Under Lock and Key

Security measures and systems in ***Millennium's End***

In this world there are those that have, and those that have not. And those that have spend a lot of time and money making sure they keep what they have from those that have not.

There are a million and one ways to protect what is yours from those who should not have access to it. Some require vast financial resources to install and maintain; others do not. This article builds upon the basic information given in the ***BlackEagle Tactics and Investigations Handbook*** *(pages 40 to 44), taking a look at the common types of system and measures that operatives might either encounter or consider installing and the strengths and weaknesses of those systems.*

Conceptual considerations for a security system

A security system is comprised of a series of physical measures designed to protect the objective, combined with means of how these measures are used by those operating security. There are a few factors regarding how the security system operates, which must be considered when designing scenarios and assignments. The main consideration here is that the level of realism for the system must feel right. There should be strong foundations in fact naturally (since *Millennium's End* is a system at the forefront of current technological capability). However, the level of realism is a little more than that.

How / why the hell have they put it there?

Considerations such as the geographical remoteness of locations should be accounted for. Such locations require extensive resources to build technologically complicated systems, because there is a need to get technicians and materials to the site, as well as a requirement to construct many of the 'basics' (e.g. electricity supply) that are available in less remote areas. There is also the question of what part remoteness plays in the security of the installation. Locating an important site in the depths of Siberia for example may be a pig to get materials to, but the sheer distance and climate form parts of the security of the location. Having chosen such a location, is it then necessary (or financially viable) to equip the location with all the latest mod cons in terms of security, especially when the most frequent visitors are the local fauna?

A technique used by most business organisations is that of 'risk assessment'. The organisation evaluates the level of threat posed to its assets by certain factors, against the likelihood of that threat actually occurring. Certain measures reduce the likelihood of a threat, and these measures have a cost. From this, the organisation takes what it deems to be 'reasonable and practical' measures to protect the assets. The level of formality of this varies from organisation to organisation and country to country, ranging from formal, written assessments to informal, subconscious decisions. However, the principle remains the same.

Equally, bear in mind the legal and political framework within which organisations and individuals operate. Many countries have health and safety legislation that applies to organisations, requiring not only assessment of the level of risk, but also 'reasonable action to protect employees'. Of course, such niceties are strenuously avoided by those on the wrong side of the law, but this is yet another consideration.

Organisations and individuals in *Millennium's End* are no different in how they make their decisions, and when designing security systems in scenarios, cognisance needs to be given to this.

We're not at home to Mr. Cock-Up

The biggest threat to the breach of a security system is posed by human error. No matter how robust a security procedure is, and no matter how infallible a piece of equipment is, introduce a human and you have the capacity for things to go breasts skyward. Humans become complacent with routines, particularly in the absence of a perceived threat or a low level of auditing and checking by those responsible for security. They are also inherently lazy by nature unless otherwise stimulated, always searching for an easier, quicker and less complicated way of doing things.

How often do security guards check through the spy-hole in the door or look on the CCTV camera at those ringing the bell? How much attention do they pay to detail? Will they notice if the person outside the door is not someone they normally see or do they just give a quick visual check? Do they have the correct resources to do the job or is the company doing things on the cheap? Are they rushed off their feet? How often is security audited and how seriously are the recommendations adhered to? All these are human factors that present the possibility for a breach. They can also provide opportunities for characters in the face of seemingly overwhelming odds provided by high-tech security. However, they should usually present themselves as a result of careful reconnaissance and observation, not mere happenstance.

Players just want to have fun

It is important to remember though that *Millennium's End* is **only a game**. Theoretically, it is possible to put together a virtually impenetrable security system for a location – one only accessible using the correct 'keys'. But to what end? The Games Master is responsible for managing the level of challenge for the players in any role-playing game. Too much challenge is no fun. Too little isn't much cop either. The level of challenge posed should generally be in direct relationship to the reward to be gained. You won't find $1m in cash behind the unlocked door of a cleaning cupboard. Or if you do, there will be a damn good reason why! The principle here is that players won't enjoy the game if they are frustrated by nonsensical challenges. There should always be a reasonable means of penetrating security, related to the ability of the players / characters and the goal to be achieved.

The Elements of a Security System

Once you have looked at the context of the security system, it is time to consider the elements that actually make up that system. In concept, the system is comprised a range of overlaid factors, a combination of physical measures and how human beings (if any) interact with them. The following sections look at some of the measures available, how they work, what makes them good, and how they can be defeated. For ease, this is broken up into the following areas:

- Physical Design Elements;
- Locking Systems;
- Monitoring Systems;
- Mobile Elements.

Physical Design Elements

These are elements that by their very physical nature provide some degree of security.

Visibility and Illumination

Simple design elements regarding visibility can radically increase the security of a location. Measures included within this include:

Approach areas to a site should ideally be free from obstructions such as foliage, in order to provide a clear field of view for security personnel and cameras.

Doors and means of accessing secure areas should permit visibility of those on the other side of the door before opening it. This could be through a fish-eye spy-hole in the door or a camera.

Areas should be well lit to enhance the visibility of intruders. This could be permanent illumination (although be conscious that this can

be expensive for large exterior areas), by passive motion sensors linked to spotlights (illuminating only when movement is detected) or manually controlled illumination (searchlights or other lighting).

Areas where human guards require visibility at night require red lighting to preserve night vision. Whilst this does not completely negate the effects of lost night vision, it speeds adjustment (it takes between 30 and 45 minutes for the human eye to adjust from white light to darkness). Spotlights and lighting may help the guards, but they can also put them at a significant disadvantage if thrown into darkness.

