Sample Matrix Sites

by Khadim Nasser

The Shadowrun 4th Edition rules for Hacking actually work quite well. The problem is that there is very little in the way of examples of how a Matrix Site is actually put together. By 'very little', I of course mean 'bugger all.' This document is meant to be a quick overview of some of the salient points along with a few example Matrix structures. Each example matrix structure includes a few brief notes to suggest the power-level of the system, along with its purpose and suggested ways of modifying it.

People may also wish to look at the 'in character' History of the Matrix piece that I wrote, which is available on my site. It acts as a sort of companion to this, filling in some of the flavour gaps in the same way this fills in some of the example gaps.

One thing that is intended is that this document should be fully RAW compliant. Any suggested change or ambiguity will be explicitly noted. If you notice anything that you think is not RAW, please email me at K@knasser.me.uk letting me know what, where and especially why. I do these things for non-profit, and so feedback if it's useful to you, is always appreciated in return.

-Khadim.

Table of Contents

Matrix Design Notes

Physical Location

It's important to note that in the Matrix, physical location is often irrelevant. There is no reason why the node of the house in Seattle where you live (which orders your food and handles accounts, etc) is not linked to your holiday home in Dubai. A hacker might step virtually from one to the other without a second thought. This is important to grasp because there is a hold-over from previous editions in which people think that to travel from one to the other, a hacker would have to somehow bounce through an entire telecom system to make the connection. This is not the case in 4th edition. The underlying structure of the matrix handles these details. What is of concern to the user (whether legitimate or not), is the *conceptual* structure of the system. If you want the security cameras in your sprawling Bellevue mansion to be controlled by a node in the business office you own, you can do that without any added complexity.

Definition of a Node

A node is the basic building block of the Matrix. It can be a large number of things. It could be a single drone or an office network. It could just as easily be a traffic co-ordination system for Downtown, Seattle. Or it might be your fridge. In some ways, a node is a rules conceit. The essential defining quality of the node is that it is a discrete entity as far as interaction goes. For example, if all the terminals on the floor of an office building are interlinked and share accounts and data, then they are a node. The GM doesn't *have* to treat them as such, but it's very much the logical way of handling it for most situations. When the hacker hacks the office node, he has access to all of these terminals. Yet on the same principle, when the hacker comes across a group of drones, threatening his team-mates, they all have individual security systems and pilot programs are in fact each a separate node. The hacker would have to treat each one as a separate target unless perhaps, all the drones took their orders from a single controlling security system (yet another node), but that would be a separate issue.

One thing to grasp however, is that the node is a rules entity. In the example of the office network node, IC could be installed on the node and that IC would be protecting all of the terminals. In the example of the drones, separate programs would be required for each (though mobile IC with suitable access rights could leap from drone to drone).

There are some cases where it is not clear whether you are dealing with a group of nodes or a group node. For example, the security cameras in an office block. A GM *could* treat each camera as a separate node if desired. This would be a cumbersome approach however, both in terms of the supposed practicalities and costs in setting it up for the company, and in terms of game-play where the hacker character had to tackle each camera individually. The sensible approach would be to set up a security node to which each of the cameras is subscribed as a device. A device is still a node of a kind, but the hacker is not normally going to be targeting them individually, not if he wants to affect more than one, anyway. Instead, the security node itself will be hacked, enabling him to command all the cameras however he wants.

Security Levels

There are three security levels in Shadowrun – User (normal), Security and Administrator. It is not always clear when to use the different levels. In particular, it can be unclear when you would not expect a device to have different security levels. Let's take a few examples: An office network, a Doberman drone, a car and your fridge. The office network will have three distinct security levels. If hacking in as a user, then the hacker will be able to access standard files on that network, carry out the standard things that network is used for, perhaps planting a fake document, etc. If hacked in with Security level access, then the hacker will be able to do additional things, such as monitor other user's usage, access times, perhaps access all the user files regardless of owner, etc. If hacked in with Administrator level access, then the hacker can do all sorts of things such as delete user accounts, alter access times on files (making them appear older or newer than before), perhaps even erase back-up data. These are all examples of course. A GM could have any particular node set up differently. Now the drone will be different. The user level access is likely to grant very little functionality. Perhaps the drone can be ordered to return some information on owner identity (Lonestar would probably require this sort of thing for drones on UCAS territory), current charge levels, maybe. But a GM would be perfectly entitled in saying that there was no user level access available at all. At least on a security vehicle like a Doberman. Security level access however, would probably be sufficient to issue orders to the drone, make it shut down or return to base or shoot it's owner. There shouldn't be any significant functionality that the drone's legitimate owner would need that wasn't available at this level. Administrator access would only be required for serious stuff such as editing the drone's registration details to disguise the fact that it's stolen, editing user accounts so no-one else can command it, etc. You can hack control of a drone away from its owner with Security level access, but if you want to stop them from keeping taking it back, you need Administrator to shut them out. The car is a similar case to the drone in some ways, but undoubtedly user level access would be sufficient for most tasks. If you want to make it take you across town, user level should be sufficient. That's what the car is supposed to do, after all. Security level probably wouldn't have much functionality. Maybe a GM would require it make the car refuse to respond to a Lone Star override or to exceed the speed limit and violate traffic laws. Administrator would be required to add new family members to the user list, or perhaps even to disable the car's safety features. The fridge is a special case. Maybe it's a smart 2070 fridge which reports the current contents and requests services when appropriate etc. But it doesn't really do anything more than that. It's hard to imagine what Security or Administrator access would mean in this case. There are lots of devices like this in the world of 2070. So if there's only one level of access, does the GM say everything is Administrator or everything is User? In the case of the fridge, it's probably best to say everything is User. Maybe disabling the rental restrictions that turn it off when you miss the payments requires Administrator, but surely nothing else. If we were talking about a security camera though, we might go the other way. Again it's a simple device with few functions, but this time, we'd probably remove the User level access and leave it with only Security and Administrator access. A GM determines what functionality is available at a given level, so there's nothing to stop a GM saying there is none at all on a given node or device.

