Redjack's Matrix Primer

SR4.5 v.08

In 2075, the matrix fundamentally changed. For the average user, the change was mostly insignificant. They could still buy their morning soycaf, upload to their Me Feeds® and check on the dismal state of their retirement account. For those of us in the shadows, the game changed, we lost a lot of control, and the costs of doing business went way up.

What is this?

This document is an overview of the matrix from multiple perspectives. It is a narrative to provide an understanding of the SR5 matrix, contrasted against the backdrop of an SR4 understanding of the matrix. Some liberties have been taken in explanations in order to make definitions plausable.

This document takes some creative liberty on the story: It is written under the auspice that the SR5 matrix is an evolution of the SR4 matrix. That the Public Grid is the remnants of the SR4 matrix. When the terms “Matrix v4”, “mesh”, or “legacy” is used, it refers to SR4. When the terms “Matrix v5” or “next generation” are used, the reference is to SR5.

This document is also written in a fashion that elevates the complexity step by step matching the narrative to the needs of a character's level of technological understanding. Matrix 101 targets the average matrix user and how they see and use the matrix. Next, the average shadowrunner. Evolving third into the team's hacker/decker's understanding and finally, that of a technomancer.

This primer targets two real-life audiences simultaneously: New SR5 players and SR4 players seeking to understand how the SR5 matrix is different than SR4.

THE MATRIX

The Matrix 101: The Average User

From the time we're born until the time we die, we are electronically connected. Almost all of the money is now electronic; bartering still exists among the SINless and, to a lesser degree, various printed scripts are used as currency. However, given the ability to counterfeit the various script easily, they are quickly fading into disuse. Documents of citizenship, passports, and other government or corporate issued documents from drivers licenses to professional licenses to weapon permits are all digital.

There are two paired basic components that every meta-human, not raised in a cave, is familiar with for accessing the matrix: A commlink and a persona. A commlink is the cell phone sized piece of hardware and the persona is the interface and software that rides on the commlink's operating system to present an online identity for a user. A citizen, corporate or government, also has a SIN (System Identification Number). A SIN is used to uniquely identify a citizen; a SIN is comparable to the super version of a modern day passport. A person with a SIN is a SINner.

Identity is a complicated thing on the matrix. The average user will have one commlink, one persona, one SIN. Linked to that those, they will have various legitimate accounts, licenses, and digital keys. They will also have one commcode (think phone number and email address rolled into one) and one identity. This combination completely replaces a modern person's wallet, passport, cell phone, personal computer, and most of their keys.

A number of methods exist for accessing a commlink. The first is via a piece of cyberware called a datajack (or an implanted commlink) which is the most reliable form of DNI (direct neural interface). A datajack may interface with the commlink either via fiber-optic cable, skin-link, or wireless connection. The second method for interfacing with a commlink are with trodes (*electrodes*) assembled into a net, headband, or a wireless mesh of individual trodes affixed to person's head with nano-paste. This second method also allows for DNI without sacrificing essence. The third method is via a combination of eyes, glasses or contacts with imagelink vision enhancement, earbuds or a headset, and AR gloves. The final method is simply using the commlink's screen, speakers, and touchscreen to interface with it. It should be noted that the various inputs/outputs of the latter two methods may be interchanged at will.

For those who access the matrix either via DNI or imagelink, the world of augmented reality (AR) is opened up. AR effectively paints a digital layer over reality in a user's field of vision. AR can be life-like to the point of being indistinguishable from reality. AR can be used to dress up the appearance of a physical location and it can also be used to present location based notices or spam to all users in an area. It can be used to feed in displays only to an individual user to manipulate their commlink or other nodes they are accessing, either nearby or half a world away.

Passing digital data between people and/or systems uses an interface known as an ARO (pronounced: *arrow*). An ARO is simply a visual object used to represent that data in AR. Example: Handing someone an ARO business card that exists only in the matrix.

A second, more immersed method exists for accessing the matrix: Virtual Reality (VR). In order to fully immerse into VR, a user requires both a sim module and a DNI method for accessing the matrix. Once a user immerses in VR, a person's motor functions are completely overridden to keep them from thrashing about and harming themselves. Standard VR, with all the safety protocols in place is referred to as 'cold sim'. Hot Sim VR, where safety protocols are overridden to allow a person to interact with the matrix without buffers, allows a person to act considerably faster. Hot Sim also activates pain inhibitors, which stops a user from being distracted by any meat body sensations and making a person subject to lethal feedback from systems in matrix.

