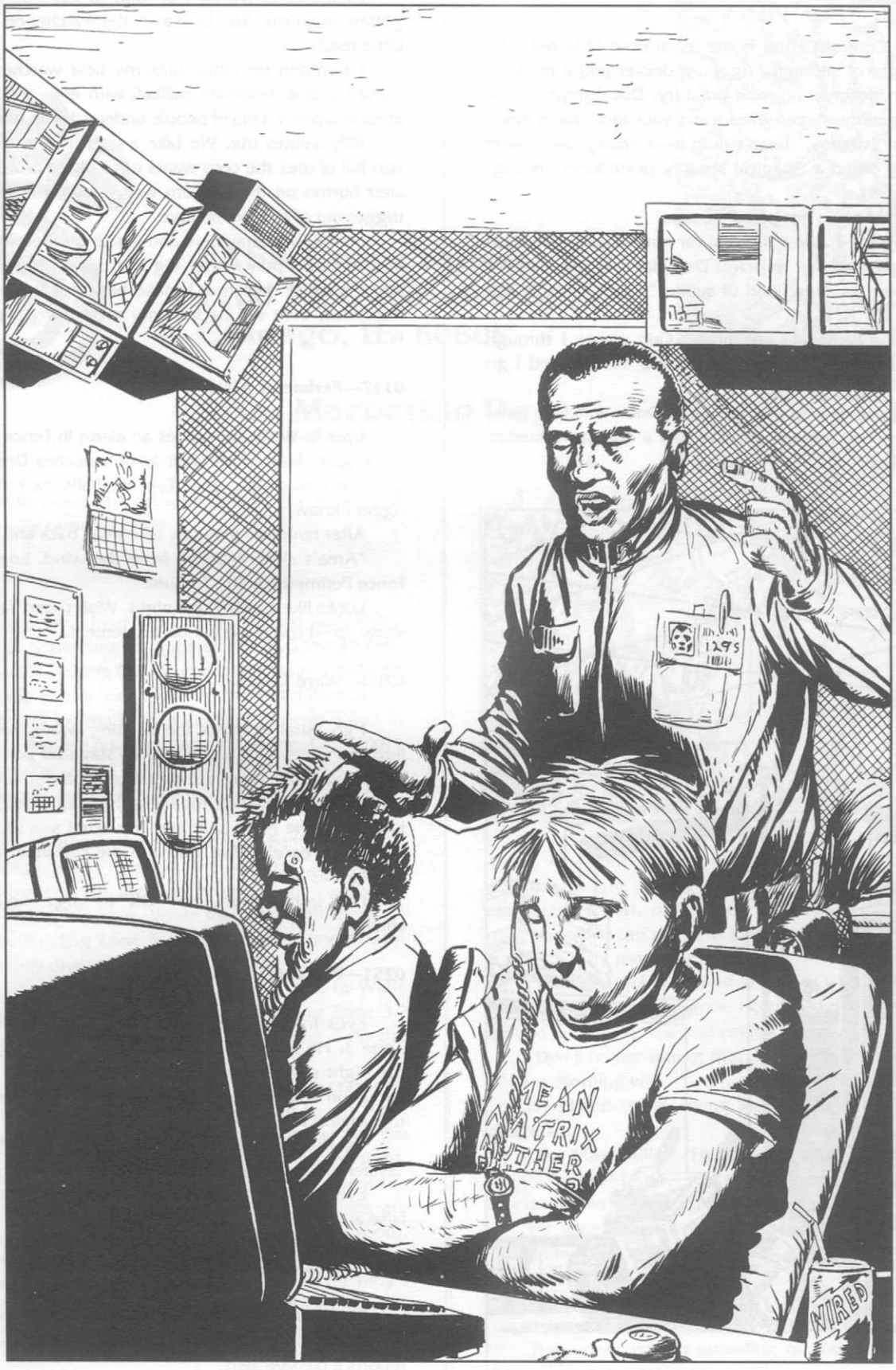
2230—Night Shift Roll Call

Got my cup of soykaf first thing and grabbed a corner seat in the back. Usual nap interrupted when the captain walked in. Captain never shows up at roll call. Swung my feet back to the floor, sat up, and gave an ear.

Cap said the Intelligence boys got a tip about a run against the R&D building, set for tonight. Nothing on who, what, or how.

"So stay sharp tonight, and maybe you boys'll finally earn some of your nuyen," Cap says, with a big chummy smile. I look over at Bodge. We both wince. Cap never was too good with the buddy-buddy stuff.

He walks out and Sarge takes over, mumbling something about Kaplinski's memorial service. Sarge always mumbles. I hate that. I start wondering how in the name of Dante's seven little hells the runners plan on cracking into this kind of high-tech installation. I hope they make it inside; that'll give us a chance to test the new system. Poor suckers.


1295
MEAN
TRIX
WIRED

2300—Shift Change

Integrated Control Center is the usual drab little hellhole. Whoever thought of sticking a rigger, a decker and a mage in the same room deserves a good brain-fry. Doc Sampson, the evening-shift security mage, gives me a sour look. He hates it when I call him "wizboy." I can't help it—a cranky dwarf who insists on being called a "magical security practitioner" is begging to be laughed at.

"It's about time you got here," he says.

"Evening, Doc." I adjust the seat for normal size—I'm tired of stiff necks and cramped muscles. Doc glares at me, like I'm jimmying the seat as some kind of subtle "short" joke. To hell with him.

"Deactivating Bacterial Containment Grid, zones 1 through 5, at 2304 hours," I tell Sarge. He gives me the OK, and I go astral.

Something comes after me; its one of Doc's watchers making faces at me. Doc appears dressed like a big game hunter, and starts giggling.

I tell Doc to tell his pet spirit to get lost. Happy that he's gotten under my skin, he waves the watcher off and disappears. Little toad.

I summon up Little Billy, my best watcher. He prefers to show up as a dandelion puffball with eyes and hands, but he's great in a pinch. Lots of people underestimate him.

Billy salutes me. We take a jaunt to the classified section, labs full of drek the corp wants us to die to protect. I stop by the alert button on the western wall—huge red thing, like a nuke trigger out of Dr. Strangelove.

I tell Billy to stay here and watch on the astral plane, and to manifest and punch that big red button if he sees any astral strollers other than me. I make him repeat the orders back to me twice, then sail back to my meat body and reactivate the BCG.

0117—Perimeter Alert

Eyes-In-Walls announces an alarm in Fence Perimeter Zone 3. He goes limp in his chair as he launches Drone 1 to investigate. Not much gets past Eyes-In-Walls; he's the best security rigger I know.

After ten or so minutes, he comes back and sits up.

"Area's clear. Must've been the wind. Log as false alarm, Fence Perimeter 3, 0117 hours."

Looks like another dull night. Wish those fragging runners'd show up—I could use a little excitement.

0200—Ward Check

I go astral to check the building wards, including peeking into the vents. One more way to stave off boredom. I like this part of my job; there's something soothing about a big office block gone to sleep for the night. No wageslaves, no salarymen, just us on the night shift and my astral self slipping down the hallways. Peaceful. The wards in the classified labs shimmered, as bright as always.

I call in the check as an "OK" to Sarge and drift back to my chair.

0251—Perimeter Alert

Eyes-In-Walls senses another alarm in Fence Perimeter Zone 3. He sends Drone 1 off again while Sarge talks to Cray, the night shift security decker. Cray's nineteen and constantly wired on FizziPop and StufferSweets. His face looks like the topological map of Mars.

"Nothing in the Matrix, Sarge," he says in his reedy voice. "System load minimal. No unusual activity."

Eyes-In-Walls comes back and logs the alert as another false alarm. Says the wind is rising.

0352—Passive Alert

Cray, who's been trying almost as hard as me not to fall asleep, sits up straight like somebody stuck him with a pin and reports a passive alert.

This is it, I catch myself thinking, even though I know it could be anything from a harmless noise to the ghost in the machine. Cray goes to check it out, flopping over in his chair as he accesses the Matrix. A few minutes later Cray's voice comes over a pair of speakers in his console-desk.

"Approaching the public access SAN. Looks like some kids tried to sleaze by it. They didn't get through. I'll check the private-access SAN just in case it's a decoy."

Just as Cray shuts up, something booms from a distance. It sounds like a mini-thunderstorm, and it's coming from the lab floor. Eyes-In-Walls slides into action, but seconds later Cray tells us everything checks out okay. The noise is coming from the weapons lab, where crazy Doc Uzial is testing one of his new toys.

Frag. I was hoping for some action.

0421—Perimeter Alert

Fence Perimeter Zone 3 screams again: another false alarm. Looking wicked pissed off, Eyes-In-Walls leaves an e-mail note for Maintenance to check the sensitivity settings. Be nice if Maintenance actually came for once.

0436—Activation

I wake up fast from a dream about my girlfriend Janet and a nice, warm beach. Something's triggered the BCG. Sarge calls the captain to the ICC, orders Cray to check the Matrix, and tells Eyes-In-Walls to slip two drones pronto to Perimeter Zone 3.

Meanwhile, I deploy the BCG in Zones 1 through 3 and 5. Just as I tell Sarge that the building's astrally secure, Cap strides in and starts bellowing.

"I want all security officers on full alert. And turn those fraggin' speakers down!"

Eyes-In-Walls reports an intrusion through Fence Perimeter Zone 3—some bright jokers bypassed the sensors. Cap, looking tense (it's his hind end on the line, after all), transmits the intruder alert to the inside units. While the meat with the guns pounds it over to Building Zone 3, Eyes-In-Walls connects with his cameras and Cray dives into the Matrix.

After several seconds of silent hunting, Eyes-In-Walls speaks. "Drone 2 reports movement outside Building Zone 3." He pauses, then says, "Got them, sir. Exterior Zone 3. In the stairwell."

Cap orders the gunsels to pick up the party-crashers. Before he can tell me to, I'm checking the astral to see what set off the BCG. Before floating off, I take a look through the room's fiber-optics. The ICC on full alert is a funny sight. There's Cap, looking over Sarge's shoulder at the monitors and barking orders, while his three security specialists are slumped in front of their consoles at the front of the room, apparently sleeping on the job.

I work my way back to the classified lab; Little Billy's there, watching, but all's clear. I sail toward the perimeter, watching the BCG seal me inside the building as I move. Astrally active bacteria flow and pulsate in the two-centimeter gap in all the walls and ceilings. Living walls, we call

them. Any poor sap gets trapped behind one, he's not getting out before talking to the local sec-mage. Me, in this case. Either that, or he dies. First rule of magic: an astral magician who can't get back to his meat is a dead magician. It takes a little time, but it happens.

I found the joker—an elf in leather with a buzz cut—frantically searching for a way out. I coughed; he jumped and turned around to face me, magical energy crackling from hand to hand.

"Don't bother hitting me," I said. "That won't get you out of here. Nothing will."

He glared at me, trying to look tough. Instead, he looked desperate.

"Dr. Maximillian, Th.D., Magical Security Specialist for Knight Errant," I said. "But my friends call me Max. I've got a few questions for you, if you can spare a moment."

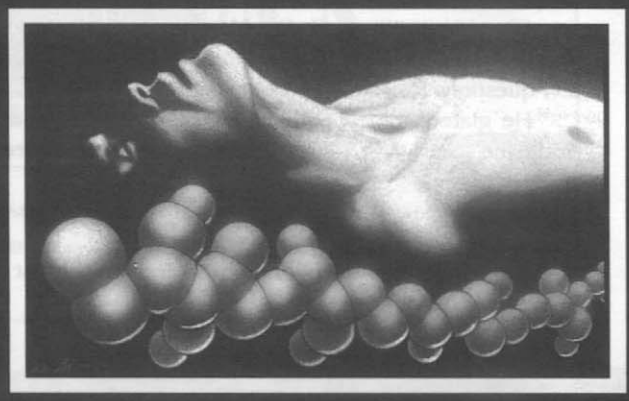
He glared harder, then turned his back on me and scrutinized the living wall. Nice display, but I can smell fear. The elf stank of it.

"Let me know when you're ready to talk," I said. "Take your time. Think about your answers. I can wait."

The runner started pounding on the wall. I just watched. Sometimes I love this job.

ARES SECURITY INTERNATIONAL

FALL 2055 CATALOG



For nearly twenty years, our customers have counted on Ares Arms and Ares Security International to provide the best paramilitary and security equipment on the market. Like its predecessors, this catalog shows you why! Ares remains as committed as ever to progressive, creative technological research and advancement. We're the best, and we give the best to our customers.

>>>>>(Yeah, yeah, blah blah blah, yadda yadda ... whatever. We've posted shadow versions of Ares catalogs before, so this stuff shouldn't be much of a surprise. Of course, you won't see abso-fragging-lutely every peashooter and popgun on the market—just the drek most relevant to the topic at hand. I mean, the unadulterated Ares Arms catalog lists twelve different models of handguns. Twelve different models! What's the fraggin' point?? The drek in this posting's the drek you need, and that's it.)<<<<<

—Juice (05:11:45/11-19-55)

>>>>>(Twelve different kinds of handguns ... wiz! Where can I find that file?)<<<<<

—Street Anemone (10:18:52/11-22-55)

ARES SUPERSQUIRT II™

Ares Arms is happy to introduce the Ares SuperSquirt II™, the advanced model of the popular Ares Squirt™. New developments in dimethyl sulfoxide (DMSO) containment now allow the gel reservoir to be contained in removable clips. Taking full advantage of this innovation, the SuperSquirt II™ also uses an extended chemical-round clip that has twice the number of available shots as the original Squirt. The Ares SuperSquirt II™ uses the same compressed-air technology, making it completely silent and recoilless.

Type	Conceal	Ammo	Mode	Damage	Weight	Availability	Cost	Street Index
Light	7	20*	SA	Special	2	9/14 days	800¥	1.5

*This weapon uses DMSO (see p. 92, **Shadowtech**) in a gel reservoir shaped like a regular clip and good for 20 shots. A second clip mounted parallel to the weapon near the grip contains the chemical. Extra reservoir clips cost 10¥. The grip of the weapon contains a canister of compressed CO_2 that may be recharged for 50¥.

NOTE: This is a variant of the Ares Squirt (p. 92, **Shadowtech**).

The Ares SuperSquirt II™ may be drone-mounted, but cannot accept any top-, barrel- or underbarrel-mounted accessories.

ORDER HERE

>>>>>(It's about time they updated the Squirt. With the old version, once you empty the handle reservoir the weapon's a hunk of useless metal till you get it refilled.)<<<<<

—Wraith II

(21:05:43/11-22-55)

>>>>>(The extended clip is real handy, too.)<<<<<

—Slag

(05:48:40/11-23-55)

>>>>>(Speaking of clips, isn't handling two clips kinda awkward? I mean, don't you get them mixed up?)<<<<<

—Delunidai

(22:54:36/11-24-55)

>>>>>(I'd have thought so too, but Ares actually thought hard about this redesign. They used specific lands and grooves on the clips and clip receptacles to make it impossible to load the wrong clip in the wrong hole.)<<<<<

—Doomstar

(14:58:31/11-29-55)

ARES CASCADE™ RIFLE

Three years ago, Ares Arms introduced the Squirt™. Our technologists thought it was time for an improvement—the Ares Cascade™! We've increased range and accuracy, and greatly expanded the reservoir. In addition, the Cascade™ has a selectable nozzle that lets the user choose between a longer-range stream (similar to the SuperSquirt II™) or a wide-angle, area-effect spray. The Cascade™ is powered by a replaceable compressed-gas canister that attaches to the stock of the weapon.

Type	Conceal	Ammo	Mode	Damage	Weight	Availability	Cost	Street Index
*	4	60**	SA	Special	5.5	12/14 days	1,800¥	2

*If using stream mode, treat the weapon as an SMG for range purposes. When using spray mode, treat the weapon as a shotgun with an effective choke of 2 (this cannot be changed). See p. 95, **SRII**, for information on shotgun spread patterns. Power reduction should be applied to the chemical user to reflect dispersal.

**This weapon uses DMSO in a gel reservoir shaped like a regular clip and good for 100 shots. A second clip contains the chemical. Extra reservoir clips cost 20¥. The stock of the weapon contains a canister of compressed CO_2 that may be recharged for 50¥.

The Cascade™ may be drone-mounted. This weapon accepts all standard top- and underbarrel-mounted accessories, but no barrel-mounted accessories.

ORDER HERE

>>>>>(I've heard the Cascade has serious reservoir contamination problems. Something about the coating on the inside of the reservoir breaking down after a day or so and destabilizing the compound. Anybody else heard this?)<<<<<

—Waco Bill
(23:41:19/11-21-55)

>>>>>(Huh. I'd have assumed they'd use the same material in the Cascade as in the Squirt. Weird, cuz my Squirt works fine.)<<<<<

—Duane Pain
(02:45:28/11-24-55)

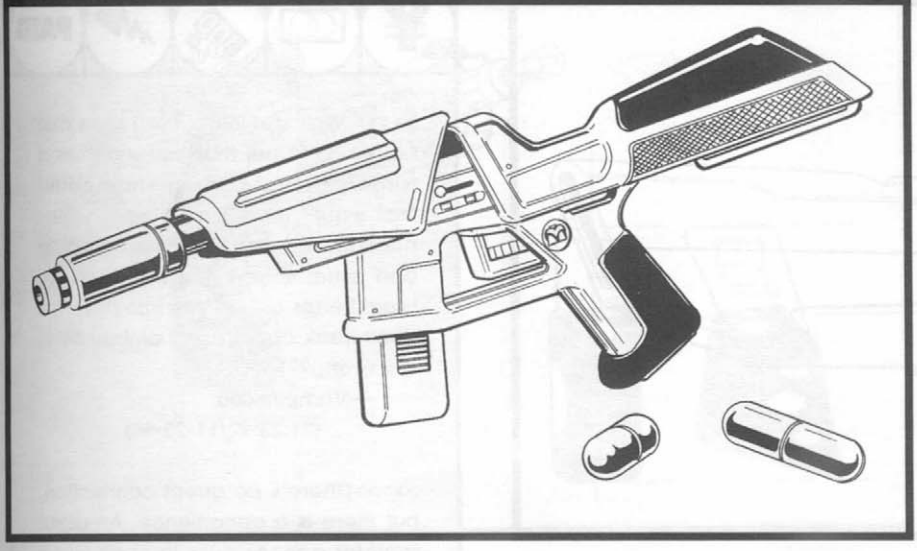
>>>>>(Nice to know, Duane.)<<<<<

—Wanda
(06:41:56/11-28-55)

>>>>>(Be careful. One of my cobbers had her Cascade rupture on her. Not a pretty sight, let me tell you.)<<<<<

—Warder
(23:35:08/11-29-55)

ARES ELD-AR™ ASSAULT RIFLE



Used by the UCAS military and various corporate security forces, the ELD-AR™ (Encapsulated Liquid Delivery-Assault Rifle) assault rifle has been a standard training weapon for years. The ELD-AR's compressed-gas canister provides an almost silent and recoil–free shot. Even under burst-fire conditions, the ELD-AR™ is quieter than an SMG equipped with sound suppression. A variety of colored ammo is available for determining firing accuracy. If your security forces need a weapon for practice drills or other needs, the ELD-AR™ is the weapon for you!

Type	Conceal	Ammo	Mode	Damage	Weight	Availability	Cost	Street Index
Assault	4	50 (c)	SA/BF	Special*	4.5	9/7 days	950¥	2

*Standard ammunition is a gel-coated round filled with biodegradable paint or other marking agents. Paint rounds are 5¥ for a package of 10. Damage is 4L Stun. A gelcoat round with special fillings may be fashioned with a kit that costs 300¥. These special rounds may cause damage based on their contents. The weapon is powered by a refillable compressed-air canister in the stock. Refilling the canister costs 50¥.

The ELD-AR creates negligible recoil that is absorbed by the shoulder stock. Treat the weapon as having a sound suppresser.

The ELD-AR may be drone-mounted. The weapon accepts all standard top- and underbarrel-mounted accessories, but no barrel-mounted accessories.

ORDER HERE

>>>>>(Gee, ain't this grand. Paying almost a thousand nuyen for a lousy paint gun! I thought that fad went out of style at the turn of the century?)<<<<<

—BitRunner
(23:05:20/11-25-55)

>>>>>(Will you look at this buildrek?! Training, my ... I've seen CorpSec thugs use these little puppies to mark a runner's getaway vehicle. They fill the pellets with a gel that glows under thermographic light. Once they've marked the vehicle, they call in the airborne pursuit, who follow the runner using infrared.)<<<<<

—Voight
(09:11:23/11-28-55)

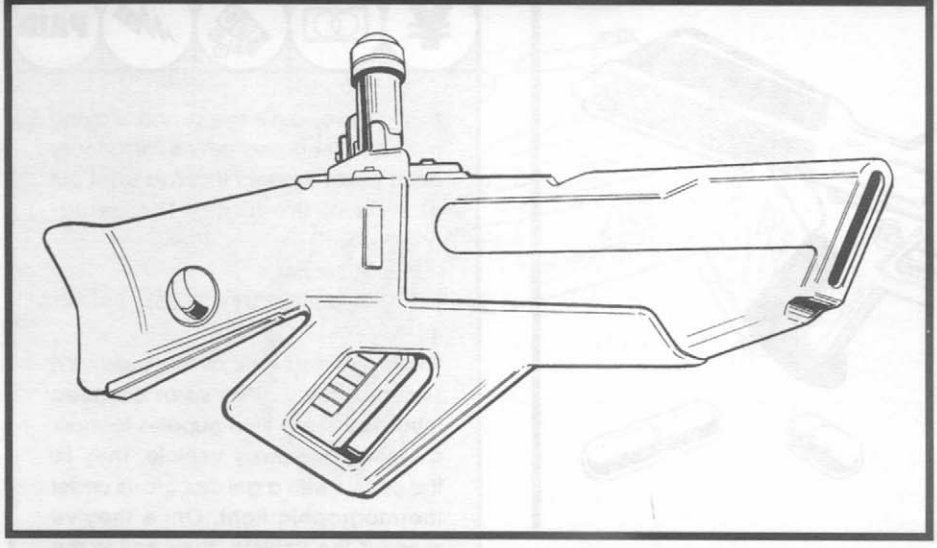
>>>>>(You guys realize that you can put just about any chemical in the pellet, right? Think of what that means ... You have to be careful about what goes in there, though, because it might react with the material the pellets are made of.)<<<<<

—Turner
(20:15:47/12-01-55)

>>>>>(I've seen ELD-AR rounds rupture when fired. Definitely a no-no if you're firing some airborne agent ...)<<<<<

—Warder
(06:45:31/12-02-55)

BACTERITECH™ FAB-NG™ NETGUN



In conjunction with Ares Arms, BacteriTech™ has modified the Williams Technologies netgun to allow it to capture astral targets. The BacteriTech™ FAB-NG™ (Fat Bacteria Netgun) fires a net comprised of interconnected hollow polymer tubes filled with FAB-1 (Fat Bacteria, Strain 1). The FAB-NG™ has a dual trigger mechanism. Pulling the first trigger primes the net by forcing the FAB-1 from its holding vat into the net in firing position; pulling the second trigger fires the net. Once primed, a net stays active for six to eight hours. Each net can only be used once.

As with the Williams Technologies netgun, the FAB-NG™ is available in two sizes, one for human-sized or smaller assailants and a larger version for large orks and trolls. The larger version can fire both sizes of FAB-NG™ nets.

Type	Conceal	Ammo	Mode	Damage	Weight	Availability	Cost	Street Index
Standard	3	4(b)*	SA	Special**	4.5	8/14 days	1,500¥	4
Large	2	4(b)*	SA	Special**	5	8/14 days	2,500¥	5
Additional Net Shots								
Standard	7				0.5	8/14 days	300¥	4
Large	5				0.75	8/14 days	500¥	5

*Requires a self-contained feeding canister that costs 1,000¥ for 4 standard nets or 1,500¥ for 4 large nets.

See **Fat Bacteria, pp. 103–104 in the **Gamemaster Information** section.

The FAB–NG™ may be drone-mounted. This weapon accepts all standard top- and underbarrel-mounted accessories, but no barrel-mounted accessories.