Advantages:

Clear areas of visibility provide easier observation of intruders and make intrusion significantly more difficult.

Disadvantages:

Illumination and visibility can work for intruders as well as those protecting the area. Potential intruders can also see into the area clearly, and see what security measures are operating inside, the frequency of guard patrols and so forth. This may mean that an intrusion is not actually necessary (for example, if the intention of the intruder is to assassinate someone, they can do this using sniper fire from outside the area). In the event of combat resulting, the intruders are generally at the same advantage of visibility as the defenders.

Physical Restraint

Again, a little thought applied to the physical design of a location can either restrain or slow down potential intruders. Many of these measures have been used for centuries in the design of fortifications, and there is little new science here. Measures included within this include:

- Physical containment of entry: in order to access an area, you must first pass through another area. Entry at both sides of this area is controlled from within. This is commonly used in many areas where cash security is important. Cash is contained within the inner area; those who do not need to access the inner area enter a lobby where they can converse through a window with a movable drawer to enable items to be passed inwards and outwards.
- Obstacles to entry, such as moats, trenches and ditches. Such obstacles need not be immediately visible and could conceal traps designed to physically injure intruders (such as a ha-ha or oubliette). At the very least, such measures allow defenders to take other action whilst the intruders are occupied with the obstacle.
- Control of information about the location is important. Those who use the location frequently can be expected to be fully conversant with the layout. However, if there are a large number of visitors, then sign posting is necessary. If visitors are discouraged from moving around without an escort, then the need for sign posting can be reduced.
- Controlling the ability to pass information outside of the area (either detected or undetected) can be an effective means of catching intruders once they are inside. The penetrability of a building to radio signals can be controlled by the use of dense materials in the construction of the building. Even in lightly constructed buildings (such as those made of wood) this can be achieved using lead sheeting. Other options could include restricting the number of telephone landlines or for computer access ports to go through controlled security points. This can deny intruders communication with outside parties.

Advantages:

Many of the measures in this area do not involve high technology, and can even be improvised by characters with **Military Strategy / Tactics** *skill.*

Disadvantages:

In some instances these measures may not be desirable – such as where the aesthetics of the location are important (you wouldn't want to improve the security of your luxury villa by building fortifications around it). These measures can also be intensive in terms of the time taken to construct them (it takes a lot of manpower to dig a trench overnight). They also tend to be immediately obvious to those who intend to intrude.

Doors

The principal means of controlling access to an area are doors and there is a vast array of choice available. The key factors to be considered with doors include the following:

- Doors to secure areas should open outwards, be self-closing, have strengthened and recessed hinges and have no exterior handles (to prevent an intruder grabbing them and holding them open).
- Fitness for purpose. Doors range from armour-plated doors capable of stopping a bullet (or heavier) through pressure doors and fire doors (designed to contain pressure or the spread of fire) to interior doors (which may not even have a lock).
- Visibility through the door. Fire doors can include a panel of reinforced safety glass to enable someone to see through. Doors to secure areas may include a spy-hole. Visibility can be combined with extra security by fitting a mesh or barred gate on the exterior, allowing the door to be opened, but the area to remain secure.
- Traffic routes: it is necessary to consider whether the door is on a main traffic route through the site. High usage areas within a secure area generally have low security doors, simply for reasons of partitioning the area or safety reasons (such as a fire door).
- Suitability for the locking system. You won't have a great deal of success fitting a multiple bar mechanical locking system to an interior door. And even if you do, what's the point if the door can simply be kicked in?

Advantages:

Secure doors are readily available from a range of security companies on the market. They can be fitted relatively quickly once made, and can provide a robust security measure for most areas.

Disadvantages:

The door is only as strong as the lock that closes it and the material that surrounds it. A strong door in a weak frame or wall is no protection, and a cheap lock won't stand the pressure that the door is created for. Similar to other physical defences, the issue of the door blending in with the overall aesthetics of the building may be important.

Windows

Similarly to doors, there is a vast array of windows available. However, the key difference is that the window is not designed as a means of entry, and can accordingly be made more secure.

- Fitness for purpose. Windows can be required for illumination, ventilation or decoration. By making a window no wider than it needs to be for its purpose, is inherently more secure.
- Locking mechanisms are important. Some windows do not have locks, only closure systems. Others have removable locks or restraining arms, which limit the aperture of the window.
- Varying strengths of window material are available, ranging from bullet-resistance composites (either glass or plastic), through wired safety glass, double-glazing or opaque / frosted glass.

Advantages:

Since windows are not intended as a means of accessing an area (patio doors excepted), they can generally be made more secure than doors through their physical design.

Disadvantages:

A window can be broken, given enough of the right kind of force. A window should not be used in any area that needs to be impenetrable, unless it is smaller than a man can get through.

Shutters

Shutters are an additional means of protecting (usually exterior) doors and windows, and serve not only as a physical but also as a visible deterrent. Shutters generally tend to be more common in business premises (due to the cost of installation and the additional security they can provide to assets) but domestic variations are also available. They also tend to be used in areas that are secured when not in use (such as at night).

- Visibility through the shutter. Some shutters are necessary to prevent visibility, and are therefore solid. However, where this is not required, links, concertina or mesh can be used to cut down on weight and cost (the materials and the mechanism to raise and lower the shutter can be cheaper if it is lighter).
- Means of opening. Modern security shutters are raised and lowered by electric motors; older versions use straightforward manual lifting or manual pulling of the operating chain. In some cases (such as window shutters), they may be manually locked in place.
- As with doors, locking systems can be important, especially with manually operated shutters. Generally, manual shutters are secured with either padlocks or locking bolts that are inserted into the shutter frame.

