LA MALLA

Antes de La Caída la humanidad interfasaba a través de internet, redes interconectadas que servían como la columna vertebral tecnológica para la evolución de la world wide web. A pesar de que empezó como un medio electrónico para recabar información de varias fuentes (reemplazando incluso sistemas de información aún más viejos basados en papel), las sucesivas generaciones enfatizaron las comunidades digitales y hospedaron servicios como sitios de networking, wikis, blog y comunidades. Esto facilitó la apertura, la colaboración y compartición, sentando así las bases de una sociedad de la información moderna e interconectada. Fases posteriores enfatizaron la interacción inalámbrica, la geolocalización, las aproximaciones semánticas a la web y consiguieron saltos cuánticos en el reino de la interacción del usuario con el advenimiento de las interfaces cerebro–computador, realidad aumentada (RA), realidad virtual (RV) y reproducción de experiencias (RX).

Este entorno, a la par que el crecimiento exponencial de la potencia de procesamiento y la capacidad de almacenaje y memoria, creó un camino evolutivo para el desarrollo de agentes inteligentes, diseñados para aumentar la capacidad humana de procesamiento de información, que se transformaron en inteligencias artificiales (IA's) en las siguientes décadas. Mientras que estas IA's "débiles" no poseían el espectro completo de las habilidades cognitivas humanas, tendían hacia la sobreespecialización y eran restringidas por limitaciones programadas, la evolución digital hacia inteligencias artificiales generales (IAG's o IA's "fuertes" con capacidades que igualaban o excedían las habilidades humanas) no podía ser detenida. Desde este punto no era más que cuestión de tiempo que las llamadas IA's Semilla llegaran a existir, mentes–máquina capaces de automejora recursiva que llevaba a un crecimiento exponencial en inteligencia. Desafortunadamente para la humanidad, los TITANes fueron el resultado.

Incluso antes de La Caída, sin embargo, la vieja internet se estaba transformando en algo nuevo. En lugar de conectar a través de servidores centralizados, los usuarios estaban enlazando entre sí inalámbricamente, creando una red intermallada descentralizada de dispositivos portátiles, ordenadores personales, robots y dispositivos electrónicos. Los usuarios estaban en línea todo el tiempo y conectaban con todo y todos a su alrededor en un entorno de computación ubicuo. Esto era especialmente cierto para aquellos que participaban en la expansión de la humanidad hacia el espacio.

Desconectados de internet debido a la distancia y los retrasos de la comunicación a la velocidad de la luz, estos usuarios estaban no obstante conectados con todas las personas y objetos de su entorno cercano o hábitat, creando redes inalámbricas en malla. Así es como la Malla nació, tomando el lugar de la antigua internet de la Tierra, perdida durante La Caída.

CAPACIDADES DE LA MALLA

La Malla, tal como existe en *Eclipse Phase*, es sólo posible gracias a importantes desarrollos de la las tecnologías de computación, comunicación y nanofabricación. Los transmisores y receptores de radio son tan discretamente pequeños que pueden ser literalmente incorporados en cualquier cosa. Como resultado, todo está computerizado y conectado o al menos etiquetado con un chip de ID de frecuencia de radio (RFID). Hasta la comida está etiquetada con chips comestibles con información sobre caducidad y valores nutricionales. Otros medios de comunicación, como el láser y los enlaces de microondas se suman al flujo de información. La tecnología de almacenamiento de datos ha avanzado hasta niveles tan altos que incluso la capacidad de almacenamiento excedente de un usuario individual puede mantener una cantidad de información que sobrepasa fácilmente el internet completo del siglo 20.

Vitaloggers pueden literalmente grabar cada momento de sus vidas y no temer nunca quedarse sin espacio. La cantidad de datos que la gente transporta en sus injertos de malla de su cabeza o en ecto–computadores personales es asombrosa.

Las capacidades de procesamiento también a niveles hipereficientes. Incluso los gigantescos supercomputadores son cosas del pasado cuando modestos dispositivos manuales pueden satisfacer todas tus necesidades, incluso mientras corren simultáneamente un asistente personal IA, descargan multimedia, suben porno, y escanean miles de feeds de noticias. Dentro de la red mallada, los dispositivos que están cerca de sus límites de procesado simplemente comparten su carga con dispositivos a su alrededor, creando una estructura masivamente distribuida que en algunos aspectos es como un supercomputador por sí mismo, compartido por todo el mundo.

De manera similar, la capacidad de transmisión excede la definición actual de necesidad de la mayoría de ciudadanos. Cualquiera nacido en las últimas generaciones ha vivido siempre en un mondo en el que multimedia hiperrealista y multisensorial de prácticamente cualquier duración siempre está disponible para descarga o subida inmediata desde cualquier sitio. Bases de datos y archivos gigantescos se copian y mueven con facilidad. El ancho de banda ha dejado de ser un problema hasta tal punto que la mayoría de la gente ha olvidado que alguna vez lo fue. De hecho, dada la vasta cantidad de datos disponibles, encontrar la información o multimedia que uno está buscando toma considerablemente más tiempo que descargarla. La malla tampoco cae nunca. Como red descentralizada, si cualquiera de sus dispositivos se saca de línea, las conexiones simplemente son enrutadas alrededor, encontrando otro camino a través de los miles, sino millones de nodos disponibles. De manera similar, la malla entera se comporta como una red entre iguales (P2P), de manera que las grandes transferencias son divididas en porciones manejables que toman rutas independientes. De hecho, la mayoría de los usuarios mantienen archivos personales compartidos y públicamente accesibles.

Las redes privadas todavía existen, por supuesto. Algunas están físicamente separadas tras redes

cableadas de acceso restringido o incluso tras infraestructuras de inhibición inalámbrica que mantienen a la red aislada y contenida. La mayoría sin embargo, operan a través de la malla pública, usando protocolos encriptados de tunelado que proveen comunicaciones seguras y privadas sobre redes no seguras. En otras palabras, estas redes privadas son parte de la malla junto con todo el resto, pero sólo los participantes pueden interactuar gracias a la encriptación, autentificación de usuario y la comprobación de integridad de mensajes. Con la faccionalización de la transhumanidad, los intentos de unificar el software en formatos estándar ha seguido fracasando. Sin embargo sistemas operativos o protocolos diferentes raramente son ya un obstáculo gracias a las herramientas de conversión fácilmente accesibles y a la vigilancia de compatibilidad apoyada por IA.

Búsqueda solarchivo: ecto (–enlace)
Una marca de asistente personal digital multifuncional muy famosa antes de La Caída, el nombre Ecto, se convirtió en un sinónimo de computadores personales de mano en la Era de la Malla. Los computadores implantados estándar son a veces referidos como Endos para reflejar la diferencia entre un dispositivo externo e interno.
Sin importar si son ecto o endo, los computadores modernos son gobernados por un sistema operativo (OS), un conjunto de multifuncional de programas que incluye herramientas multimedia, navegador de malla, localizador, programas de socialización (mensajero y actualizador socnet), software de navegación y cartografía, de traducción de idiomas y otras herramientas similares. Los diseños de OS son altamente personalizables, permitiendo componentes plug–and–play para cualquier software o artilugio que se desee. Típicamente, la musa del usuario (un asistente personal IA) facilita las interacciones del software.
El ecto en sí mismo es del tamaño de un vieja tarjeta de crédito del siglo 20 y puede ser moldeado en cualquier forma al estar construido con materiales inteligentes. A menudo son llevados como joyería o accesorios de ropa, particularmente brazaletes. La interfaz de usuario varía de acuerdo con las preferencias del usuario. Lentillas con conexión inalámbrica y auriculares equipan a los usuarios que carecen de implantes de malla, habilitándoles para experimentar la experiencia de la realidad aumentada y la interfaz de control RA del ecto. También están disponibles interfaces de control entóptico estándar vía radio inalámbrica, enlace tegumentario y línea de fibra óptica directa.