ORDER HERE

>>>>>(Wait a minute! Did I read that correctly? A net that can snag astral targets?? That's smeg—how could that work? There's no physical connection between the physical world and astral space. The mage on my team keeps drilling that into us so we don't freak about astral ambushes. Is she wrong??)<<<<<

—Vampire Lou
(21:23:42/11-25-55)

>>>>>(There's no direct connection, but there is a congruence. An astral traveler cannot pass through living matter. We know that. What this net allegedly does is surround an astral target with a flexible biomatter barrier. The astral target has "casual" mass and can't get past it. That's the theory anyway.)<<<<<

—Vince
(05:32:08/12-01-55)

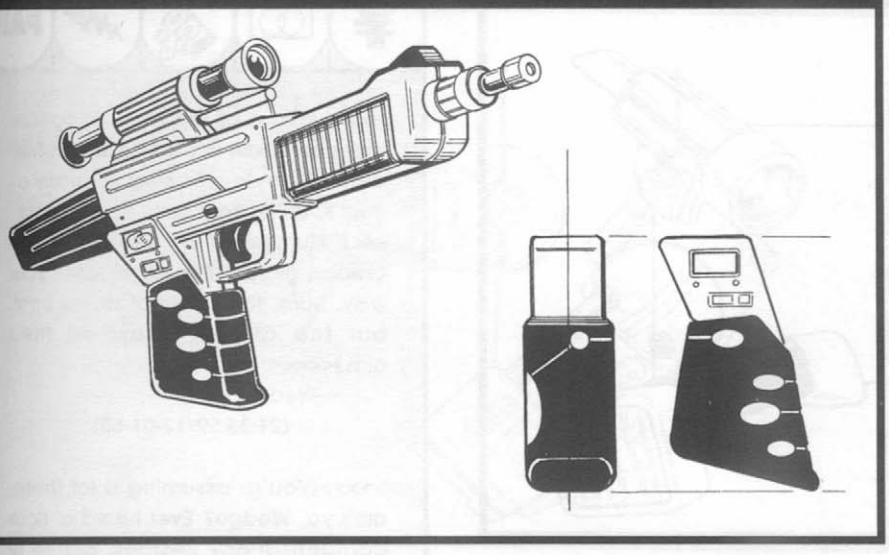
>>>>>(Wait, that makes no sense. Following that logic, if I drop one of these nets down on an astral target, it should wrap around him and be supported by him because he can't pass through it. BUT AN ASTRAL FORM HAS NO MASS! HOW CAN IT SUPPORT ANYTHING??!! I don't understand how this can possibly work.)<<<<<

—Silver Star
(21:48:53/12-05-55)

>>>>>(Now you understand the problem. I think Ares is pulling a fast one.)<<<<<

—Amber Mage
(13:27:50/12-06-55)

INDIVIDUALIZED BIOMETRIC SAFETY (IBS)



Tired of reading about yet another police or security officer killed by his or her own weapon? Individualized Biometric Safety (IBS) developed by Ares Arms can end these incidents once and for all. First, we modify a weapon's grip with a specialized biometric identification reader attached to the weapon's internal safety. Next, we store an image of the weapon-owner's palmprint in non-reprogrammable firmware. Whenever someone picks up the weapon, the biometric reader scans that person's palm and compares it to the image stored in the firmware. If they match, control of the weapons safety is released. If not, the safety freezes in the safe position, rendering the weapon harmless. The IBS system is fully compatible with most smartlink/smartgun technology.

	Concealability	Weight	Availability	Cost	Street Index
IBS	—	.1	3/36 hours	2,250¥	1.5
Cyber modification	—	—	3/36 hours	800¥	1.5

To change ownership of a weapon, players must burn in a new firmware optical chip. Blank chips cost 50¥ and can be programmed using a computer repair shop or facility. Users with a cyberarm or cyberhand must use the cyber modification; designed to be mounted in the cyberhand, it contains a pass-chip that links to the weapon.

ORDER HERE

>>>>>(2250¥ seems a lot to pay for a safety, especially when you can't wear any gloves to use it.)<<<<<
—Slag
(01:11:53/11-26-55)

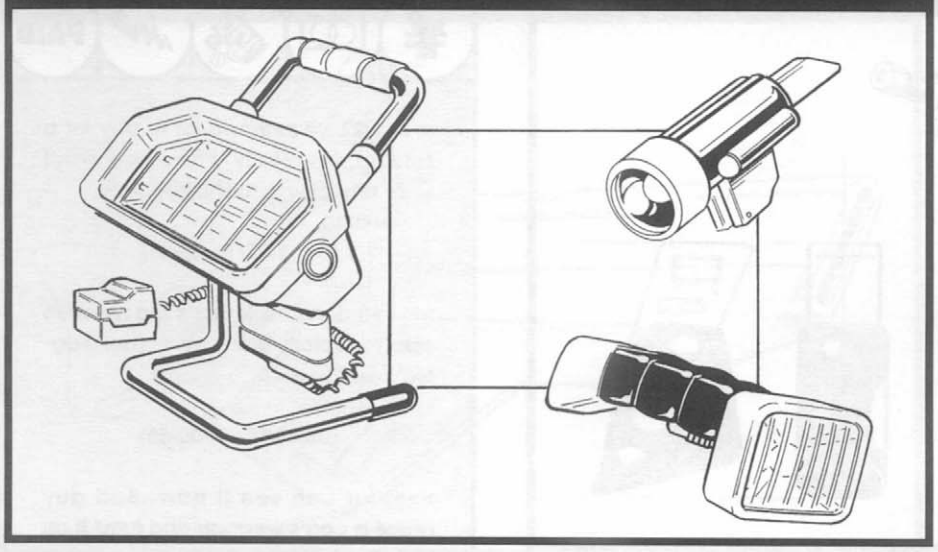
>>>>>(I don't think that's too much to ask. Especially if it'll save your fraggin' neck.)<<<<<
—Quess
(08:45:50/12-05-55)

>>>>>(I can see it now. Bad guy grabs a cop's weapon and turns it on him. The cop knows the weapon is inert, but bad guy don't know. Imagine his surprise when that gun don't work. Hee hee hee.)<<<<<
— BitRunner
(15:30:56/12-06-55)

>>>>>(Field-tested one of these a year or so back. The user got his hand caught in a blender and needed quick and powerful magical attention. He got it, saving his life and his hand. The kicker is, the gun refused to acknowledge him for about four or five hours afterward. Then everything was wiz. Odd, *neh*?)<<<<<
—Shawn Born
21:18:39/12-09-55)

>>>>>(Sounds like a system glitch to me. Magic could cause that.)<<<<<
—Amber Mage
(04:05:55/12-13-55)

PORTABLE SECURITY LIGHTING



Ares Security International now produces portable security lighting devices in all spectrums, from low-wattage flashlights to active infrared floodlights. All lights come with long-life lithium batteries.

Item	Availability	Cost	Street Index
Low-wattage*			
Flashlight	Always	10¥	1
Top/Underbarrel-mounted	2/24 hrs	100¥	1
Portable Floodlight	Always	150¥	1
Active Infrared**			
Flashlight	4/48 hrs	100¥	2
Top/Underbarrel-mounted	6/48 hrs	250¥	2
Portable Floodlight	5/48 hrs	350¥	2
Ultraviolet***			
Flashlight	4/4 days	200¥	2
Top/Underbarrel-mounted	6/4 days	500¥	2
Portable Floodlight	8/4 days	750¥	2

*Low-wattage lighting allows characters with low-light vision (natural or enhanced) to see clearly: up to 20 meters with the flashlight and barrel-mounted light, 100 meters with the floodlight. Low-wattage lighting has no effect on normal human vision, except to provide faint indirect lighting.

**Active infrared lighting allows characters with thermographic vision (natural or enhanced) to see clearly: up to 20 meters with the flashlight and barrel-mounted light, 100 meters with the floodlight. Active infrared lighting has no effect on normal human vision.

***Ultraviolet lighting is used in conjunction with FAB-UV (see **FAB-Ultraviolet**, p. 103, **Gamemaster Information**). The flashlight and barrel-mounted light have a range of 5 meters; the floodlight has a range of 35 meters. UV lighting has no effect on normal human vision.

ORDER HERE

PAID

>>>>>(Some of the tactical options that come with this drek aren't immediately obvious. Using a beam as your spotting light serves two purposes: it illuminates the target and also creates glare if the target looks your way. Sure, they'll shoot at the light, but the glare'll throw off their aim.)<<<<<

—Wedge
(21:36:59/12-01-55)

>>>>>(You're assuming a lot there, ain't ya, Wedge? Ever heard of flare compensation? Besides, active IR and UV lights don't glare.)<<<<<

—Trueheart
(05:48:34/12-06-55)

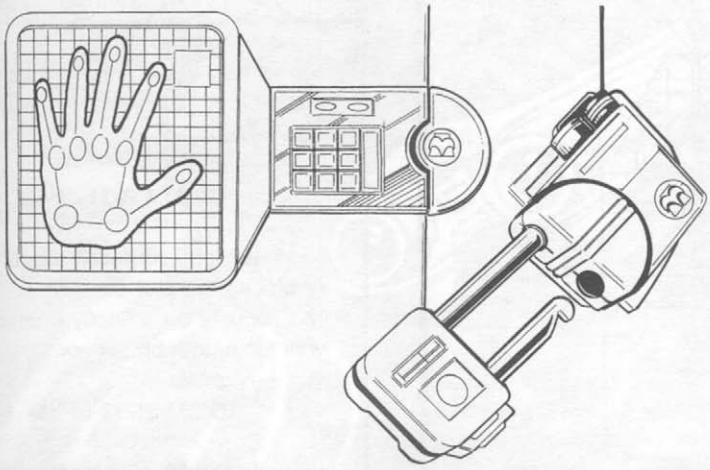
>>>>>(IR flares thermo. Been there.)<<<<<

—Teach
(21:47:30/12-09-55)

>>>>>(Make sure you're using as tight a beam as possible. You can only temporarily blind a target if he's directly in the heart of the beam. Also, keeping your beam tight cuts down on the risk of others spotting it.)<<<<<

—Lando V.
(11:35:08/12-11-55)

MAGLOCKS



Ares Security International has developed maglock technology into a fine art. The Type I Maglock offers you better protection than the strongest padlock, at close to a padlock's price. The Type II is tougher, but not top-level security: perfect for a corporate facility's common areas. The Type III is ideal for higher-security areas—or, for areas protected by closed-circuit simsense, try the Type IV. All Ares Security International maglocks are available at different levels of complexity. All maglocks above the Type I come with a lithium backup power supply good for one year: the Type I comes with a five-year battery. As with the original maglock, a PANICBUTTON™ hookup option is available for all locks except the Type I.

Item	Availability	Cost	Street Index
Type I Maglock (Rating 1–3)	Rating/2 days	75¥ x Rating	.75
Type II Maglock (Rating 4–6)	Rating/3 days	100¥ x Rating	1
Type III Maglock (Rating 7–9)	Rating/3.5 days	150¥ x Rating	1.25
Type IV Maglock (Rating 10)	Rating/4 days	250¥ x Rating	1.5
Biometric Maglock*	Rating/5 days	350¥ x Rating	2

*Biometric maglocks come in Type III or Type IV configurations. For attempts to bypass a Biometric maglock, add 2 to its effective rating. See **Maglocks**, p. 100, **Gamemaster Information**.

ORDER HERE

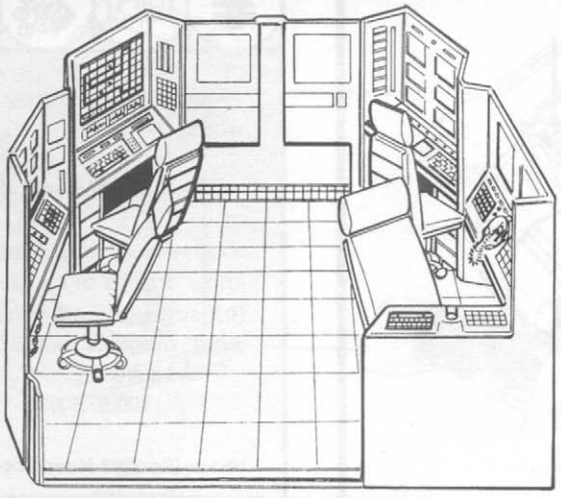
>>>>>(Seems fairly straightforward.)<<<<<
—Toad
(20:08:26/12-08-55)

>>>>>(Yeah, you'd think that. Still, I know dozens of runners who've gotten scragged when a "straightforward" maglock fouled 'em up.)<<<<<
—Squint
(00:07:51/12-12-55)

>>>>>(Really? How?)<<<<<
—Twenton
(11:08:25/12-12-55)

>>>>>(Can you tell the difference between a Type II and a Type IV at a glance? Too many runners think they can.)<<<<<
—Squint
(02:21:17/12-13-55)

INTEGRATED CONTROL CENTER (ICC)



Ares Security International, in conjunction with Fuchi Cyber, is happy to introduce the Integrated Control Center (ICC). The ICC provides the ultimate command, control and communication capability for mid- to large-sized security systems.

The ICC consists of three individual operator stations and a command console. Operator Station 1 (OS1) provides central control for all of a system's surveillance and control devices, CCTV, CCT, CCSS, and security drones. In the basic model, this station can handle up to twelve cyberlinks and three drones, all easily controlled from one of Ares Security's patented, ergonomically designed chairs through state-of-the-art cybernetic links. A security rigger's dream come true!

Operator Station 2 (OS2) is the heart of the ICC, containing the main CPU and computer controls. OS2 provides both cyberterminal and cyberdeck links to the CPU, equivalent to a Fuchi Cyber-4; it also acts as an I/O node to the protected area's matrix. This setup allows a security decker to provide matrix security while maintaining computer support.

Operator Station 3 (OS3) integrates magical security into a well-designed security system. Located at OS3 are six hook-ups to a security-systems fiber-optic observation network, as well as the latest in six-position motorized prism switches. This arrangement allows a security magician immediate visual access to almost anywhere in the protected area while he also monitors pre-established wards.

The command console is the ICC's control center, allowing the security commander to maintain radio communication with officers throughout the protected area as well as with the three operator stations through audio links and built-in vidscreens.

In addition to the powerful basic model, upgrades are available (see table).

*Only available in four-zone packages, with a maximum number of zones equal to four times the number of slave ports.

**Multiple image-links can be installed, but one prism switch must be delegated to interconnect the image-links.

NOTE: The ICC and upgrades are not normally available on the street. Availability is therefore at the gamemaster's discretion. See the **Gamemaster Information** section.

Item	Cost
Basic ICC	500,000¥
CPU Upgrades	
Fuchi Cyber–6	+100,000¥
Fuchi Cyber–7	+250,000¥
Fairlight Excalibur	+500,000¥
Cyberlink Upgrades	
Additional Links*	+5,000¥/4 links
Drone Slave Port Upgrades	
Slave Port	+25,000¥/port
Fiber-Optic Image Links**	
Nine-Position Motorized Prism Switch	+20,000¥
Twelve-Position Motorized Prism Switch	+25,000¥
Image Links	+3,000¥/optical camera

ORDER HERE

PAID

>>>>>(Talk about mixing magic and technology! If this isn't an abomination, what is?)<<<<<

— Wraith II

(02:24:458/11-30-55)

>>>>>(Uh-oh—someone feels threatened. <grin> Get used to it, Wraith. The security biz is finally catching up with the runner biz.)<<<<<

—Nightfire

(22:35:51/12-01-55)

>>>>>(Actually, I welcome this kind of challenge. Running had started getting a little stale. Sneak in, grab the dingus, sneak out. Bust a head or two for old times' sake. Dull. Dull. Dull. Thank you, Ares, for making my life interesting again!)<<<<<

—Hangfire

(20:17:43/12-04-55)

>>>>>(Do I sense some sarcasm here?)<<<<<

—Uncle Vanos

(02:57:34/12-06-55)

>>>>>(Nah, he's serious.)<<<<<

—Findler-man

(03:54:26/12-08-55)

FIBER-OPTIC OBSERVATION NETWORK

Ever wondered how to integrate a security magician into a well-designed security system without having to put him or her on the front line? Ares Security International has solved the problem of mixing magic and technology with the Ares Fiber-Optic Observation Network. Based on the ever-popular fiber-viewers found on military-grade combat vehicles, the Fiber-Optic Observation Network allows a magician to see his or her desired target without exposing himself to that target. We accomplished this feat by running machine-pulled, fiber-optic cables from the magician's control console to a precision-ground optical lens. The magician looks through specially designed goggles into the fiber, and he or she can "see" out the lens without the aid of electronics. A magician only needs to see his or her target to cast a spell; the Fiber-Optic Observation Network extends the magician's "line of sight" much farther than his or her physical eyes. An optical monitor is also available.

For security systems that require more than one camera, Ares Security International offers our patented Prism Switch in six-, nine- or twelve-position models.

Item	Cost
Fiber-optic Cable	100¥/meter
Camera	10,000¥
Goggles	5,000¥
Prism Switch	
Six Position	15,000¥
Nine Position	20,000¥
Twelve Position	25,000¥
Optical Monitor	15,000¥

NOTE: The above items are not normally available on the street, and so their availability is at the gamemaster's discretion. See **Fiber-Optic Image Links,** p. 102, **Gamemaster Information**.

ORDER HERE

>>>>>(Okay—all you cynical bastards who have no space for newbies or the uninitiated, please frag off—I have a dumb question. A magician needs to see her target, right? And since a fiber-optic line transmits the light/image directly, it's usable, right? So a magician using this system can be somewhere else in a building and see her target?? I hope I'm wrong.)<<<<<

—New Nell
(20:54:38/12-05-55)

>>>>>(Unfortunately, you got it right. Of course, the text above doesn't talk about the disadvantages—fuzzy and dim images, cable-length limitations, no thermographic or low-light capability, and so on.)<<<<<

—Shriven
(03:54:29/12-06-55)

>>>>>(The system doesn't need low-light or thermo systems—the observing mage just uses his own cybereyes.)<<<<<

—Nightfire
(05:54:47/12-07-55)

>>>>>(OK, voice of experience here. I've cast spells through an optical link—IT'S A PAIN! Don't let anyone tell you otherwise. It's harder to achieve symmetry, harder to manage the linkage, harder to cast, period. Yeah, a security mage may be able to see, and may even be able to cast at you. But your odds of avoiding damage are higher, as are his odds of popping a blood vessel doing it.)<<<<<

—Leanna (23:59:42/12-08-55)

CLOSED-CIRCUIT SIMSENSE (CCSS)

Security-system design engineers at CerebroTech™ are proud to present closed-circuit simsense (CCSS). The latest in technical security countermeasures, CCSS allows a trained security rigger to "drive" a security system just as he or she would a vehicle. CCSS-equipped security devices let a security rigger feel a door being opened, a fence being climbed, or a window being broken. CCSS also hooks the rigger into the security system's drones and other surveillance and control devices, which act as his or her eyes and ears throughout the protected area. For a small additional fee, the engineers at CerebroTech™ will modify any existing security device to handle CCSS. To operate a CCSS system, a security rigger simply needs to install a CCSS decoder in his or her remote-control deck or security station and modify all security devices to handle CCSS protocols.

Item	Availability	Cost	Street Index
CCSS Decoder			
External	8/2 weeks	10,000¥	3
Internal	12/3 weeks	+7,500¥	3
CCSS Device Retrofit	N/A	25 percent of original cost	N/A
CCSS Device	N/A	+20 percent of original cost	N/A
CCSS Drone/Vehicle Modification	N/A	1,500¥	N/A

NOTE: Whereas a simple cyberlink hookup to an integrated control center allows a rigger to actively or deliberately monitor and control a remote device, a CCSS link allows passive awareness of the device. The rigger is automatically aware of any changes in the status of the device without having to expend an action. Active control of the device, however, still requires an appropriate action. See **Closed-Circuit Simsense**, p. 102, **Gamemaster Information**.

ORDER HERE

PAID

>>>>>(Sorry, me again. So this setup allows a security rigger to "sense" when an alarm is tripped or tampered with?)<<<<<

—New Nell
(21:19:12/12-05-55)

>>>>>(Tripped, certainly. Tampered with, depends. Clumsy tampering, yes. Skilled, no.)<<<<<

—Shriven
(04:18:44/12-06-55)

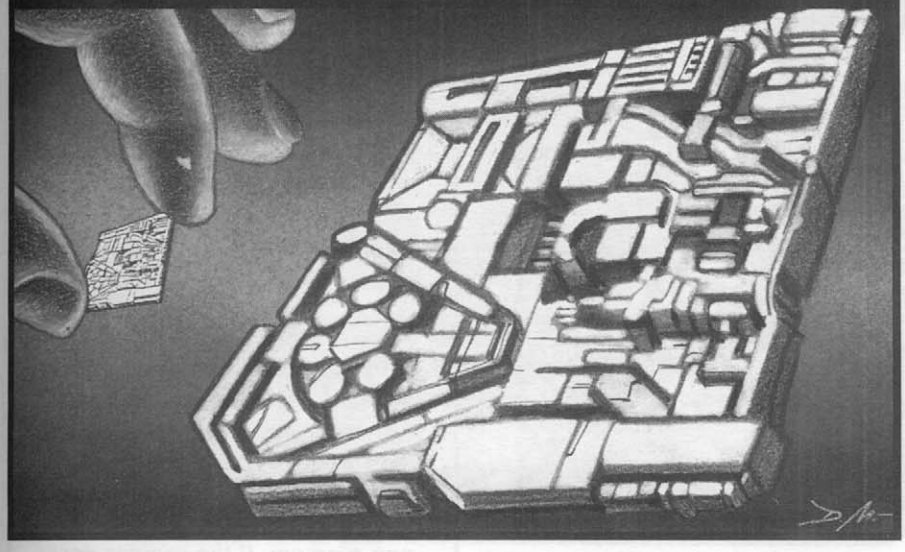
>>>>>(Not entirely true. The tolerances of most security expert systems might ignore tell-tales of the best tampering, but human senses and intuition usually won't.)<<<<<

—Nightfire
(05:54:47/12-07-55)

>>>>>(The worst part of this is that a high-security area has all its doors and such rigged with CCSS. Every time you or someone else goes through a door, the rigger knows. He can follow your movements passively while actively routing security forces or drones. Real pain in the hoop.)<<<<<

—Jurgen
(05:21:04/12-09-55)

RIGGER PROTOCOL EMULATION UTILITY



The Rigger Protocol Emulation Utility is a program that translates a deck's software inputs and outputs into a rigged system's hardware language. This utility allows a decker to emulate any of the various protocols used by riggers and their systems and drones. Available at varying levels of sophistication; each higher-rated module includes all the protocols in the lesser levels.

	Size (in Mp)	Availability	Cost	Street Index
Rigger Protocol Emulation	(Rating x Rating) x 4	*	*	*

*Varies by rating; see Utility Programs, p. 262, **SRII**.

NOTE: The delays caused by using an SCRE (see p. 78) and the emulation utility impose a blanket +2 modifier to the target number for any tests conducted using the device. Initiative is reduced by a –2 modifier, and players gain no dice for Response Increase in the cyberdeck. Players do gain a Control Pool equal to one-half the rating of the emulation utility (rounded up).

ORDER HERE

>>>>>(Yeeesh, these things are slow. You'd think there'd be a better way.)<<<<<

—Yuri

(04:34:12/12-02-55)

>>>>>(A geeker friend of mine once tried to explain it, but he lost me. I remember it had something to do with interference or a lack of interface with the simsense signal in the cyberdeck (or something). Remember, the cyberdeck is trying to translate signal into symbology ... ugh, you'd think that'd be exactly how you'd want this to work. I give up.)<<<<<

—Ignorant and Proud

(10:58:15/12-03-55)

>>>>>(Ignorant and proud? What a great thing to say. Unknowledgeable and happy about it. Great. I hope you never breed.)<<<<<

—Connie Casualty

(22:08:54/12-05-55)

>>>>>(Stick your tongue in a wall socket, eh Connie? I'm Ignorant, she's Proud. We share the account.)<<<<<

—Ignorant and Proud

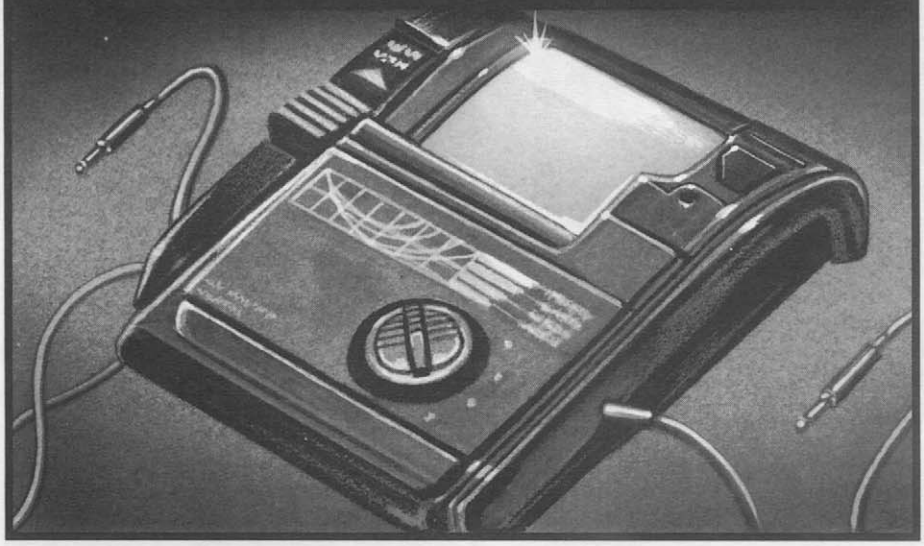
(18:02:50/12-06-55)

>>>>>(Spirits, they're either comedians or clowns ...)<<<<<

—Treasure Seeker

(11:39:08/12-07-55)

SYSTEM-CONTROL RIG EMULATOR



Ever wondered if a decker could access a rigged system? He can do it with the System-Control Rig Emulator (SCRE) from Ares Security International! This device is a must for every security-system design engineer responsible for system diagnostics. The external module attaches between a cyberdeck and the rigged security system or remote-control deck; the internal module can be installed right inside a cyberdeck. The SCRE acts as the interface between the deck and rigged system or remote control deck by imitating the machine language of the standard system control rig. Note that a rigger protocol emulation utility is required to use the SCRE.