Advantages:

Aside from the visibility of the deterrent, shutters can be a strong and effective way to secure areas. They are also commonly available.

Disadvantages:

Shutters can be a cumbersome means of protecting an area, and are not as quick and accessible as a door. Good quality security shutters are also not cheap.

Fences and Walls

Fences and walls are a principal means of protecting external, boundary areas. Naturally, there are many different kinds of fence available, depending upon the purpose. Consideration needs to be given to the following:

- Fence or wall? Fences are cheaper and quicker to build than walls, but are generally not as solid. A wall however offers the additional protection of not allowing visibility into the area, as well as being less penetrable.
- Height is a major factor if there are no other security measures, particularly in the case of walls. Putting a wide, deep ditch with steep sides in front of the fence can also enhance the effect of height.
- Additional measures such as barbed wire, razor wire, electrical current or overhangs can be used to improve the security of fences by physically preventing, slowing or encumbering intrusion. Higher technology measures include Sabretape (razor wire containing fibre-optic sensors to detect whether it has been cut).
- Combining fences and walls with sensors linked to alarm systems can also improve security. The level of sensitivity of such sensors is important (see the section later on *Monitoring Systems*).
- Smooth plastering on the side, or metal spikes or broken glass on the top can enhance the security of walls. These make it more difficult to pass over the wall without injury.

Advantages:

These are effective measures to either slow intruders (or escapers) down, and to prevent intrusion by 'casual intruders' (such as opportunistic intruders, who do so without preparation).

Disadvantages:

As a general rule, with the aid of the appropriate equipment, fences and walls can be either cut or climbed over. Given that they are visible obstacles, they also permit intruders to observe and prepare for the obstacle.

Locking Systems

These elements provide a means of securing an entry point.

Mechanical Locks

Mechanical locks are those where the physical locking device is entirely mechanical, and the user requires a key to open the lock. As such, they are not given to remote operation. Low quality locks are simple and easy to defeat, even for those with little skill or inappropriate tools. Higher quality locks provide increasing complexity of mechanism, as well as multiple locking points (multiple bars inserting into the top, bottom and sides of the door frame) and increased resistance to physical abuse. Generally, even the higher quality locks do not extend beyond 'medium' levels of expense, and as a consequence there is a high general use of this kind of lock.

Standard Door Locks

Defeating standard door locks by lockpicking is covered on page 50 of the rulebook. Some additional points to consider are as follows:

- Complexity of the locking mechanism directly affects how difficult the lock is to open without the correct key. High quality locks have multiple locking pins and unusual arrangements of the pins to reduce the ease of picking them.
- Location of the locking mechanism is important. With lower quality locks the locking mechanism is easily separable from the door. Better quality locks are integral to the door and also have protection from physical abuse (such as a steel plate surrounding them), in order to prevent them being forced off.
- An increased number of locking points increase the ability of the door to withstand physical assault.
- Some locks use simple but effective methods such as different geometric shaped keys (hexagonal or triangular usually).

Advantages:

Standard mechanical door locks are relatively cheap, easy to install and provide moderate levels of security. Keys can usually be copied easily as required for those who need access.

Disadvantages:

Any mechanical lock can be picked, given enough time, skill and suitable tools. Mechanical locks also suffer from the shortcoming that he who has the key can enter.

Car / Vehicle Door Locks

Car and vehicle locks generally work on the same principles as standard door locks. However, there is an increasing tendency to use electro-mechanical locks, especially operated by infrared remote control. Modern vehicle locking systems are also combined with relatively complex alarm systems and engine immobilisers.

Removable Locks

Removable locks are similar to standard door locks in principle and operation, although they are generally simpler and therefore easier to defeat. This type of lock covers padlocks, tubular locks and removable bolt locks (such as those used to protect roller shutters).

Advantages:

These locks are cheap and easily available and provide adequate security where casual intrusion needs to be prevented. They also require little maintenance.

Disadvantages:

They are relatively easy to defeat or force for someone with the right equipment.

Cabinet and Cupboard Locks

These simple mechanical locks are basically designed to protect privacy, rather than provide any serious level of security. The reason for this is that the material surrounding the lock is generally easy to force, and they are therefore common in offices (such as filing cabinets or desk drawers). The challenge for characters is in opening these without leaving signs of intrusion.

Safes and Vault Combination Locks

These are among the most difficult mechanical locks to defeat, because they are contained within a strong and durable material, and have no visible means of attacking the actual mechanism. The actual safe or vault can be made to withstand physical and elemental damage, making it suitable for protecting a wide range of property. They may also include the use of a conventional key (or keys), along with the combination.

Safes see widespread application in business, and also limited domestic application (generally on a smaller scale).

Advantages:

These locks provide extremely secure protection, requiring specialised equipment (drills, stethoscope, etc) and considerable skill to defeat. They are also generally fire and explosion resistant.

Disadvantages:

They are expensive (even a small safe costs over $ 1,000), and not very portable due to their great weight. The combination cannot easily be changed, and once known can be passed on to others.

Electronic Locks

An electronic lock is a lock where although the physical locking device is usually mechanical, the key to open the lock is generated by some electronic means. At the lowest cost levels the locks are simple electro-magnetic locks; as cost levels increase they include multiple bar locks, locking to top and bottom in addition to the side frame. Generally, all electronic locks have some form of remote operation whereby the lock can be released from a control point (such as a security office, reception desk and so forth). They are also usually 'fail safe'; an interruption in power or a system failure causes the lock to fail closed. Whether the building has an emergency generator and how long this takes to kick in also affects this.