Hot Sim is required for BTL (better than life) chips. This, *digital drug*, provides sim experiences with emotional content that is outside the ranges that normal people can experience. Happier highs, sadder lows, sexual pleasures beyond reality. BTL is highly addictive and many addicts sink into depression and commit suicide; if they don't burn their brains out first.

For the average SINner, the matrix pervades every aspect of their life and without it they would be outside the flow of society. Their commlink is their alarm clock, their house key, their address book, their phone, their personal computer, their identification, their driver's license, their wallet and their checkbook; they would be lost without it.

It used to be that one could just open their search program (called web browser) and connect to one of several central sites that would have previously indexed all publicly available hosts (servers). From there, you simply went from host to host searching for the information you wanted. That time is a world away. Now, a browse program scours any data store to which the owner has permissions to access, and data is nuyen (standard currency), so most of the information that the average user gets is carefully controlled and edited.

The average SINner hears stories of hackers, technomancers, AIs and other matrix phenomena, but is never directly impacted by one. The average user walks through their life asleep.

THE MATRIX

The Matrix 201: Matrix Basics for the Shadowrunner

A shadowrunner needs to be worried about all the traces they leave in the matrix and all of the information that can be taken from their commlink. Little bits of data leaving an effective trail to them using their commlink's access ID (unique ID representing their commlink in the matrix). For legacy commlinks, one can buy hardware and software to routinely change that access ID in order to hide their data trail. For next generation commlinks those options have not yet made it to the black market. The options are currently limited to throw away commlinks when on a shadowrun or having a team decker along to protect them.

For the average user, one commcode is all they will need from the time they are born until they die. For shadowrunners, separate commcodes should be used to communicate with their contacts, Johnsons, friends and family; the more paranoid the runner, the more commcodes they have.

A shadowrunner may or may not have a real SIN and probably has one or more fake SINs to manage safe houses, bolt holes, various bank accounts, licenses, and the registration of vehicles & weapons. A great deal of care should be taken to manage SINs as once a SIN is burned (determined and reported to be falsified) the various accounts, licenses, and registrations associated with that SIN are also burned. Burned SINs must then be disposed of and a new SIN purchased to replace it.

As far as accounts and nuyen goes, a shadowrunner effectively has four ways to receive their illicit gains: get paid with a certified credstick containing some amount of certified cred, have certified cred uploaded to their commlink, have nuyen transferred into the bank account of one of their SINs, or get paid in script be it nuyen, dollars, or even some corporate script.

Certified cred can be validated online at anytime to insure that it is the one true copy of the cred. While this should be done quickly after receiving certified cred, it does create a data trail, even if only a small one. Certified cred can also be transferred to another credstick, transferred to a commlink, or laundered into an account tied to a SIN (real or fake), the latter option requiring a fee. Those with real SINs will also be assessed taxes on the gains laundered into their legitimate account. The various scripts suffer from both a lack of universal acceptance and high rates of counter-fitting.

A shadowrunner needs to be concerned about having their commlink hacked or worse yet, bricked (damaged and mode inoperable), by a hacker working for law enforcement or the opposition. Most times, this matrix over watch is facilitated by adding a hacker to the team. Other times a shadowrunner can only rely on their own firewall program.

Most shadowrunners don't care how the matrix works, just how they can exploit it and do what they need to do to protect themselves. They pay for multiple fake SINs as well as multiple commcodes and if they aren't a little paranoid, they aren't doing it right. One item of note for the paranoid shadowrunner is the fact that in addition to their persona having an icon in the matrix, the security aspects of the matrix force every wireless enabled firearm to have a separate, attached icon.

Most shadowruns require legwork to complete. Searching for data is always part of that legwork. Some things simply are not on the matrix but most data is out there somewhere. The average shadowrunner, without a team hacker to search for them, have few options when searching for data:

1) Search the matrix yourself. Search data stores, Me Feeds, blogs, and other publicly available hosts. Matrix v4 commlinks require a browse program, v5 commlinks have the capability built in. This only works, however, if the information you are seeking is either posted to a public host or available on a secure host to which you have legitimate access.