	Availability	Cost	Street Index
System Control Rig Emulator			
External	6/72 hrs	25,000¥	2
Internal	8/72 hrs	20,000¥	2

NOTE: Installing the SCRE in a cyberdeck is a Computer (B/R) task with a base time of 24 hours and requires a Computer (B/R) Test against a Target Number of 5.

ORDER HERE

>>>>>(Interesting. Why is Ares selling this? It seems to me the only purpose it serves is to aid a decker in overriding a rigged security system.)<<<<<

—Hangfire

(02:18:56/12-02-55)

>>>>>(On the surface, yes. Its primary use (at least as far as Ares is concerned) is as a backup for the ICC system. I know of a number of systems where an SCRE is built into the decker's console and the emulation utility prepped as the console's storage memory. If the security rigger goes down, the decker can step in and take over in a matter of milliseconds. He can retain control, or at least maintain it until another security rigger steps in.)<<<<<

—Teague

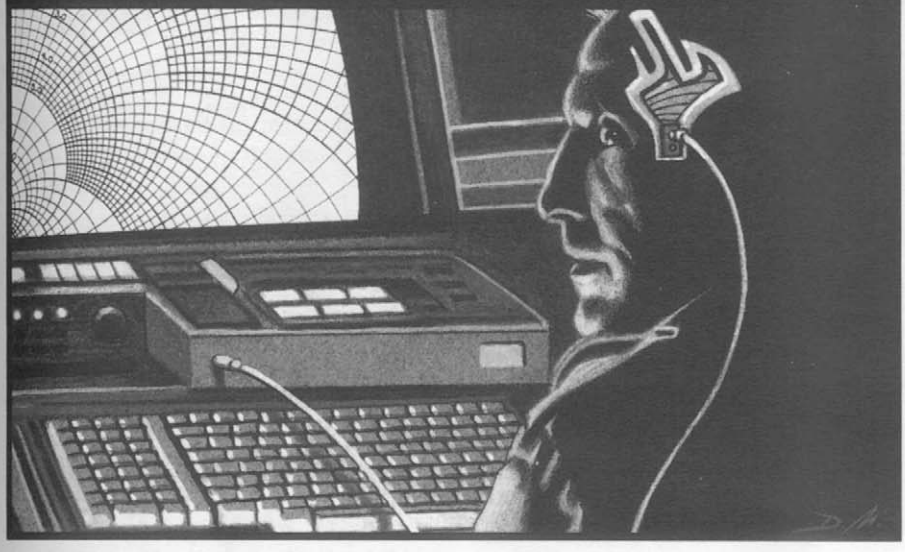
(21:17:30/12-06-55)

>>>>>(This would make an excellent backup for a lot of shadowrunning teams I know ... for those times when things get sloppy. <grin>)<<<<<

—Loki

(05:24:14/12-07-55)

RIGGER PROTOCOL EMULATION MODULE



The Rigger Protocol Emulation Module is a important tool for security riggers who perform their own diagnostics. The module allows a rigger to emulate many of the various protocols, including CCSS, used on contemporary rigged security systems and drones. The external version of this module is mounted in-line between the rigger's system control rig dataport and the system undergoing diagnostics. Remote systems require the internal model, which must be installed inside the remote control deck. The higher-rated the module, the more protocols are programmed into its firmware, up to a maximum rating of 10.

	Availability	Cost	Street Index	
Rigger Protocol Emulation Module				
External		(Rating)/(Rating) days	5,000¥ x Rating	2
Internal		(Rating + 2)/(Rating) days	4,500¥ x Rating	2

NOTE: The number of devices a rigger may control is equal to the number of slave nodes on the remote-control deck.

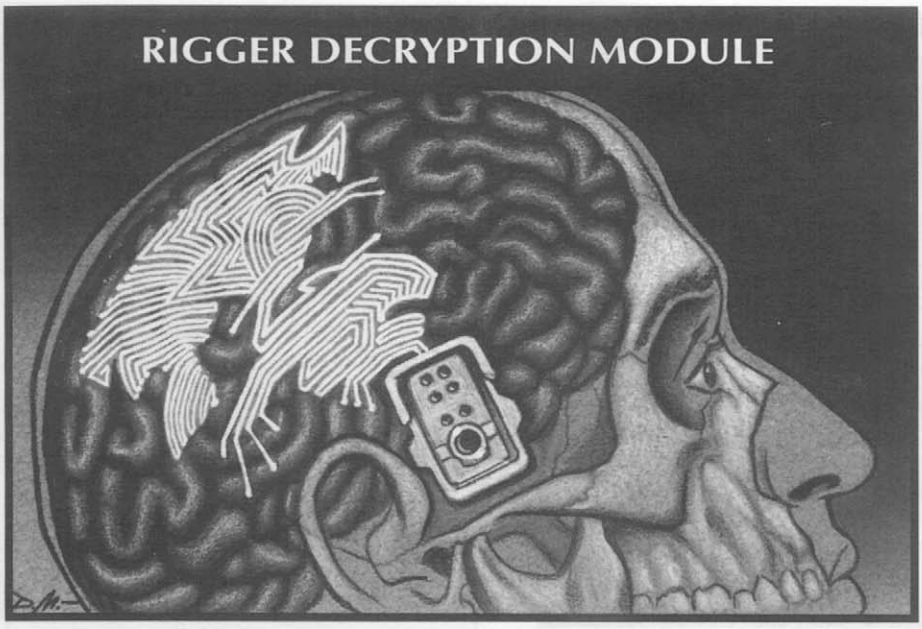
ORDER HERE

>>>>>(Yeah, right. Diagnostics. That's just what I'll use this for.)<<<<<
—Gadfly
(09:20:18/12-02-55)

>>>>>(Is that sarcasm?)<<<<<
—New Nell
(03:29:15/12-05-55)

>>>>>(Good catch there, Nell. This device is the interface a regular rigger needs to run a rigged security system. A standard vehicle control rig isn't set up to handle CCSS and such. That's why you need this puppy and a remote control deck.)<<<<<
—Taylor Tom
(20:52:28/12-06-55)

>>>>>(If the system is encrypted, you also need the next item. Dontcha just love component systems?)<<<<<
—Blackflash
(10:29:20/12-05-55)



The Rigger Decryption Module is yet another diagnostic tool used by security riggers. This module contains sophisticated cryptographic routines programmed into its firmware that allow security riggers to test the encryption on their rigged security systems and drones. The external version of this module is mounted in-line between the rigger's system control rig dataport and the system undergoing diagnostics. Remote systems require the internal model, which must be installed inside the remote control deck. The higher-rated the module, the more protocols are programmed into its firmware, up to a maximum rating of 10.

Availability	Cost	Street Index	
Rigger Decryption Module			
External	(Rating)/(Rating) days	7,500¥ x Rating	2
Internal	(Rating + 2)/(Rating) days	7,000¥ x Rating	2

ORDER HERE

>>>>>(Hmmm, so internal security system protocols are encrypted. How does that impact performance?)<<<<<

—Davis

(20:29:18/12-01-55)

>>>>>(Astute question, but there's no measurable impact on either end.)<<<<<

—Paolo Picasso

(23:18:38/12-04-55)

>>>>>(That would make an interesting security approach though, wouldn't it? Run an encryption algorithm sufficiently complex to slow a system down, unless you're running custom cryptographic chips.)<<<<<

—Zardoz

(04:21:54/12-05-55)

>>>>>(What a great idea!)<<<<<

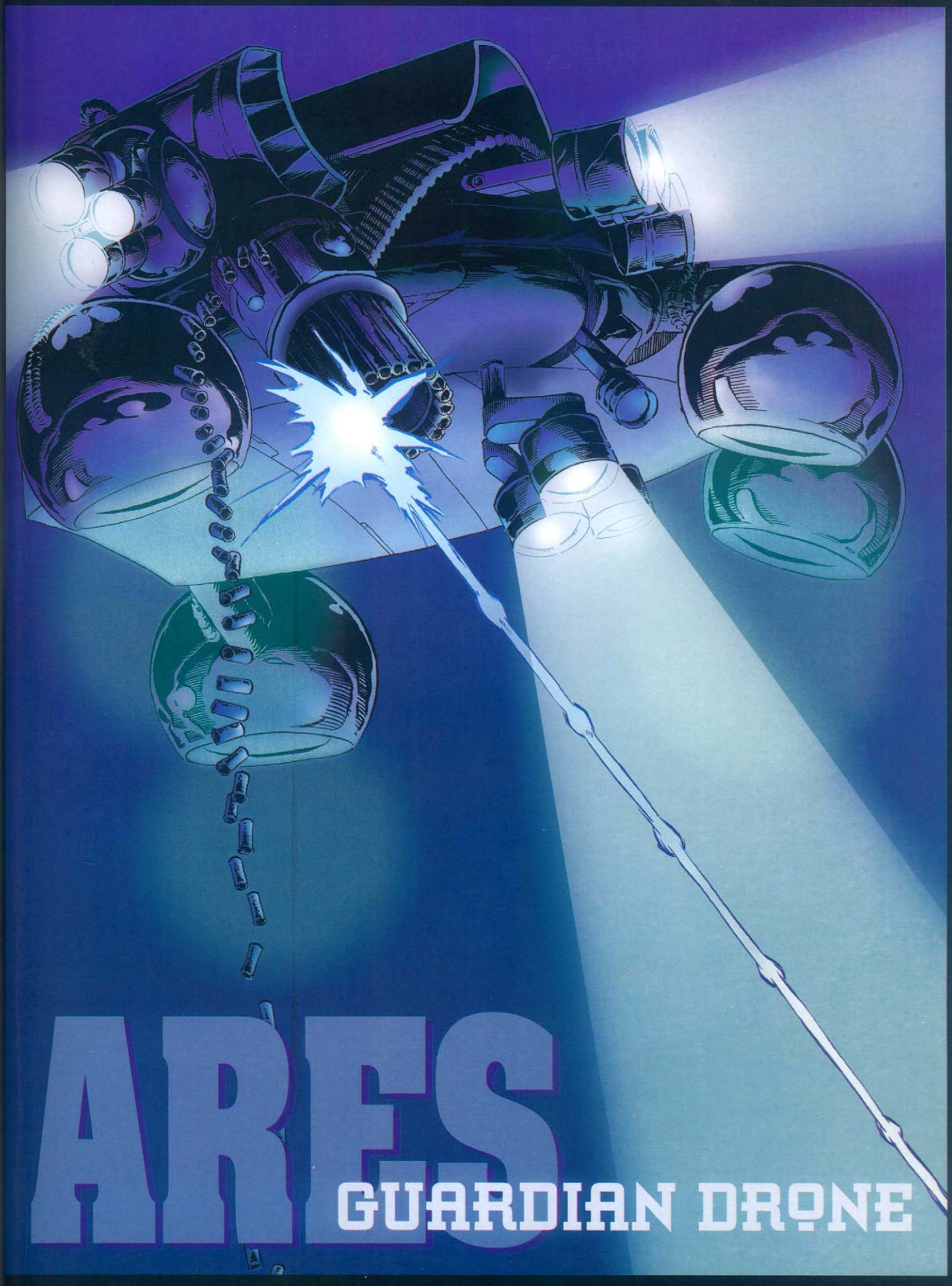
—Nightfire

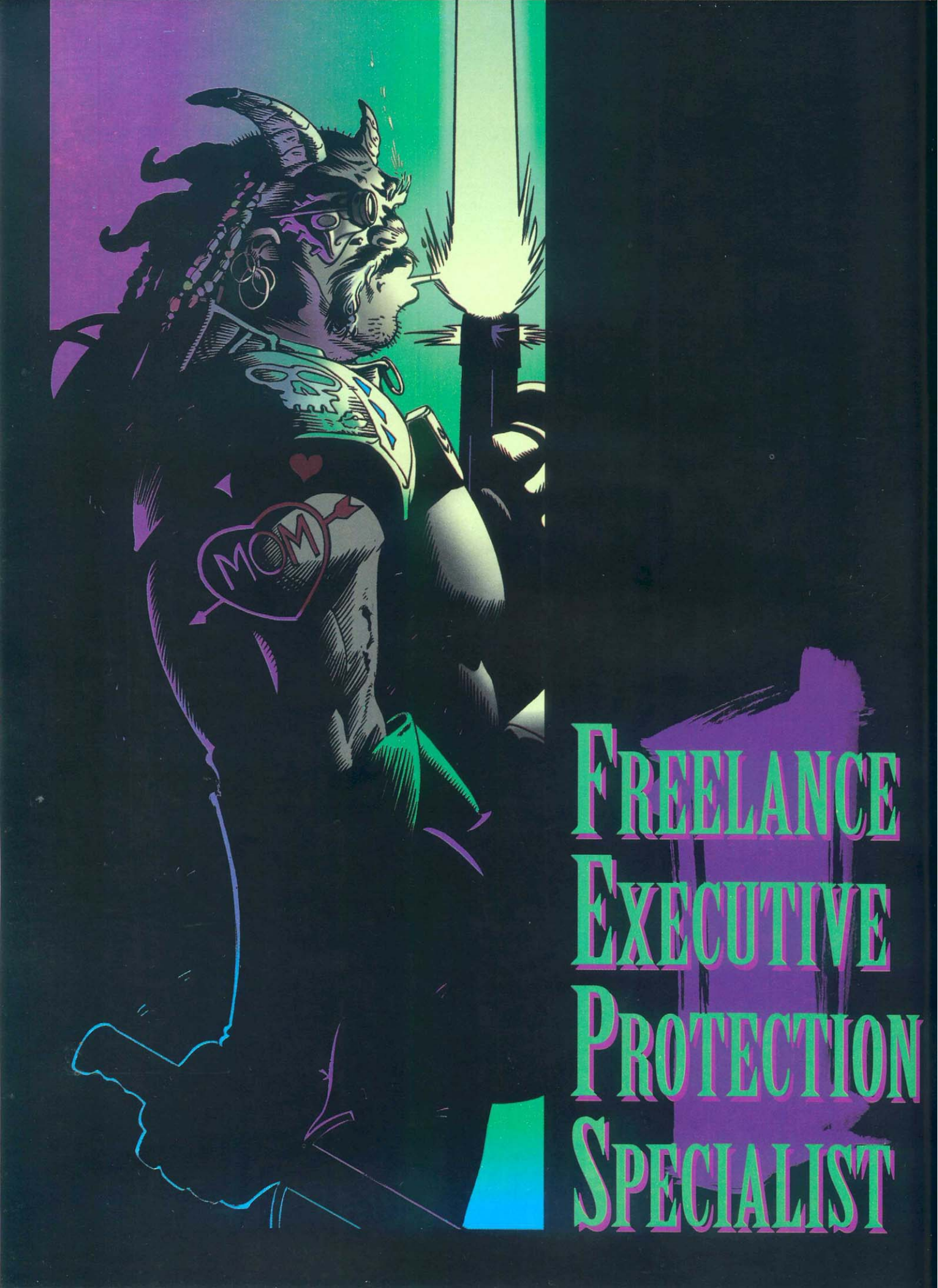
(09:10:51/12-06-55)

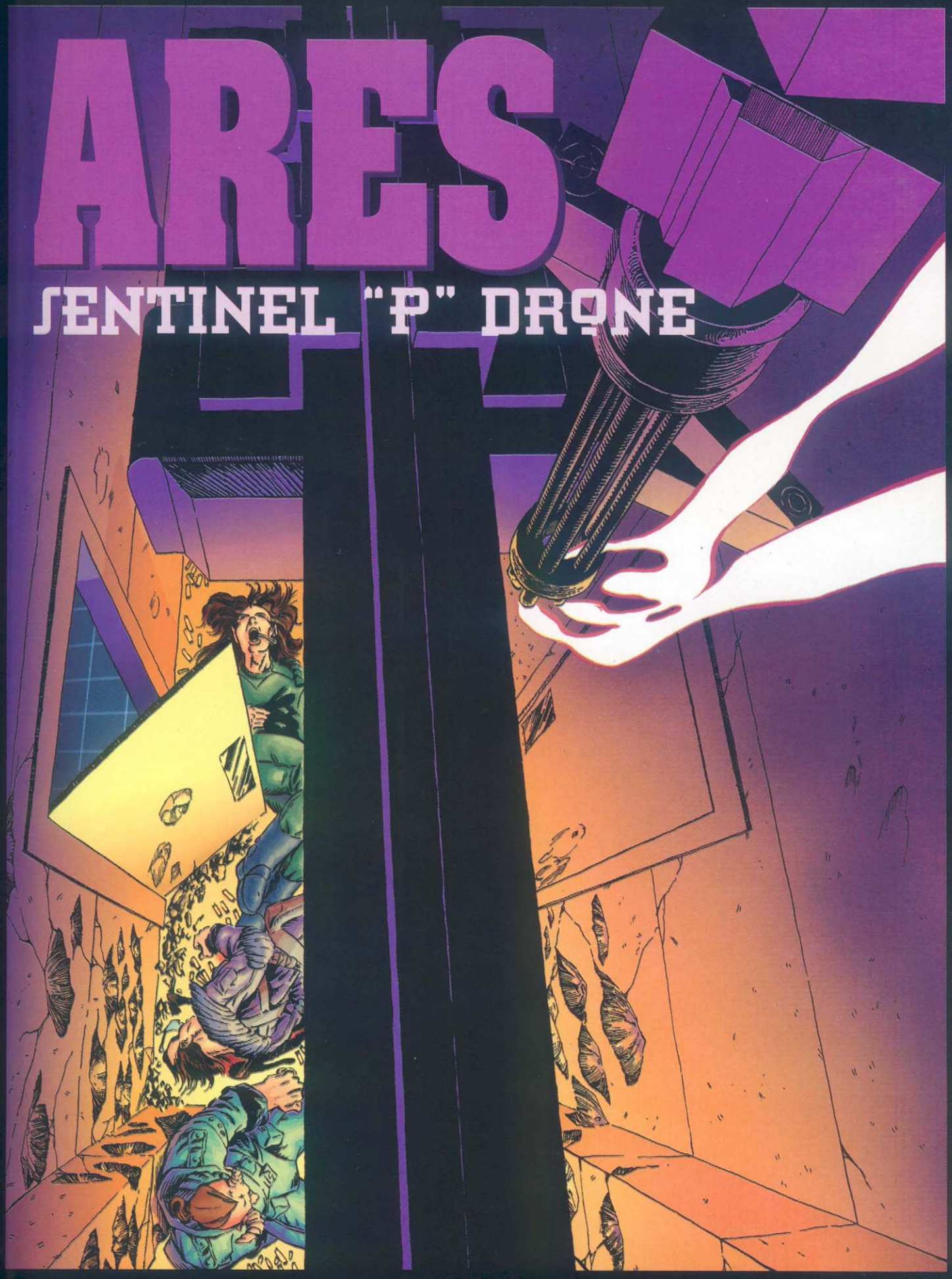
>>>>>(Smooth move, Zardoz.)<<<<<

—Weiner

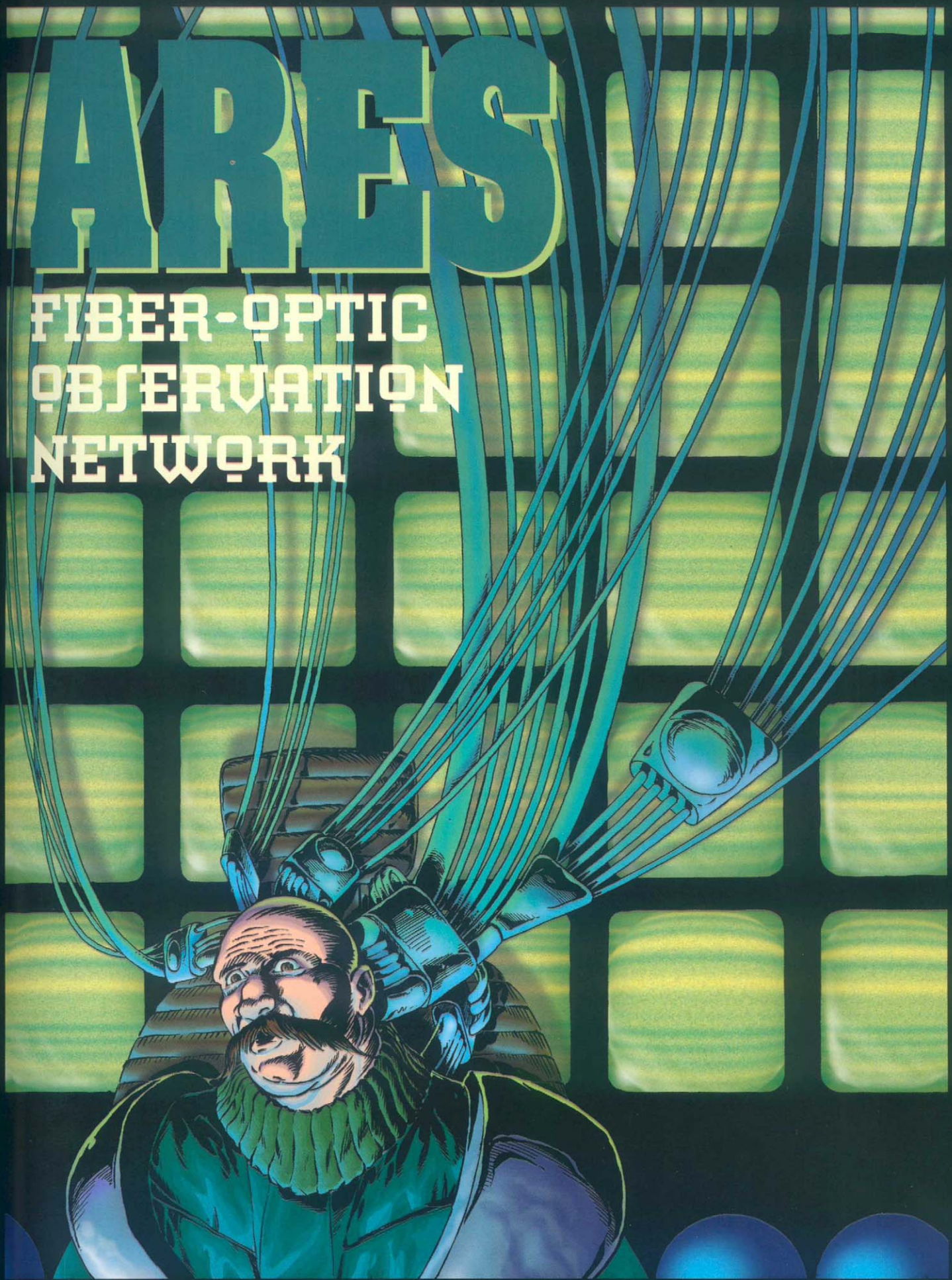
(21:41:40/12-07-55)


ARES
GUARDIAN DRONE


MOM
FREELANCE
EXECUTIVE
PROTECTION
SPECIALIST


ARES
SENTINEL "P" DRONE

FREELANCE
MAGICAL
SECURITY
CONSULTANT

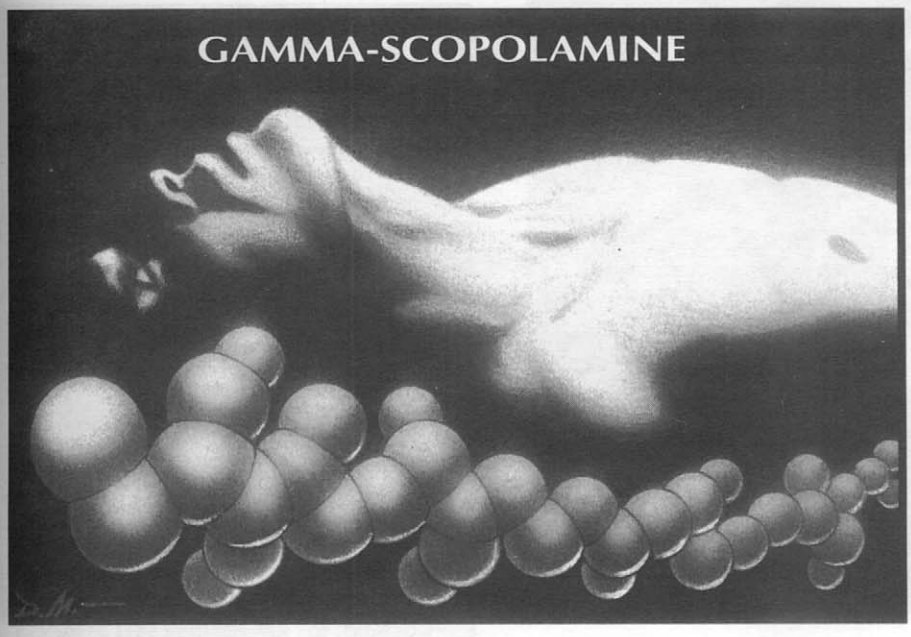

ARES
FIBER-OPTIC
OBSERVATION
NETWORK

FREELANCE SECURITY RIGGER


BACTERITECH
BACTERIAL
CONTAINMENT GRID

SECURITY SYSTEM DESIGN ENGINEER

GAMMA-SCOPOLAMINE



Since the introduction of DMSO in 2052, many customers have expressed an interest in a chemical compound designed to stop unauthorized personnel without permanently harming them. Ares Arms Chemical Division answers the call with gamma–scopolamine [$C_{17}H_{21}NO_5$]. This neuromuscular blocking agent prevents the uptake of acetylcholine, thereby rendering a target unable to move. Derived from the natural toxin found in *Atropa Belladonna*, commonly known as nightshade, gamma-scopolamine gives you the edge you need against intruders.