Electronic locks increasingly make use of a three point security system, utilising any of or a combination of something you:

- **Know** (e.g. a personal identification number);
- **Have** (e.g. a magnetic swipe card);
- **Are** (e.g. your biometrics: fingerprint, voiceprint, retina pattern).

They also see a widening range of applications, from not only controlling entry into buildings or areas, but also access to PCs, financial information and so on.

Advantages:

Electronic locks are becoming more widely available because they can provide extremely high and flexible levels of security.

Disadvantages:

Electronic locks are the most expensive types of locking device available, and those that use biometrics are at the top end of the range. They generally require a link to a PC with appropriate software, and the invulnerability of the PC is reliant upon protecting against hacking or deception (deceiving the PC that the information it receives is actually correct).

Electronic Key Card / Numeric Key Pad

This is the simplest kind of electronic lock, involving a magnetic strip reader (MSR) close to the actual lock and the user opens the lock by swiping a magnetic card. It is sometimes combined with a numeric keypad to provide additional security. The MSR refers to the control PC or control unit (it can be as simple as a panel the size of a large book) to determine whether the cardholder has access to the area. Cards may also contain additional security features such as digitised photos of the cardholder and personal information either encoded in the magnetic strip or retrievable from the control PC.

The electronic numeric keypad is similar to the electronic key; the numeric keypad is a more technologically advanced version of the mechanical numeric keypad (above). The numeric keypad is often combined with the electronic key for additional security. It requires that the user enter an alphanumeric code (usually a combination of A to D plus 0 to 9) to release the lock.

Common uses include offices and business premises (especially in office blocks where there are more than one company).

Advantages:

Cheap and allows access to areas to be controlled individually, even to specific zones of an office or building (the only restriction is the number of doors fitted with the MSR). Such access is also individually transferable and for example, when an employee leaves, obtaining their card from them prevents further access.

Disadvantages:

Anyone with the card (and numeric code, if additionally required) can get in.

Infrared Key Transmitter

Infrared key transmitters are becoming a common means of locking vehicles, but also see application with electrical roller shutters. The key transmitter has a line of sight range of at least 30 metres, and need be no larger than a key fob. The transmitter may also simultaneously deactivate alarm and immobiliser systems.

Advantages:

Small and portable.

Disadvantages:

This is no different to a normal key. He who has the key can open the door.

Magnetic and Electro-Mechanical Locks

These are the actual locking system used in electronic locks. Magnetic locks use electromagnets to hold the door closed; electro-mechanical locks use an electrical motor as the 'turning' mechanism for the lock. An electro-mechanical lock usually uses multiple bolts to lock the door.

Advantages:

Magnetic locks are relatively cheap to install and provide a simple means of securing doors from casual intruders. Electro-mechanical locks are more secure and provide a robust means of securing the door.

Disadvantages:

Electro-mechanical locks are relatively expensive and require the locking mechanism to be integral to the door. Cheap magnetic locks can be easy to force with an appropriate tool.

Retina and Palm Scanners

These laser scanners utilise scans of the biometrics of the individual as the key to open the lock. They consist of a scanner and a link to a controlling PC with the appropriate recognition software on it. The scanner compares an image presented by the user (either by pressing a palm or looking into the scanner) against the version on the control PC and determines whether to release the lock.

These are among the most complex kinds of electronic lock, requiring expensive sensory equipment at the entry point, high-specification PCs and sophisticated software to operate the systems. As such, they are generally reserved for protecting areas of the highest security within highly affluent and technologically advanced organisations. They can also be used to protect items of equipment (PCs are the most common application) and access to information (retina scanners have been introduced on some ATMs in the USA).

Advantages:

Release of the lock is restricted to authorised persons only, period. Without an authorised person, the lock simply cannot be released at the entry point.

Disadvantages:

An authorised person can be coerced into releasing the lock for others to enter. Additional measures are required to counter this eventuality. This puts such authorised personnel at additional risk. Additionally, the complexity of the equipment means that it is inevitably sensitive and requires a high level of maintenance (especially cleaning of the optical scanners). The equipment is also extremely expensive.

Voice Print Analyser

On a similar basis to the retina and palm scanners, the voice print analyser uses a sample from the user's voice to analyse and compare against a version on the control PC.

Common uses are as above for Retina and Palm Scanners.

Advantages:

In addition to the benefits described above for retina and palm scanners, the voiceprint can also be used to measure the level of stress that the individual is

under. Therefore, if someone is holding a gun to his or her head then the lock may not release.

Disadvantages:

As above for Retina and Palm Scanners.

Monitoring Systems

These elements either monitor security in an area and / or provide a means of alerting a breach of security. Most have been developed from industrial applications to detect failures in a production process (leaks, fires, machine parts behaving abnormally, etc). It is common for a number of monitoring systems to be combined in a single security system, and there are a number of considerations that apply to each of the sensors described below:

- What does the sensor actually do when it detects what it is designed to detect? (Light an alarm panel, send a pager message to human guards, sound an audible alarm, etc).
- How sensitive is the sensor? What tolerances has it been set or manufactured to tolerate before triggering?
- Can the sensor be accidentally triggered? Motion sensors for example, have limited application outside, where they can be triggered by animals or the weather.
- What is the range and area covered?

Audio Sensors

Audio sensors are effectively microphones that measure the amount of noise (sound level) in a given zone. Like other sensory devices they are most effective when mounted in an array around the zone.

Sound levels are measured in decibels (dB). In a quiet domestic residence the ambient sound level is about 38 dB. An ordinary conversation would increase the sound level to around 70 dB. The sound intensity of an air-raid siren could reach about 150 dB; that of a jet plane, around 120 dB. When perceived sound intensity is doubled, its power level increases by 10 times, or 10 dB.