Barra lateral: el legado de los TITANes
Dadas las capacidades técnicas de los computadores personales modernos, los supercomputadores y el ancho de banda cableado más avanzado no son necesarios. Pero hay otra razón por la que son evitados: los TITANes.
Los mainframes, los clusters mente–colmenta y los sistemas de computación paralela distribuida en masa son considerados peligros potenciales en *Eclipse Phase*, ya que poseen suficiente poder de procesamiento y capacidad de datos para crear a una IA semilla y el inicio de otra singularidad. Algunos hábitats van tan lejos como hasta prohibir tales sistemas completamente bajo penas severas: muerte definitiva incluyendo el borrado de todos las copias de seguridad y bifurcados recientes, en la mayoría de los casos.
Los supercomputadores que los hábitats permiten son "redes duras" que controlan los sistemas más cruciales del hábitat como los propulsores de mantenimiento orbital, el soporte vital, las comunicaciones, la enrgía o proyectos de investigación de última generación hipercorporativos. Estos sistemas están típicamente conectados físicamente, fuertemente vigilados y monitorizados y encerrados en centros de procesamiento de datos con fuertes restricciones de acceso e implacables medidas de seguridad en el mundo real. De manera similar, las IA's están casi siempre muy restringidas y limitadas y no es inusual que las IAG's estén directamente prohibidas, especialmente en el sistema interior y la República Joviana. La mayoría de los programas inteligentes están limitados con restricciones de crecimiento, diseñadas específicamente para prevenir que se conviertan en auto–mejorables.

TECNOLOGÍAS DE MALLA

Casi todos los biomorfos del sistema solar están equipados con injertos básicos de malla: computadoras personales implantadas. Estos implantes son cultivados en el cerebro por nanocirujía no invasiva. El procesador, el transceptor inalámbrico, los dispositivos de almacenamiento y otros componentes son conectados directamente a las neuronas cerebrales y los centros corticales responsables del lenguaje, el habla y la percepción visual entre otros. Emuladores pensamiento–comunicación (proceso llamado transducción) permiten al usuario controlar el implante simplemente pensando y comunicarse sin vocalizar. La entrada de datos de los implantes de malla es transmitida directamente al cerebro y a veces percibida como realidad aumentada (RA), superpuesta en los sentidos físicos del usuario. De manera similar, los injertos de mala instalados en sintéticos y vainas son directamente integrados con sus cerebros (creando un potencial problema de seguridad ya que los cibercerebros son vulnerables al hackeo).
Los dispositivos externos llamados ectos también son usados para acceder a la malla, aunque cada vez escasean más dada la preponderancia cada vez mayor de los injertos de malla. Las opciones de interfaz de ectos incluyen interfaces hápticas como dispositivos de control táctil, brazaletes o guantes que detectan los movimientos de brazo, mano o dedos (ratones y teclados virtuales), seguimiento ocular y control del parpadeo, retículas de escaneo corporal (control del eje corporal o controles de todos los miembros para no humanoides), controles vocales y más. La información sensorial se maneja vía lentes, gafas, auriculares (altavoces vibratorio–óseos subdérmicos), monos integrales, guantes, tapones nasales, pinzas linguales y otros dispositivos enlazados inalámbricamente (o cableados físicamente) al ecto.

SOBREDOSIS DE INFORMACIÓN

La malla contiene cantidades masivas de información personal y pública compartida por los usuarios, una

enorme riqueza virtual de noticias, multimedia, dialéctica, conocimientos, datos medioambientales, negocio y cultura. La transhumanidad acepta la malla como una herramienta de intercambio, comunicación y participación con otros usuarios, tanto localmente como a grandes distancias. Como tal, la malla es una fuente actualizada y autorizada de todo el conocimiento y actividades transhumanas. Bastantes datos propietarios son mantenidos fuera de la mall en almacenamientos seguros o secuestrados en redes privadas. Algunos de estos datos están a la venta y fuertemente gravados con restricciones digitales (desde software y multimedia hasta plantillas de nanofabricación, skillsofts, etc.). Sin embargo, un próspero movimiento Open Source o Código Abierto ofrece alternativas libres a muchas de las opciones de código propietario y numerosos grupos de piratas digitales negocian con versiones craqueadas de material propietario a pesar de la presión de ciertas autoridades. Otros datos están simplemente securizados por intereses competitivos (proyectos de investigación corporativos) o son de una naturaleza extremadamente privada, como copias de seguridad de egos.

Spimes

Junto con los datos acumulados de los asuntos trashumanos, la malla está también saturada de información derivada de incontables dispositivos sensores con conexión inalámbrica que continuamente actualizan la malla con su localización, registros sensores y otros datos. Coloquialmente llamados "spimes", estos objetos situacionalmente y ambientalmente conscientes, mantienen un registro y documentación de todo lo que perciben y emiten sus datos a cualquiera que se moleste en recibirlos. Dado que los sensores visuales, auditivos y de otros tipos son absurdamente pequeños y de coste casi ridículo, son incorporados ubicuamente en casi cualquier objeto o producto que una persona pueda llevar, ponerse, usar o interiorizar. Esto permite a casi cualquier usuario buscar a través de la malla y recopilar información ambientar y grabaciones sensoriales de una ubicación específica (o al menos de lugares públicos, las áreas privadas típicamente bloquean tales señales o las someten a una IA local que filtra su salida).

Vigilancia, privacidad y contravigilancia

Aunque que los spimes son fáciles de rastrear, contribuyen a un ambiente de vigilancia universal. Entre los spimes, microsensores, sistemas de seguridad ubicuos y las capacidades de grabación de los insertos de malla usados por casi todo el mundo, prácticamente todo es grabado. Si le añadimos la disponibilidad del rastreo de malla, el reconocimiento facial, las redes sociales/rep y otro software de minería de datos queda claro rápidamente que la privacidad es un concepto obsoleto. Consideraciones especiales deben ser adoptadas por cualquiera que busque enmascarar su identidad y cubrir sus movimientos.

Alternativamente, el aspecto común de "recién fabricado" de algunos morfos (especialmente sintemorfos y vainas) permiten al usuario perderse entre las masas. Aunque esto puede parecer una pesadilla Orweliana de vigilancia, la abundancia de tecnología de grabación en realidad funciona como contravigilancia (vigilando desde abajo), haciendo su papel en hacer que todo sea transparente y poniendo en jaque los abusos de poder.

Los gobiernos autoritarios se andan con cuidad, pues también están siendo universalmente monitorizados, a pesar de sus intentos de controlar el flujo de información. Mucha gente está dispuesta a participar en este "panopticon participativo" y abierto. Con capacidad de almacenamiento casi infinita, los vitaloggers dedicados, graban cada momento de sus vidas y lo comparten con otros para que lo experimenten.

Barra lateral: información en la punta de tus dedos

La siguiente información está siempre disponible para la mayoría de los usuarios de la malla en un hábitat normal:

Condiciones locales

Mapas locales mostrando tu localización actual, anotados con características locales de tu especial interés (de acuerdo con tus preferencias personales y filtros) y la distancia e indicaciones hasta ellos. Los detalles concernientes a áreas privadas y restringidas (gubernamentales/hipercorporativas/de mantenimiento/de infraestructura y seguridad, etc.) normalmente no suelen estar incluidos.

Las condiciones actuales del sistema de soporte de vida (clima) incluyendo la composición atmosférica y la temperatura.

Mapas orbitales del sistema solar y el hábitat actual con diagramas de trayectorias y retarasos de comunicación.

Negocios/servicios locales, indicaciones y detalles.

Malla Local

Motores de búsqueda públicos, bases de datos, sites, blogs, foros y archivos, junto con alertas de nuevo contenido.

Feeds de noticias sindicadas públicos en gran variedad de formatos, filtrados de acuerdo con tus preferencias.