Rating	Speed	Vector	Availability	Cost	Street Index
10D Stun	Immediate	Injected	8/2 weeks	300¥/dose	3

NOTE: Gamma-scopolamine takes effect immediately, causing dizziness, dilation of the pupils, speech loss, delirium and paralysis. Deadly stun damage indicates full paralysis; for lesser damage, apply an additional +2 to all modifiers appropriate for the stun wound (for example, a Serious stun wound applies a +5 modifier to all target numbers and a –5 modifier to Initiative). The full effects last for one hour. After the hour has passed, the residue remaining in the body acts as a "truth serum" for an additional hour. Adjust the target's Willpower by –2 (down to a minimum Rating of 1) for the duration of the chemical's effect. Increase the Availability and base time by 1 and 1 day respectively for every 3 doses desired.

ORDER HERE

>>>>>(Another manmade abomination. Why must people mess with perfection and manipulate something that works fine au naturel?)<<<<<

—Whisper

(04:02:18/12-02-55)

>>>>>(If I understand you correctly, Whisper, you are advocating the use of pure nightshade. That stuff is poisonous. At least gamma–scopolamine doesn't kill.)<<<<<

—Dybbuk

(07:08:14/12-03-55)

>>>>>(Don't be fooled by the ad-talk—this stuff can be just as lethal. I've seen people OD on GS in the field. Obviously they were on the receiving end of the drek, but it's so powerful it can easily push an already taxed body over the limit.)<<<<<

—Hangfire

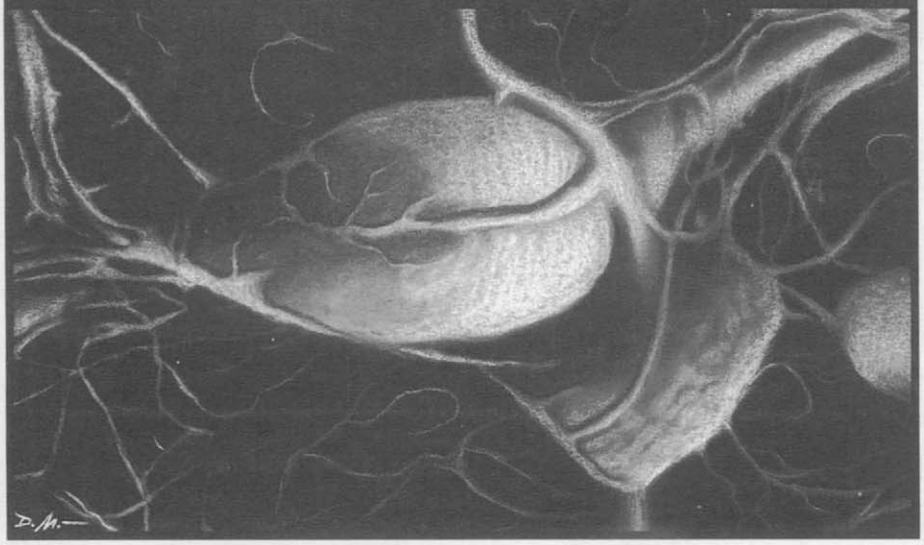
(20:17:54/12-05-55)

>>>>>(I hear Ares quietly sells a temporary antidote to those who ask. Don't know what it is or how to get it, but it allegedly neutralizes GS and related chemical doses inflicted within ten minutes of the antidote's ingestion or injection.)<<<<<

—Vancouver

(22:54:07/12-06-55)

FAT BACTERIA, STRAIN 1 (FAB-1)



BacteriTech™ is happy to release "fat bacteria," strain 1 (FAB-1) to the general security market. This rugged, long-lived, genetically engineered bacteria has proven effective as an astral containment device. An enclosed space filled with FAB-1 traps an astral being as easily as does an ivy-covered wall. However, FAB-1 has the advantages of being mobile, relatively inconspicuous and easily deployable. FAB-1 is usually stored in large, pressurized "coolant/feeding vats" and released into the controlled area when needed.

BUYERS' NOTE: Even though FAB has been stringently tested under controlled situations, it has received minimal field testing. Buyers who must deploy a non-contained FAB-equipped countermeasure (i.e. the Bacterial Containment Grid or FAB-UV Aerosol) are strongly urged to contact BacteriTech™ as soon as the situation is under control. BacteriTech™ will send specially equipped debriefers and clean-up specialists to your site free of charge. If you use a contained FAB product (i.e. Astral Containment Devices), please send the used product to BacteriTech™ as soon as possible. BacteriTech™ thanks you in advance for your cooperation and offers a 10 percent discount on recharging and refills for all expended products returned. Failure to contact BacteriTech™ relieves BacteriTech™ of all responsibility for any and all damages resulting from the use or misuse of this product.

	Cost
FAB-1	
50 m^3 canister	3,000¥
500 m^3 canister	25,000¥
5,000 m^3 canister	200,000¥
Coolant/Feeding Vat	
50 m^3 canister	2,500¥
500 m^3 canister	20,000¥
5,000 m^3 canister	175,000¥

NOTE: FAB-1 is shipped in huge coolant/feeding vat transports, Once a canister is removed from the vat the FAB-1 begins to die immediately and cannot be reused. This material is not generally available on the street; its Availability is at the gamemaster's discretion. See **Fat Bacteria**, p. 103, **Gamemaster Information**.

ORDER HERE

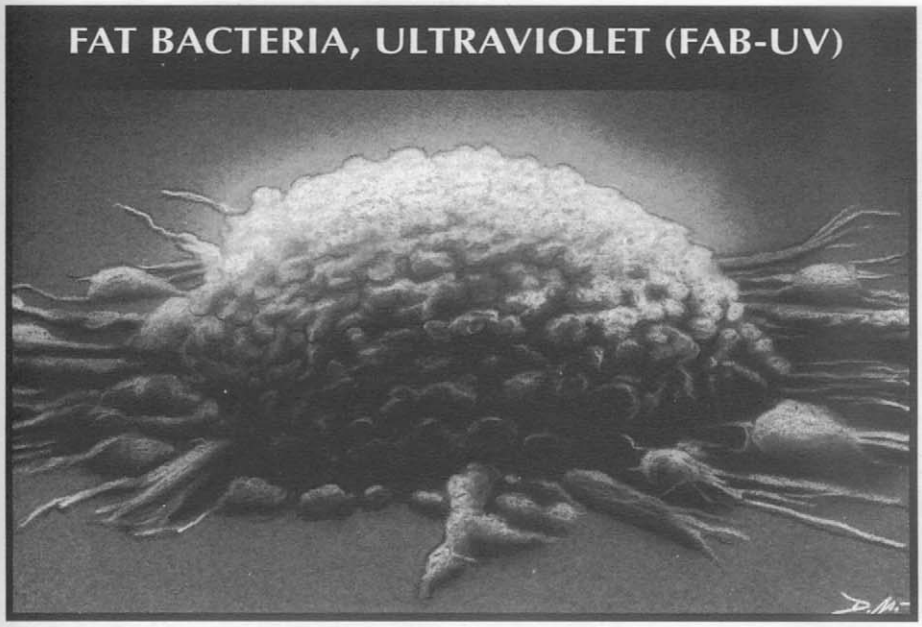
>>>>>(That means exactly what it says. BacteriTech™ has no idea what it has "created.")<<<<<
—Whisper
(14:11:33/12-04-55)

>>>>>(BULLDREK! Ares is definitely spooking us here. How can this stop an astral traveler??)<<<<<
—Moote
(03:28:19/12-12-55)

>>>>>(The theory is very simple—a sufficient concentration of massive bacteria, so "fat" (as they say) as to be almost visible, is pumped into a room until the atmosphere becomes a veritable "soup" rather than simply air. That air-soup is dense enough to restrict the passage of an astral body.)<<<<<
—Devon
(12:29:18/12-15-55)

>>>>>(Ah, you unschooled speculators. Even back in the section about the bio-net this discussion was flawed because of one simple misconception—you're all assuming that an astral body has no mass and therefore cannot pass through a living body that does have mass. Astral space has nothing to do with mass. Astral passage is restricted by living matter because the intervening body is organic, not because it's alive and has mass. Auras cannot intersect; the two life forces try not to interact, and the more powerful one wins and pushes or repels the other.)<<<<<
—Magister (20:18:54/12-18-55)

FAT BACTERIA, ULTRAVIOLET (FAB-UV)



Also available from BacteriTech™ is FAB-Ultraviolet (FAB-UV). FAB-UV has a unique property; it glows when subjected to ultraviolet light. To trap astral intruders using FAB-UV, lightly flood an area that you suspect an astral traveler has entered. Then illuminate the area with ultraviolet light. As the astral intruder moves through the flooded area, he or she displaces the glowing FAB-UV, casting a "shadow" that reveals the intruder's location.

Once released, FAB-UV has an approximate life span of three to four hours. FAB-UV aerosol canisters should be stored in sub-zero freezers until needed.

	Cost
FAB-UV	
50 m^3 aerosol	5,000¥
500 m^3 aerosol	45,000¥
FAB-UV Freezers	
50 m^3 aerosol	10,000¥
500 m^3 aerosol	50,000¥

NOTE: FAB-UV aerosols are shipped frozen. Once removed from the freezer, the bacteria immediately begins to die and cannot be reused. The 5,000 m^3 aerosol canister can be equipped with underbarrel mounts for mounting on a BacteriTech™ FAB-Netgun. See **Fat Bacteria**, p. 103, **Gamemaster Information**.

ORDER HERE

PAID

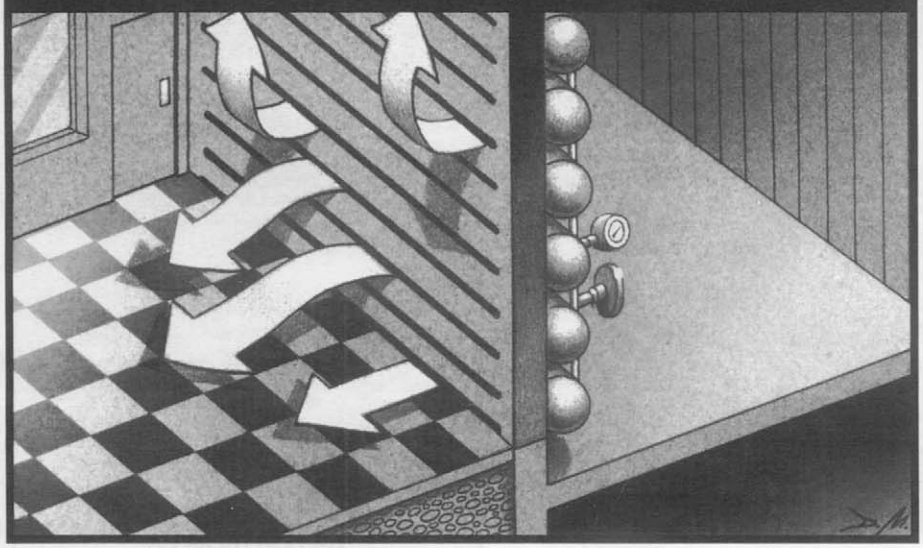
>>>>>(So a sufficiently dense FAB soup can restrict the travel of an astral body.)<<<<<
—Lyle
(09:28:19/12-19-55)

>>>>>(Theoretically.)<<<<<
—Magister
(02:22:14/12-20-55)

>>>>>(Wait—how does that affect the FAB netgun? Will an astral body support a living physical object??)<<<<<
—Moote
(10:14:51/12-20-55)

>>>>>(No. If intersection is forced by, say, a living net dropping over an astral body, and the weaker will (the net) cannot be displaced because of its mass, the superior will retreats to avoid intersection. In this case, it would retreat through the floor.)<<<<<
—Magister
(11:18:19/12-20-55)

BACTERIAL CONTAINMENT GRID



Building a secure site from the ground up? How about building protection against astral intruders right into the walls? Design engineers from Ares Security International, in conjunction with magical security engineers from BacteriTech™, are available for subcontracted design and construction of astral protection at your site. Depending on the size and budget of the site, these engineers can design and install an appropriate Bacterial Containment Grid (BCG). All the site's exterior walls, doors and windows are double-layered, with FAB-1 pressurized release units attached. When an astral intruder is detected within the protected area, the on-site security magician simply activates the BCG, automatically deploying the fat bacteria. Once the grid is fully deployed, it traps the astral intruder within the protected area. Once again, Ares offers its customers the most advanced security innovations!

	Cost
CerebroTech™ Computerized Release Control	5,000¥
Pressurized Release Conduits*	5,000¥
FAB–1	See FAB-1 price list
Coolant/Feeding Vat	See FAB-1 price list
Construction Costs	Call for estimate/appointment
Portable Dispenser (50 m^3)	7,000¥

*One conduit is required for each FAB-1 canister in the system.

NOTE: See **Fat Bacteria** in **Gamemaster Information**. These items are not normally available on the street; Availability is at the gamemaster's discretion.

ORDER HERE

>>>>>(OK, they've dropped a living net on your astral body and its mass repels you downward through the floor. Let's say the floor has this bacteria grid in it. It's so dense that you can't pass through it. What happens?)<<<<<

—Lyle
(11:23:56/12-20-55)

>>>>>(<Sigh> You remind me of my six-year old. What happens is very painful. Metathesis is induced—intersection is forced. One living spirit attempts to pass through another. I wouldn't wish the experience on my worst enemy.)<<<<<

—Magister
(12:01:28/12-20-55)

>>>>>(Can the two merge?)<<<<

—Lyle
(12:03:20/12-20-55)

>>>>>(No. One of them will die.)<<<<<

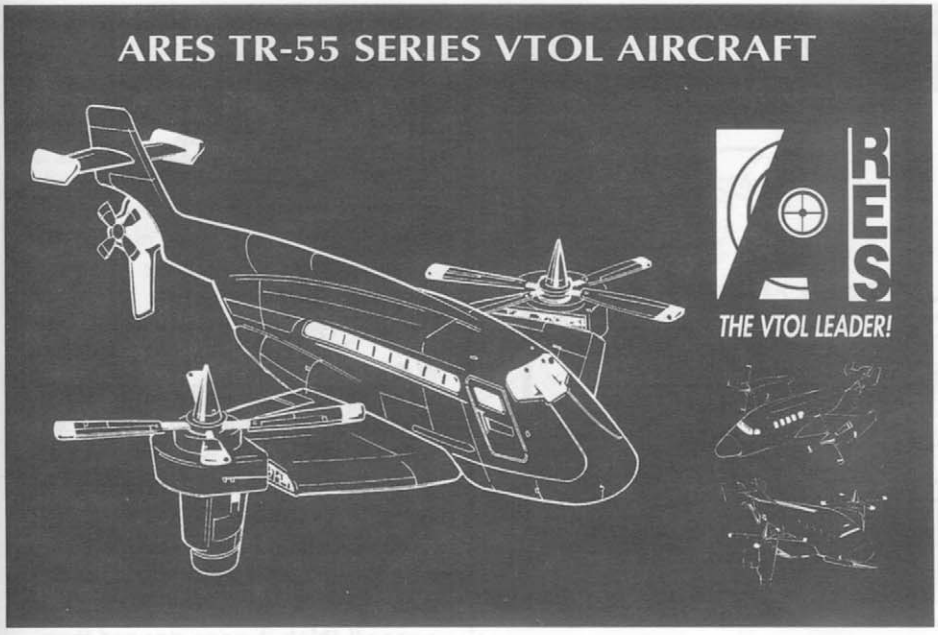
—Magister
(12:04:23/12-20-55)

>>>>>(Can a mage or spirit in astral space force himself through a mundane and kill him?)<<<<<

—Devon
(12:10:29/12-20-55)

>>>>>(No. A mundane is not present in astral space, so there's nothing for a spirit to pass through. The spirit deflects around the mundane. Sometimes I regret educating people.)<<<<<

—Magister
(12:15:41/12-20-55)



The tilt–wing Ares TR–55 series combines the VTOL capability of a standard rotorcraft with the fuel efficiency of a conventional fixed-winged aircraft. The TR-55 may seem similar to the competition's VTOL; however, the TR-55E (Executive) version can seat three additional executives. It's true the TR-55 has half the fuel economy of the competition's model, but it easily compensates with double the fuel capacity. The TR-55 excels over the competition with its hover mode. Double-slotted, independent flaperons provide exceptional yaw control, and a hydraulic fan in the upper tailplane controls pitch. Lateral control is provided by varying propeller power output. This reduces rotor lift by roughly 10 percent, but the downwash of the propellers is distributed over the wing, leaving a calm area between the two columns of air to facilitate picking up loads or passengers from a hovering position.

ORDER HERE

>>>>>(Who are these Ares slags trying to fool? Anybody who's anybody knows "the competition" is the Federated–Boeing Commuter 2050.)<<<<<

—The Unknown Rigger
(03:20:21/12-03-55)

>>>>>(Hey, watch who you call slag!!!)<<<<<

—Slag
(21:08:09/12-06-55)

>>>>>(Why are VTOL craft in a security catalog?)<<<<<

—The Roving Rover
(23:11:28/12-09-55)

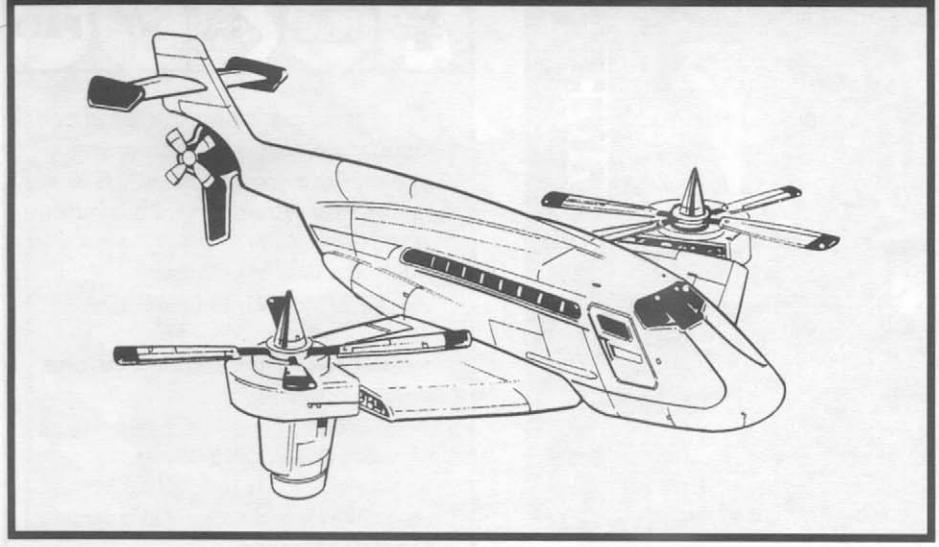
>>>>>(Why not? The corps use these aircraft all the time: the Traveler for short hops from corp to corp and the Executive for the bigwigs.)<<<<<

—BitRunner
(08:11:32/12-10-55)

>>>>>(Guess what? Fed-Boeing builds these puppies, but to Ares' specs. Go figure.)<<<<<

—Opus 12
(21:56:59/12-11-55)

TR–55T TRAVELER VTOL



The most popular version of the tilt-wing TR-55 series is the TR-55T Traveler. The TR–55T is specifically designed to transport short-distance commuters. Sales of the Traveler have surpassed those of its competition ever since this craft's debut, because it gives more passengers a smoother ride to their destinations in less time. The tail fan, vital to this aircraft's renowned stability, creates a smooth, even lift and descent, as well as smoothing the critical transition from vertical to horizontal movement. The wider body of the TR-55T allows for an extra five passengers per flight.

	Handling	Speed	B/A	Sig	APilot	Cost
TR-55T (Traveler)	5	170/350	3/0	3	3	500,000¥

Seating: Twin bucket seats + 20 bucket seats
Access: 1 + 1 standard
Economy: 1.2 km per liter*
Fuel: IC/1,600 liters
Storage: 10 CF storage + 20 CF cargo
Landing/Takeoff Profile: VTOL/STOL
Availability: 50/25 days**
Street Index: 2

Options:	Cost	CF Required
Rigger Control System	10,000¥	6
Wet Bar/Steward Area	2,500¥	5

*VTOL Economy: 0.75 km/liter

** Divide Availability target number by 3 (round up) for the mercenary contact known as the Dealer (see p. 81, **Fields of Fire**).

ORDER HERE

>>>>>(Why does Ares market these? Especially if they're made by Federated Boeing ...)<<<<<

—Killjoy
(20:19:29/12-01-55)

>>>>>(Exploitation of the Ares name. People associate it with security on some level, so why not make use of that to bring in some extra nuyen?)<<<<<

—Shadowmagu
(09:28:41/12-02-55)

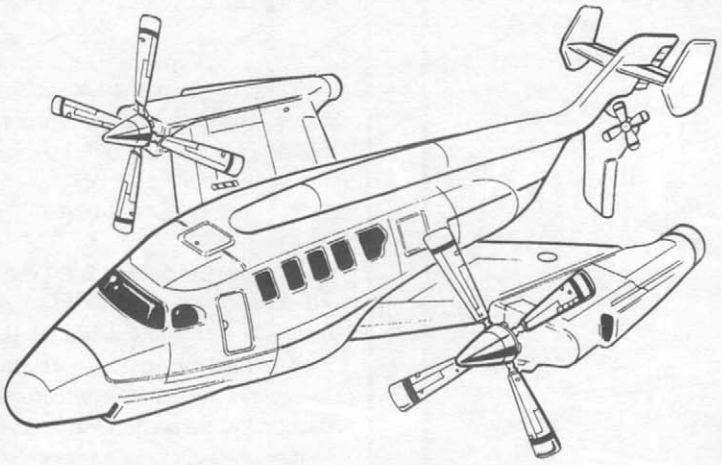
>>>>>(I think it goes deeper than that. Sure, F-B puts the plane together, but Ares provides most of the parts. I think it's quality control. Ares knows what goes into each plane—they inspect each one themselves before it leaves the factory. They know exactly what the craft can and cannot do.)<<<<<

—Doodles
(21:01:55/12-05-55)

>>>>>(Maybe, but I'll bet they could run enough tests on an F-B Commuter or an Osprey II to get enough knowledge to make those kind of evaluations about those craft.)<<<<<

—Iopa
(17:49:20/12—06-55)

TR-55E "PRESIDENT'S EDITION" EXECUTIVE VTOL



The "President's Edition" has twin bucket seats in the separated cockpit for the pilots and deluxe leather lounge seats for nine passengers. A communications suite, rigger control gear and a wet bar are just some of the options available.

	Handling	Speed	B/A	Sig	APilot	Cost
TR-55E (Executive)	5	170/350	3/0	3	3	650,000¥

Seating: Twin bucket seats
+ 9 Executive bucket seats

Access: 1 + 1 standard

Economy: 1.2 km per liter*

Fuel: IC/1,520 liters

Storage: 10 CF storage + 10 CF cargo

Landing/Takeoff Profile: VTOL/STOL

Availability: 65/65 days

Street Index: 2

Options:	Cost	CF Required
Full Communications Suite	5,000¥	2
Wet Bar	1,000¥	2
Lavatory	10,000¥	4
Kitchenette	8,000¥	4
Entertainment System	5,000¥	2
Rigger Control System	10,000¥	6

*VTOL Economy: 0.75 km/liter

Divide Availability target number by 3 (round up) for the mercenary contact known as the Dealer (see **Fields of Fire).