The more expensive sensors are sensitive enough to detect minor noises such as anything louder than a whisper. However, these require the system to be able to measure and distinguish noise differentials of minor levels (less than 10 dB).

Advantages:

Audio sensors are a good measure to detect significant changes in ambient sound levels (greater than 10 dB). However, they rely upon effective insulation from external noise and good internal acoustics in the zone (soft furnishings and materials negate this by absorbing sound).

Disadvantages:

Difficult to use in outdoor areas due to the sensitivity of the system. The most sensitive audio sensors are expensive to install and maintain and rely upon the zone in question having adequate external noise insulation to enable minor changes in ambient noise levels to be detected.

Fire / Smoke Sensors

Less of a security measure than a safety precaution installed in most modern buildings, fire and smoke sensors are frequently coupled to fire prevention systems such as sprinkler units to prevent the spread of fire. The sensors are small (less than 20mm in diameter) and are typically mounted in ceilings or high on walls, where there is an adequate flow of 'normal' air across the sensor. Frequently they are set up in zones within large buildings, enabling sprinklers to be activated only in zones where fire or smoke has been detected. The sensitivity of the sensor depends upon the area it is protecting: they may be sensitive enough to detect cigarette smoke in areas where smoking is a safety hazard (e.g. where there are flammable or delicate materials stored) or they may have a degree of tolerance for this.

Intrusion and Panic Alarms

Intrusion alarm systems range in complexity from simple alarm panels to ones with multiple sectors, allowing those responding to the alarm to know exactly where the problem has occurred. They may provide a warning on an alarm panel or an audible and / or visible alarm within the premises.

Security companies may also monitor alarm systems, which is a more expensive option. Triggering the alarm sends a message (usually by a phone line) to the security company, who in turn notify the police and / or respond to the alarm.

Panic alarms are a variation on intrusion alarms, whereby there is a panic button, enabling those under attack to raise the alarm manually. Such panic buttons generally provide little or no indication that the alarm has been raised at the point where they have been pressed.

Advantages:

Alarm systems provide a visible deterrent and an additional element of complication to intruders. They can also be used to protect remote locations, replacing or reducing the need for human security.

Disadvantages:

An alarm system is only as effective as the sensory systems it uses and the response to the alarm itself. If there is a casual attitude to alarms (caused by numerous false alarms), then responses may be lethargic.

Motion Sensors and Infrared Beams

There are different types of motion sensor available:

- Wide angle infrared sensors (such as those found on domestic alarm systems).
- Fibre-optic sensors using bundled fibre-optic cable to detect motion beyond a given tolerance. These can also be combined into other preventative measures such as razor wire (Sabretape).
- Door and window sensors, where two opposing connections detect movement in the door.
- Single infrared or visible light beam sensors, which operate like an 'electronic trip wire'.

Advantages:

Extremely effective and difficult to defeat in interior areas.

Disadvantages:

Motion sensors have limited application in outdoor areas because of the number of factors that can accidentally trigger them. Variable tolerance sensors are also relatively expensive.

Pressure Sensors

Pressure sensors work by detecting a change (increase or decrease) in the pressure upon the sensor plate. Typically they are mounted under floors, but can also be used similarly to a motion sensor (e.g. to detect if an item has been lifted – such as a valuable item in a display case).

Advantages:

Extremely effective and difficult to defeat in interior and exterior areas, if deployed correctly, because they are generally not visible. They are also relatively cheap as far as sensors go.

Disadvantages:

If not set up correctly, they can be deceived or avoided.

Surveillance / CCTV

Closed Circuit TV cameras are a growing part of everyday life, providing recordable data on events, as well as straightforward visibility of remote areas. Cameras can be either static or movable, and can also be equipped with standard video systems such as light-intensification and infrared imaging.

At their simplest, CCTV systems record onto a long-play VCR at the site in question. Tapes are generally changed daily and a supply of tapes is rotated over a weekly, fortnightly or monthly basis. More complicated systems pass the CCTV images through a PC. This allows multiple images to be seen at once on the same screen, fast access to specific areas of the recording, and transfer of stills or sections of video to others for communication of threats.

Cameras may be covert or overt. Covert cameras can be hidden behind fittings, or can be so small that they are difficult to spot. Even overt cameras can be disguised. For example, the kind of CCTV camera in use in many shops to deter shoplifters involves a dome-shaped fitting, which covers the camera body. The camera can then be rotated and / or zoomed as required, without it being obvious that the camera is in use.

Advantages:

Multiple areas may be observed from one console. Data from the cameras can be recorded simultaneously to provide post-event analysis.

Disadvantages:

CCTV systems are not cheap to install and to be fully effective need to provide full visibility of all key areas. They require continuous monitoring, and their effectiveness can be limited by stealing or erasing the tape, or by someone forgetting to change it when required.

Temperature Sensors

Similar to pressure sensors in principle, temperature sensors are small devices (less than 20mm in diameter), which measure changes in ambient air temperature in a given zone. They are typically mounted in an array to ensure effective coverage of the desired zone. At the most expensive end of the scale they can be used to detect whether someone has entered the zone being monitored, but these require the system to be able to measure microscopic changes in temperature (less than 0.1°C).

Advantages:

Temperature sensors are a strong precaution against large changes in temperature (e.g. failure of heating or cooling devices, or fires).

Disadvantages:

Difficult to use in outdoor areas due to the sensitivity of the system. The most sensitive temperature sensors are expensive to install and maintain and rely upon the zone in question having adequate climate control systems to enable minor changes in ambient temperature to be detected.