Travel and Hacking in the Matrix

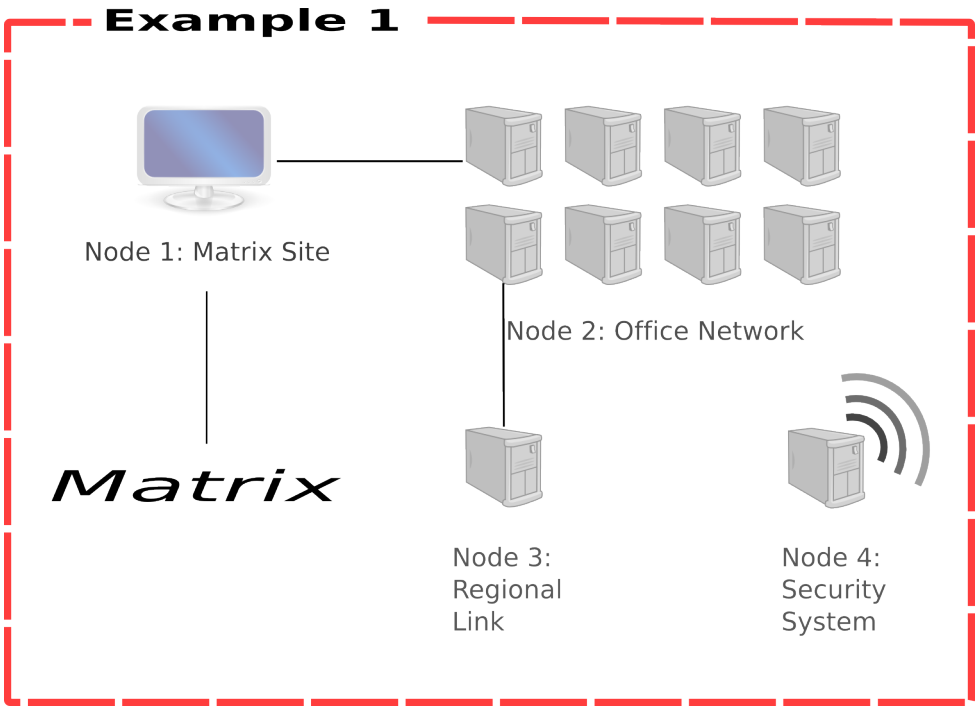
The question occasionally comes up of what is between nodes in the Matrix. By RAW, it doesn't

appear that anything is. You are in a node or you are outside a node, and if you are outside a node, you are wherever in the matrix you currently are.

Example Systems

Example 1: Small Company Office

Notes: *This is an example of a small company's network. It's geared toward a beginning Shadowrunner in terms of challenge offered. Most starting hacking characters should be able to go through it without too much trouble, and even a character with secondary hacking skills could manage it with a greater degree of risk. What it does do is give a new hacker a primer in how to go about breaking into an office system. There are enough pitfalls in hacking for the inexperienced player that a low-security system such as this can still pose plenty of risk. The regional link is the dangerous node.*



Node 1 - Matrix Gateway (System 3, Response 3, Firewall 3, Analyse 1):
Purpose: A chokepoint system that guards remote access to the internal systems of the site and manages all external connections.

Accessibility: This node has a matrix address tied to the company and can be located on the matrix

with a "Easy" Data Search roll - Data Search + Browse (2, 1 minute). The node can be accessed wirelessly from within the building.

Agent (Pilot: 2, Analyze 1): A user-interface system operates on this node to deal with visitors, i.e. take messages for the company, direct people to the appropriate person for their enquiry, etc. In VR, it takes the image of a japanese elf in a crisp, tight suit. The corporate logo glitters in gold on her lapel and her face is VR perfection. If in AR, then the secretary's face appears as a connection icon in the interface. It is capable of holding moderately sophisticated conversations in areas of its expertise. If unable to deal with a visitor, it will contact a (meta-)human for assistance. The agent will approach any visitor to the node that it detects with a matrix perception test (Pilot Rating + Analyze vs. Hacking + Stealth). If "killed", the agent will be restarted later.