ORDER HERE

>>>>>(Figures that the executive types get the cushiest ride. I bet they make the team members ride in the cargo hold!)<<<<<

—Wittman

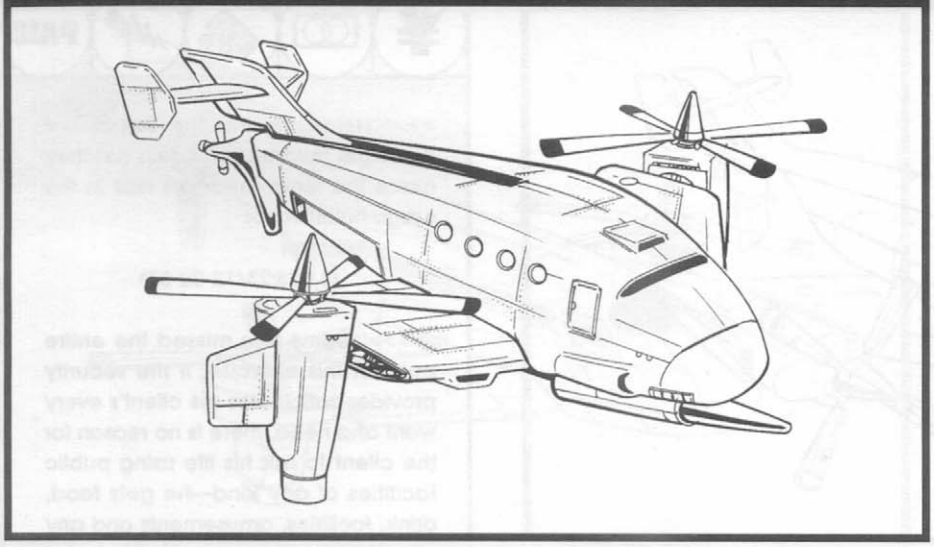
(11:23:23/12-02-55)

>>>>>(Seems you missed the entire point of this exercise. If the security provider anticipates the client's every want and need, there is no reason for the client to risk his life using public facilities of any kind—he gets food, drink, facilities, amusements and any other distractions he might desire without going to the airport's executive lounge, executive bar, or executive washroom. Executive security is all about controlling the client's environment to reduce outside risk, and this is a very acceptable form of control to most executives.)<<<<<

—Dybbuk

(11:54:12/12-02-55)

TR-55C CARGOLINER VTOL



This version of the TR-55 tilt-wing offers all the benefits of the TR-55T, plus an extra-rugged design that makes it perfectly suited for paramilitary and military forces. The TR-55C adds an armored skin, at the price of a marginal loss of fuel economy and flight performance. The TR-55C is the favored VTOL of the UCAS Coast Guard for search-and-rescue missions because of its unique ability to hover in place with a relatively calm area underneath the aircraft. The TR-55C is also ideal for transporting cargo into hard-to-reach areas.

The ventral hatch provides the means for lifting cargo or personnel from a hovering position. The standard TR-55C comes with a winch capable of lifting up to one metric ton. Standard folding webbed seating is provided along the sides of the cargo hold, with the option of conversion to fixed benches for use as stretchers or for other needs.

Military organizations or those with special needs may choose a rear cargo ramp/hatch at an additional charge. This option reduces the craft's overall cargo capacity by 25 percent, but provides added flexibility for loading and unloading.

	Handling	Speed	B/A	Sig	APilot	Cost
TR-55C (Cargo)	5	170/350	4/9	3	3	550,000¥

Seating: Twin bucket seats + 12 folding bench
Access: 1 + 1 standard
Economy: 1.0 km per liter*
Fuel: IC/1,600 liters
Storage: 10 CF storage + 50 CF cargo (75 CF if seats folded/removed)
Landing/Takeoff Profile: VTOL/STOL
Availability: 55/55 days**
Street Index: 2

Options:	Cost	CF Required
Rigger Control System	12,000¥	6
Rear Access Ramp***	25,000¥	15

*VTOL Economy: 0.5 km/liter

Divide Availability target number by 3 (round up) for the mercenary contact known as the Dealer (see **Fields of Fire).

***The rear-access ramp creates additional access (up to a total of 4) but decreases overall capacity to 8 CF storage + 35 CF cargo.

ORDER HERE

>>>>>(OK, I can understand why the Traveler and the Executive are here, but why a military craft?)<<<<<
—The Roving Rover
(20:44:09/12-02-55)

>>>>>(The Cargoliner is the transport vehicle of choice for the Knight's executive protection teams. It lands first, deploying the team. An Executive lands shortly after into a (hopefully) controlled landing zone. A real pretty sight to see.)<<<<<
—Dybbuk
(09:20:41/12-03-55)

ARES SENTINEL™ SERIES DRONES

The success of our Ares Arms Sentry™ series has driven us to develop the next step in zone control—the Ares Arms Sentinel™ drone system. As with the Sentry system, the Sentinel can be customized to suit the specific needs of different security systems. All Sentinel units come with integrated thermographic and pulse-radar security sensors. Though the basic Sentinel drone is immobile, its diverse arsenal of lethal and non-lethal weapon systems allow it to control a wide variety of zones. The Sentinel is also designed to be compatible with Ares Security International's Fiber-Optic Observation Network™ and has one optical port installed on all units. Remote operation is standard, but the Sentinel may also be rigged for direct neural control. Standard placement for the indoor model is on the ceiling; the outdoor model is normally mounted on a stationary platform or pole. The drone draws power from standard building power systems and has a built-in battery for operation during power outages. All Ares Sentinel drones and accessories are equipped to accept closed-circuit simsense (CCSS) protocols.

	Handling	Speed	B/A	Sig	APilot	Store	Cost
Sentinel	5	N/A	4/12	8	3	N/A	40,000¥

Economy: N/A **Power:** 2 PF

Operational Duration: Building supplied/unlimited. Back-up battery power: 2 hours

Setup/Breakdown Time: N/A **Sensor Package:** Security II (5)

Additional Features: Indoor model standard installation includes a badge proximity interrogation system (see p. 30, in **Technical Security**), Neuro-Stun VII gas delivery system, and a firmpoint that accepts any Ares Sentinel weapons pod. The Sentinel™ provides 6 points of recoil compensation. A fully weatherproofed outdoor model is available at an additional cost of 10,000¥. The outdoor model is identical to the indoor model except that it does not normally contain the gas delivery system.

NOTE: This item is not generally available on the street; Availability is at the gamemaster's discretion.

ORDER HERE

>>>>>(Wait a minute—this is a drone? Sounds like a gun emplacement to me.)<<<<<

—Wittman
(03:20:18/12-03-55)

>>>>>(Pretty much. It's controlled through a drone interface, which is probably why Ares classified it as a drone.)<<<<<

—Teague
(23:54:48/12-05-55)

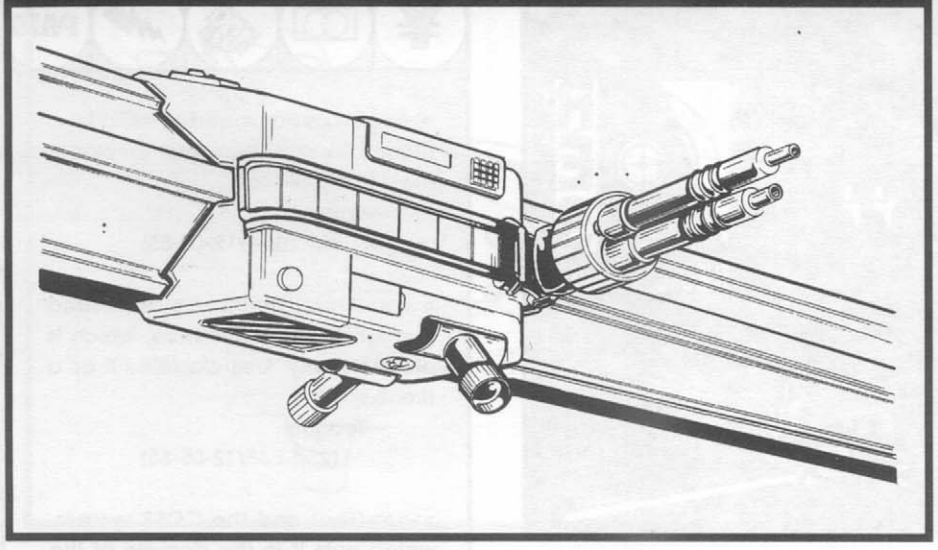
>>>>>(That and the CCSS system, which puts it in the domain of the security rigger. Also, "drone" is so much sexier a term than "gun emplacement.")<<<<<

—Findler-man
(19:31:50/12-09-55)

>>>>>(Walks like a duck, quacks like a duck ...)<<<<<

—Lost Waldo
(17:42:30/12-10-55)

ARES SENTINEL™ "P" SERIES DRONES



No perimeter security system would be complete without the addition of the Ares Arms Sentinel™ P drone series. Based on the stationary Sentinel, the P version is semi-mobile, performing a fixed patrol circuit around sensitive zones. Available in both indoor and outdoor models, the Sentinel P is ready to follow any path set down for it by the use of our revolutionary EMMA™ (ElectroMagnetic Movement and Articulation) system. Just mount the monorail-style track where you want the drone to patrol and let it do the rest! The unit draws power from the track, which in turn pulls its power from building power sources. In the case of a power failure, the Sentinel P releases safety clamps to grip the track and draws backup power from an internal battery.

	Handling	Speed	B/A	Sig	APilot	Store	Cost
Sentinel P	5	10	4/12	6	3	N/A	60,000¥

Economy: N/A **Power:** 2 PF

Operational Duration: Building supplied/unlimited. Backup battery: 2 hours

Setup/Breakdown Time: N/A **Sensor Package:** Security I (4)

Additional Features: Indoor model standard installation includes a badge proximity interrogation system (see p. 30 in **Technical Security**) and a firmpoint that accepts any Ares Sentinel weapons pod (see p. 93 of this section). The Sentinel P provides 4 points of recoil compensation. A fully weatherproofed outdoor model, identical to the indoor model, is available at an additional cost of 10,000¥.

Track for the drone costs 100¥ per meter and can be mounted on walls and ceilings indoors, or along the top of a fence, wall or other barrier outdoors. Only 10 centimeters wide, the track can be connected to any building's electrical power supply.

NOTE: This drone is not normally available on the street; Availability is at the gamemaster's discretion.

ORDER HERE

>>>>>(Interesting. It follows a locked-down path: seems restrictive.)<<<<<

—Kong

(20:27:07/12-04-55)

>>>>>(Not really. Why use a free-ranging drone when you only need to patrol a limited area? I've seen a lot of these running on monorails suspended from warehouse ceilings. They can range across almost the whole interior without worrying about what's on the ground or in their way. They've also got a fabulous field of view—and that means field of fire—from on high.)<<<<<

—Tauros

(03:24:55/12-06-55)

>>>>>(I've also seen them set up to run on a track that moves from room to room via small passages in the wall. Security doors remain intact and sealed, but the drone can range throughout the area.)<<<<<

—Hangfire

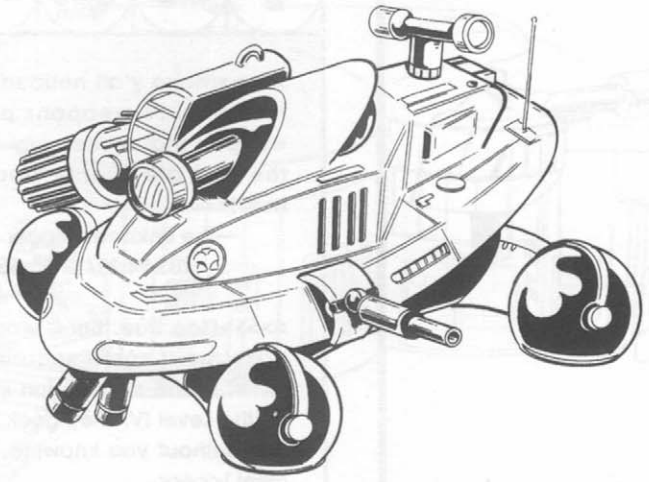
(05:18:41/12-07-55)

>>>>>(The track is the weak link.)<<<<<

—Gorgo

(11:28:54/12-10-55)

ARES GUARDIAN™ DRONES



Complete your security blanket with the Ares Arms Guardian™ drone. A vectored-thrust vehicle small enough to be used indoors, Guardians are sturdy enough for outdoor activity as well. If you liked our Sentinel line, you'll love the Guardian!

	Handling	Speed	B/A	Sig	APilot	Store	Cost
Guardian	4/6	30/60	4/12	6	3	20 CF	75,000¥

Economy: 5 km per PF **Power:** 30 PF
Operational Duration: Limited by battery power: 2 hours
Setup/Breakdown Time: 3 minutes **Sensor Package:** Security I (4)
Availability: 8/8 days **Street Index:** 2
Additional Features: The Guardian drone is a free-ranging model of the Sentinel series. Its micro-turret is designed to accept any Ares Sentinel weapons pod. It also has special attachments on the rear of the turret for mounting external tanks and compressed air for use with the Ares Cascade™ delivery system. An additional 3 CF is available for vehicle control gear or other electronic options.

ORDER HERE

>>>>>(A vector-thrust drone?? Wild.)<<<<<
—Ernie
(20:29:18/12-02-55)

>>>>>(What's so wild about it?)<<<<<
—Joo
(10:29:19/12-05-55)

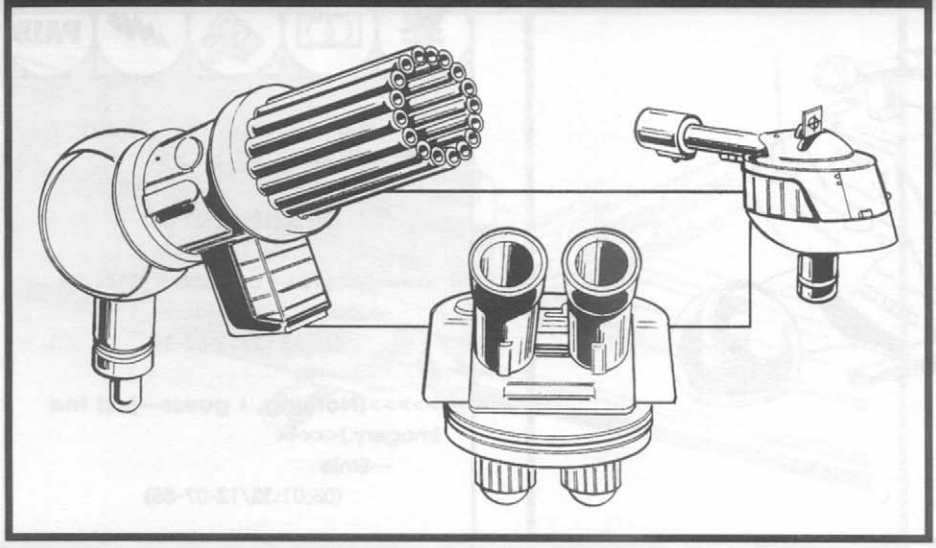
>>>>>(Nothing, I guess—just the imagery.)<<<<<
—Ernie
(05:01:32/12-07-55)

>>>>>(Weirdo.)<<<<<
—Joo
(22:09:17/12-08-55)

>>>>>(Baton twirler.)<<<<<
—Ernie
(21:47:58/12-12-55)

>>>>>(?????)<<<<<
—Joo
(15:28:46/12-18-55)

ARES SENTINEL™ WEAPONS PODS



Ares Arms Sentinel™ weapons pods let you arm your Sentinel drones with a variety of topnotch weapons and ammunition in single, modular units. A corporate security rigger can change non-lethal drones to killers simply by replacing one pod with another. It's that simple! All Sentinel and Guardian™ drones accept the Sentinel weapons pods, automatically adjusting their internal inertial compensators and targeting information for each weapon through onboard CerebroTech™ processors and preprogrammed firmware. For a slight additional fee, Ares Arms will design and build custom weapons pods.

	Weapons Installed	Ammo	Availability	Cost	Street Index
Weapons Pod I	Ares Squirt II	40	5/1 week	3000¥	2
	Defiance Super Shock	20			
Weapons Pod II	Ares Viper Slivergun	75	6/1 week	3500¥	2
	Narcoject Pistol	20			
Weapons Pod III	HK227–S	150	6/2 weeks	5000¥	2
	Narcoject Rifle	20			
Weapons Pod IV*	Ares MP–LMG	500	8/2 weeks	7,500¥	2
	Ares Cascade™	**			

*The Weapons Pod IV can only be installed on an Ares Guardian drone.

**The Ares Guardian drones have built-in storage for two sets of 100-shot canisters (DMSO Gel and the chemical reserve). The Weapons Pod IV carries twin compressed-gas canisters for up to 200 shots. These canisters can be recharged at a cost of 100¥.

Both removing and installing a weapons pod are Complex Actions, and so it takes two Complex Actions to change a pod. The pods can only be installed on Ares Sentinel and Guardian drones; installation on any other drones requires major hardware and firmware modifications.

ORDER HERE

>>>>>(Have y'all noticed that only the Level IV weapons pod has a weapon that makes any noise? All the rest are silent—kinda scary, huh?)<<<<<

—The Unknown Rigger
(03:54:29/12-05-55)

>>>>>(Too true. But it wouldn't surprise me if some security riggers install sound suppression in the LMG on the Level IV. They geek your buddies without you knowing. Very efficient.)<<<<<

—Dybbuk
(23:07:54/12-09-55)

>>>>>(Bet they only use gel rounds in the LMG, too.)<<<<<

—Slag
(14:31:57/12-10-55)

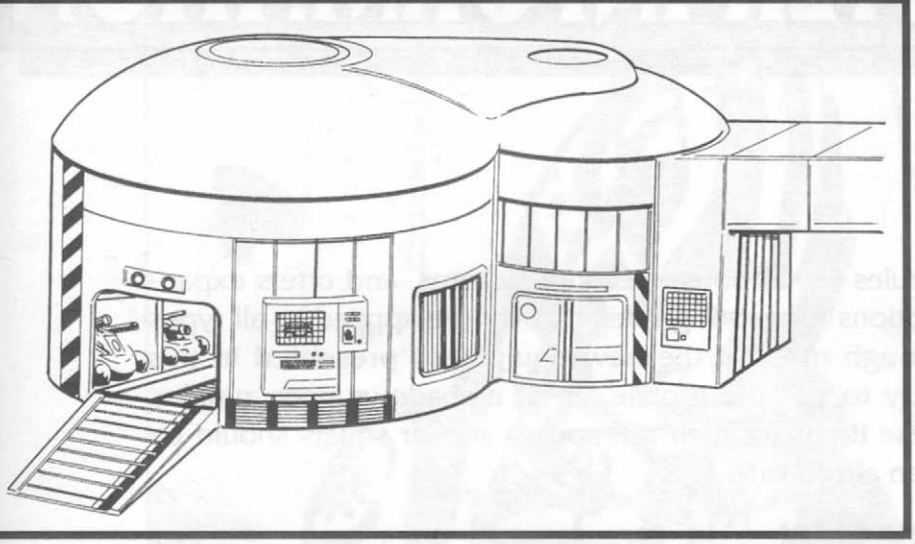
>>>>>(Interesting. I assume that since they can swap systems on the fly, they can recalibrate drone weaponry for any threat that rears its ugly head?)<<<<<

—Somma
(02:54:37/12-11-55)

>>>>>(Good guess. Read on!)<<<<<

—Hangfire
(03:48:35/12-12-55)

ARES SENTINEL™ DRONE STORAGE SYSTEM



Store your Ares Arms Sentinel™ drones easily and efficiently with the Ares Arms Sentinel Drone Storage System! The basic unit can house up to three Ares Sentinel P drones, two Ares Guardian™ drones, and 10 Ares Sentinel weapons pods. Also included is an automated rearming system that can change two weapons pods at the same time. The security rigger sends the system a "rearm" command, and the unit's CerebroTech™ processor does the rest! Storage capacity can be increased and additional rearming systems installed for a modest additional cost. The Sentinel Drone Storage System is completely self-contained, operates off building power sources, and can be fully weatherproofed for outdoor use. Also includes backup power supply in case of power failure.

	Cost
Sentinel Drone Storage System	100,000¥
Additional Features	
Backup Power Supply (2 hours)	+5,000¥
Additional Sentinel P Storage	+5,000¥/drone
Additional Guardian Storage	+7,500¥/drone
Additional Weapons Pod Storage	+1,500¥/drone
Additional Rearming System*	+10,000¥
Weatherproofing	+10,000¥

*Only one rearming system can be added for every three drone-storage capacity upgrades. Each rearming system can change one weapons pod per Combat Turn.

NOTE: This item is not normally available on the street; Availability is at the gamemaster's discretion.

ORDER HERE

>>>>>(Great, a drone factory. And with Ares making custom weapons pods, who knows what'll roll out.)<<<<<

—Lost Waldo
(20:29:10/12-04-55)

>>>>>(Actually, I'm heartened by the fact that Ares places such emphasis on non-lethal technology.)<<<<<

—Butch Carmody
(05:47:13/12-09-55)

>>>>>(Yea, Butch is happy `cause he's going against an Ares-protected facility next week and he's been worried about it.)<<<<<

—Xerxes
(10:28:49/12-10-55)

>>>>>(When the lead starts to fly, you can bet those "non-lethal" drones won't be squirting snooze juice.)<<<<<

—Aaron
(01:47:52/12-11-55)

GAMEMASTER INFORMATION

This section provides new rules for corporate security systems, and offers expansions, clarifications, and options for existing rules that can be applied to all types of security systems. Although most of the new equipment presented in this sourcebook is too unwieldy to suit the mobile life of a shadowrunner, runners who want to purchase these items for their safehouses and/or squats should be allowed to do so (if they can afford to).

SECURITY SYSTEM DESIGN

A typical corporate security system includes some kind of physical security, technical security, magical security, Matrix security, and personnel security. When designing a security system, the gamemaster chooses the level of security for all the components in each of these areas (described in the following pages). The level chosen determines the basic types of equipment available, from which the gamemaster selects what he wants his runners to face. If appropriate, the gamemaster may also assign individual ratings to each piece of equipment. Unless otherwise noted, equipment available at a given security level has a rating equal to that level. If a given piece of equipment is first available at a lower security level than the level chosen by the gamemaster, a good rule of thumb is to assign it an individual rating of twice the chosen level. Gamemasters should, of course, use common sense when applying this guideline to security systems.


BERGTING-95

LEVELS OF SECURITY

Each component of a security system has its own level of effectiveness on a scale of 0 to 4. **Level 0** indicates that no security of that type exists in that particular security system. **Level 1** indicates that minimal security measures for the component in question are present. **Level 2** indicates the presence of standard security measures. **Level 3** indicates higher-level security devices. **Level 4**, the highest level currently available, indicates maximum security for the component in question. Level 4 components tend to be active security measures; components at Level 3 or lower tend to be passive. Each successive level includes equipment available at lower levels.

Physical Security

Physical security includes the following components: barriers, lighting, guards, and security-trained animals. The gamemaster may assign any of these four components a separate security level of 0 through 4.

Level 0: The site has no substantial barriers and uses no special lighting. Neither guards nor trained animals are anywhere on the premises.

Level 1: All of the protected site's interior doors are reinforced. The site has perimeter lighting and security guards only at exterior entrances, and mundane security animals on-site.

Level 2: The site has perimeter fences and perimeter lighting with spotlights at key locations. On-site security guards patrol on a fixed schedule, accompanied by mundane security animals.

Level 3: All exterior and interior walls are reinforced and built slab-to-slab (they start at the floor and continue to the true ceiling, above the drop ceiling). The site has extensive lighting throughout the perimeter and grounds, with spotlights added at all points along the perimeter. Security officers are assigned to all exterior and important interior entrances; additional officers patrol at random times, accompanied by mundane security animals.

Level 4: The site has "living walls" at pertinent locations to prevent astral intrusion. The interior and exterior have special forms of lighting in various places: active infrared, low-level or magical lighting, and so on. Security officers patrol constantly, accompanied by paranormal and/or cybered security-trained animals.

Technical Security

Technical security includes two types of components: alarms and access controls, and surveillance equipment. The gamemaster may assign either of these components a separate security level.

Level 0: No alarms, access controls, or surveillance equipment has been installed.

Level 1: The site has Type 1 maglocks on interior doors and perimeter fence gates, and Type 2 maglocks on exterior doors. Closed-circuit TV cameras monitor the exterior of the protected area.

Level 2: The site has exterior door and window sensors, as well as fence alarms. Type 2 maglocks are installed on interior doors, Type 3 maglocks on exterior doors. Closed-circuit TV cameras monitor the interior, and a rigger from the corporate motor pool doubles as an on-call security rigger when necessary.

Level 3: The site has interior volumetric sensors and door sensors. Type 3 maglocks are installed on all doors; the maglocks are biometric in extremely sensitive areas. Drones patrol the perimeter and/or grounds. A full-time security rigger is on-site and on-call; he/she monitors the perimeter fence (if any) and all exterior doors via closed-circuit simsense.

Level 4: Deterrent devices in place include Type 4 maglocks and some biometric systems. Drones patrol major interior hallways; the site is also equipped with extensive closed-circuit simsense and stationary drone emplacements.

Magical Security

On-site magical security is a single component of corporate security, and refers to magically active personnel within the Magical Security Department, as well as the specialized equipment they use. It does not include security magicians on special assignment to other departments.

Level 0: There is no magical security on-site.

Level 1: A security magician is on-call, usually a corporate magician who doubles as a security magician as needed.

Level 2: A full-time security magician is on-site.

Level 3: The site is protected by wards and/or has a fiber-optic observation network for the security magician's use.

Level 4: Watchers, nature spirits and/or elementals augment astral patrols, alarms and/or fast response teams.