Mobile Elements

These elements are in addition to the physical elements described above, and introduce the human factor into the equation, as well as covering automated mobile sentries and guard dogs.

Human Guards

Although many of the factors relating to human guards are covered by the actual skill-set of the individuals and other attitudinal factors discussed here, there are a few factors that are worthy of mention here.

- Patterns of patrol. Where do the guards patrol? Do they like patrolling outside when the weather isn't nice? Do they like to sit and watch TV when left alone on a night shift?
- Expectations of the guards. What are they expected to do in response to an intruder? This has key implications upon their equipment and what they actually do when they find an intruder.
- The proficiency of the guards in using the security measures available to them is important. Are they fully trained on using the intricate CCTV system they have at their disposal? Do they understand what the flashing light on the panel means?
- The strength of response procedures for the guards will determine their response, and is partly derived from their experience and training. A Federal building can be expected to have good responses to threats; a disused warehouse with one contracted in security guard may have a lesser level of response.

Automated Guards

Automated guards can get around many of the factors associated with human error, and are an option used in some industries to reduce (but rarely entirely replace) the required human element.

Generally, automated guards consist of a mobile robot platform with a number of sensory, audio and video devices attached. Essentially, most of the sensors described above can be mounted on the platform.

Advantages:

They can reduce the degree of human error by reducing the need for humans to be ***involved in the system.***

Disadvantages:

Automated guards are better suited to interior areas, and can't go upstairs. As with an alarm system, automated guards are only as good as the sensory equipment they employ. They are also extremely

expensive, although this is a generally one-time investment.

Guard Dogs

Guard dogs provide a useful element to any security system, providing both a deterrent and an alarm system. They also have unique capabilities, superior to those of humans, as well as being potentially expendable.

The use of guard dogs is covered in the article *Man Bites Dog*, which can be found elsewhere on ***Mission Priorities***.

Game Applications

Two (albeit Hollywood) examples are given below of how the measures presented here can be put together to form a system. The examples are included as a demonstration for GMs of the level of detail that they can go to in planning a security system that is a central feature of a scenario.

There are a number of ways that issues regarding security can be incorporated into *Millennium's End* assignments. BlackEagle is a company specialising in security and investigations, and there is a wide array of assignments and elements of assignments to which these points are pertinent. The following are some suggestions for elements of and entire assignments where security is a key part of the goals for the operatives. Of course, in true *Millennium's End* tradition, these are only the bare bones – there are multiple twists that can be added!

- ***Stealing a protected item:*** This could be something tangible that another party wants, such as an individual item of value or importance. Or it could be less tangible, such as stealing data or information.
- ***Testing security arrangements:*** People spend a lot of money on security arrangements. Occasionally BlackEagle are hired as consultants to test exactly how good the arrangements are, and to recommend improvements.
- ***Protecting the client:*** Just as clients often hire BlackEagle to breach someone else's security, they also hire them to improve their own systems. Care needs to be exercised in these kind of scenarios – largely because the characters are in a defensive position, and this can affect the game pace.
- ***Rescuing people:*** Another area BlackEagle become involved in is resolving kidnappings and hostage taking, particularly where the authorities either have no knowledge of, or no interest in the imprisoned party. This could be a rescue from a prison facility or a hostile kidnapping of someone with specialised knowledge.
- ***Planting surveillance equipment:*** Some people want to know things that others would rather keep from them. BlackEagle's technical expertise in surveillance, combined with the proficiency of its operatives in intrusion techniques provides for some interesting assignments to obtain information. This could be incriminating, or of industrial significance.

The Black Vault

This is presented here as an example of a security system, using 'The Black Vault' from the film ***Mission: Impossible***. The vault is located within Central Intelligence Agency Headquarters at Langley, Virginia. The vault is used to protect highly secret data on a PC regarding CIA operatives – not your run of the mill *Millennium's End* scenario, but it does give some ideas of locations that could be the objective of an assignment.

Rather than covering the full security of the entire Langley complex here, only the internal security measures around the vault itself are described here in any detail.

Security Measures:

The vault is physically isolated. There are only two points through which the vault can be entered: the main door and an air conditioning duct.

The PC in the vault is entirely stand-alone, with no modem access. The only way to get data from the PC is to physically be in the vault to get it. Entry is restricted to one nominated person.

Access to the lobby outside the vault is direct from the main building corridor. It requires a voice-print identification and a six digit code to be entered. Approved access is granted to the operator and those security staff who work in the vault lobby.

Inside the door is the lobby, which is staffed twenty-four hours a day. The lobby works on the airlock principle: the vault door cannot be open at the same time as the door to the corridor. The member of security staff is armed with a pistol and has a concealed alarm point under their desk.

From the lobby entry to the vault requires a retina scan for the single operator who has access, and two electronic key cards to be inserted into the machine (one carried by the operator, the other by the security staff). The door to the vault is a six-inch thick armoured door with multiple-point, electro-mechanical locks.

Whilst the operator is in the vault, he can work normally. However, whenever the vault is unoccupied, there are three systems in operation to protect it.

The first is an audio sensor, with sensitivity such that any noise above a whisper (about 50 decibels) will trigger it.

Secondly, there is a temperature sensor, with a sensitivity of +1°F. The temperature is maintained within the vault by the building air-conditioning system (see below). However, even the presence of one person inside the vault unless their movement is very slow (to minimise the rise in their body temperature from movement / exercise) will trigger this sensor.

The air conditioning vent can be accessed from the main building system. The vent in the vault is about 100 x 75 cm in size – just large enough for one person to access. There is a laser motion sensor forming a grid across the duct side of the vent. The vent is screwed vertically into the ceiling at four points from the inside of the vault.