Node 2 - Office Network (System 4, Response 4, Firewall 2, Analyse 1):
Purpose: The mesh of terminals and servers in the office which the employees use for their day to day work. All the systems comprise one big integrated node. Logging on to almost any terminal in the building is logging onto this node.

Accessibility: This node has no direct external access to the matrix. It is subscribed to both the gateway node (Node 1) and the Regional Office Sub-System (Node 3) and can be accessed from both of these. Note that any authorised user accounts gained from hacking Node 1 are not necessarily valid for Node 2, meaning it has to be re-hacked. However, the reverse is not true. This means that hacking all the way in from the outside is harder than hacking via the office building's internal wireless signal.

IC (Pilot 2, Analyze 2, Attack 2, Armour 2): The purpose of this IC is to investigate and deal with any unauthorised intruders on the network. It is normally inactive and will only be triggered if the node itself detects an intruder or if it is approached / attacked by an intruder. After doing so, it will remain on alert for up to an hour, investigating any other intruders. Note that when the IC activates, this reduces the node's repsonse time to 2. The IC will not pursue users beyond the current node, but it will send an alert to it's masters if left active after a confirmed encounter with an unauthorised user.

Matrix / AR Imagery: This is a standard off-the-shelf Renraku "White Samurai" package. The corp haven't even modified the standard oriental swordsman imagery or gleaming white colour. If an AR user is attacked, he will likely see diagnostic and security messages flashing across his interface.

Node 3 - Regional Office Subsystem (System 4, Response 4, Firewall 3, Analyse 2):
Purpose: This node is a sub-system of the remote, regional office system. For practical purposes it is part of another system and acts as a choke-point preventing unauthorised access or usage by ordinary employees. From here, a hacker would proceed to other office systems within the company, but that is beyond the scope of this example. This node will likely not represent an actual machine within the office, but a shared network with other offices and can be used for secure meetings between regional offices, shared data, etc. Remember that a node need not be a physical device. It can also represent a network and it makes no difference if that network fits into a single office, or if the connectivity runs across several sites. The technology remains the same.

Accessibility: This node is accessible only from the internal network of this office (and other regional offices). It is not directly accessible wirelessly. That is not to say that a user could not be connected to the system through a wireless commlink, but that they would be connected first to Node 2 and then make their way from there to Node 3. A user account valid for Node 2, is not necessarily valid for Node 3, meaning that the node must be hacked independently of any previous successful hacks into Node 2. The reverse is not true, however, should a user enter from the regional office.

IC (Pilot 4, Analyze 4, Stealth 5, Track 3): The security of this node is important and it is not sufficient to merely boot off an intruder. Instead, it is necessary to locate and investigate the intruder. The IC on this node is active, but will normally be running on Stealth and Analyze. On detecting an intruder (whether through it's own analysis of subscribed users or through the node going on the alert), it will load the Trace program from a data store in the node itself. This can alert savvy hackers who notice the sudden degradation of the node's response time but did not detect the IC on entering. The IC attempts to locate the user with an extended Track test (SR4, pg. 219). If the user is connected to a physical location off-site then either corporate security or Lonestar will be passed the details. If the user is located within the premises then details are immediately passed to the security systems. In all cases, information is preserved for future investigation. If detected, the IC has a visual representation as a grey-clad electro ninja. Again, Renraku off-the-shelf imagery.

Node 4 - Security System (System 2, Response 2, Firewall 4, Analyse 3):

Purpose: This node controls the security cameras, door locks, etc. throughout the site. It *only* has Security and Admin levels of access, meaning any hacking attempt must accept these penalties. Individual cameras, doors, etc, can be attacked on their own of course, but access to the security node is the real prize. There is no IC on the security node, but it is frequently interacted with by the security staff, so care must be taken not to take any actions that will alert those using it. E.g. Edit actions should be taken to pass false images back to the terminals in the security office, so that cameras that are turned off continue to appear to function, etc.

Accessibility: The node is accessible wirelessly throughout the site, but has no direct connection to the other nodes.

Agent (Pilot: 3, Analyze 2,): A user-interface system operates on this node to deal with visitors, i.e. take messages for the company, direct people to the appropriate person for their enquiry, etc. In VR, it takes the image of a japanese elf in a crisp, tight suit. The corporate logo glitters in gold on her lapel and her face is VR perfection. If in AR, then the secretary's face appears as a connection icon in the interface. It is capable of holding moderately sophisticated conversations in areas of its expertise. If unable to deal with a visitor, it will contact a (meta-)human for assistance. The agent will approach any visitor to the node that it detects with a matrix perception test (Pilot Rating + Analyze vs. Hacking + Stealth). If "killed", the agent will be restarted later.