Matrix Security

Matrix security is a single component of an overall security system, and refers to the protection of a corporation's private matrix.

Level 0: The corporation has no matrix or does not protect it.

Level 1: Corporate deckers doubling as security deckers are on-call.

Level 2: Full-time security deckers are on-site, but only access the corporate matrix during an external alert.

Level 3: The site security deckers access the matrix during internal alerts.

Level 4: A security decker is in the site's matrix 24 hours a day.

Personnel Security

Personnel security is a single component of an overall security system, and refers to the way the corporate security provider screens, educates and investigates a client's employees.

Level 0: The corporation has no personnel security measures in place.

Level 1: The personnel security department conducts background investigations of new employees, generally limited to various computer checks (such as credit and criminal history) and a few cursory interviews (supervisors at the subject's most recent place of employment and one or two friends).

Level 2: The personnel security department conducts full background investigations of new employees. These investigations include nationwide computer checks of criminal history; interviews of supervisors and co-workers at all previous employers as far back as fifteen years; and interviews of neighbors, college professors, friends and enemies.

Level 3: The personnel security department has implemented active security awareness programs.


BERGTING

Level 4: The personnel security department conducts periodic loyalty checks and re-investigations of all employees. All employees must take lie-detector tests to verify information provided or obtained.

The gamemaster decides that surveillance (a component of technical security) at a site should be above average. According to the definitions of the different levels of security, above average is equivalent to Level 3. Level 3 surveillance includes exterior perimeter drones, interior and exterior closed-circuit television (CCTV) and limited closed-circuit simsense (CCSS). Drones have no rating, so the gamemaster must choose a few that seem appropriate or design new ones. CCTV is available at Level 1 and Level 2, and so the CCTV equipment has a Rating of 6 (twice the chosen security level). CCSS is only available at Level 3 or higher, and so it has a Rating of 3.

Overall Security Level

A protected site also has an overall security level (OSL). The OSL reflects how well a security system's individual components are integrated. To determine the overall security level, add up the levels of the individual components and divide by 6 (round down). The OSL becomes important when determining whether or not a component of a system has been bypassed. Players must not only bypass the individual component, but also the entire system (see **Defeating a Security System**, p. 104 of this section).

Several factors can modify the OSL, including the training given to personnel, their morale, and fatigue. Highly trained personnel tend to operate lower-level security systems at maximum efficiency, thereby giving such systems the equivalent of a higher level. Similarly, a sophisticated security system run by overworked or poorly trained personnel may not actually perform up to its given level. For example, a Level 3 security system run by highly trained and motivated employees may raise the OSL to a maximum of 4; the same system run by inadequate employees may lower the OSL to 2. Modifiers are cumulative. Note that the OSL cannot be modified above 5 or below 0.

Integrating Security Ratings from Corporate Shadowfiles

The **Corporate Shadowfiles** sourcebook assigns Security Ratings to each of the major megacorporations discussed within it. To find the Overall Security Level for sites belonging to those corporations, divide the given Security Ratings by 2 and round down. Note that the result represents an average for all of a given corporation's security assets; actual levels may vary from location to location. **Corporate Shadowfiles** Security Ratings also have a maximum of 5.

PHYSICAL SECURITY

The following rules apply to various measures described in **Physical Security**, pp. 12–23.

NATURAL PERIMETER BARRIERS

Hedges, tree lines, dense brush, hills, and so on are all examples of natural barriers. Often, these barriers are supplemented by perimeter alarms and/or wire. Players may traverse dense brush, but must add a +2 modifier to any Stealth Tests they make while getting through it. Solid or area-wide obstructions must be skirted.

MANMADE PERIMETER BARRIERS

Manmade barriers include walls, fences, manmade lakes and hills, and so on. For the ratings of various barrier materials, see **Barriers**, pp. 98–99, **SRII.** Note that fences usually cannot be damaged by firearms because their latticework lets the rounds pass harmlessly through them. Manmade barriers are also often supplemented by perimeter alarms and/or wire. Game mechanics for climbing walls and fences appear on pp. 74–75 of the **Fields of Fire** sourcebook; rules for swimming (across manmade lakes, for example) appear on p. 77 of that sourcebook.

WIRE

Natural and manmade perimeter barriers often incorporate obvious or concealed barbed, razor, concertina, or monowire. Barrier Ratings, Damage Codes, and the base target numbers for noticing the various types of wire appear on the table on p. 99.

The following modifiers apply to the Perception Test target number for spotting wire:

Situation	Modifier
Visibility	see p. 89, **SRII**
Obscured by brush	+1 to +4 (depending on amount of brush)
Character distracted/running	+2
Illumination level fluctuates	Add +1 to modifier for worst level

Trip Wires

Trip wires are a simple but effective type of perimeter security. All trip wires have the same Visibility as monowire (see above), but most do no damage when tripped (other than setting off the alarm). At the gamemaster's discretion, some corp sites may use monowire as a trip wire; if so, it does the Damage listed for monowire on the Wire Table, p. 99.

Trip Beams

Lasers or beams of high-intensity conventional lights serve as the equivalent of trip wires when fired across an area at a detector. Mirrors or reflectors may bounce the beam around an area before it reaches the detector, thereby increasing the amount of space covered and also creating an intricate web that player characters will find difficult to navigate. Interrupting the beam triggers an alarm.

Some trip beam emitters are obviously placed to be a visible deterrent. Others are concealed. To notice an intentionally obvious emitter and/or detector requires a successful Perception (2) Test with appropriate Visibility modifiers (p. 89, **SRII**). If the system is deliberately concealed, apply a +4 modifier in addition to appropriate Visibility modifiers. The old trick of spraying an aerosol into the area protected by the beam(s) still works, but at

WIRE TABLE

Wire Type	Perception Target	Damage* Grab/Walking/Running	Barrier Rating**
Barbed	2	3L/4L/6L	6
Razor	2	4L/5L/4M	6
Concertina	0	4M/5M/8M	6
Monowire	6	4S/5S/7S	5

*Impact armor offers one-half (round down) standard protection against this kind of damage. Combat Pool dice may not be used for the Damage Resistance Test.

**Damage must be applied directly to the wire. Wire clippers double a player character's Strength for the purposes of cutting the wire. If a player makes a Strength Test against the Barrier, every 2 successes achieved boosts the character's effective Strength by 1 for the purposes of cutting the wire.

the gamemaster's discretion may trigger certain sensitive alarm systems often found in environmentally controlled interior areas.

To bypass trip beams, a player character can make a Quickness Test against a target number ranging from 4 to 8, depending on the extent of the beam coverage (gamemaster discretion). Player characters will find it impossible to bypass some trip beams in this manner, however. Emitters and reflectors can be constructed to reroute the beam(s), but to do so requires knowledge of the system in advance, a steady hand, and luck. A player character trying this tactic under the best possible conditions (possession of the trip beam's design schematics and plenty of time to study them) must make a successful Quickness (8) Test. The target number for this test rises to 12 if the character has only a picture of the system, and to 16 if the character has neither a picture nor the design schematics. The base time for coming up with a scheme and the necessary equipment to bypass a trip beam is 1 week. Rumor has it that some people have come up with magical spells designed specifically to fool these systems; if the gamemaster wishes, he or she may allow players to attempt to devise such spells.

The most common method of bypassing a trip beam is to create a proxy beam by aiming additional emitters of the appropriate type at the detectors. When the player character breaks the trip beam, the proxy emitter is sending sufficient beam wattage to the detector, fooling it into thinking everything is fine. Each proxy emitter costs 200¥; one is required for each detector used by the trip beam. Setting up the proxy beam requires a successful Reaction (4) Test. If the test is unsuccessful, breaking the trip beam triggers the alarm.

TECHNICAL SECURITY

The following rules apply to various measures described in **Technical Security**, pp. 24–33

RATING TECHNICAL SECURITY DEVICES

Rather than going to the trouble of placing individual alarms, maglocks, and so forth on the game map and then determining their power levels, sensor capabilities, the area they cover, and so on, the following rules allow the gamemaster to assign each individual device a rating, depending on the security level of the component to which it belongs. Appropriate ratings for various types of equipment at various security levels appear on the table on p. 100. The gamemaster may, of course, feel free to assign higher ratings to equipment in particularly sensitive areas.

PERIMETER ALARMS

Perimeter alarm systems are often used to supplement perimeter barriers as well as within protected areas.

Motion Sensors

Motion sensors usually transmit an ultrasonic field and react to changes in the field when someone enters the area. Simple ultrasound detectors, available on the open market for 40¥, can detect the presence of an ultrasound field within 5 meters. Player characters can defeat motion sensors by moving very slowly through the area, one half-meter per Combat Turn, and making a successful Stealth Test against the specific sensor's rating (see the Alarms column of the Technical Security Ratings Table), or the security level for that component of the security system. An unsuccessful test triggers the alarm. Moving faster than one meter per Combat Turn raises the target number by +1 for each additional quarter of a meter moved.

Player characters may also try to spook or confound the sensor by using an ultrasound emitter/detector that analyzes the ultrasound field and transmits a series of ultrasound pulses designed to fool the sensor. This device weighs .5 kilograms.

Ultrasound Emitter/Detector
Concealability: 8 **Availability:** (Rating x 2)/72 hrs
Cost: Rating x 400¥ **Street Index:** 3

Use of the device requires an opposed test between it and the motion sensor, against either the sensor's rating or the security level for that component of the system. If the opposed test is successful, a player character using this device can move

TECHNICAL SECURITY RATINGS TABLE

Security Level	Alarms (Interior/Exterior)	Maglocks*	CCTV Exterior/Interior	CCSS
0	0	0	0	0
1	0	2–3	2–3/0	0
2	2–3/0	4–5	4–5/2–3	0
3	4–5/2–3	6–7	6–7/4–5	3–4
4	6–7/4–5	8+	8+/6–7	5–6

*For biometric maglocks, add +2 to the rating provided for the security level.

2 meters per Combat Turn. A successful Stealth Test adds dice to those available for the opposed test in that same Combat Turn. Moving slower than one-half of normal walking speed reduces the target number for the opposed test by 1 for every one-half meter slower than 2 meters that the character moves. Moving faster increases the target number by 1 for each additional quarter of a meter moved.

Pressure Mesh and Pads

Pressure mesh and pads are weight-triggered sensors usually concealed beneath the ground (pressure mesh) or flooring (pressure pads). Both are difficult to spot and easy to trip. The sensitivity of these pressure devices may differ, however, especially in areas where patrol animals or drones are used. The less sensitive the device, the easier it is to avoid tripping it.

To notice the mesh or pad, the player must make a successful Perception Test against the appropriate target number, applying the modifiers for **Wire** (p. 98). If the test is successful, the character notices the sensor. If unsuccessful, the character steps on the sensor. The player then makes a second Perception Test against the same target number, with a –2 modifier. If the test is unsuccessful, the character trips the alarm. If the test is successful, the character knows he or she has stepped on a pressure sensor and can try to remove the pressure before it exceeds the device's sensitivity. To accomplish this, the character must make a successful Reaction Test against the appropriate sensitivity level, plus the character's natural Body Rating. Apply a +2 modifier if the character is running.

The sensitivity levels of pressure devices under various circumstances and the target numbers for noticing them appear on the table below.

VIBRATION DETECTORS

Runners may use their Stealth Skill to attempt to move undetected through an area protected by a vibration detector (if they know it's there, of course). To determine success, make a Success Test each turn using the character's Stealth Skill against a target number equal to the vibration analysis software's rating. A single success means the character avoids detection for the turn. The character may only move half a meter per turn when trying to avoid detection. Characters who want to move faster (1 meter per turn) must add +3 to the target number of the Stealth Test. Characters who move faster than 1 meter per turn automatically set off vibration detectors. Because vibration detectors pick up such low movement rates, defeating this type of system is difficult.

Typical analysis algorithms are Rated from 6 to 10+.

MAGLOCKS

The following rules for defeating the parts of various types of maglocks are reprinted, with appropriate changes, from pp. 86–87, the **Neo-Anarchists' Guide to Real Life.**

Keypads

Keypad systems carry standard Ratings from 0 (available at local electronics stores) to 10 (custom-designed systems; see **Ares International Equipment Catalog**, p. 73). Unless the character knows the access code, he or she can only defeat a keypad by rewiring the internal electronics. This requires two steps: removing the casing and tampering with the circuits.

Breaking A Keypad: First, the runner must remove the keypad casing. This requires a successful Electronics (B/R) Test against a target number equal to the Barrier Rating of the casing. Usually, the Barrier Rating of the casing is equal to the rat-

PRESSURE SENSOR TABLE

	Perception Test Target Number	Sensitivity Level		
		Normal	Animals	Drones
Pressure Mesh	8	7	4	3
Pressure Pad	6	7	3	4

ing of the actual keypad system. It is possible to install a keypad system of one rating in a casing of a different rating, but the cost of the procedure is too prohibitive to make this a standard practice. All but the very high-end security systems will have a keypad and casing of equal rating.

The character must generate at least 1 success to remove the casing. Failure to generate any successes simply means that the character could not remove the case. This task requires a base time of 60 seconds, and extra successes may be used to reduce the base time as per the standard rules (see p. 56, **Shadowrun**, or p. 68, **Shadowrun, Second Edition**).

The character adds the rating of any anti-tamper alarm system attached to the casing to his or her Electronics (B/R) Test target number. Anti-tamper systems are usually rated from 1 to 4. The character must generate at least 1 success to defeat the anti-tamper system and remove the casing. Failure to generate any successes in this case sets off the alarm.

To avoid revealing too much information to the players, keep the target number for this test a secret and simply indicate success or failure as appropriate.

Once the character breaches the keypad case, he must tamper directly with the keypad circuits. Resolve the success or failure of this effort using a standard Electronics Test against a target number equal to the rating of the keypad system. The test has a base time of 60 seconds, and the character must achieve 1 success to override the alarm and may use any additional successes to reduce the base time required for the task. Failure to achieve any successes means that the computer system controlling the keypad noticed the penetration attempt and triggered a passive alert.

For both the above tests, apply the appropriate modifiers from the Build/Repair Skill Situational Modifiers table (p. 154, **Shadowrun**) or the Build/Repair Table (p. 183 of **Shadowrun, Second Edition**).

Of course, modern technology provides a device to assist in this task, called a sequencer. It is specially designed to feed the security system a series of passcode sequences based on very advanced mathematical algorithms. The device must be attached to the keypad's circuits, however, and so a character using a sequencer must still remove the keypad case. Sequencers are available in Ratings 1 through 6, and cost 500¥ multiplied by the square of the device's rating (500¥ x Rating x Rating). To defeat the keypad system using a sequencer, roll a number of dice equal to the rating of the device against a target number equal to the rating of the keypad. At the same time, roll a number of dice equal to the keypad's rating against a target number equal to the rating of the sequencer. The sequencer must achieve 1 success to penetrate the system. The base time for this test is 10 seconds, and additional successes can be used to reduce the base time. Ties have no result. If the keypad generates more successes than the sequencer, the monitoring system triggers a passive alert.

Cardreaders

Cardreaders are normally rated from 1 to 10 and can be defeated using the same method as for keypads—by tampering with the works or applying a special device. As with keypads, the "guts" of cardreaders are protected by cases that must be removed before the circuits can be tampered with. The target number for the Electronics Test used to remove the casing is equal to twice the rating of the cardreader. The base time for the task is 60 seconds. A player who succeeds in removing the casing can tamper with the circuits in the same manner as for a keypad, but must add +2 to the target number for the Electronics Test.

A device designed to defeat a cardreader is variously known as a passcard, passkey, or skeleton card. It functions in the same way as the sequencer described under keypads, except that the passcard can be inserted into the same slot used for the legitimate passcard, leaving the case in place. To determine whether or not the passcard deceives the cardreader, roll a number of dice equal to the passcard's rating against a target number equal to the cardreader's rating. The base time for this task is 10 seconds. Failure to generate any successes triggers an alarm.

A maglock passcard costs 10,000¥ times the square of the device's rating (10,000¥ x Rating x Rating).

Print Scanners

Physical print scanners, security devices that scan fingerprints or palm prints, carry Ratings of 1 to 10. Synthetic print duplications, which require a casting of the original print, carry a Rating of 1 through 8, depending on the technology used to make the phony print. The cost for the materials to manufacture a phony print is 200¥ per Rating Point. Characters must make a successful Intelligence Test against a Target Number of 3 to make an original cast accurate enough to create a usable phony print. The final product is a "sleeve" or glove-like membrane that fits over a wearer's hand.

Actual fingers or hands, removed from the owner, have a Rating of 8, but lose 1 Rating Point per hour after being removed from the original owner. Proper care of the appendage can slow the rating loss to 1 point per 3 hours. These guidelines also apply to the use of a finger or palm still attached to a dead person.

The finger or palm still attached to its living owner always works properly for a print scan.

A standard cost of 50,000¥ and Essence Rating loss of .1 are required to surgically implant retinal duplication of a Rating 1 retinal pattern. Each additional point of rating costs an additional 25,000¥, and so a Rating 4 duplication would cost 125,000¥. This cost is in addition to the standard cost of surgery. Essence cost is .1 for Rating 1 duplication, .25 for Ratings 2–4, and .5 for Ratings 5+. These Essence costs are in addition to the standard Essence costs required for surgery.

Retinal scanners are commonly available in Ratings from 3 to 9.

To use the print or retinal scanner systems, players must roll a number of dice equal to the rating of the print scanner against a target number equal to the rating of the phony print. If the scanner achieves at least 1 success in this test, it detects the fake and triggers a passive alert.

Characters can tamper with and defeat print scanners in the same way they can defeat keypads, but must add +4 to the target number (see **Keypads**, p. 100).

VOICE RECOGNITION SYSTEMS

Unlike other scanner or recognition systems, voice recognition systems have an active component. These sys-

VOICE TECHNOLOGY TABLE

Device	Rating	Cost	Availability	Street Index
Pocket Recorder (Cheap)	1	50¥	2/12 hrs	.75
Pocket Recorder (Expensive)	2	200¥	4/12 hrs	1
Portable Recorder (Basic)	3	900¥	4/36 hrs	1
Portable Recorder (Advanced)	4	1,600¥	6/72 hrs	1.5
Professional Deck (Basic)	5	25,000¥	8/7 days	1.5
Professional Deck (Advanced)	6	36,000¥	10/7 days	2

tems demand a response from an approved user's voice within a certain amount of time. If the response is not given within the time limit, the system sounds an alarm. These systems prove very difficult to tamper with physically because the security checkpoint requires only a simple microphone/speaker combination; the system's circuitry is secure in another part of the building.

Characters can only defeat voice recognition systems by "speaking" with the voice of an approved user—by using a recording, some other simulation, or the real voice.

Voice recognition systems carry Ratings of 1 to 10. The technology used to deceive these systems uses the same ratings scale. The Voice Technology Table lists the available voice reproduction technologies and their associated ratings and costs.

The voice modulator listed in the basic **Shadowrun** rules has a Rating of 1. Each additional point of rating added to this system raises the cost by 20,000¥, adds 1 to the Availability, and .1 to the Street Index. The maximum Rating available is 10.

In order to defeat a voice recognition system, the player must roll a number of dice equal to the recognition system's rating against a target number equal to the rating of the deception system. At the same time, the gamemaster rolls a number of dice equal to the deception system's rating against a target number equal to the recognition system's rating. The system that generates the most successes wins. Ties produce no results for either system, and the recognition system repeats its request for a response. The character may make another attempt to deceive the security system.

The voice mask system described in the **Street Samurai Catalog** cannot be used to deceive a voice recognition system. This system is designed to distort voices and cannot be used to replicate other voices.

CLOSED-CIRCUIT SIMSENSE (CCSS)

Closed-circuit simsense integrates several technical security devices into one cohesive unit. Drones work in concert with access controls and alarms, all under the control of a single security rigger. To simulate this, a rigger may actively operate a number of parts of the entire technical security system equal to his or her Intelligence.

Eyes-In-Walls has an Intelligence of 5, meaning that he can control five devices at once (say, two mobile drones, one fixed drone, the main entrance access-control system and the northern perimeter fence alarm). Whenever something affects any of these devices, Eyes-In-Walls can detect it (based on sensors, perception, and so on).

Devices not currently under the rigger's active control operate on "autopilot." If the autopilot detects an anomaly or an automatic alarm goes off, the security system's main computer contacts the security rigger, who shifts his or her concentration to the device in question.

Additionally, security riggers using CCSS are passively aware of all units connected to the circuit. This means that the rigger must make a Perception Test to notice any changes in the state of those units (a door opening or closing, and so on). Consult the table below for the Perception Test target number.

RIGGER PERCEPTION TEST TABLE

Situation	Perception Test Target Number
Binary state (door open or closed)	5
Attempted lock tampering, no alarm	3
Successful lock tampering	3 x tamper successes
Alarm/sensor triggered	Automatic
Device destroyed	4
Device carefully deactivated	6

MAGICAL SECURITY

The following rules apply to various measures described in **Magical Security**, pp. 34–43.

FIBER-OPTIC IMAGE LINKS

As described earlier in this book, magicians can cast spells through contiguous fiber-optic links. The optical path cannot be interrupted by any electronic system that enhances, strengthens, or rebroadcasts the signal. For this reason, the cables for these fiber-optic image links can only run 2,500 meters before image degeneration renders them useless.

Magicians casting a spell through a fiber-optic image link receive a blanket +1

modifier to the target number for the Spellcasting Test for every 500 meters (or part thereof) between the caster and target, up to 2,500 meters. The Drain Target Number rises by +2 for every 500 meters. Spirits cannot be conjured through such a link.

Changing the prism switches so that the magician can see through a different camera requires a Simple Action if done manually, and a Free Action if the magician uses some form of cybernetic hookup.

ASTRAL PATROL MODIFIER TABLE

Situation	Modifier
Patrol area is:	
Less than 2,000 m^2	+0
2,001 to 5,000 m^2	+1
5,001 to 10,000 m^2	+2
10,001 to 20,000 m^2	+4
20,001 to 40,000 m^2	+6
40,001 to 80,000 m^2	+8
Patrol area is:	
Open Terrain (open, flat countryside)	–4
Normal Terrain (typical countryside)	–2
Restricted Terrain (Light woods, suburban streets)	+0
Tight Terrain (urban mazes, dense woods)	+2
Complex Terrain (building interiors)	+4
Background count	+ Level
Intruder(s) has active magical items/spells	–1 per 2 Rating Points
Intruder(s) present astrally	–1 per 2 Magic Attribute Points*
Intruder(s) includes or are spirits	–1 per 2 Rating Points
Nature spirit has search power	–2
Additional spirits are patrolling the same area	–1 per spirit

*Unless masked

ASTRAL PATROLLING

Elementals, nature spirits, and watchers can act as guards and patrol a given area, generally 10,000 square meters per spirit. How well the spirit guards the area and how likely it is to notice an intruder depends on the area it patrols, the spirit's type and Force Rating, and the circumstances under which it is doing its job.

Beginning with a Base Target Number of 2 to detect an intruder within the patrolled area, apply the modifiers given on the Astral Patrol Modifier Table as appropriate.

Depending on the instructions given to it, a spirit that detects an intruder will either engage him or alert security forces. In some cases, depending on the sensors used in the patrolled area, the spirit may be able to trigger alarms or active deterrents such as bacterial containment mechanisms simply by manifesting.

FAT BACTERIA

Fat bacteria (FAB) devices and systems (**Magical Security**, pp. 38–40) use a newly developed, genetically engineered form of bacteria that can be introduced into an area in large enough quantities to make that area difficult to pass through in astral form. The morass of living bacteria form an organic "soup" that prohibits "fast" astral movement (see **Astral Movement**, p. 146, **SRII**) and restricts astral travelers to normal movement (Astral Quickness x 4). Additionally, the atmospheric soup adds a +4 modifier to the target number for any Astral Perception Tests made by a character in a fat bacteria-filled zone. The fat bacteria does not affect spellcasting and astral combat.

FAB Netguns

The FAB netgun entangles its astral victim, restraining him and forcing him to the ground. The victim must make an Astral Reaction Test against a Target Number 5 for the standard-sized net and a Target Number 8 for the large net. If a standard net is used against a large target, the Target Number drops to 3. To escape, the victim must achieve more than twice the number of successes generated by the attacker. Once entangled, the victim is immobile and unable to take any action. If twice the number of the attacker's successes exceeds the total number of dice the victim can roll (Astral Reaction dice plus all available dice in his or her Astral Pool), no escape is possible. In all other cases, the victim may attempt to escape from the net once per Combat Turn, applying a –1 modifier for every turn in which he remains entangled.

FAB-Ultraviolet

The detection of astral intruders using FAB-UV requires a successful Perception Test against a Base Target Number 6. A single success means that the intruder has been spotted. Increase the target number by 1 for every 50 square meters being searched; reduce the target by 1 for every two individuals involved in the search. Once an intruder is detected, any attacks against him (such as firing a BacteriTech™ Netgun) receive a +4 penalty. Reduce this penalty by 1 for each additional success achieved in the Perception Test. For example, 5 total successes eliminates the penalty (+4 penalty – 4 additional successes = 0). Six or more successes eliminates the penalty, but does not grant a bonus. If the astral intruder is aware of the searchers, he or she may make a Stealth Test against a target number equal to the searchers' Intelligence. Each success achieved in this test reduces the searchers' success total by 1.