2) Contract a hacker to perform the digital legwork. When all else fails and you simply have to have information that is not publicly available and you lack a team hacker, this is your final option. The only question is once they get the data, are they trustworthy enough to keep it on the down low? Or, can they be paid enough to?

** Command an agent program: It should be noted that legacy commlinks had the ability to run agents & browse programs as well as exploit and stealth toolkits to not only search the matrix but also infiltrate some secured nodes as well. Next generation commlinks simply lack the resources to run upgraded versions on the newer “secure by design” grids.

Matrix 202: Advanced Concepts for the Shadowrunner

PANs (Personal Area Network) are the collection of a commlink and the wireless devices slaved to it. That, of course, begs the question: What is slaving? Slaving a node (commlink or other stand alone device) is a logical function where it becomes linked in a master-slave relationship to another node. The master protects and in many ways, controls, the slaved device. In both legacy and next generation devices, a commlink may be slaved to another commlink.

THE MATRIX

In the legacy matrix, the two devices must remain in mutual signal range (be in range to communicate directly, without going across the matrix) or be connected via a fiber optic cable. The slave's mode also cannot be less restrictive than the master (ergo if the master is hidden mode, the slave(s) cannot be active mode). About the only way for a hacker to exploit a slaved node is trying to spoof a command to a slave, pretending to be its master.

In the next generation matrix, all devices connect to the matrix via an access point then to each other. This removes any range restrictions on slaving. While it extends protections from the master to the slave(s), it also makes the master vulnerable to hacking attacks on the slave.

Grids: Everything is interconnected via the matrix but you can't always access everything from the your connection to the matrix because of the separation of the matrix into grids. Grids represent either physical or logical separations of the matrix.

Users with next generation commlinks can select which grid they are on, subject to them having an account on the desired grid. Some lifestyles come with accounts on the various grids. While some hosts are on multiple grids, others are not. Although the different grids have different default AR and different corporate resources, for most users the difference is negligible. Let's discuss each type of grid:

The Public Grid: This grid is THE matrix from the post matrix 2.0 crash days until 2075. Using legacy devices, every wireless device connects to every other wireless device in mutual signal range automatically to form the "wireless mesh". With the advent of the new grids, the Public Grid has been augmented with access points to allow next generation hardware to access it. This matrix is free and open to all... and that is it's strength and it's weakness; no one controls the Public Grid. Congestion and spam are high; hackers run rampant and quality of service is a non-existent practice. A commlink cannot be connected to both the Public Grid and any of the other grids at the same time.

Local Grids: In 2074, corporations and municipalities began investing in the next generation of infrastructure, marketed as "secure by design". Access points for a local grid blanket a geographical area so that when a device connects to that local grid, it connects directly via an access point rather than via the mesh (which does not exist in the next generation hardware). Marketed as simply an upgrade to the matrix, this is, in fact, a brand new matrix that requires new hardware, new software, and is completely different than the matrix of the past.

Global Grids: There are ten global grids, one for each of the AAA corporations. A technology akin to a VPN (virtual private network) allows a connection to all global grids from anywhere on the planet via either the Local Grid or a satellite connection. By extension, all local grids of the matrix are required to provide priority support for connections to Global Grids. In many cases, the operator of a Local Grid may be one of the AAA corporations, but that Local Grid is still separate from their Global Grid.

Device modes are settings for commlinks (and other nodes) that describe how they interact with the matrix around them.

Legacy devices operate in one of three modes: Active, Passive, or Hidden. Active devices communicate with all devices around them. Active mode does not diminish the security of the device, nor affect spam filters, but it does broadcast the SIN of the user to all nearby devices. In some locations, it is illegal to operate in any mode other than Active mode. Neither Passive nor Hidden modes broadcast the user's SIN. While Passive mode does broadcast AR, the experience is less than optimal as system interaction is by pre-authorized access only and spam filtering is aggressive. Hidden mode AR is completely non-interactive and users in Hidden mode do not broadcast any AR.