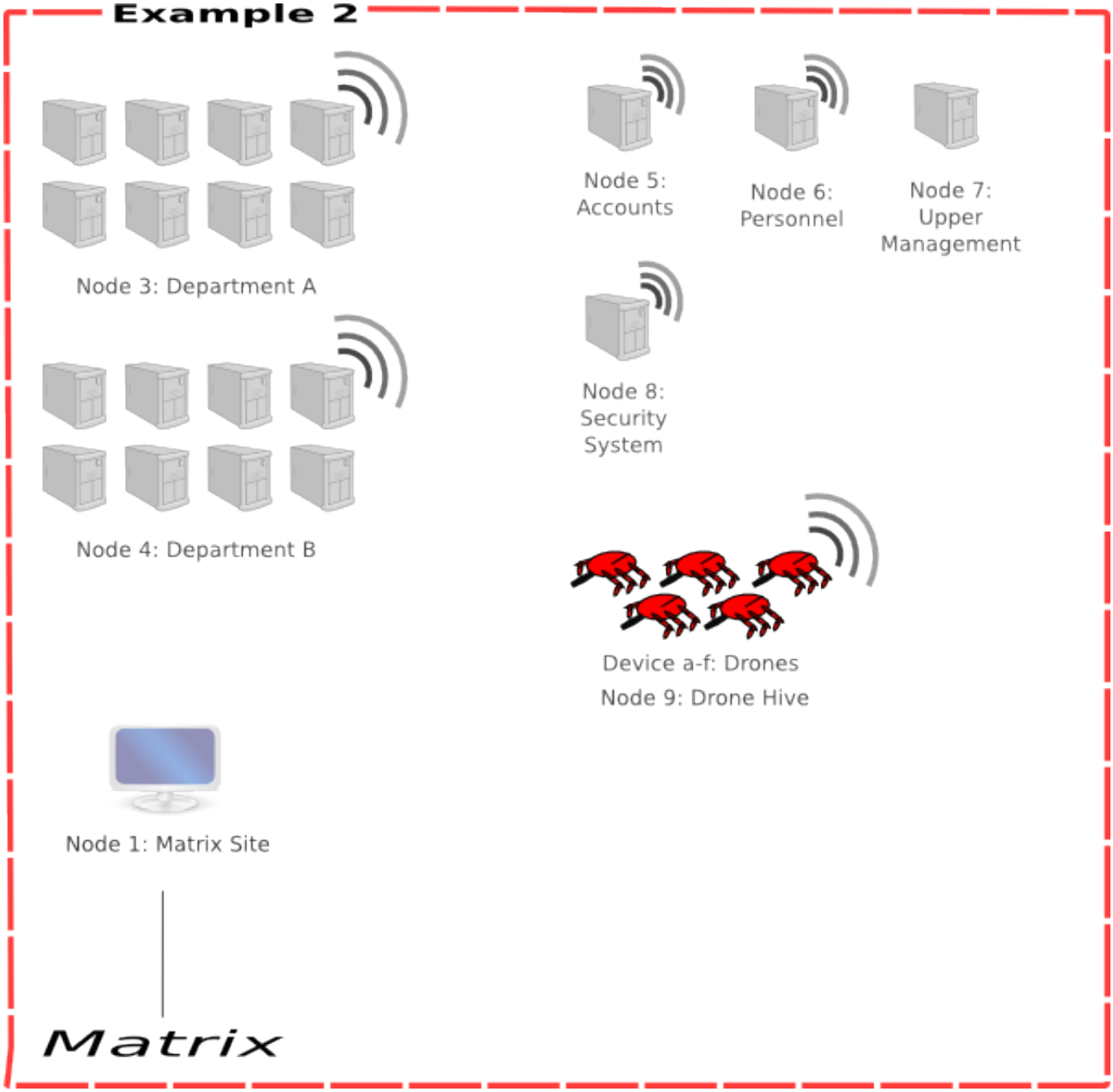
Suggestions for changes:

Swap the IC on the regional sub-system node for something more direct if that suits you better. And

you might want to add an Armour program if you feel it's too vulnerable. Running a sample encounter between the PC and that node / IC to see if it hits the balance is a good idea.

Example 2: Large Corporate Site

Notes: *This is intended to be a reasonably secure corporate office. It could be the headquarters of a mid-sized corp, or a regional office of one of the AAA "Megacorps." If it's the latter, then the matrix site will undoubtedly have a lot of corporate imagery and themes running through it. Whilst the site is not unbeatable by a long shot, it is well-structured and an incautious or weak hacker has a good chance of getting into trouble. As will be seen, even a pure AR hacker might end up in serious drek, whilst the hacker that goes full VR will appreciate her extra dice. The expectation is that the hacker will probably go in with the rest of a team and thus take advantage of direct access to some of the site. It is still possible to successfully achieve the same things by hacking in remotely, however. A couple of suggestions for altering this are at the end of the example.*



Node 1 – Matrix Site (System 3, Response 3, Firewall 4, Analyse 4):
Purpose: This node serves as a switchboard for the office, accepting incoming messages and calls and enquiries, and directing them to the appropriate recipient if unable to deal with them itself. There is no IC installed, but the system will report any alerts to the rest of the nodes on the site attracting the notice of either an agent or a security decker.