Gamemaster Note

Fat bacteria adds a significant level of conceptual difficulty to the **Shadowrun** game, and therefore should only be used if all players and the gamemaster fully understand how it works.

GOOSE TOTEM

With geese increasingly popular as a passive security measure, more Goose shamans are becoming interested in security work. These individuals are few and far between (and difficult to work with), but because player characters may meet one or two Goose shamans, the Goose totem is described below.

Characteristics: Goose is aggressively territorial. Jumpy and easily startled, Goose is also loud and boisterous.
Favored Environment: As a wilderness totem, Goose favors open fields. As an urban totem, Goose prefers parks.
Advantages: +2 dice for detection spells; +1 die for combat spells. As a wilderness totem, +2 dice for conjuring wind spirits. As an urban totem, +2 dice for conjuring field spirits.
Disadvantages: Goose is easily startled and often honks loudly when surprised. Goose shamans suffer a +1 penalty on all Surprise Tests.

EXECUTIVE PROTECTION

The following rules apply to the physical adepts described in **Executive Protection**, pp. 54–61.

PHYSICAL ADEPT ABILITIES

Physical adepts assigned to executive protection must have astral perception. Most of them also have one or more of the following powers: Combat Sense, Improved Physical Senses, Increased Reaction, Increased Reflexes, and Pain Resistance. Some particularly dedicated adepts have one or both of the following new powers.

Extended Missile Parry
Cost: 1.5 points

Similar to the Missile Parry power (p. 34, **Grimoire II**), Extended Missile Parry allows the physical adept to extend that power to an individual he or she is protecting, up to 3 meters away from the physical adept.

Enhanced Perception
Cost: See below

Enhanced Perception gives the physical adept additional dice to apply toward Perception Tests based on the degree of ability purchased, as indicated below.

Perception Bonus	Cost/Point
Less than or equal to 1/2 racial maximum Intelligence	.25 points per +1 rating
Up to racial maximum Intelligence	.5 point per +1 rating
Up to 1.5 x racial maximum Intelligence	1 point per +1 rating

DEFEATING A SECURITY SYSTEM

Players can defeat a security system through abstract dice rolls, roleplaying, or a combination of the two.

USING DICE ROLLS

When using abstract dice rolls to bypass any component of a security system, a player makes the appropriate skill tests for his or her character. The target number for these tests is equal to twice the level of the component being bypassed, and the player must generate a number of successes equal to the OSL (see p. 98). If the player succeeds, the character has defeated the component temporarily. If the player fails, an alarm goes off. Note that the player must make the necessary skill tests every time his or her character needs to bypass components of the security system. (In other words, folks, you've got to defeat the surveillance cameras on the way in *and* on the way out.)

ROLEPLAYING

Roleplaying is the foundation of the **Shadowrun** game, and many players may find yet another series of abstract dice rolls a little dull. If they would rather roleplay their way past a security system or system component, let them. In fact, some of the devices presented in this sourcebook (such as those using "fat" bacteria) may be more easily handled through roleplaying because such high-level security devices are almost impossible to bypass using dice. The only way to defeat them is to exploit the human factor. For example, the runners may track down the engineer who designed the security system for their target site and obtain from him the access codes to parts of the system or the protocols needed to access the CCSS. Alternatively, the team might run across a disgruntled employee who can get them into the site. The possibilities are endless. With the right tidbits of information, shadowrunners might well waltz into even the most secure corporate facilities.

COMBINING DICE ROLLS AND ROLEPLAYING

Combining dice rolls and roleplaying is the most effective way to run a security system. Encourage players to make abstract dice rolls to defeat simple components or penetrate low-security sites (why bother tracking down the design engineer just to get over a wall?). When a system goes on alert or for high-security break-ins, roleplay. Above all, the process should be fun for gamemaster and players.

Keep in mind that most corporations view shadowrunners as assets to be captured rather than killed. After all, a captured shadowrunner can reveal much more to a corp than a dead one.

RIGGER COMBAT

Rigger combat occurs whenever an outside rigger attempts to control a system being run by another rigger (for example, a security rigger). Of course, the outside rigger must have access to the protected area's rigged security system or

remote frequencies. To access a rigged system, the outside rigger must follow the steps listed below:

1. Find a hardwire access point
2. Use a Dataline Tap (if necessary)
3. Defeat Encryption (if any)
4. Adjust to the system's protocols

Finding a Hardwire Access Point

Before attempting to access a rigged system or drone, the rigger must find some point in the system to which he can hardwire a dataline tap or a Remote Control Deck (RCD). This usually means that the rigger must get into the protected area of the site, as rigged systems are not usually accessible from outside. The rigger must use a RCD to take over remote-control systems and/or drones. For hardwired systems, he must use a dataline tap (see below).

Using a Dataline Tap

If the rigger wants access to non-remote systems and/or drones, he must use a dataline tap at an appropriate hardwire access point. The player rolls a number of dice equal to the rating of the dataline tap plus the character's Electronics skill, against a target number equal to twice the security level of the surveillance equipment (a component of technical security; see **Levels of Security**, p. 96). The player must achieve a number of successes equal to the Overall Security Level. If the OSL is 0, only a single success is necessary.

Defeating Encryption

Many high-security systems encrypt their remote signals and/or hardwires. If an outside rigger runs into encryption, he can use a decryption module (see **Ares Security Catalog**, p. 80). To do so, the player makes a test using a number of dice equal to the module's rating plus the rigger's Intelligence. The target number is the level of encryption (2 x security level for alarms/access control; see **Technical Security**, p. 99). The player must achieve a number of successes equal to the Overall Security Level. If the OSL is 0, only a single success is necessary. If the test is unsuccessful, the security system goes on alert.

Adjusting to System Protocols

Not all rigged systems and drones use the same protocols and frequencies. Therefore, a rigger intent on crashing a rigged security system must find out beforehand what protocols and frequencies the targeted security system uses for its remote vehicles. Once the team rigger has this knowledge, he or she can use the Rigger Protocol Emulation Module (see **Ares Security Catalog**, p. 79) installed on his or her RCD. To do so, the rigger must make a test using a number of dice equal to the RPEM's rating plus the rigger's Intelligence. The target number is twice the security level of the surveillance equipment (a component of technical security). The player must achieve a number of successes equal to the Overall Security Level. If the OSL is 0, only a single success is necessary. If the test is unsuccessful, the security system goes on alert.

Battling the Security Rigger

Once the outside rigger has completed the preceding steps, he must fight the security rigger for control of the system. Because rigged systems operate through hardware rather than software, no hardening, defensive programs or intrusion countermeasures exist. The two riggers use hardware to attack each other, causing real damage. Combat should follow the sequence described below:

1. Roll for Initiative using each opponent's rigged Initiative and dice. The rigger with the highest result (the attacker) goes first. This roll should occur as part of the normal Combat Turn sequence.

2. The attacker may choose to attack or disengage. If he chooses to attack, roll an opposed Willpower Test augmented by the attacker's Control Pool if the attacker so desires. The maximum number of dice available for this test is equal to the attacker's Willpower. The rigger who generates greater net successes on this test does (Willpower)L Stun damage to his or her opponent. Increase the Damage Level by 1 for every 2 successes generated. The losing rigger than makes a Body Test to resist the damage, augmented by his or her Control Pool if the rigger so desires. The maximum number of dice available for this test is equal to the losing rigger's Body. Note that attacking requires a Complex Action.

If the attacker decides to disengage, he or she jacks out of the system, giving control to the other rigger. Disengaging is a Free Action; re-entering the system requires a Complex Action.

3. Combat proceeds per the standard combat rules until one of the two riggers disengages or passes out. If the outside rigger manages to overcome the security rigger, the outside rigger can manipulate the rigged system and/or drones at will.

DECKING A RIGGED SYSTEM

It is possible to deck into a rigged system, though a decker will never be as efficient as a rigger at controlling the system. A decker modifies the user interface and operating system through programs, whereas a rigger has a direct interface into the rigged system at the hardware level. In essence, the rigger is "speaking" in machine code.

To deck a rigged system, the decker needs a cyberdeck outfitted with a System Control Rig Emulator (see **Ares Security Catalog**, p. 78) and the software to run it. Combat between a decker and a rigger in a rigged system is the same as rigger vs. rigger combat, except for the following restrictions applied to the decker:

- No Matrix programs can be used.
- The decker receives a +2 modifier to all tests.
- The decker's Initiative is at –2, and he or she gains no dice from the deck's Response Increase.
- The decker has a Control Pool equal to one-half (round up) the rating of the emulation utility.
- The decker takes damage as if from black IC. See p. 171, **SRII**.

SECURITY PERSONNEL

This section contains brief descriptions, including Attribute and Skill Ratings, for non-player characters assigned to a typical corporate security department. The quotes and commentaries are provided to help gamemasters add life and color to their roleplaying of these NPCs by providing a "feel" for the characters. In most cases, gear has been listed as "as appropriate" to provide gamemasters with wide leeway when outfitting these NPCs. For more information on using Contacts, see p. 200, **SRII.**

EXECUTIVE PROTECTION ADEPT

"Protecting you allows me to use all the tools of my experience and training: my stealth, my quickness, my magical senses, and my honor. Could any job be more noble?"

QUOTES

"I'll go first and survey the area. Follow me only after I have given the OK."

"This doesn't feel right—I can't put my finger on it but I'm uncomfortable ... "

COMMENTARY

The executive protection adept is a highly specialized member of one of the most elite security details—executive protection. The protection adept acts as the execsec team's advance man, using superior perception and stealth to simultaneously monitor activity in the mundane world and astral space. The adept is quick to spot trouble and quick to stop it, enabling the rest of the team to focus on protecting the client.

Attributes

Body: 5
Quickness: 5
Strength: 4
Charisma: 3
Intelligence: 4
Willpower: 5
Essence: 6
Magic: 6
Reaction: 4 (5)

Skills

Biotech: 2
Conjuring: 3
Etiquette (Corporate): 2
Firearms: 4
Stealth: 4
Unarmed Combat: 6

Initiative: 4 (5) + 1D6 (+ 2D6)
Professional Rating: 3–4

Physical Adept Talents

Astral Perception
Enhanced Perception: 2
Improved Physical Senses
- Flare Compensation
- Low-Light Vision
- Vision Magnification: 2

Increased Reaction: 1
Increased Reflexes: 1

Gear

As appropriate

EXECUTIVE PROTECTION DECKER

"I like to ride the Matrix to find information for my client. But finding data is only half of the fun—planting the wrong information for *you* to find is the other. Remember that the next time you think you have something hot, *omae*."

QUOTES

"Yes sir, all the arrangements have been made. You will not be bothered."

"The information you requested has been obtained and the information you wanted erased has been removed."

COMMENTARY

The executive protection decker rides the Matrix, monitoring everything from the client's reservations to black information. The protection decker keeps tabs on the client's contacts, private and public dealings, business concerns, itineraries, and public access. The decker may also plant misinformation and monitor the police, rescue, and air traffic communications frequencies.

Attributes

Body: 3
Quickness: 5
Strength: 2
Charisma: 3
Intelligence 6 (7)
Willpower: 5
Essence: 1
Reaction: 4 (8)*

Skills

Biotech: 2
Computer: 6
Computer Theory: 4
Computer (B/R): 4
Electronics: 4
Etiquette (Corporate): 3
Firearms: 2

Initiative: 4 (8)* + 1D6 (+ 3D6)*
Professional Rating: 3–4

Cyberware

Cranial Cyberdeck
- MPCP: 8
- Persona: 8
- Hardening: 4
- Memory
  - Active: 100 Mp
  - Storage: 500 Mp
- Input/Output: 80
- Response Increase: 2

Datajack: 4
Encephalon: 2
Headware Memory: 100 Mp
I/O SPU: 2

Gear

As appropriate

*Applies only when decking.

EXECUTIVE PROTECTION MAGE

"No, I'm not a combat mage, and I've never wanted to be one. My job is to keep people *alive*, not kill them. I find it much nobler to use my magic to keep someone safe than to use it to simply destroy enemies. Of course, if I have to, I won't hesitate to toast anyone."

QUOTES

"One mana blast spell will flush those boys into the open."
"Sit still, a protection ward ain't like going to the barber."

COMMENTARY

The executive protection mage is not an ordinary mage. She must juggle protection, detection and offensive spells with equal ability and quickness. And she must be ready at all times to provide immediate magical medical aid. These abilities and training make the protection mage a vital member of any exec-sec team.

Attributes

Body: 3
Quickness: 5
Strength: 3
Charisma: 3
Intelligence: 5
Willpower: 6
Essence: 5.8
Magic: 5
Reaction: 5

Skills

Biotech: 4
Conjuring: 3
Etiquette (Corporate): 2
Firearms: 3
Magical Theory: 4
Sorcery: 6
Unarmed Combat: 2

Initiative: 5 + 1D6
Professional Rating: 3–4

Cyberware

Cybereyes with Electronic Magnification 3, Flare Compensation and Low-Light

Spells

Blast Barrier: 3
Bullet Barrier: 3
Combat Sense: 3
Detect Enemies (Extended): 3
Stabilize: 3
Spell Barrier: 3
Treat: 3

Gear

As appropriate

EXECUTIVE PROTECTION RIGGER

"You can call me a glorified chauffeur if you want, but when some go-gangers start hounding your pretty little simsense star and you want her out of there fast, who are you going to trust to get her home safe—a chauffeur? I didn't think so."

QUOTES

"Two cars will pull up—a black one and a red one. Get into the back seat of the red one and hang on tight. You'll be home safe and sound before you know it."

"The helipad is clear, checked it out myself. We'll be taking off any second."

COMMENTARY

The executive protection rigger coordinates all the transportation needs of the client and the execsec team. He is responsible for all armored protection vehicles (well armed, of course), drones, air transport, and water transport. The execsec rigger prides himself on getting everyone home safe and sound and providing a smooth ride as he does so. Never call an executive protection rigger a chauffeur. They really don't like that.

Attributes
Body: 3
Quickness: 6
Strength: 3
Charisma: 3
Intelligence: 5
Willpower: 5
Essence: 1.25
Reaction: 5 (9)*

Skills
Biotech: 2
Car: 5
Computer: 3
Electronics: 3
Etiquette (Corporate): 2
Firearms: 2
Gunnery: 4
Vectored Thrust Vehicles: 4

Initiative: 5 (9)* + 1D6 (+ 3D6)*
Professional Rating: 3–4

Cyberware
Cybereyes with Flare Compensation, Low-Light and Thermographic
Datajack (Lvl 4)
Radio
Orientation System (with collection of softmaps)
Vehicle Control Rig (2)

Gear
As appropriate

*Applies only when rigging.

EXECUTIVE PROTECTION SPECIALIST

"Hey, it ain't my place to slug it out with some drek-for-brains shadowrunner. My job is to make sure no one hurts you. If that means I take a bullet that has your name on it, that's the breaks of the game."

QUOTES

"Get Down!"
"Move! Move! Move!"
"Duck!"

COMMENTARY

The executive protection specialist is the client's personal shield, the basic unit of every execsec team. He is trained to instinctively protect the client's life, even if that means sacrificing his own. The execsec specialist is much more than a bodyguard—he is a highly trained and dedicated professional who is noticeably more intelligent and less macho than the average muscleman.

Attributes
Body: 6 (9)
Quickness: 6
Strength: 5
Charisma: 3
Intelligence: 5
Willpower: 5
Essence: 0.6
Reaction: 5 (9)

Skills
Biotech: 2
Car: 4
Etiquette (Corporate): 3
Stealth: 2
Unarmed Combat: 6

Initiative: 5 (9) + 1D6 (+ 3D6)
Body Index: .6
Professional Rating: 3–4

Bioware
Damage Compensator (3)

Cyberware
Cybereyes with Electronic Magnification 3, Flare Compensation, Low-Light, Rangefinder, and Thermographic
Dermal Plating: 3
Smartlink II
Wired Reflexes: 2

Gear
As appropriate

INVESTIGATOR

"The corporation views all of its employees as assets. It is my job to make sure none of those assets become stray debts. Are you an asset or a debt? Please think before you answer."

QUOTES

"You can trust me, I work for the corporation too."

"Again, exactly where were you last Tuesday? And this time, please try and be a bit more specific."

COMMENTARY

The investigator is trained in all aspects of espionage, interview and interrogation techniques, and data gathering. He handles all security related investigations dealing with personnel. Beware when you answer one of his questions, because it's a good bet he not only knows what you are going to say, but the truth as well.

Attributes

Body: 3
Quickness: 4
Strength: 3
Charisma: 5
Intelligence: 5
Willpower: 6
Essence: 3.8
Reaction: 4

Skills

Etiquette (Corporate): 4
Etiquette (Street): 3
Firearms: 3
Interrogation: 5
Negotiation: 3
Psychology: 2
Sociology: 2

Initiative: 4 + 1D6
Professional Rating: 2-3

Cyberware

Datajack
Retinal Modification: Display Link
Headware Memory: 100 Mp
Video Link with Internal Transmitter

Gear

As appropriate

MAGICAL SECURITY SPECIALIST

"I'm not some magical hack. I specialize in wards. Each is a work of art, a masterpiece of both defense and offense, the ultimate protection. You do not agree? Then go ahead—open that door. It has been good knowing you."

QUOTES

"I don't do _____ (conjuring, astral monitoring, wards, executive protection, and so on)."

"I was hired to protect this and protect it I will, even if it means calling forth every spirit in astral space!"

COMMENTARY

Magical security specialists are magical adepts assigned to magical security—and usually they are the most egocentric of all security personnel. These mages specialize in specific areas of magic, most commonly wards, astral monitoring, or conjuring. Most magical security specialists believe that they and their constructs are invincible (many are) and assume the temperamental attitudes that many equate with simsense stars. Most security teams endure such attitudes because good magical security specialists are worth their weight in gold.

Attributes
- Body: 3
- Quickness: 4
- Strength: 3
- Charisma: 3
- Intelligence: 5
- Willpower: 4
- Essence: 6
- Magic: 6
- Reaction: 4 (5)

Skills
- Etiquette (Corporate): 2
- Firearms: 3 (4)
- Interrogation: 2
- Unarmed Combat: 4 (5)

Special Skill
- Security Systems: 2

Initiative: 4 (5) + 1D6 (+ 2D6)
Professional Rating: 2–3

Physical Adept Talents
- Astral Perception
- Improved Unarmed Combat (1)
- Improved Firearms (1)
- Improved Physical Senses
  - Flare Compensation
  - Low-Light Vision
- Increased Reaction (1)
- Increased Reflexes (1)

Gear
- As appropriate

MAGICAL SECURITY ENGINEER

"Research is the key to effective magical security. You can throw all the spells you want, but if you don't understand where they come from and where they go, you'll never stop one. Sure, sometimes I wish I could fire off a fireball spell. But devising a way to stop one is an even more useful feat."

QUOTES

"This worked on paper. Let's see those charts again."
"Hey, control that spirit. This is a laboratory, not a zoo!"

COMMENTARY

A mundane and proud of it, the magical security engineer uses magical theory, the physical sciences, and trial and error to help bolster the client's magical defenses. Often ridiculed by those with magical powers, these scientists work to develop both technical aids for the mage such as fiber-optic viewing systems and magical defenses such as bacterial containment grids.

Attributes
Body: 2
Quickness: 3
Strength: 2
Charisma: 2
Intelligence: 6
Willpower: 4
Essence: 4.7
Reaction: 4

Skills
Electronics (Security Systems): 5
Electronics (Security Systems) (B/R): 6
Etiquette (Corporate): 1
Firearms: 1
Magical Theory: 6
Physical Science: 3

Special Skills
Security System Design: 5

Initiative: 4 + 1D6
Professional Rating: 1–2

Cyberware
Datajack
Headware Memory: 100 Mp
Retinal Modification: Display Link

Gear
As appropriate

PERSONNEL SECURITY SPECIALIST

"I don't spy. I look after the best interests of the corporation. And the best interests of the corporation are served by maintaining a happy and loyal work force. So you see, my job is to ensure that you remain happy and loyal."

QUOTES

"According to our records, Mr. Brown has been to the doctor five times in the past two weeks. Maybe we should talk to him."

"Miss Jenkins has been spending a lot of time with Mr. Springer in Data Processing. Should I continue to watch them?"

COMMENTARY

Personnel security specialists form the backbone of the corporate persec division. These professionals perform the day-to-day operations of personnel security. Their duties include conducting background checks of job candidates, employees, and business associates of the corporation; monitoring employee work habits; and providing security clearances to employees when necessary.

Attributes

Body: 4
Quickness: 4
Strength: 3
Charisma: 4
Intelligence: 4
Willpower: 4
Essence: 5.5
Reaction: 4

Initiative: 4 + 1D6
Professional Rating: 1–3

Skills

Etiquette (Corporate): 4
Firearms: 2
Interrogation: 3
Negotiation: 1
Psychology: 1
Sociology: 1
Unarmed Combat: 2

Special Skills

Security Systems: 2

Cyberware

Smartlink

Gear

As appropriate

SECURITY COMMANDER

"You start trouble and I'm the face you'll be seeing. Nobody handed this position to me—I've earned it. I've been in the trenches when the bullets and spells start flying, and I've been stopping low-life runners, go-gangers, and corp extraction teams since you were born. I know how they think and I know how to defeat them."

QUOTES

"Is everyone in position? Do not fire until I give the signal."

"What do you mean Sector 7 hasn't checked in? Send a drone out there with two security guards—now!"

"I don't wanna hear your lame excuses. When I send you out to tail some slag I want you to stick to him like a pair of cheap underwear!"

COMMENTARY

The security commander is no office drone. She has served on the front lines and survived, and she has the scars to prove it. Toughened by years on the corporate security detail, experience has taught her lessons that no book or instructor could ever teach. She commands all of the security forces on patrol like a general commanding combat troops. In fact, she sees security as nothing short of war, and she'll do anything to win.

Attributes

Body: 4
Quickness: 4
Strength: 4
Charisma: 5
Intelligence: 5
Willpower: 6
Essence: 4.25
Reaction: 4

Skills

Etiquette (Corporate): 4
Firearms: 4
Leadership: 5
Negotiation: 2
Military Theory: 2
Unarmed Combat: 4

Special Skills

Security Systems: 4

Initiative: 4 + 1D6
Professional Rating: 3–4

Cyberware

Cybereyes with Flare Compensation, Low-Light, and Thermographic
Radio with Commlink II
Smartlink

Gear

As appropriate

SECURITY DECKER

"Chummer, once you bust the Matrix and enter one of my nodes you're all mine. I don't wait for clearances, and I don't play games. I'll hunt you down like the smelly piece of rancid meat you are. Your hot new codes and countermeasures, your baddest programs—I'll strip them all from you. I'll chew you up and spit you out. You frag with me and you're not fragging with some pathetic little byteboy—you're fragging with the best."

QUOTES

"Meet my friend Mr. Black Ice."

"We got an anomaly over in research, a dummy terminal was just turned on. I'm checking it out."

COMMENTARY

Roaming the nodes of corporate matrices, the security decker is the meat behind all the IC and other matrix defenses. Like a shark in still water she patrols her corporation's matrix, waiting for any sign of intruders. Wander into one of her nodes and WHAM—you're fish food. The security decker watches for break-ins and internal anomalies and monitors internal matrix usage.

Attributes
Body: 3
Quickness: 4
Strength: 2
Charisma: 2
Intelligence: 5
Willpower: 4
Essence: 5.2
Reaction: 4

Skills
Computer: 5
Computer Theory: 4
Computer (B/R): 2
Etiquette (Corporate): 2
Firearms: 1

Special Skills
Security Systems: 3

Initiative: 4 + 1D6
Professional Rating: 2–3

Cyberware
Datajack
Headware Memory: 50 Mp
Retinal Modification: Display Link

Gear
Appropriate cyberdeck and programs (MPCP equal to twice Professional Rating + 1).

SECURITY EXECUTIVE

"Security may be the most important function at this corporation. Without it we are an open book, easily available to the lowliest gutterpunk. I work very hard to make sure the Board never forgets that fact. And every time our employees walk through a safety check, they know they are protected and secure. Our job is to stay on top of the action, and I'm here to make sure we do it."

QUOTES

"Research tells me they made another breakthrough on Project T-771. Double the security and update the magical barriers on Warehouse 9."

"You may think we are spending too much nuyen, but until we get the new security rigger up to speed, we need to set up security checkpoints in every corridor and buy more guard animals."

COMMENTARY

The security executive is in charge of the of the corporate security division. Unlike most of the other members of the security division, he has never been on the front lines. His experience and expertise lie in organization, budgets and boards of directors. He makes sure that the security division has all the resources it needs to do its job. His head is the first to go when a serious security breach occurs.