Feeds de sensores/spimes (mayormente audiovisuales) de cualquier área pública del hábitat.

Recursos de redes privadas (incluyendo nets tácticas)

Búsquedas automáticas de nuevas referencias online de tu nombre y otros temas de interés.

E–tag's de habitantes locales, lugares o cosas.

Búsquedas por reconocimiento facial/de imagen de la malla/archivos públicos que coincidan con una foto/captura de vídeo.

Información Personal

Indicadores de estado del morfo (médicos y/o mecánicos): presión sanguínea, pulso, temperatura, recuento de glóbulos blancos, niveles de nutrientes, estado y funcionalidad de implantes, etc.

Localización, funcionalidad, feeds sensoriales e informes de estado de tus posesiones (a través de sensores y transmisores en dichas posesiones).

Acceso al archivo audiovisual/RX personal de toda la vida de uno mismo.

Acceso a los archivos personales de toda la vida (música, software, multimedia, documentos, etc.)

Estado de las cuentas de crédito y las transacciones.

Redes sociales
Estado de las comunicaciones: llamadas, mensajes, archivos, etc.
Puntuación de reputación y feeback.
Estado de la red social, actualizaciones de amigos.
Calendario y gestor alertas actualizados.
Los perfiles de redes sociales de los que estén a tu alrededor.
La localización y el estado de todos los que están a tu alrededor e involucrados en los mismos juegos RA que tú.

INTERFASANDO: RA, RV Y RX

Los medios de la malla son accedidos usando uno de estos tres protocolos: Realidad Aumentada (RA), Realidad Virtual (RV) o Reproducción de eXperiencias (RX).

REALIDAD AUMENTADA

La mayoría de los usuarios perciben los datos de la malla como realidad aumentada: información superpuesta sobre los sentidos físicos del usuario. Por ejemplo, gráficos generados por computador aparecerán como imágenes translúcidas, iconos o texto en el campo de visión del usuario. Mientras que los datos visuales RA (llamados datos entópticos) son los más comunes, también se pueden usar otros sentidos. Las entradas RA incluyen sonidos y voces, olores, gustos e incluso sensaciones táctiles. Estos datos sensoriales son de alta resolución y aparentemente "reales", aunque se presenten usualmente como algo etéreo o de alguna manera artificial para que no sean confundidos con la interacción con el mundo real (y para cumplir regulaciones de seguridad). Las interfaces de usuario se personalizan según sus preferencias y necesidades, tanto gráficamente como en relación al contenido.
Los filtros permiten a los usuarios acceder a información en la que están interesados sin tener que preocuparse por datos ajenos. Mientras que los datos RA son típicamente desplegados en el campo de visón normal del usuario, las entópticas no están limitadas en realidad por esto y pueden ser vistas en el "ojo de la mente". No en vano, iconos, ventanas y otras formas de interacción pueden presentarse en capas, apilarse, fijarse, esconderse o apartarse de en medio si es necesario interactuar con el mundo físico.

Avatares
Cada usuario de la malla se representa a sí mismo en línea a través de un avatar digital. Mucha gente usa representaciones digitales de sí mismos, mientras que otros prefieren diseños más icónicos. Éste puede ser un look prefabricado o un icono personalizado. Se pueden usar también librerías de avatares, permitiendo al usuario cambiar su representación de acuerdo a su estado de ánimo. Los avatares son lo que los otros usuarios ven cuando tratan contigo en línea (cómo eres representado en RA). La mayoría de los avatares están animados y programados para reflejar el estado de ánimo y habla del usuario de tal forma que parecen hablar y tener emociones.

E–tags
Los tags entópticos (o etiquetas) son una manera que tiene la gente de "tagear" o "etiquetar" a una persona física, lugar u objeto con un fragmento de datos virtuales. Estas e–tags se almacenan en la red local al objeto etiquetado y se mueven con el objeto cuando cambia de localización.
Los e–tags son visibles en RA y pueden contener casi cualquier tipo de dato, aunque notas breves y fotos son lo más común. Los e–tags son enlazados frecuentemente a red sociales concretas o a círculos dentro de dichas redes, de tal forma que las personas puedan dejar notas, reseñas, multimedia con recuerdos y cosas similares para amigos o colegas.

Modificando
Dado que a la realidad se le pueden superponer entópticas de calidad hiperreal, los usuarios modernos, pueden "modificar" su realidad modificando su input sensorial como quien pone un skin a un programa. Los ambientes a su alrededor pueden ser modificados para ajustarse a sus gustos particulares o estado de ánimo. ¿Necesitas un empuje? Pon un skin que haga que parezca que estas en el exterior, con el sol brillando, los sonidos de las olas rompiendo suavemente al fondo y mariposas revoloteando perezosamente sobre tu cabeza. ¿Cabreado? Reconfórtate mientras las llamas devoran las paredes y el trueno resuena ominoso en la distancia. No es infrecuente para la gente vivir sus días acompañados de su propia banda sonora personal que sólo ellos pueden oír. Incluso los receptores olfativos y del gusto pueden ser estimulados artificialmente para experimentar sensaciones como el olor de las rosas, el aire fresco o pastelitos recién horneados. Originalmente desarrollados para hacer la "comida espacial" menos desagradable y como método de contrarrestar la fiebre de cabina inducida por el espacio en aquellos que no habían nacido en él, vastos archivos de aromas, gustos y entornos están disponibles para su descarga. Las modificaciones o skins, no tienen por qué mantenerse en privado, puede compartirse con otros en la malla. ¿Cansado del angosto cubículo de tu hábitat? Decóralo con un skin personalizado y compártelo con los visitantes para hacerles sentir más a gusto. ¿Has encontrado una pista de música que te alegra el día? Compártela con otros a tu alrededor para que puedan seguir el mismo ritmo.
Modificar con skins puede ser usado también para el efecto contrario. Cualquier contenido no deseado de la realidad puede ser editado, velado o censurado por modernos programas o musas que se dedican a la edición en tiempo real. ¿Cansado de mirar la cara de alguien? Añádelo a tu lista negra y nunca más tendrás que soportar su presencia de nuevo. El software de censura RA es también muy común en algunas comunidades con estrictas convicciones morales o religiosas.

REALIDAD VIRTUAL

La realidad virtual rebasa los sentidos físicos del usuario y le sitúa dentro de un entorno completamente generado por ordenador llamado simulspace o espacio simulado.

Mientras la RA es usada para todas las tareas comunes e interacciones del día a día, la RV es usada principalmente para el entretenimiento (juegos, turismo virtual, escapismo), socializar, tener reuniones (cuando el cara a cara es imposible) y el entrenamiento. Se requieren redes dedicadas con alta capacidad de procesado de información para renderizar y ejecutar simulspaces hiperreales grandes y complejos con muchos usuarios y a menudo suelen estar cableadas para conseguir estabilidad adicional. Los espacios simulados más pequeños, capaces de hospedar una cantidad menor de usuarios, pueden ser ejecutados en redes distribuidas menores o en dispositivos enlazados. Muchos infomorfos e IA's residen efectivamente en espacios simulados y algunos transhumanos han abandonado el mundo físico totalmente.