What does it matter? Why not just run hidden anytime that it is not illegal (and a shadowrunner cares about legalities)? Its back to the issue of AR. Imagine you enter the lobby of a building, no people, but there is an interactive AR attendant. If you are running in Active or Passive the attendant the attendant notes you and attempts to interact. In active mode, you are automatically able to interact with it. In Passive mode, you must instruct your commlink to allow. In Hidden mode, interaction is not possible. What about just walking through the lobby, through the attendant, ignoring it? In Active and Passive modes you are broadcasting, so the AR moves out of your way to avoid "collision", maintaining the illusion that it is a person, instead of just an AR projection. In hidden mode, you go right through it; that's a social faux-paux. Change the example to a bar; You can't order from an AR menu in hidden mode and in passive mode you must take a moment to explicitly allow your comlink to interact with the bar node.

Next generation device modes are either Active or Running Silent; corporations and law enforcement don't want you to hide. Active resembles legacy Active, but Running Silent is unique. To be on the Matrix, you must be logged into an access point, so when Running Silent you are only mostly hidden. Your commlink spends a considerable amount of processing power covering your tracks and unlike Hidden mode, other commlinks can nearby find you without much effort. Running silent is not full proof and it is not hidden. Running silent is rather: obscured. It does reduce the data trail left by your commlink and it hides you from casual observation in AR, requiring an active attempt to locate a device. Unlike legacy devices, you always interact with AR around you.

THE MATRIX

The Matrix 301: Hackers and Deckers

Hackers and deckers are people who attempt to subjugate the matrix and bend it to their will. They do this with specialized, and many times custom, hardware and software. For hackers and deckers to do what they do, they need more than just super tools, they need a greater understanding of what the matrix is and how it works.

Let's start with the simplest part to understand: the tools and a brief history lesson. Twenty years ago, your average Jane or Joe used a device called a pocket secretary (think super, voice interactive smart phone). Matrix experts meanwhile used keyboard sized cyber-decks, which were simply referred to as *decks* and those experts were referred to as *deckers*. After the second matrix crash in '65, a matrix with nearly universal wireless access came back in vogue like it had been prior to the first matrix crash. Commlinks replaced pocket secretaries and had enough power that hackers could exploit anything and everything from a powerful, custom commlink equipped with the right software tools.

By '74, governments and corporations had grown tired of hackers running amok, so they built the next generation matrix, “secure by design”. It was brought online New Year's day, 2075. Next generation commlinks strongly resembled legacy commlinks in both appearance and function for regular people. For the matrix professional, they simply lack enough horsepower to make holes in this new matrix. Deckers were reborn when hackers realized they had to cobble together multiple commlinks with custom software to be able to once again crack the matrix. These Frankenstein commlinks, and their commercial counterparts (which resemble turn of the century tablets), are once again referred to as decks and their users deckers.

Before we dive deeper into how everything works, let's talk now about the tasks the hacker/decker performs for his/her team. When a team first meets, the first task is to get them together in the matrix to collaborate securely and privately. Depending on the tools available, this may evolve into a full fledged tactical network.

> **TeamNet**: This is the modern day equivalent to a matrix integrated conference call where the participants can share video & audio feeds, GPS data, and converse privately. A teamnet can be whipped up on the fly by a hacker.
>
> **TacNet**: This legacy, integrated tactical network took advantage of the mesh architecture of the matrix combined with the slaving of various sensors to take a TeamNet to the next level. Benefits included auto tagging of targets, as well as tactical recommendations to increase efficiency. Drawbacks include diverse sensor requirements and a minimal number of squad members to provide effective recommendations. Due to the lack of mesh support in network generation commlinks, TAC-Nets are quickly being depreciated through attrition.
>
> **PI-Tac (Personal Integrated Tactical Network)**: The next generation of the Tac-Net, this self contained kit comes with a sensor harness, software, and hardware license management unit that direct connects to a commlink or deck and requires a matrix connection. This system can work stand-alone, though low-end commlinks will limit scalability. PI-Tacs are prohibitive expensive.

The next task for the matrix support is to secure the team's matrix presence. Slaving a teammate's commlink or wireless enabled weapon to your deck is one way. In the new, secure matrix, this is definitely a requirement where the opposition includes a competent decker themselves. The power of your deck will limit how many devices you can protect so choose wisely.

Another tactic to protect your team is to assign an agent to provide overwatch, looking for hacking activity on team commlinks or gear. While not full proof, the agent can cycle through the various teammate's comlinks looking for *marks* (explained later) or other signs of hacking.