Thirdly, there is a pressure sensor in the floor, which will be triggered by even the slightest increase in weight (a drop of condensation could trigger it).

Any of these triggers will lead to an automatic lock-down of the PC system in the vault, as well as sealing the vault entirely and lighting up every security panel in the building.

Suggested Game Mechanics:

Aside from the difficulties of getting into the building and actually getting to the corridor, there are numerous difficulties in going in through the main entrance.

There are no external mechanisms on the exterior and interior doors to access the locks. Conventional picking, even with electronic equipment, is therefore impossible.

The mechanism for the retina scanner, numeric keypad and card swipe are recessed into the wall. To access them requires that the wall panel be removed. Having the time required to do this undetected while the building is occupied is extremely unlikely.

Hacking into the Building Control PC requires

- A **Computer Systems / Security** roll at –50 modifier to hack into the PC, and
- A **Computer Systems / Networks** roll at –20 modifier to find the relevant server

To operate any of the building control systems (such as fire alarms, lighting and power) from this requires further **Computer Systems / Security** rolls at –30 modifier.

It is not possible to access any of the vault control systems from the main building control system. The link between the two systems is simply a one-way alarm node from the vault.

The interior of the vault is shielded with dense materials, preventing penetration by radio signals (including mobile phones).

The PC is also completely stand-alone, with no modems or linkages to any other systems. It

requires a number of authentication passwords to enter the system containing the NOC list. Only the nominated user knows these passwords.

Hacking into the PC requires

- A **Computer Systems / Security** roll at –50 modifier to hack into the PC, and
- A **Computer Systems / Civil Systems** roll at +0 to find the relevant data.

When the authorised user is using the PC, it is common for him to leave the PC accessible whilst taking breaks, because the physical security of the vault is robust. Only when his work is completed does he enable all security measures on the PC.

How They Did It:

In the film it took a four-person team to do it. The core role involved hacking in and establishing a computer link into the building control system. The other three members of the team entered the lobby disguised as firemen and the smoke detectors were triggered in a sector close to the vault.

This enabled the team to get into the building (although didn't entirely prevent curiosity from one of the security staff). The next key phase was for one of the team to enter the canteen, and wait for the operator. They then sat next to the operator and injected a substance into his coffee to induce vomiting a stomach upset almost immediately.

At the same time, a minute tracer was put on his shoulder to enable him to be tracked. This was a little unreal as it is inconceivable that somewhere as important as Langley does not operate a system of controlling or monitoring radio transmissions into and out of the building.

With the operator now constantly and uncontrollably rushing to the toilet, one member lowered the other into the vault through the air conditioning vent. The laser was immobilised with a frame to contain all the reflection, and the screws in the vent were removed.

It's only a film, and there are large areas of artistic licence used, but it does provoke some ideas.

Stealing Las Vegas

Another example of a security system from a film is from ***Ocean's Eleven*** (the re-made, 2001 version). Essentially the aim was to steal the take from the combined vault of three Las Vegas casinos on a World Heavyweight Title Fight Night – an estimated take of over $150 million.

This represents an extreme example of the level of security measures that can be taken. It arises in an environment where there is a combination of extremely lucrative private business with personally obsessive levels of security and routine on behalf of the casino owner. To pull off the job requires a level of complexity, skill, ingenuity and bare-faced cheek that only the very best can consider.

Security Measures:

The three casinos in question (The Bellagio, The Mirage and The MGM Grand) are all located in the 3000 block of Las Vegas Boulevard. The vault in question serves all three casinos, and is located beneath 200 feet of solid earth beneath The Strip. There are motion sensors in the ground around the vault for 100 yards in every direction, to detect tunnelling. Considering that the vault safeguards every dime that passes through the three casinos, such elaborate measures are not insufficient.

The initial security measure is to get within the casino cages (where the cash and chips are counted for each section). This requires an electronic key card, which is only held by members of security and maintenance personnel.

The casino cages themselves form a virtual labyrinth. Whilst constructed on a grid principle, there are a number of similar corridors and it is easy for someone to get lost.

To pass beyond the cages there is a set of electronically locked doors with a numeric keypad. The keypad requires a six-digit code,

which is changed every twelve hours. The code is known to the casino owner and manager and a small number of personnel who are required to pass through the doors during the twelve hour period. New codes are issued at 0730 and 1930 hours daily.

Through the doors is the elevator to the vault level. To move the elevator requires three combined security checks:

- A fingerprint scan on the elevator button
- Vocal authorisation from within the casino, and
- Vocal authorisation from the main security control room itself.

Without these three measures, the elevator won't move. Additionally, the elevator shaft has a grid of motion sensors (approximately one every two feet (around 100 beams) that become active when the elevator is not moving. These prevent the elevator being bypassed through the escape hatch in the ceiling of the elevator car. If these alarms are tripped the elevator doors at ground and vault level are sealed, as is the vault door.

At the bottom of the elevator shaft is a corridor with two guards, equipped with Uzi SMGs and pistols. They guard the vault door.

The vault door is a large (two metres in diameter, 50 cm thick) steel pressure door with a number of electro-mechanical bolts around the circumference. There are no external features to pick. It can be accessed by code, fingerprint scan and independent authorisation from the control room. Aside from legitimate entry, the only alternative is explosives.

There are (as might be expected from a Vegas casino) also sound and vision CCTV cameras extensively throughout not only the entire vault complex, but also the floor of the casino. These systems are monitored by the central control room.

Suggested Game Mechanics:

To talk through the specific game mechanics to cover all of the scenes in the movie would be extremely repetitive, excessive, and above all else, dull. However, the principles of the keys parts are as follows.