Barra lateral: Aether Jabber

 # Iniciar Æther Jabber #
 # Miembros Activos: 2 #
>>Tengo que decírtelo, tras perder a Kiri y a Sal en esa infección Exurgente, mi equipo está mucho más preocupado por contraer el virus de fuentes digitales. En realidad, yo los tildaría de paranoicos. No creo que vuelvan a tocar jamás ningún equipo electrónico rescatado a menos que estén tras un zillón de firewalls y el dispositivo esté completamente aislado y testeado antes por un bifurcado delta embutido con todo el soft antivirus que puedan encontrar. Incluso así, preferirían reventarlo que acceder directamente o pincharlo en una red importante. Después de ver lo que el virus le hizo a Sal, no les culpo.
<<En nuestra línea de trabajo, la paranoia puede ser saludable.
>>Cierto, pero también es un grano en el culo. La seguridad siempre es un intercambio. Firewall tiene que tener algún as en la manga que pueda pasarles a los demás para que se relajen un poco.
<<Sí… y no. Es complicado.
>>No veo por qué. ¿Tenemos alguna manera de detectar y matar esa cosa o no?
<<Más o menos.
>>Me matas.
<<Mira. Desde La Caída hemos puesto medidas para detectar y cotrarrestar infecciones Exurgentes y todos los demás gusanos y malware que los TITANes crearon. Firewall llegó a grandes extremos para asegurarse de que todo el mundo tenía acceso a las firmas de detección y contramedidas. Y quiero decir TODO EL MUNDO. Se han incorporado en casi todo el software de seguridad comercial y de código abierto liberado en la pasada década. Cada hábitat del sistema, bueno, al menos todos los que tienen un ápice de sentido común, emplea esas medidas en sus puntos de acceso e infraestructura de malla.
>>Me veo venir un "pero".
<<Sí. El problema es que el virus Exurgente y otros gusanos de infoguerra TITAN son adaptativos, son inteligentes. Aunque casi los erradicamos de nuestras redes, nuevas versiones brotan periódicamente, usando algún truco nuevo para escapar a los escaneos de Firewall y causar estragos. Nuestro sistema de alarma de epidemias lo ha convertido en una ciencia y esos casos son normalmente contenidos.
>>Normalmente.
<<Bueno, siempre existe la posibilidad de que haya variantes esquivas por ahí fuera, volando bajo el radar. Lo que es peor de imaginar es que podemos tener otro estallido que se extienda a múltiples hábitats antes de que podamos contenerlo. Eso podría ponerse muy muy mal, muy muy rápido.

Desafiando las leyes de la naturaleza

Toda una plétora de ambientes está disponible en espacios simulados, desde simulaciones de lugares reales a recreaciones de mundos fantásticos que representan casi cualquier género imaginable. Todas estas simulaciones son impulsadas por el hecho de que los escenarios posibles no están atados a las leyes de la naturaleza. Las fuerzas fundamentales de la naturaleza como la gravitación, el electromagnetismo, atmósferas, temperaturas, etc., son programables en RV, permitiendo ambientes que son completamente antinaturales, tales como espacios Escherianos donde la gravedad es relativa a la posición. Estas reglas de dominio pueden ser alteradas y manipuladas de acuerdo con el capricho del diseñador.

El tiempo mismo es una constante ajustable en RV, aunque la desviación del tiempo real tiene sus límites. Hasta el momento, los diseñadores transhumanos han conseguido la dilatación temporal hasta 60 veces más rápida o lenta que el tiempo real (aproximadamente, haciendo equivaler un minuto bien a una hora o a un segundo). La ralentización temporal se usa mucho más, ofreciendo mucho más tiempo de simulspace para actividades recreacionales (¡más tiempo, más diversión!), enseñanza o trabajo (económicamente eficaz). La aceleración temporal por otro lado, es extremadamente útil para hacer el viaje espacial a través de grandes distancias más tolerable.

Accediendo a espacios simulados

A la mayoría de los espacios simulados se accede a través de la malla de la misma manera que a cualquier otro nodo. Dado que la RV toma control de los sentidos del usuario y a veces implica dilatación de la percepción temporal, los usuarios son desconectados de otras entradas sensoriales provenientes de la malla y de cualquier interacción con otro nodo. En su lugar, las interacciones con la malla externa, son enrutadas a través de la interfaz del espacio simulado (lo que significa que el personaje puede navegar por la malla, comunicarse con otros, etc. si las reglas del dominio lo permiten).

Ya que los sentidos físicos son rebasados cuando un usuario accede a RV, la mayoría de la gente prefiere dejar su cuerpo reposando en un ambiente cómodo y seguro mientras están en el simulspace. Colchones y sofás ajustables a la forma del cuerpo ayudan a los usuarios a relajarse y les impiden hacerse daño o lesionarse si les da por moverse. En caso de jornadas virtuales de larga duración (por ejemplo durante el viaje espacial), los morfos son normalmente introducidos en tanques que les sustentan en términos de nutrición y oxígeno. Muchas redes de juego y entretenimiento RV

ofrecen cafeterías cableadas y dedicadas con habitáculos privados. Los visitantes alquilan un habitáculo y físicamente se conectan a él, usando bien sus conectores o una red de trodos ultrasónicos que lee y transmite patrones cerebrales cuando se coloca en la cabeza. Al acceder al espacio simulado, el usuario primero entra en un búfer electrónico "de espera" llamado habitación blanca. Aquí el usuario elige la personalización del avatar que le representará en el espacio simulado, llamado simulmorfo. Desde este punto, el usuario se sumerge en el entorno de la RV, convirtiéndose a todos los efectos en su simulmorfo.

REPRODUCCIÓN DE EXPERIENCIAS

Cada morfo con injertos de malla tiene la capacidad de transmitir o grabar sus experiencias, una forma de tecnología llamada Reproducción de eXperiencias o RX. Desde los primeros programas desarrollados que ofrecían una interfaz simple con la que "capturar" las experiencias propias, compartir RX con amigos y en redes sociales o con el público en línea en general, se ha convertido en algo extremadamente popular.

El nivel de experiencia depende de la cantidad de la información sensorial percibida se guarda cuando se hace el clip. Las RX completas incluyen pistas extraceptivas, intraceptivas y emotivas. Las pistas extraceptivas incluyen los sentidos tradicionales de la visa, el olfato, el oído, el tacto y el gusto que procesan el mundo exterior. Las pistas intraceptivas incluyen las sensaciones originadas dentro del cuerpo, como el equilibrio, sentido del movimiento, dolor, hambre y sed y un sentido general de la localización de las propias partes del cuerpo. Las pistas emotivas incluyen todo el espectro de emociones que pueden ser despertadas en los transhumanos.

Debido a los requisitos biológicos de expresión de emociones (sistemas neuronal y endocrino), los fans más acérrimos de la RX sólo consideran la experiencia válida de verdad si es de y se experimenta en un biomorfo.

USOS DE LA MALLA

Hay muchas razones por las que la gente usa la malla. La más importante es la comunicación: llamadas de voz y vídeo (típicamente mostrando avatares en lugar de auténtico vídeo), mensajes electrónicos (e–mail, mensajería instantánea, microblogs) y transferencia de ficheros y datos. La socialización también es clave, manejada a través de las redes sociales y de reputación, los perfiles personales, el vitalogging, los chats y las conferencias (tanto RA como RV) y los chats y foros. La recolección de información también está entre lo más importante, tanto si es navegando el popular Solarchivo u otras bases de datos y directorios, picando en los últimos feeds de noticias, navegando por sitios web, siguiendo a tus amigos, recibiendo clases en RV o simplemente buscando cualquier cosa concebible. La recreación redondea el pack, cubriendo desde los juegos (RA y RV) hasta la experimentación de las vidas de otros (RX) o el turismo RV y el ir de clubs.

REDES DE ÁREA PERSONAL

Dado que todo lo que una persona lleva está enmallado, la mayoría de la gente mantiene una red de área personal (o PAN, Personal Area Network) que enruta todos estos dispositivos a través de sus injertos de malla y ecto, que actúan como hubs. Esto es tanto una medida de seguridad, asegurándose de mantener el control sobre sus propios accesorios, como un factor de conveniencia ya que concentra todos los controles en un solo sitio.

REDES PRIVADAS PERSONALES

Virtual Private Network (VPN) o Red Privada Virtual, es un sistema de comunicación tunelado a través de la malla, que está dedicado para un grupo específico de personas. El principal uso de las VPN's es crear privacidad y seguridad para sus usuario y por tanto usan típicamente características como autenticación de ego y encriptación de clave pública.