Attributes
Body: 3
Quickness: 3
Strength: 3
Charisma: 5
Intelligence: 5
Willpower: 5
Essence: 4.2
Reaction: 4

Skills
Etiquette (Corporate): 5
Firearms: 1
Interrogation: 4
Negotiation: 4

Special Skills
Security Systems: 1

Initiative: 4 + 1D6
Professional Rating: 2–3

Cyberware
Datajack
Headware Memory: 100 MP
Retinal Modification: Display Link
Smartlink

Gear
As appropriate

SECURITY GUARD

"I know the score, I'm the first on the food chain. I'm on the firing line—the "weakest link" from a runner's point of view. But I'm the one who gives the employees a sense of security and protection. And if I do my job right, I'm the one who gives any low-lifer second thoughts about trying to break in."

QUOTES

"I'm sorry, but I can't let you pass unless your retinal scan and finger and voice prints match the information on your security pass."

"Sign here."

"Sorry for the delay."

COMMENTARY

Security guards are the most numerous and visible members of the corporate physec team. Security guards man checkpoints and routinely perform foot patrols of perimeters and designated areas. Generally these personnel setup in low-threat or even non-threat locations and are assigned very specific duties. Security guards are primarily entry-level workers who receive minimal training from the security company or the corporation that employs them.

Attributes

Body: 4
Quickness: 3
Strength: 3
Charisma: 2
Intelligence 2
Willpower: 2
Essence: 6
Reaction: 2

Skills

Etiquette (Corporate): 2
Firearms: 3
Interrogation: 2
Unarmed Combat: 3

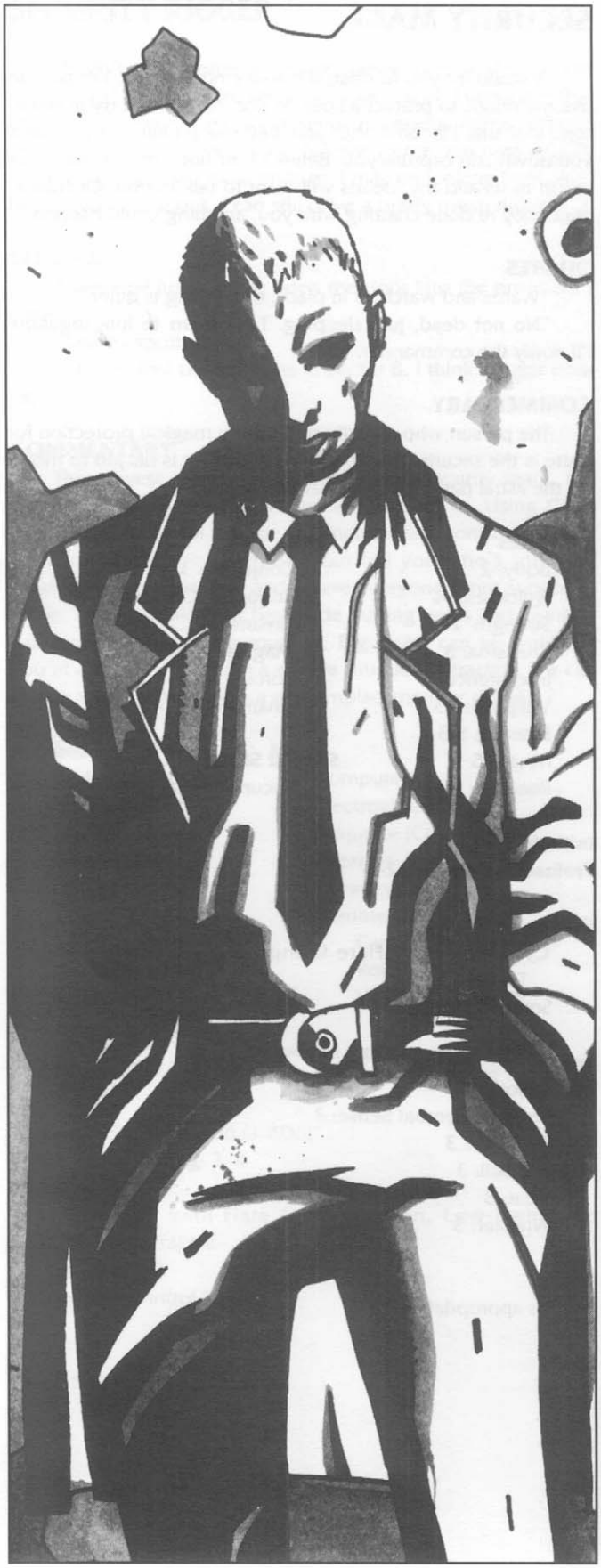
Special Skills

Security Systems: 1

Initiative: 2 + 1D6
Professional Rating: 1–2

Gear

As appropriate



SECURITY MAGE

"I could fry you to dust, but that's not my job. I'm paid to use my magic to protect a specific site. Now if you try to penetrate that site, I'll come after you. Oh, I won't kill you, just slow you down and capture you. Believe it or not, you actually have worth to us and my friends will want to talk to you. Of course, once they're done chatting with you, anything could happen."

QUOTES

"Wards and watchers in place, everything is quiet."

"No not dead, just sleeping. Take them to interrogation, I'll notify the commander."

COMMENTARY

The person who actually sets up the magical protection for a site is the security mage. While on duty, it is his job to monitor the astral paths and magical defenses.

Attributes

Body: 2
Quickness: 4
Strength: 2
Charisma: 3
Intelligence: 5
Willpower: 5
Essence: 5.3
Magic: 5
Reaction: 4

Skills

Conjuring: 3
Etiquette (Corporate): 3
Firearms: 2
Magical Theory: 4
Sorcery: 6
Unarmed Combat: 2

Special Skills

Security Systems: 3

Initiative: 4 + 1D6
Professional Rating: 2–3

Cyberware

Cybereyes with Flare Compensation, Low-Light, and Thermographic
Smartlink

Spells

Chaos: 3
Personal Combat Sense: 3
Stun Bolt: 3
Stunball: 3
Treat: 3
Wrecker: 3

Gear

As appropriate

SECURITY OFFICER

"My job is simple—I protect Warehouse 72-C. I don't ask what's in it and they don't tell me. But you trip a security wire, your hoop is mine. I don't care who your father is and I don't care what you tell him in the morning. Here I'm in charge and if you want to live to see your father, you'll get your sorry hoop out of my sight."

QUOTES

"OK everyone, this is how we're going to set up. It's a little different, but I think you'll like it."

"Call the commander for backup! We're gonna have a fire fight tonight!"

COMMENTARY

The security officer is responsible for the complete security of a single location or area. He answers only to the security commander. These well-trained individuals have usually worked their ways up through the ranks and usually form the next generation of security commanders. With complete control over his area, the security officer must juggle the security responsibilities assigned to him and traverse the often treacherous terrain of office politics of the modern megacorporation.

Attributes
Body: 4
Quickness: 4
Strength: 4
Charisma: 3
Intelligence: 3
Willpower: 3
Essence: 4.75
Reaction: 3

Skills
Etiquette (Corporate): 3
Firearms: 5
Interrogation: 3
Leadership: 2
Unarmed Combat: 4

Special Skills
Security Systems: 3

Initiative: 3 + 1D6
Professional Rating: 3–4

Cyberware
Radio
Smartlink

Gear
As appropriate

SECURITY RIGGER

"It ain't just drones anymore, *omae*—that's history. I'm the "driver" of the entire security system now. Everything that can be tied into my rig is: cameras, maglocks, lights, infrared beams, trip wires—everything. So every time you pass a CCTV camera, take a good look, because I may be looking back. And in case you're curious, I can still drive a pretty mean drone."

QUOTES

"Someone just tried to open the door into the president's suite."

"Drones secured."

"We just lost two cameras in Sector B. I think we got trouble."

COMMENTARY

The newest member of the corporate security team, the security rigger is more than just a drone driver. Using CCSS and a system control rig, she can monitor and control an entire technical security system. She can tell you who's touching what, where everyone is, and where everyone is not supposed to be. This improvement has made cutting wires and painting cameras just that much tougher. Big Sister can be watching you at any time, and with a simple muscle contraction she can fill you with hot lead from a gun emplacement or drone.

Attributes
Body: 4
Quickness: 6
Strength: 3
Charisma: 3
Intelligence: 5
Willpower: 6
Essence: 0.55
Reaction: 5 (11)*

Skills
Computer: 3
Electronics: 3
Etiquette (Corporate): 1
Firearms: 3
Gunnery: 3
Remote Ops
Cars: 5
Rotorcraft: 5
Vectored Thrust: 5

Special Skills
Security Systems: 5

Initiative: 5 (11)* + 1D6 (+ 4D6)*
Professional Rating: 2–4
Cyberware
Cybereyes with Flare Compensation, Low-Light, and Thermographic
Datajack (4)
Vehicle Control Rig (3)

Gear
As appropriate

SECURITY SPECIALIST: ANIMAL HANDLER

"This is not some kind of pet shop. These animals are trained to kill, and they gotta try hard to remember who the good guys are and who the bad guys are."

QUOTES

"Keep those hell hounds under control!"
"The cockatrice is loose! Be very careful!"
"The dogs are on the scent. Call the commander."

COMMENTARY

Animal handlers are security specialists who have been specially trained to handle, control, and command security animals. They train paranormal and mundane security animals and some have even worked with the rare cybered animals.

Attributes
Body: 4
Quickness: 4
Strength: 3
Charisma: 5
Intelligence: 3
Willpower: 4
Essence: 5.3
Reaction: 3

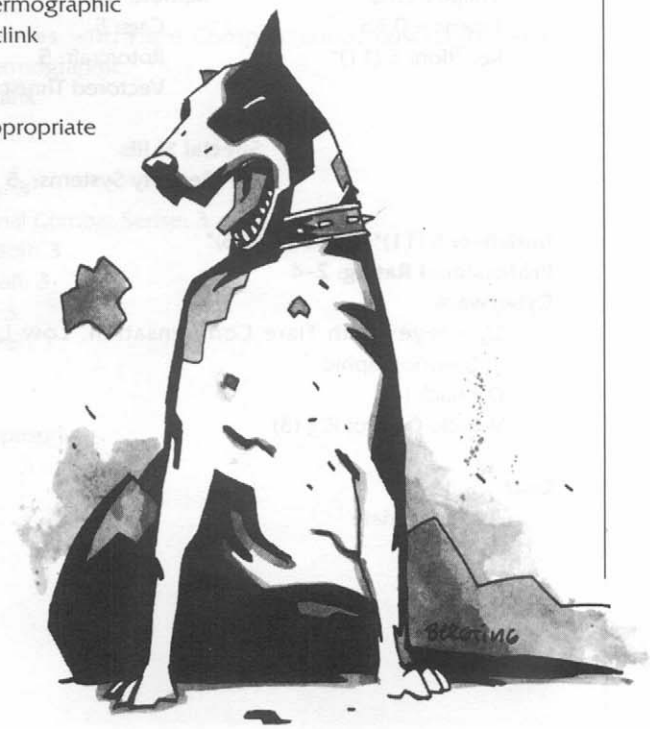
Skills
Biotech: 2
Etiquette (Corporate): 2
Firearms: 3
Unarmed Combat: 3

Special Skills
Animal Handling: 5
Security Systems: 2

Initiative: 3 + 1D6
Professional Rating: 2–4

Cyberware
Cybereyes with Flare Compensation, Low-Light, and Thermographic
Smartlink

Gear
As appropriate



SECURITY SPECIALIST: FAST RESPONSE OFFICER

"I love my job. I'm the one they call when the drek hits the fan. Me and my team are there before you can blink, with our munitions in hand and itchy trigger fingers. Our job is to bring down the scum that intruded and I'm glad to say we usually do."

QUOTES

"They're holed up in Warehouse 12. Surround the building and set up in Alpha Blue formation."

"They have too much firepower to be a regular team of runners. These guys are professionals."

COMMENTARY

The fast response officer is highly trained in Special Weapons and Tactics (SWAT). Usually only the most powerful megacorporations can afford to maintain and outfit teams of such personnel. Fast response officers are trained to deploy and engage intruders at a moment's notice, and they don't take prisoners. Outfitted with state-of-the-art weapons and equipment, the face of the fast response officer is generally the last face most intruders see.

Attributes
Body: 5
Quickness: 5
Strength: 5
Charisma: 2
Intelligence: 5
Willpower: 4
Essence: 2.8
Reaction: 5 (7)

Skills
Armed Combat: 4
Biotech: 4
Demolitions: 2
Etiquette (Corporate): 2
Firearms: 6
Gunnery: 4
Unarmed Combat: 5

Special Skills
Security Systems: 1

Initiative: 5 (7) + 1D6 (+ 2D6)
Professional Rating: 3–4

Cyberware
Cybereyes with Flare Compensation, Low-Light, and Thermographic
Dermal Armor: 1
Smartlink
Wired Reflexes: 1

Gear
As appropriate

FREELANCE EXECUTIVE PROTECTION SPECIALIST (TROLL)

"You say you want a what? A bodyguard? Well that ain't what I do, omae. I'm an executive protection specialist—a professional. You hire me to keep your suit alive and that's what I'll do. When the drek hits the fan I'll make sure she gets out alive and—if I'm doing my job right, and I always do—unscathed.

"Takes a lot to bring me down. That's what I got goin' for me. When trouble comes, all the client's gotta do is just get behind me, do exactly what I do and what I say and she will live to a ripe old age. We got a deal? Good."

Commentary: The freelance executive protection specialist is a rarity in the Sixth World—someone willing to sacrifice his life for yours. This troll is not a low-life gang member or thug, but a highly trained, dedicated professional who has tailored his body and mind to perform his duty—keeping his clients alive and well. Many executive protection specialists are said to become closer to their clients than even their family members. And many are so well paid that they become worth more than their clients.

Attributes
- Body: 9 (10)
- Quickness: 2
- Strength: 7
- Charisma: 1
- Intelligence: 2
- Willpower: 2
- Essence: 1.9
- Reaction: 2 (6)

Initiative: 2 (6) + 1D6 (+ 3 D6)

Dice Pools
- Combat: 3

Cyberware
- Optical Vision Magnification: 3
- Retinal Modification: Flare Compensation
- Skillsofts
  - Biotech: 3
  - (4) Etiquette skillsofts at 3 points each
- Skillwire: 3
- Smartlink
- Wired Reflexes: 2

Contacts
- Choose (2) Contacts

Gear
- Ares Predator II (with 4 Spare Clips)
- Concealed Holster
- DocWagon™ Contract (Gold)
- Fineblade Long Blade
- Form-Fitted Body Armor: 3
- Medkit
- Pocket Secretary
- Portable Phone (Earplug with Booster)
- Tres Chic Clothing

Starting Cash: 1,255¥ + (3D6 x 1,000¥)

Skills
- Armed Combat: 3
- Firearms: 6
- Gunnery: 3
- Negotiation: 3
- Unarmed Combat: 5

Note: The troll freelance executive protection specialist has natural thermographic vision, +1 Reach for armed/unarmed combat, and natural dermal armor (1). Choose an allergy if using that option (see p. 46, **SRII**).

FREELANCE MAGICAL SECURITY CONSULTANT

"Guns, IC, drones and the like can stop the meat from penetrating your security easily enough, but all it takes is one astral intruder and all your secrets are the simsense of the week. I know—I've seen it happen. Hell, I've been that astral intruder.

"But now I work for the good guys. Some employers get a little nervous when they learn about my past, but it's precisely what makes me such a valuable consultant—I know firsthand how astral intruders work, so I know how to protect against them.

"Of course, I'm not in this business to help the world. I work for corps because it pays better than being on the other side. So if you want my services you'll have to pay up, *omae*. It's simple—if you wanna see some magic, just show me some money."

Commentary: Magical security is a must, and the freelance magical security consultant can provide all that you need. He can devise ingenious traps that simply stop or detain intruders, or cook up something with a bit more bite for these truly unwelcome guests. He is an expert at designing and implementing magical security systems, and he bills his clients for everything he does. Magical security consultants can become quite wealthy, as most clients quickly learn not to quibble over a few million nuyen with individuals who know their magical security arrangements inside and out.

Attributes
- Body: 2
- Quickness: 5
- Strength: 2
- Charisma: 4
- Intelligence: 5
- Willpower: 6
- Essence: 6
- Magic: 6
- Reaction: 5

Initiative: 5 + 1D6

Dice Pools
- Combat: 8
- Magic: 6

Cyberware
- None

Contacts
- Choose (2) Contacts

Gear
- Fetishes
  - (1) Combat
  - (1) Detection
  - (2) Illusion
  - (1) Manipulation
- Narcoject Pistol
- Pocket Secretary
- Secure Long Coat

Spells
- **Combat:**
  - Stun Bolt: 3
  - Stunball: 3
- **Detection:**
  - Analyze Truth: 2
  - Mind Probe: 2
- **Illusion:**
  - Chaos: 3
- **Manipulation:**
  - Influence: 2

Skills
- Conjuring: 4
- Electronics (Security Systems): 4
- Electronics (Security Systems) (B/R): 3
- Etiquette (Corporate): 3
- Firearms: 3
- Magical Theory: 4
- Sorcery: 6

Starting Cash: 3D6 x 1,000¥

FREELANCE SECURITY RIGGER

"I don't care how many fancy drones you have scurrying around your buildings, how many maglocks you have hanging from the doors, or how much your fancy new CCSS control system cost. Any CCSS-based security system is only as good as the slot who's running it. If you hire a second-rate security rigger or try to get off cheap by having one of your vehicle riggers run the show, you're going to have second-rate security, no matter how much nuyen you've sunk into your hardware.

"You hire me, you hire the best. Give me three minutes at your system rig and I'll tell you who's where, what doors are open, which locks are set incorrectly, how many light bulbs have burned out—drek, I'll tell you if you're out of toilet paper.

"Remember, no cycle hopper or flyboy can give you the level of protection I can. When I plug into your system I AM the building, and not even a roach is gonna crawl across your desk without me knowing it."

Commentary: The newest of the new in the protection field, the freelance security rigger is the oddball of the security business. Willing to sit for hours jacked into a building security system, the security rigger can monitor everything from drones to maglocks to provide a level of surveillance and response that seemed impossible even a few years ago. Although the massive egos of most security riggers can make them difficult to work with, they are a vital part of any security system. Security riggers provide only their decks, training, and innate abilities—all other components of a rigged security system must be provided by the client.

Attributes
- Body: 3
- Quickness: 6
- Strength: 2
- Charisma: 3
- Intelligence: 5
- Willpower: 5
- Essence: 1.05
- Reaction: 5

Skills
- Car: 5
- Computer: 4
- Electronics: 4
- Electronics (B/R): 5
- Etiquette (Corp): 3
- Firearms: 4
- Gunnery: 4
- Rotorcraft: 5
- Vectored Thrust: 5

Initiative: 5 (9)* + 1D6 (3D6)*

Dice Pools
- Combat: 8
- Control: 5 (9)

Cyberware
- Cybereyes with Flare Compensation, Flare Protection and Thermographic
- Datajack
- Radio with Commlink II
- Smartlink
- Vehicle Control Rig: 2

Contacts
- Choose (2) Contacts

Gear
- Ares Viper Slivergun (with 2 Spare Clips and 90 Flechette Rounds)
- Camo Jacket
- Dataline Tap: 6
- DocWagon™ Contract (Platinum)
- Form-Fitted Body Armor: 3
- Remote Control Deck
  - (4) Slave Ports
  - ECM (Security I)/ECCM (Security I)**
  - Internal Rigger Decryption Module: 6
  - Internal Rigger Protocol Emulation Module: 6

Starting Cash: 1,130¥ + (3D6 x 1,000¥)

*Applies only when rigged

See p. 127, the **Rigger Black Book (disregard if that book is unavailable).

SECURITY SYSTEM DESIGN ENGINEER (DWARF)

"You can spend millions of nuyen on the best security technology available, but your system won't keep out a green newbie if it's not well designed. Everything has to work together. Trust me—if your system has any holes in it, the bad guys will find them.

"Remember, when some runner tries to penetrate your system, he's not just going up against your security personnel and your system. He's really going up against the individual who designed the system. That's why skimping on a system design engineer doesn't pay in the long run. You can hire the best personnel in the world and outfit them with state-of-the-art technology, but if the system is flawed they will be powerless to stop a determined intruder.

"Just be careful and take your time making your decision. Remember, your designer is going to know all the ins and outs of your system, as well as what it's protecting. So you have to be able to trust implicitly anyone you hire.

"So there you have it. You can pay now, or you can pay later—it's your choice."

Commentary: A security system is like a puzzle, comprising components that must fit together seamlessly. The security system designer is the master of the puzzle, assembling the various and seemingly incongruous pieces and making them work. He is always testing and rechecking, repairing and redesigning the system to keep it operating at peak efficiency. System designers are more than just guns for hire—they are the hearts and and souls of the security systems they design and often become targeted for kidnapping, extortion, bribery, and extractions by the very forces they protect their employers from.

Attributes
- Body: 2
- Quickness: 2
- Strength: 3
- Charisma: 3
- Intelligence: 6
- Willpower: 4
- Essence: 3.2
- Reaction: 4

Initiative: 4 + 1D6

Dice Pools
- Combat: 6
- Control: 4

Skills
- Computer: 5
- Computer (B/R): 6
- Electronics: 5
- Electronics (B/R): 6
- Etiquette (Corp): 2

Special Skills
- Security System Design: 6

Cyberware
- Datajack
- Headware Memory: 50 Mp
- Retinal Modification: Display Link
- Vehicle Control Rig (1)

Contacts
- Choose (2) Contacts

Gear
- Computer Tool Kit
- Dataline Tap (1)
- Electronics Tool Kit
- External Rigger Decryption Module (1)
- External Rigger Protocol Emulation Module (1)
- Pocket Computer with 100 Mp Memory
- Remote Control Deck with two Slave Ports
- Wrist Phone with Flip-Up Screen

Starting Cash: 155¥ + (3D6 x 1,000¥)

Note: The dwarf security system design engineer has natural thermographic vision, and +2 Body for disease resistance only. Choose an allergy if using that option.

INDEX

F

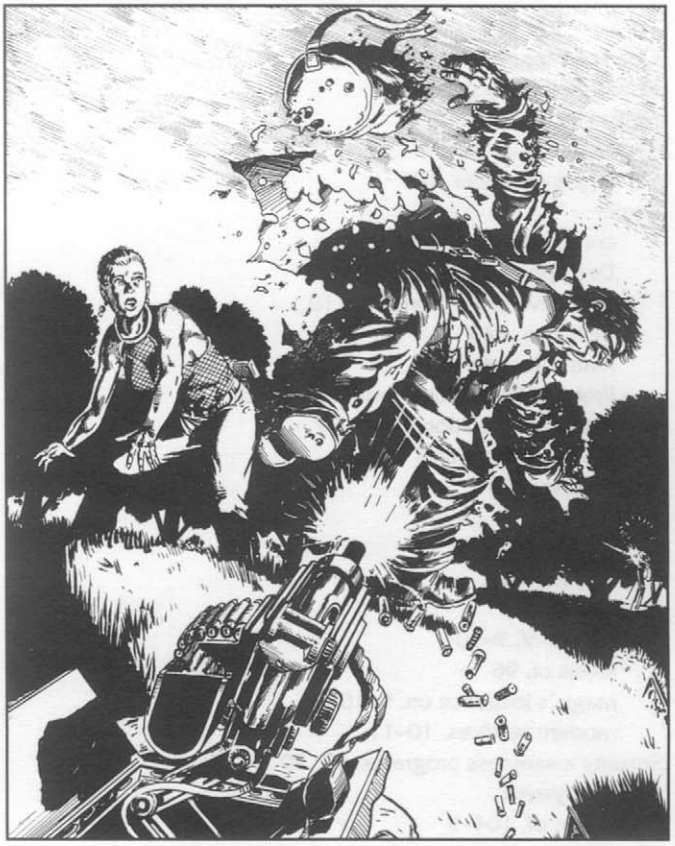
G

H–I

K–L

M

N–P



Q–R

S

T

U–V

W

CORPORATE SECURITY

Think corp security means a donut-snarfing security guard and a high fence? Think again, chummer! You want inside the corp enclaves, first get past the security wage mages, drek-hot deckers, and really big guys with really big guns ... plus a few hellhounds and watcher spirits just to keep you on your toes. The blackest ice, the toughest barriers, and the trickiest booby traps are just waiting for you to make one mistake ... your last! Want to survive your next run against the megacorps? Read this book and learn how they'll try to stop you. Once you know how the enemy thinks, you've won the first battle.

The CORPORATE SECURITY HANDBOOK describes in detail how corporations defend their facilities, valuable data, personnel, and nuyen. This sourcebook provides rules for setting up and getting around all kinds of security measures, including cutting-edge security systems never before seen in SHADOWRUN. Also included are new equipment, new contacts and archetypes, and guidelines for gamemasters on how to make a comprehensive corporate security system part of a SHADOWRUN adventure.

SHADOWRUN®
SECOND EDITION

FASA CORPORATION

41800
9 781555 602611
ISBN# 1-55560-261-4 $18.00