Firstly, there is a lot of bluff and acting, especially use of the **Acting / Con** skill. There are also particular elements of **Electronics / Wiring** and **Computer Systems / Security** related to breaking into the systems concerned. In most cases there are particularly straightforward skill rolls attached to what went on; the ingenuity lies in the cheek of the plan itself.

How They Did It:

The scheme to breach the security was an extremely complex operation. It involved eleven people to finance and carry out the job; in some cases, even more could practically have been used. Those carrying out the job were technically of supreme proficiency in their respective areas. This was definitely not a concept for amateurs.

The scheme involved an extremely detailed and intense information-gathering process. The information gathering also involved operating a number of scams, ruses and distractions. Further scams were used in the execution phase to get members of the team into place so that they could do the job.

Underpinning the security were two elements of flawed reliance on the part of those running the casino. The first was complete confidence in the technological systems used for security. They genuinely believed it to be virtually infallible. The second was the domination of routine. Whilst routine in operations means that they can operate with efficiency, that very efficiency makes the operations vulnerable to surveillance. Observations will therefore provide a high level of reliability.

The key elements of the operation to breach the vault were as follows. Firstly, the surveillance system was accessed, allowing the team to see all areas of the vault complex. This was critical for understanding what was going on, and being able to control the environment.

The first phase of the actual operation was smuggling the acrobat into the vault to enable

the vault door to be blown from the inside. This required

- A ruse at the hotel door, entering as waiters, with the cash cart disguised as a service trolley
- A quick change in the casino elevator, and then
- Some play-acting at the entrance to the cages to convince the security guard that they had forgotten their key cards, and that the cash cart needed to be taken directly to the vault.

All this was time-limited because the acrobat only had 30 minutes of air in the cart. However, installing breathing equipment could have eased this.

The second phase of the operation was to get the team in place to blow the vault door from the outside. This involved two separate ruses to get team members inside the cages from where they could get away from their accompaniment. This enabled them to meet and access the elevator shaft.

Once the outer team were in place at the top of the elevator shaft, the power system for the whole of Las Vegas was taken out using an electro-magnetic pulse, generated by a pinch stolen from the California Institute of Advanced Science. With the power momentarily out, the team could rappel down the elevator shaft to the bottom.

Upon the return of power, the control over the CCTV and surveillance system was used to substitute video of a mock-up of the vault and outer corridor. This allowed the team to control the perception of the environment by the security staff.

The guards outside the vault were taken out with gas, and the vault was simultaneously blown from the inside and outside.

Another ruse was used to convince the casino owner that he was being robbed and put out a call for the police – knowing that he would do so and expect a SWAT team response. The 911 call was intercepted and the SWAT team sent were members of the team. They simply walked out the door with the cash.

As in the case with *The Black Vault* above, there are a few fanciful Hollywood parts to the operation. Using an electromagnetic pulse in a major city of the USA would probably considered using a weapon of mass destruction in the current political climate, and would cause more damage than a momentary interruption of power supplies, even if a 'pinch' such as that stolen could be easily obtained. Buildings with security systems like casinos also have back-up generators. And radios, if they aren't fried by EMP don't tend to work terribly well underground.

Defeating Security Measures

Notes for Millennium's End

In a game context, defeating security measures is a combination of:

- The complexity and quality of the measure.
- The tools used to defeat it.
- The skill of the individual.

In the below sections, references to equipment refer to items presented in *The Equipment Listing*. These are by no means prescriptive answers for handling attempts in defeating security measures in the game: they are intended as guidelines for GMs, based upon the basic information given in the rulebook.

Mechanical Lockpicking

Picking a mechanical lock requires the skill ***Miniature Mechanics / Locksmithing***, as well as an appropriate tool to do the job. These of course assume that there is no degree of forcing the door. Suggested modifiers for lockpicking attempts are as follows:

Quality of the lock:	**Modifier:**
Low (Desk / Drawer / Filing Cabinet / Padlock / Standard Domestic Door)	+5 to +20
Average (Domestic Security Door)	+0
High (Multiple Bar Lock / Commercial Security Door)	-5 to -50
Tools Used:	**Modifier:**
Lockpicking Tool Set (Car Entry, Specialist or Standard, as appropriate to the task)	+10
Improvised Lockpick	-10
Electric Lockpick	+0
Jiggler Key Set	-5
Lock Release Gun	+20
Pocket Knife Lockpick	-10
Time Taken:	
300 seconds – [Modified Locksmithing Target – Roll]	

E.g. For a character with a Locksmithing skill of 45 to pick an Average lock with an improvised lockpick (target roll (45 + 0 –10 = 35)), who rolls 22 takes

300 – [(45 + 0 –10) – 22] = 287 seconds

Electronic Lockpicking

Electronic locks require different skills, depending upon the approach taken. This depends very much on the particular lock and how the character approaches defeating it, and consequently it is difficult to suggest appropriate modifiers.

In some cases it is possible to hack into the building control computer and release the door. This would use the ***Computer Operations / Security*** or ***Civil Systems*** skills.

Attempting to defeat the lock by deception at the locking point requires a different approach. The character first needs to get access to the lock control system (***Electrics / Wiring***, modified by how easy it is to access the controlling system). Next, an attempt to deceive the locking system is necessary (***Computer Operations / Security*** or ***Electrics / Electronics*** depending upon the approach used). The equipment required for this might be a precision screwdriver, connecting cables, a laptop or palmtop PC and a dummy swipe card.

Following all this there may still be an element of mechanical lockpicking necessary (to move the locking bolts) once the locking system has been disabled.