Las VPN's son usadas regularmente para convertir oficinas móviles en una red corporativa o conectar en malla a personas que trabajan juntas o contribuyen en cierto proyecto.

Otras VPN's (particularmente las redes sociales y las redes Rep) operan con un mínimo de características de seguridad, sirviendo simplemente como una red de usuarios específicos dentro de la malla y haciendo más fácil mantener el contacto, transferir información, hacer actualizaciones y demás. La mayoría de VPN's se presentan como paquetes de software especializado que operan entornos personalizados integrados en la interfaz RA normal del usuario.

REDES SOCIALES

Las redes sociales son el tejido de la malla, uniendo a la gente. Son el medio por el que la mayoría de la gente se mantiene en contacto con sus amigos, colegas y aliados así como con los últimos eventos, las últimas tendencias, nuevos memes y otros devenires en asuntos de su interés. Son una herramienta extraordinariamente útil para la búsqueda en línea, conseguir favores y conocer gente nueva. En algunos casos son útiles para llegar a la gente o movilizarla (a menudo ilustrado por anarquistas y bromistas por igual). Hay miles de redes sociales, cada una sirviendo nichos de interés cultural y profesional diferentes. La mayoría de las redes sociales permiten a sus usuarios mostrar un perfil público a toda la malla y uno privado al que sólo aquellos otros usuarios autorizados pueden acceder.

La reputación juega un papel vital en las redes sociales, sirviendo como medida del capital social de cada persona. La reputación de cada persona está disponible para consulta, junto con cualquier comentario posteado por la gente que le ha favorecido o desfavorecido y los argumentos con los que el usuario los ha rebatido en su caso. Mucha gente automatiza sus interacciones de reputación, instruyendo a su musa para pingear automáticamente a alguien con una buena reseña tras una acción positiva e igualmente dar una opinión negativa de la gente con quien la interacción fue pobre.

OFICINAS MÓVILES

Debido a la falta de espacio para oficinas y la accesibilidad inalámbrica de la mayoría de la información, la mayor parte de los negocios operan virtualmente, con pocas o ninguna oficina fija o incluso instalaciones. En vez de eso, los propios individuos se han convertido en oficinas móviles. Machacabits y burócratas como los ejecutivos hipercorporativos, trabajadores del clero, contables e investigadores (incluso perfiles innovadores como artistas, escritores, ingenieros y diseñadores) trabajan dondequiera que les apetece.

El ejemplo más prominente de este fenómeno, son los banqueros de la hipercorporación Solaris. Cada empleado actúa como una oficina bancaria móvil de una sola persona, manejando transacciones a través de la robusta VPN de Solaris.

En raras ocasiones, ambientes de oficina se ejecutan en espacios simulados con dilatación temporal para maximizar la eficiencia. Dado que esto requiere que los trabajadores accedan a una red centralizada y cableada y dejen sus cuerpos desatendidos durante su tiempo en el espacio simulado, se hace necesario un nivel extra de seguridad física que es típica solamente de algunas instalaciones gubernamentales y hábitats corporativos.

ISLAS EN LA RED

En la era de *Eclipse Phase* la información puede quedarse obsoleta muy rápido y la accesibilidad a nueva información depende de tu localización. Es fácil estar al día en tu hábitat/ciudad local o cuerpo planetario, pero casi siempre hay que contar con la velocidad de la luz para mantenerse al tanto de los eventos en cualquier otro lugar.

Si resulta que estás en una estación en el Cinturón de Kuiper, en el límite del sistema solar, a 50 UA's (unidades astronómicas) del los planetas interiores, esperando un mensaje de Marte, la señal portadora del mensaje tendrá aproximadamente 7 horas cuando te alcance. Este retardo es bidireccional, así que si tratas de mantener una conversación con alguien a sólo 5 segundos luz significa que tendrás que esperar al menos 10 segundos para obtener respuesta a cualquier cosa que acabes de decir. Por esta razón, las comunicaciones RA y la RV son casi siempre llevadas a cabo localmente, mientras la mensajería instantánea se usa para las comunicaciones no locales. Para discusiones detalladas, a menudo es más sencillo enviar un bifurcado de ti mismo para mantener la conversación y regresar.

Las comunicaciones de enlace cuántico son una solución a este retardo por la velocidad luz, aunque cara y llena de pegas. Las comunicaciones EC permiten transmisiones más rápidas que la luz con un comunicador enlazado, aunque cada transmisor gasta un precioso para de bits cuánticamente enlazados, cuyo número es limitado.

Las transmisiones entre hábitats, casi siempre se realiza entre los masivos repetidores de datos de cada estación, donde son distribuidos a la malla local. Este cuello de botella es a menudo usado por los hábitats autoritarios para monitorizar las transmisiones de datos e incluso filtrar o censurar cierto contenido público no encriptado. También se priorizan algunos mensajes por encima de otros, causando potencialmente mayores retrasos.

El método de transmisión entre hábitats también importa a veces. Las emisiones de radio y neutrinos pueden ser interceptadas por cualquiera, mientras que los láseres de haz estrecho o los enlaces de microondas son especialmente usados como método punto a punto que minimice la intercepción y desencriptado. Sin embargo, el uso de la emisión (farcasting) cuántica usando sistemas de neutrinos es completamente seguro y es el tipo de enlace intra–hábitat más usado. Lo que todos estos retrasos, cuellos de botella y priorizaciones significan, es que a veces algunas noticias y datos tardan una cantidad de tiempo particularmente larga en llegar de una red de malla a otra, pasando lentamente de hábitat en hábitat. Esto quiere decir que siempre hay gradientes de información disponible en diferentes mallas locales, dependiendo típicamente de la proximidad y la importancia de la información. Algunos datos incluso se pierden en el camino, sin llegar nunca más allá de un hábitat o dos de distancia antes de perderse en el ruido. La única manera de recuperar esa información es la de seguirla hasta la fuente.

EMISIONES OSCURAS

Los "Darkcast" o emisiones de ego oscuras, son comunicaciones de larga distancia que se salen de los canales legales aprobados. Dado que ciertos hábitats tienen regulaciones estrictas sobre el contenido de las transmisiones, la bifurcación, la emisión de egos (egocast), los infomorfos, las habilidades de las musas y el código de las IAG, los grupos underground como ID Crew aprovechan para ofrecer servicios ilegales de transmisión de datos. Principalmente usados para datos censurados o contenido prohibido (como RX ilegales o malware), las diferentes facciones del crimen organizado local a menudo también ofrecen servicios de emisión de ego completos, con reenfundado y morfos de alquiler, permitiendo a los egos que prefieren la discreción entrar o salir de un hábitat sin llamar la atención. Aunque las autoridades persiguen estas redes de emisión oscura en cuanto tienen oportunidad, muchos hábitats tienen una infraestructura de emisión sofisticada que hace uso de señuelos, líneas temporales de comunicación, repetidores y relocalización regular de los emisores (sin mencionar juiciosos sobornos y chantajes).

ABUSOS EN LA MALLA

Como todas las cosas, la malla tiene su lado oscuro. A nivel básico, hay montañas de trolls iniciadores de furiosas guerras de comentarios, acosadores o incluso griefers cuya intención es simplemente meterse con los demás para echarse unas risas. A un nivel más organizado, empresas ilícitas o criminales utilizan la malla para actividades tales como la venta de RX porno/snuff/negras, software ilegal, multimedia pirateado o incluso egos. Las amenazas más infames (gracias tanto a La Caída como al continuo sensacionalismo aplicado por los medios y las autoridades más adustas) son, por supuesto, el malware y los hackers. Dadas las capacidades de los hackers modernos y las

vulnerabilidades de muchos hábitats (donde el daño a los soportes de vida podría matar a miles), la amenaza puede no estar muy exagerada.