Accessibility: This node has a matrix address tied to the company and can be located on the matrix with a "Easy" Data Search roll - Data Search + Browse (2, 1 minute). The node can also be accessed wirelessly from within the building. Note that for "user" level access, no hacking attempt is actually required as this is a public node. However, user level access is limited to requesting information and services from the resident agent.

Agent (Pilot: 3, Analyze 2, Armour 1, Medic 1): A sophisticated and robust user-interface system operates on this node to deal with visitors, providing an efficient information service for visitors, e.g. directing calls to the suitable person or department, providing information on services, etcetera. It is a quality program, not one, but two cuts above the average UI agent and will carry on a near-human level of conversation within its areas of knowledge. The agent will approach any visitor to the node that it detects with a matrix perception test (Pilot Rating + Analyze vs. Hacking + Stealth). If "killed", the agent will be restarted later. It is also capable of conducting basic repairs on itself if necessary. It is not intended as a security measure, but it is intended to be resistant to mild cyber-attacks.

Node 2 – Site Management (System 2, Response 2, Firewall 2, Analyse 2):
Purpose: This node has limited functionality and provides a range of simple functions for subscribed users. These include generating AROs to guide visitors to the appropriate area (typically by arrows appearing on the floor, visible only to them), similarly directing people during a fire alarm, room bookings for meetings, choice of piped music and other such tasks, useful to only the most imaginative of runners.

Accessibility: This node is available wirelessly throughout the site, though it spills out only marginally beyond the company's actual boundary. Valid accounts gained from hacking this node, will not be valid for other nodes in the site.

Access Level: Most of this node's functionality is available at user level. Security and Administrator access do not offer much more, though Administrator might offer access to log files, etc., or allow one to shut things down.

Important Note: The display of AR information to visitors or staff does *not* indicate that the node is tracking everyone on site (and so cannot be used to locate guards, etc). It works on a request-response basis, meaning people have to ask it for information first, i.e. from their commlink.

Node 3 – Department A (System 4, Response 4, Firewall 3, Analyse 3):
Purpose: This mesh of terminals and servers cover most of a floor and represent a single branch of the company's business. When the employees come into the office and login to a terminal, they are

logging in to this node or the similar node on the floor above (Department B). Throughout the day, their icons can be seen buzzing about the internal VR imagery of the node, engaged in all sorts of hectic work.

Accessibility: The wireless signal rating of this node (managed through many small repeaters throughout the building) does not extend much beyond the main office building and certainly not beyond the perimeter of the physical site itself. It does not have a direct Matrix connection, but is connected to the Matrix interface (Node 1) so that connections can be made from within to the outside world and vice versa via the proper route (i.e. a hacker must first go through the connecting node). Accounts valid for this node are not necessarily valid for other nodes in the site.

IC#1 (Pilot 3, Analyze 4, Attack 4, Armour 4): This IC is normally inactive but will spawn if the node goes on alert, whether from a direct hack attempt or because it receives a general alert from other nodes. Though it may not entirely be a threat in and of itself, it can provide a distraction and protection for its companion tracker IC.

IC #2 (Pilot 4, Analyze 4, Stealth 4, Track 3): This IC will normally activate alongside the more active IC in the same node. For that reason, a hacker may not notice the stealthed IC that poses a much more sinister threat to them because they will either not take the Simple Action to observe in detail (and even then, the net hits may be insufficient to provide detailed information on what the "agent" is doing) or else may not keep Analyse running as a program whilst engaged in cybercombat. If the hacker has not spoofed his data trail effectively, then this IC may determine his real location fast enough to be a serious threat.

Node 4 – Department B (System 3, Response 4, Firewall 4, Analyse 4):

This node is similar in most ways to Node 3 (Department A) and serves a similar function. It is a smaller, slightly more secure network, however. Replace IC#1 with the statistics below, however:

IC #2 (Pilot 4, Analyze 5, Attack 5, Armour 5, Medic 4)

This is a substantial and dangerous security program, a very professional piece of software.

Node 5 – Accounts (System 3, Response 3, Firewall 4, Analyse 4):
Purpose: This is a small, secure node that has a much reduced list of legitimate users. User level access can gain access to files, but not damage any records or make alterations. To do that would require Security level access, and to conceal evidence of tampering by altering historical records, would require Administrator level access, due to the permissions set on the archiving / auditing process.

Accessibility: The wireless signal rating of this node (managed through several small repeaters does not extend much beyond the accounts office in the building. Thus a user who has made her way into the accounts office can subscribe to this, and can subscribe to the Department Nodes at the same time

as these expand throughout the building, but someone at a terminal in Department A for example, may not be able to make their way to the accounts node unless they can find an intermediary link, such as the mentioned user who is subscribed to both (and in which case they would also have to make their way via that users comm or terminal). However, at certain (GM determined times), the accounts node does need to access other nodes in the building and will activate a wired link which is normally turned off at its end. With the appropriate physical security, a GM can use this to add an interesting schedule to the structure of the run.