Now that your team is communicating and relatively secure, time to really earn your nuyen. Cracking other systems is the bread and butter of the team hacker. In the legacy matrix, when a company establishes a matrix presence, they set up servers and connect them to the matrix. In the next generation matrix, that presence is a host. A host can connect to one or more grids, but is not actually on or a part of a grid it connects to. In AR and VR all hosts appears overhead. In the meat world, a host exists in the cloud; it is redundantly distributed across multiple physical locations.

The threat level of a host varies from host to host, but even small commercial hosts are formidable with powerful firewalls. Some deckers, the brave and the foolish, take hosts on head to head. The others attack hosts via a physical connection to slaved devices, like a camera or a maglock. A wireless attack on the slaved device is as bad as attacking the host directly, but an attack via a wired connection on a slaved device will attack the device on it's own merits and place *marks* on the master.

Security levels of access are slightly different. Legacy security ratings are in one of three roles: user, security, and admin. Each incrementing level grants more rights on a given device or system. In next generation hosts, devices, files, grids, etc, access is measured in how many marks (matrix authentication recognition keys) someone acquires, up to three. Unlike admin access on legacy systems, three marks is simply more likely for you to be accepted as legitimate rather than a given.

THE MATRIX

Marks are unlike legacy security roles in more ways. When you get a mark on something, it leaves an AR/VR mark that is normally invisible to others. That said, a mark can be located if one is specifically looking for marks. Your marks do disappear when you reboot though. Unlike a role in legacy systems, you cannot simply transfer marks to others or grant them marks on a system you are not the owner. Some hosts solicit a mark: a public library, a bar after you pay the cover charge, etc.

Any given matrix object has a single owner and any person can own as many objects as they like. Ownership allows a person to find every object they own, on the matrix, always. Finally, ownership also includes registration in the master ownership registry.

Transfer of ownership is somewhat complicated. A legitimate owner may transfer ownership in about a minute. Illegitimate transfer of ownership for a piece of hardware begins with a replacement of the chips that uniquely identify it. This is an involved, delicate process that takes a considerable number of hours. A file is much simpler: simply copy the file, making yourself the owner of the copy, and delete the original. A hosts and a persona cannot change ownership once created. Why is ownership a wrinkle for shadowrunners? Corporations assign ownership of corporate assets to the corporation. Looted gear can be traced relatively quickly if used.

How about a host's defenses? We've briefly discussed the powerful firewall, how marks work, and ownership. There are two remaining host defenses to talk about: IC (intrusion countermeasure software) and spiders (corporate security deckers).

Once a host, or one of it's spiders, realizes there is an attack, loading IC is the first order of defense. IC are nasty bits of software that can crash your system, corrupt your commlink, track you to your physical location, or even kill you. Spiders can do anything a decker can do, but have the resources of the host and a more powerful deck at their disposal.

Speaking of decks, let's talk about decking. First thing to understand is that deck has variable configurations. It can be optimized for defense, attack, data processing, or sleazing. Attacks can be used on matrix devices or personas.

Hacking is performed in one of two ways: Brute force or sleazing. Each has a drawback. In a brute force attack, the target knows that they are under attack. In a sleaze attack, a failure generates marks on your deck to target.

Back on the grid, there is a threat we have yet to discuss: The Grid Overwatch Division (GOD). GOD has a separate division for each of the grids (referred to as *demi-GODs*). The agents for each of those divisions are referred to as G-en. These G-men watch for illegal activities and once that confirm a significant level of illegal activities, they converge on the offenders in both the matrix and the meat world.

The final, and one of the most important, factors for a hacker to understand is noise. Noise is anything that interferes with the matrix signal. Distance is the first factor of noise. The second most prevalent pair of factors is spam zones and static zones. A spam zone is an area where signal spam degrades the quality of service. This signal spam is from one of two sources: true commercial spam and simply an overabundance of matrix subscribers in a geographical area stressing the infrastructure capabilities. A static zone is very similar to the latter; it is the inadequate amount of infrastructure. Barrens, rural areas, or areas where only a satellite signal is available service. The final aspect of noise is interference like active jamming, immersion in salt water, being underground, or under dense foliage.

Unlike the average Joe, for whom the matrix appears mostly the same, for the hacker it is a brave new world. From grids to hosts, noise to cyerdecks, the transformation from hacker to decker will not occur with adjustment to the new paradigms. In the old matrix, things were dangerous, but with G-men actively seeking you now, the stakes have risen.