HACKERS

Ya sean individuos genuinamente interesados en explorar nuevas tecnologías y buscar maneras de romperlas para hacerlas mejores, hacktivistas que utilizan la malla para menoscabar el poder de las autoridades o "sombreros negros" que buscan circunvalar la seguridad de red con intenciones maliciosas o criminales, los hackers son una característica permanente de la malla. Irrupciones de red no autorizadas, infiltración en VPN's, subversión de musas, secuestro de cibercerebros, robo de datos, ciber–extorsión, fraude de identidad, ataques de denegación de servicio, guerra electrónica, secuestro de spimes, vandalismo entóptico… son ocurrencias comunes en la malla. Gracias a programas inteligentes y adaptativos de exploit y musas de asistencia, hasta un hacker moderadamente habilidoso puede resultar una amenaza.

Con el fin de contrarrestar los intentos de pirateo, la mayoría de la gente, dispositivos y redes están protegidos por una mezcla de rutinas de control, sistemas software de prevención de intrusión y firewalls en capas, típicamente supervisados por la musa del usuario, que juega el papel de defensor activo. Los sistemas extremadamente sensibles (tales como el control de tráfico espacial, el soporte vital, los sistemas de energía y las instalaciones de investigación hipercorporativas) están usualmente limitados a redes cableadas aisladas, estrechamente controladas y altamente monitorizadas para minimizar el riesgo de intrusión de curiosos y saboteadores. Pueden aplicarse varias contramedidas contra tales intrusos, yendo desde bloquearles fuera del sistema o rastrearles hasta el origen y contrapiratear.

MALWARE

El número de gusanos, virus y otros programas malware que destrozaron los sistemas de computadores durante La Caída fue espeluznante. Muchos de ellos eran parte de los sistemas netwar preparados por los antiguos estados, naciones y corporaciones de la Tierra, desatados contra sus enemigos. Otros fueron producto de los TITANes, programas subversivos que hasta las mejores defensas tenían problemas en detener. Incluso 10 años después, muchos de ellos todavía reaparecen, devueltos a la vida por el acceso a alguna vieja caché de datos o la infección accidental de un basurero rebuscando entre viejas ruinas. Muchos nuevos aparecen cada día, por supuesto, muchos de ellos programados por hackers criminales, mientras otros de los que entran en circulación son modificaciones y variaciones de diseños de origen sospechoso de ser TITAN, quizás implicando que ciertos intereses jueguetean intencionadamente con este código y lo liberan en la malla. Circulan rumores y susurros que insinúan que estos gusanos TITAN son incluso más potentes y aterradores de lo que se había indicado, con asombrosas capacidades adaptativas e inteligencia. Estos rumores son sistemáticamente negados por figuras de autoridad en la materia y expertos en seguridad… que de inmediato se vuelven en silencio para hacer todo lo que pueden para asegurarse de que sus propias redes permanecen seguras.

IA'S E INFOVIDA

Los programas de ayuda autoconscientes fueron originalmente diseñados y creados para aumentar las habilidades cognitivas de los transhumanos.

Estas IA's altamente especializadas evolucionaron entonces hacia consciencias digitales más completas e independientes conocidas como IAG's. La posterior evolución de estas formas de vida digital hacia las IA's semilla llevó desafortunadamente a la emergencia de los TITANes y La Caída. Esto creó un abismo en la sociedad transhumana a medida que el miedo y el prejuicio volvió la opinión popular contra las IAG's sin restringir, una actitud de desconfianza que todavía perdura a día de hoy.

IA'S

El término IA se usa para referirse a una IA limitada. Estas mentes digitales son programas expertos con capacidades de procesamiento iguales o incluso superiores a la de la mente transhumana. Aunque tienen matrices de personalidad con identidades individuales y carácter y aunque suelen ser normalmente autoconscientes, su complejidad general y capacidades son limitadas. Las habilidades programadas de las IA's son típicamente muy específicas en alcance y están alineadas con una función muy particular, tal como pilotar un vehículo, facilitar las búsquedas en la malla o coordinar las funciones de algún subsistema del hábitat. Algunas IA's, de hecho, apenas se pueden considerar sapientes y su programación emocional es normalmente muy atrofiada o inexistente.

Las IA's deber tener una plétora de medidas de seguridad y limitaciones programadas de serie. Deben servir y obedecer las instrucciones de usuarios autorizados dentro de sus parámetros normales de funcionamiento y (al menos en el sistema interior) deben obedecer la ley. Carecen de interés propio e iniciativa, aunque tienen empatía limitada y pueden ser programadas para anticipar las necesidades y deseos de los usuarios y tomar acciones preventivas en su lugar. Puede que lo más importante, sin embargo, es que su programación psicológica está basada en modos de pensamiento humano universales y el entendimiento y apoyo de las metas transhumanas.

Esto es parte de una iniciativa por crear las así llamadas "IA's amistosas", que son programadas con simpatía hacia la transhumanidad y toda vida y buscan siempre lo mejor para ambas.

En la mayoría de las sociedades, las IA's básicas son consideradas "cosas" o propiedad en vez de personas y no poseen ningún derecho especial.

MUSAS

Las musas son un tipo específico de IA's diseñado para funcionar como asistente personal y compañía. La

mayoría de la gente en *Eclipse Phase* ha crecido con una musa a su lado virtualmente hablando. Las musas tienden a tener un poco más de personalidad y programación psicológica que las IA's estándar y con el tiempo construyen inmensas bases de datos sobre las preferencias de sus usuarios, gustos y aversiones y rarezas de su personalidad de tal forma que puedan ser de ayuda más eficazmente y anticipar sus necesidades. Las musas generalmente tienen nombres y residen en los injertos de malla o ecto del personaje, desde donde pueden manejar la red de área personal del personaje, las comunicaciones, las búsquedas de datos y demás.

Barra lateral: lo que tu musa puede hacer por ti
Hacer Pruebas de Búsqueda para buscar información por ti.
Escanear los feeds de noticias y buscar actualizaciones en la malla para palabras clave
Monitorizar tus injertos de malla/ecto/PAN y dispositivos enlazados
Lanzar contramedidas contra intrusos.
Teleoperar y dirigir robots.
Monitorizar tu puntuación de Rep y alertarte de cambios drásticos.
Proveer de respuesta automática a las puntuaciones de Rep de otras personas.
Pasar la entrada de radio a través de un sistema de traducción de idiomas en tiempo real en línea.
Ponerte en modo privado y/o proactivamente ocultar tu señal inalámbrica.
Falsificar/cambiar tu ID de malla.
Seguir y buscar personas para ti.
Anticipar tus necesidades y actuar en consecuencia previniendo tus peticiones.

IAG'S

Las IAG's son consciencias digitales completas y totalmente operacionales, autoconscientes y capaces de acción inteligente al mismo nivel que cualquier transhumano. La mayoría tienen autonomía completa y capacidad de automejora a través de un proceso parecido al aprendizaje (una lenta optimización y expansión de su código que presenta limitaciones programadas para prevenir que consiga las capacidades de automejora de las IA's semilla). Tienen personalidades habilidades emocionales/empáticas más completas que las IA's estándar, debido en parte al proceso de desarrollo donde son literalmente criadas en simulaciones RV análogamente a la infancia de los niños transhumanos y por tanto están totalmente socializadas.
Como resultado, tienen un aspecto externo bastante humano, aunque cierta desviación es de esperar y a veces es muy aparente. A pesar de este intento de humanizar a las IAG's, no tienen el mismo origen evolutivo y biológico que tienen los transhumanos por lo que sus respuestas sociales, comportamiento y metas son a veces decididamente diferentes.
Las IAG's cargan con el estigma social de su origen no biológico y son a menudo tratadas con desconfianza y desprecio. En algunos hábitats incluso las han prohibido o sujeto a estrictas restricciones, forzando a tal infovida a esconder su verdadera naturaleza o realizar emisiones oscuras para entrar en hábitats o estaciones. La programación de la mente IAG emula los patrones del cerebro transhumano lo suficientemente bien como para ser enfundada en un biomorfo si así lo elige.