IC #2 (Pilot 4, Analyze 4, Attack 4, Armour 4, Medic 4): This IC is normally inactive but will spawn if the node goes on alert, whether from a direct hack attempt or because it receives a general alert from other nodes. It is quite dangerous.

Node 6 – Personnel
This is similar to Node 3 and also contains access logs and work schedules for the staff.

Node 7 – Upper Management (System 5, Response 5, Firewall 4, Analyse 4):
Purpose: This is the serious node where paydata is most likely located. It has a very exclusive user list. Its matrix attributes are above average because the IC within it remains active even when the node is not on alert.

Accessibility: This node is not accessible wirelessly. It is only accessible through jacks in the directors and company secretary's offices. If a user is subscribed to both this and another node, then it may form a bridge if the commlink or terminal can be hacked, as with the accounts node. Also, one possibility would be to have a drone physically connect a commlink to the jack to provide a wireless link (though it would of course have to be loaded with an agent that was capable of hacking access).

IC#1 (Pilot 4, Analyze 4, Attack 4, Armour 4, Black Hammer 4): Whatever this company is up to, it can't be good, because they're running black IC on their node. “There was nothing about *that* in the company brochure, chummer!” The IC will investigate any visitor to the node independently of the node itself. The GM may also wish it to react if it is able to identify illegal programs running on the visiting persona (the MD doesn't normally load “Attack”). Given the exclusive list of those eligible for access to this node, it would not be unreasonable for the IC to even try to contact the legitimate user list to see if they really are in the office, or tucked up at home in bed. The hacker should be allowed Matrix perception tests to get an idea of what the IC may be doing, however. Whatever it does, this IC is highly unpleasant.

Pay Data (Encrypt 3, Data Bomb 3): This file is what the hacker wants. Alas, poor hacker, it is both encrypted and bombed. What this means is that the file is a running program. In the Matrix of 2070, almost nothing is a pure, static file of data. Everything is a running process that comes with its own interface, matrix iconography, etc. To take the data from the node, the Hacker must first defuse the data bomb and then decrypt the file. Any attempt to decrypt the file without defusing the bomb will destroy the data and quite possibly damaging the accessing persona (the hacker). And all this must be done under the nosey interest of the nodes black IC (or else in the frantic “time-running out” period

after knocking it offline while the alerts are shooting round the system and the company hackers are getting out of bed). Rules for defeating encryption and data bombs are in the main rulebook.

Node 8 – Security System (System 4, Response 4, Firewall 4, Analyse 4):
Purpose: This node is the security interface for the guards and maintains all of the physical security measures. If a motion sensor trips or a camera malfunctions, it is reported to this node. If this node crashes, then the security office loses access to all its camera feeds, location tracking of guards etc. For a physical intrusion by a shadowrunning team, this node is a prize goal.

Access Levels: This system has virtually no functionality at User level access. It will basically register your location and accept alerts from that user. This is used by the standard guards. The hacker player will not necessarily know how useless user level is before attempting to hack in, however, so valuable time may be wasted. At security level, access to camera feeds, drone locations, etc., becomes available. Essentially, it remains read only, however. Administrator access is required to do such things as stand down drones, boot security level users off the system, kill cameras, etc. Without this, the hacker is reduced to sabotaging cameras and motion sensors one by one, etc.

Accessibility: This node is accessible wirelessly throughout the site but has only one direct connection which is to the "Drone Hive." If a GM wants to complicate things, then the node can have wired connections to most of the cameras, doors, etc. and only have one or two low-signal wireless access points for communication with the drones as they go past these points as part of a routine circuit of the complex. This would be inconvenient for the security staff generally, however. They could perhaps alert drones via their comms but this may open up a larger security weakness.

IC#1 (Pilot 4, Analyze 4, Attack 4, Armour 4, Attack 4): This IC conducts its own analysis of any visitors. Additionally, there are likely to be several personas representing the guard captain and staff already active in the node who will notice a new user logging on unless successfully stealthed. A hacker who can hide from the IC can probably hide from the users... but the number of them can shorten the odds.

Node 9 – Drone Hive (System 4, Response 4, Firewall 4, Analyse 4):
Purpose: This node is a distributed network run by the drones on the site. It provides co-ordination functionality as well as an additional level of security to guard against a drone being subverted.

Access Levels: User level access is pointless for anything but a drone as all it allows is to report location, condition and alerts. Unless the hacker has some ingenious plan to masquerade as a drone (actually, that's quite a good plan as it would bypass the motion sensors, etc.), the hacker will need security level access or above. Security level access is similar to the same on the security node as it will provide access to large amounts of information. It may also allow the hacker to direct drones, or stand them down, etc., but not to shut them down and commands will be very quickly countermanded by the node itself, leading to amusing "now they shoot you now they don't" attacks by the drone squad. Administrator access will be required to achieve anything more.