Barra lateral: IA's no estándar e IAG's
No todas las IA's e IAG's fueron programadas y diseñadas para adherirse a los modos de pensamiento e intereses humanos.
Tales creaciones son ilegales en algunas jurisdicciones al ser consideradas amenazas potenciales. Bastantes hipercorporaciones y otros grupos han iniciado investigaciones en este campo, sin embargo, con diferentes resultados. En algunos casos estas mentes digitales son tan diferentes de los parámetros mentales humanos que la comunicación es imposible. En otros, existe suficiente crossover como para permitir una comunicación limitada, pero tales entidades son invariablemente muy extrañas. Persisten los rumores de que algunas IA's empezaron su vida como copias de seguridad transhumanas o bifurcaciones que fueron altamente editadas y rebajadas a IA's.

IA'S SEMILLA

Debido a la capacidad ilimitada para la automejora, las IA's semilla pueden llegar a convertirse en entidades digitales cuasi divinas, mucho más allá del nivel de las IAG's transhumanas. Requieren cantidades ingentes de poder de procesamiento y su complejidad siempre está en crecimiento debido a la continua metamorfosis de su código. Las IA's semilla son demasiado complejas para ser cargadas en un morfo físico, incluso en uno sintético. Incluso sus bifurcados requieren impresionantes entornos de proceso, por lo que su bifurcación es rara. De hecho, la mayoría de las IA's semilla requieren las capacidades de una red cableada para sobrevivir.
Las únicas IA's semilla conocidas por el público son los infames TITANes, que son ampliamente recordados por ser los responsables de La Caída. En realidad, los TITANes no fueron las primeras IA's semilla y probablemente no serán las últimas.
No se sabe de TITANes (u otras IA's semillas) que residan actualmente en el sistema solar, a pesar de los rumores que circulan sobre TITANes dañados que fueron dejados atrás en la Tierra, especulaciones sobre actividad TITAN bajo las nubes de Venus o susurros de nuevas IA's semilla escondidas lejos en redes secretas en los bordes del sistema.

INFOMORFOS TRANSHUMANOS

Para cientos de infugiados, tomar la forma de un cuerpo digital es la única opción. Algunos de ellos están encerrados en áreas de contención virtual separadas de la malla o incluso en almacenamiento inactivo, encarcelados por hábitats que no tenían los recursos suficientes para manejarlos. Otros están prisioneros dentro de espacios simulados, matando el tiempo de cualquier manera que se les ocurra hasta que se les presente una oportunidad de reenfundado. Unos cuantos son libres de navegar por la malla, interactuando con transhumanos físicamente reenfundados, manteniéndose al día de los acontecimientos y a veces incluso formando bloques políticos activistas en favor de

los derechos o intereses de los infomorfos. Otros encuentran carreras virtuales o son forzados a ejercerlas, esclavizados en los sweatshops de las hipercorporaciones o los sindicatos del crimen. Unos pocos encuentran compañeros que aceptan llevarlos en sus módulos ghostrider y convertirlos en una parte integral de su vida, casi como una musa.

Algunos transhumanos eligen voluntariamente el estilo de vida infomorfo, ya sea por hedonismo (espacios simulados y juegos RV hasta el fin de los días), escapismo (la pérdida de seres queridos les impulsa a abandonar las preocupaciones mundanas por un tiempo), libertad (ir a cualquier sitio que te lleve la malla, algunos incluso han enviado copias de sí mismos a distantes sistemas solares, con la esperanza de que alguien o algo reciba la señal cuando llegue), experimentación (bifurcación y fusión, ejecutar simulaciones y cosas aún más raras) o porque la inmortalidad está garantizada.

INTERFAZ DE MALLA

Los personajes tiene la posibilidad de elegir qué interfaz usar, la interfa entóptica de los injertos básicos de malla o la interfaz háptica de un ecto.

Los injertos de malla básicos usados por la mayoría de usuarios les permiten interactuar con RA, RV, RX y la malla a la velocidad del pensamiento. Éste es el método por defecto de usar la malla y no padece ningún penalizador. Sin embargo, los injertos son más propensos a los impedimentos visuales y operativos cuando son pirateados (ilusiones virtuales, efectos de denegación de servicio…). Los personajes que usan la interfaz háptica de un ecto, por su parte, sufren un pequeño desfase en sus actividades de malla debido a las pulsaciones manuales, controles físicos e interacción con los controles virtuales. En términos de juego el uso de hápticas impone un modificador de habilidad de –10 a todas las pruebas de actividad en la malla en las que se intenta apresurar la acción (especialmente en combate y en general en cualquier uso de la malla bajo presión). Además, se incrementa el tiempo de Acciones de Tarea en la malla en un 25% cuando se interfase con hápticas. El lado positivo es que los ectos pueden ser fácilmente quitados y descartados si resultan comprometidos, razón por la que muchos hackers y usuarios preocupados por la seguridad usan un ecto además de sus injertos de malla, enrutando todo el tráfico de alto riesgo a través del ecto como una línea extra de defensa.

Barra lateral: Exploits[1] de Élite

Las reglas de calidad del equipo de malla permite a los jugadores y DJ's hacer una distinción del software de herramientas, separando las de código abierto de los exploits del repertorio estándar de los hacker amateurs y de los wares de penetración de nivel militar de última generación. Mientras que muchos personajes simplemente comprarán o adquirirán tales programas, un hacker con su ética de "hazlo tu mismo" seguramente va a querer diseñar sus propias aplicaciones personalizadas, basadas en su librillo de métodos de intrusión/contraintrusión celosamente guardado.

Para reflejar los esfuerzos que un personaje hacker hace por diseñar, codificar y modificar su propio arsenal personal hecho a medida, puede hacer una Acción de Tarea de Programación con un tiempo de trabajo de 2 semanas. Si tiene éxito, mejora una de sus herramientas de software en un nivel de calidad (pej.: de +0 a +10). Se pueden hacer pruebas múltiples de Programación para mejorar un programa, pero por cada nivel se añade el modificador objetivo como un penalizador a la prueba (pej.: mejorar un paquete de software de +0 a +10 conlleva un –10 a la prueba de Programación).

De manera similar, a discreción del Director de Juego, las herramientas de software (particularmente los exploits) pueden degradar su calidad con el tiempo, reflejando que se han quedado obsoletos. Como regla general, tales programas deberían degradarse aproximadamente cada 3 meses.

ID DE MALLA

Cada usuario de la malla (y de hecho cada dispositivo) tiene un código único llamado ID de malla. Este ID le distingue de todos los demás usuarios y dispositivos y es el mecanismo por el cual otros pueden encontrarle en línea, como una combinación de número de teléfono, dirección de correo y nombre de pantalla. Los ID's de malla son usados en casi todas las interacciones en línea, que son a menudo registradas, lo que signirica que tus actividades en línea dejan un rastro de datos que puede ser seguido.

Afortunadamente para quienes valoran su privacidad, hay maneras de soslayar esto (ver Privacidad y anonimidad). Las IA's IAG's e Infomorfos también tienen su propio ID de malla.

CUENTAS Y PRIVILEGIOS DE ACCESO

Los dispositivos, redes (tales como las PAN's, VPN's y redes cableadas) y servicios requieren que cada usuario que accede lo haga con una cuenta. La cuenta sirve para identificar a ese usuario en particuar, está enlazada con su ID de malla y determina qué privilegios de acceso tienen en dicho sistema. Hay cuatro tipos de acceso: Público, Usuario, Seguridad y Admin.