Accessibility: This node exists wirelessly throughout the site. However, the drones that comprise it all operate in Hidden mode making it hard to initially detect the node (see rules for detecting Hidden comms in the main book). It does maintain a continuous link (subscription) to Node 8 (Security) however, so can be more readily noticed from there. Likewise it will be obvious from any drone that is hacked as they are all subscribed to it.

IC#1 (Pilot 4, Analyze 4, Attack 4, Armour 4, Exploit 4 (Track included on Node, but not normally loaded): This IC exists on the node to ensure there is no subversion of any of the drones under its command. On detecting a drone doing anything that was not instructed by the node itself, the IC will travel into that drone to engage any intruder that it finds (anyone other than the resident pilot program in effect). As it has security level access to all drones, it will be difficult to shut out unless the hacker has administrator access on that drone and immediately starts removing other accounts. If the hacker is spoofing, he may find the IC trying to hack his commlink to get at him.

Device a-f – Drones (System 4, Response 4, Firewall 4, Analyse 3):
Pilot: (Rating 3): This program runs the drone. If the hacker wishes to keep control of the drone, he will probably need to shutdown this program in cyber-combat. Spoofing commands to the drone may be more effective, but will result in continuous battles for control with the Drone Hive node. The drones have only Security and Administrator level access and all operate in Hidden mode.

Device m1-m5 – Motion Sensors (System 2, Response 2, Firewall 4, Analyse 3):
Rating 2 (all attributes): Each of these can be hacked and disabled, or their feedback edited, but each must be done individually and any failure will go straight to the security node to which each is subscribed. The better approach is to hack the security node itself, if the hacker is capable of that.

Device v1-v40 – Cameras (System 2, Response 2, Firewall 4, Analyse 3):
Rating 2 (all attributes): Each of these can be hacked and disabled, or their feedback edited, but each must be done individually and any failure will go straight to the security node to which each is subscribed. The better approach is to hack the security node itself, if the hacker is capable of that.

Device l1-l15 – Locks (System 2, Response 2, Firewall 4, Analyse 3):
Rating 4 external locks (all attributes) / Rating 2 internal locks: Each of these can be hacked and disabled, or their feedback edited, but each must be done individually and any failure will go straight to the security node to which each is subscribed. The better approach is to hack the security node itself, if the hacker is capable of that. Access logs are kept of lock openings outside of normal hours. The security node will flag up usage of the external locks during this time for the security captain's attention.

Supposed Hacking Route: Part of the design of this system is that the security system is a closed network. This makes things extraordinarily difficult for the hacker in the initial phases. In order to disable or subvert the cameras and motion sensors *en masse* the hacker must first get past some of them in order to reach the security system. This is an interesting tactical situation. The team's first priority on gaining access should be to take control of the security system generally.

Example 3: Hacker Bar

This hacker bar exists purely within the Matrix. It has no physical equivalent and if the data within it exists anywhere, it is scattered across a hundred datastores scattered around the world, shifting from one to the other according to the systems that have been cracked to support it that week. Only with diligent searching or a contact in the know, can its Matrix address be located and with each shift, that address will change. Whilst regulars will (carefully) swap details of where it may be found with each other, those not in the loop, or who have made themselves unpopular, must begin the search anew.

Node 1: (name: "*Caladan*") (System 4, Response 4, Firewall 4, Analyse 4):

Purpose: This node is the public front of the bar.

Access Levels: This system has a Public (user) level access which is available to visitors and does not require hacking to obtain. The node is protected primarily through its obscurity and it would be of little use if people who came to the bar were unable to enter. User level access allows one to enter the node and take advantage of the basic functionality. It does not allow one to run independent programs on the node (e.g. Agents). An agent could run elsewhere and visit the node however. Security level access is not normally granted to anyone but the people who run the bar itself. A hacker can hack their way up to Security, but this will very likely be noticed by either the administrators themselves (at least one of which is normally online) or passed along by other users. One thing that happens a lot in this bar, is people analysing each other's persona.

Accessibility: This node moves about, switching from disposable matrix address to disposable matrix address, sometimes a fictional employee's personal site at a company, sometimes a home-owner oblivious to the virtual commotion going on under his nose, linked to his address. If a character knows where the node is to be found, then they can go directly to it from anywhere on the Matrix. If a character does not know where to find it and can't beg an address from a contact or friend, then they are in for a long search. Roll Data Search + Browse (16, 1 minute). Needless to say, it can be quite difficult for lesser hackers to locate (use the rules for capping the number of rolls in an extended test) and most try to cultivate a good network of friends there in order to avoid this hassle. Naturally the people in charge of the place know where they've put the node, and the information usually trickles down from them quite quickly.

IC#1 (Pilot 4, Black Out 4, Armour 4): The Hackers don't mess around when someone starts interfering with their good times. Though normally passive, this bruiser IC stands ready to remove any hackers that cause problems and they'll wake up with a less than pleasant headache, too. The IC obeys the most senior person present (administrator, then security, but never just public / user access) but failing that, is usually smart enough to recognize the initiator of any aggression and will act accordingly. Note that mob-rule tends to prevail in Caladan, and an aggressive hacker might end up wishing the IC had got to him before the other patrons.

Node Functionality:

In addition to providing a simulated bar with many booths and tables where personas canrelax over a

VR coffee, trade info and data, Caladan provides a range of functionality. Users can hook themselves up with one of the many SIMs that are traded about the place. If they're hot-simming, then a few nuyen will let them try out some of the BTL SIMs that the node has on hand, too. Additional nodes can be activated, to create private rooms for those that need them. Visitors can also adapt the VR-styling of the node within reasonable limitations, though security level users and above can over-ride or remove these privileges and users who annoy other patrons quickly find themselves put back in place.

Node 2: (name: "Giedi Prime") (System 5, Response 5, Firewall 5, Analyse 5):

Purpose: This node serves a dual purpose. Firstly, it provides a more select 'backroom' to Caladan, in which more secure or long-term patrons can converse with their peers and enjoy less interruptions by newcomers. Secondly, it provides an arena in which hackers can settle their differences persona to persona, whether in friendly combat... or to settle a grudge.

Access Levels: This node has a User level access but this is not available to visitors normally – members only. Those who hack their way in may be hassled by the resident IC, but typically the resident security level members allow anyone who hacks their way in to remain and call it off. User level access does not allow one to run independent programs on the node (e.g. Agents). An agent could run elsewhere and visit the node however. Security level access is not normally granted to anyone but the people who run the bar itself. A hacker can hack their way up to Security, but this will very likely be noticed by either the administrators themselves (at least one of which is normally online) or passed along by other users. Depending on who the hacker is and whether or not they behave, they may be allowed to keep their security status, having 'earnt' it. Or they may get dumped.

Accessibility: This node is only directly accessible from Caladan and Arrakis. Theoretically, it could be hacked directly if a hacker knew where in the vast, sprawling architecture of the Matrix it was being run at any given time, but lacking an actual Matrix address, this is a near impossible task. Essentially, users must first enter Caladan and then either enter the Giedi Prime node using a legitimate user account, or else hack their way in. It is quite common for newcomers to first gain access through hacking their way in, and they will eventually be given a regular user account in recognition of this.

IC#1 (Pilot 5, Black Out 5, Attack 5, Armour 5): An extremely nasty piece of IC software originally boosted from a Renraku system and thoroughly sanitised, this IC will use Black Out whenever it can, or fall back on the Attack program only if it must.

Node Functionality:

As with the Caladan node, side rooms can be created if privacy is required. Users can also display information in various media in the node. Chiefly, though, Giedi Prime's main resource is a venue where hackers can discuss interesting developments in programming and the Matrix with skilled hackers.

Node 3: (name: "Arrakis") (System 6, Response 6, Firewall 6, Analyse 6, Stealth 6):

Purpose: Everyone guesses that Arrakis is there, but not many know how to get to it. Even fewer are able to. Used primarily by the hackers that set up and run the Bar, it is a secure place to discuss precious exploits, the trustworthiness of other hackers and what the secret manoeuverings of the megacorps. Sometimes others are brought here as guests. It's a rare event for someone new to be granted regular access, and usually only if they have successfully hacked themselves in and defeated the resident IC in cyber-combat, too. Even then, if the administrators do not feel they can trust the newcomer, then exploits will be fixed and the user will be removed. Much of the software (including the IC) is customised or written by the bar's administrators, everyone of whom is a skilled hacker, and everything is of a very high standard.

Access Levels: This system has only a Security level and an Administrator access level. There's little point in creating a user-level account as the only people who are given access are those that would typically have such access. There are no casual visitors to Arrakis, and the removal of User level access, merely adds to the difficulty of getting in.

Accessibility: This node is accessible only from the Giedi Prime node. It maintains no connections to any other node and the administrators never create such a connection. Additonally, the connection from Giedi Prime is itself hidden, requiring a Matrix Perception test against the node's Firewall + Stealth. Only if it is located, is it then possible to proceed to hack it.

IC#1 (Pilot 6, Black Hammer 6, Armour 6): A combined effort of several very talented hackers, this IC program (affectionately called "Feyd") is literally lethal. The node does contain other programs that the IC can load in place of Black Hammer (either Black Out or, in the unlikely event that someone using AR gets in, Attack), and the Administrators may adjust depending on whether they think the visitor is just a hacker with ideas above his station, or if they think the visitor is an actual threat. At least one of the administrators has proven herself willing to kill to protect the secrets of what goes on here and depending who is around, a hacker may or may not find mercy. Typically, the IC attacks with the words "You are not the Kwisatz-Haderach" before pummelling the hapless visitor.

Node Functionality:

The main service provided by Arrakis, is simply being there and being secure, but the GM can assume that it provides a range of tools to examine code, analyse and encrypt / decrypt information, etc.

Example 4: Home Office System

Example 5: Corporate Enclave

- Game Node
- Security System
- Private Sites (parents? residential spokespersons?) and community forum

- home nodes
- media distribution
- lighting systems, power and other infrastructure
- parking / garage system
- accounts and billing systems (power usage, etc).