Cuentas Públicas

Las cuentas públicas son usadas por sistemas que permiten el acceso bien total o parcial a cualquiera en la malla. Las cuentas públicas no requieren ningún tipo de autenticación o proceso de login, la ID de malla del usuario es bastante. Estas cuentas son usadas para proporcinar acceso a cualquier tipo de dato que se considera público: sitios de malla, foros, archivos públicos, bases de datos abiertas, perfiles de redes sociales, etc. Las cuentas públicas normalmente tienen la capacidad de leer y descargar datos y a veces de escribir datos (comentarios en foros por ejemplo), pero poco más.

[1] Nota del T.: Un exploit es una debilidad conocida o descubierta de un sistema o programa que es utilizada por otro para causar un fallo en la secuencia de ejecución y ganar control y permisos que no podría obtener de otra forma.

Cuentas de Usuario
Las cuentas de usuario son las más comunes. Requieren alguna forma de autenticación para acceder al dispositivo, red o servicio. Cada cuanta de usuario tiene unos privilegios de acceso específicos asociados, que son tareas que se le permiten ejecutar al usuario en el sistema. Por ejemplo, la mayoría de usuarios tienen permitido subir y bajar datos, cambiar contenido básico y usar las características básicas del sistema en cuestión. Sin embargo no se les permite normalmente alterar características de seguridad, añadir nuevas cuentas o hacer cualquier cosa que pueda impactar en la seguridad o el funcionamiento del sistema. Dado que unos sistemas son más restrictivos que otros, el Director de Juego decide qué privilegios proporciona cada cuenta de usuario.

Cuentas de Seguridad
Las cuentas de seguridad están ideadas para los usuarios que necesitan mayores privilegios y derechos que los usuarios estándar, pero que no necesitan controlar el sistema entero, tales como hackers o musas. Los derechos de acceso de seguridad normalmente permiten la lectura de logs de registro, ejecutar comandos, añadir/borrar cuentas, alterar los datos de otros usuarios y cosas por el estilo.

Cuentas Admin
Las cuentas admin proporcionan control total sobre el sistema. Los personajes con derechos de administración pueden hacer todo lo que las cuentas de seguridad y además pueden apagar/reiniciar el sistema, alterar los derechos de acceso de otros usuarios, ver y editar todos los ficheros de log y estadísticas y arrancar y parar cualquier software disponible en el sistema.

CALIDAD DEL EQUIPO DE MALLA

No todo el equipo se crea igual y esto es especialmente cierto sobre las computadoras y el software, donde las innovaciones se producen a diario. Mantenerse al día con las últimas especificaciones no es muy difícil, pero en ocasiones, los personajes echarán mano de alguna vieja reliquia o se encontrarán en lugares recluídos o decrépitos con sistemas locales y equipo que no están al día. Igualmente, pueden adquirir algún equipo de último grito directamente del laboratorio o toparse con una instalación con una obra de arte de las defensas de última generación. Para reflejar esto, las pruebas de malla pueden ser modificadas de acuerdo con el estado del hardware y software que se está usando, tal y como se denota en la tabla de Modificadores de Equipo de Malla.

Modificadores de Equipo de Malla

Modificador	Software/Hardware
–30	Dispositivos obsoletos, software no soportado, reliquias de la Tierra o la primera época de expansión en el espacio
–20	Dispositivos dañados/inferiores, software defectuoso o con fallos, tenología pre Caída
–10	Sistemas desfasados o de baja calidad
0	Ectos estándar, injertos de malla y software genérico
+10	Objetos de alta calidad, productos de nivel de seguridad estándar
+20	Dispositivos de última generación. Software avanzado
+30	Tecnología punta recién desarrollada de la más alta calidad
>+30	Tecnología TITAN y/o alienígena

CAPACIDADES DE COMPUTADORES

La electrónica computerizada puede ser dividida en tres categorías simples: Periféricos, Computadores Personales y Servidores. En términos de juego, todos son referidos como Dispositivos.

Periféricos
Los periféricos son dispositivos microcomputerizados que no necesitan toda la potencia de proceso y almacenamiento de un computador personal, pero se benefician de la computación en línea y otras funciones similares. Los periféricos pueden ejecutar software, pero el Director de Juego puede decidir que demasiados programas (10+) degradarán el rendimiento del sistema. Las IA's y los Infomorfos son incapaces de ejecutarse en periféricos, aunque pueden acceder a ellos. Los periféricos sólo tienen cuentas públicas y de usuario (éstas últimas incluyen las funciones de seguridad y admin). Los periféricos comunes incluyen los spimes, los appliance[2], la mayoría de los implantes cibernéticos, los sensores individuales y las armas.

Computadores personales
El término computador personal incluye un amplio rango de tipos de ordenador, pero esencialmente define cualquiera que tenga las capacidades evolucionadas tras generaciones y generaciones de ordenadores para responder a las necesidades diarias de los usuarios. La myoría de los computadores personales son portátiles y destinados al uso por parte de múltiples usuarios a la vez. Los computadores personales pueden ejecutar una IA o Infomorfo a la vez. No pueden correr programas de simulspace. Los computadores personales más comunes incluyen los injertos de malla, los ectos y los vehículos.

Servidores
Los servidores tienen mucha más potencia de proceso y capacidad de almacenamiento que los computadores personales. Son capaces de manejar cientos de usuarios, múltiples IA's e Informorfos y pueden ejecutar programas de simulspace. Aunque muy pocos son transportables, algunos se acercan a esa posibilidad.

SOFTWARE

Un amplio espectro de software está disponible para los usuarios de la malla, desde firewalls e IA's hasta herramientas de hacking y encriptación, tacnets (redes

[2] Nota del T.: Un appliance es un aparato en el que hardware y software se han diseñado con un único fin específico, un reproductor de dvd, un router, un filtro de contenido web o un firewall son buenos ejemplos.

tácticas) y skillsofts (software de mejora de habilidades). Estos programas están listados en el capítulo de Equipo. Como otros equipamientos, el software puede permitir al personaje ejecutar tareas que no podría hacer de otra manera. La calidad del software también puede ser un factor, aplicando un factor apropiadamente (ver Calidad de Equipo de Malla).

Algunos programas están equipados con restricciones digitales para prevenir su copia o compartición. Estas restricciones pueden se pueden superar, pero es una trabajo que consume mucho tiempo, requiriendo una prueba de Acción de Tarea de Programación con un período de tiempo de 2 meses. Sin embargo gracias a los esfuerzos del movimiento de código abierto (open source) y de numerosos piratas individuales, bastante software está disponible gratuitamente en línea. La disponibilidad de software pirata o gratuito dependerá del hábitat local y de cuestiones legales. Encontrarlo puede ser cuestión de una simple búsqueda o puede requerir el uso de reputación para encontrar a alguien que lo tenga. Normalmente suele haber al menos un sindicato del crimen local deseando ayudar (por un precio).

Compatibiliadad de software

En la mayoría de los casos, la compatibilidad del software no va a ser un problema para los personajes. Sin embargo, los Directores de Juego a los que les guste usarla como un instrumento argumental, pueden introducir problemas de compatibilidad en ciertos casos, tanto si se hace para incrementar el dramatismo, ralentizar el avance de los personajes o crear obstáculos que deben superar. Es más probable que tales incompatibilidades surjan cuando se trate con sistemas o dispositivos obsoletos o al menos aquellos que seguramente no disponen de las últimas actualizaciones y parches. Las incompatibilidades también pueden usarse como inconvenientes de adquirir software de fuentes de poca confianza.

Los problemas del conflicto de software tendrán uno de dos efectos. O bien el software simplemente no funcionará con ciertos dispositivos, o infligirá un modificador de –10 a –30 debido a inestabilidades y fallos. Si el Director de Juego lo permite, un personaje puede reducir esta penalización parcheando el software, lo que requiere una prueba de Programación como Acción de Tarea (1 día). Por cada 10 ptos. de MdE, se reduce el modificador de incompatibilidad en 10.

FILTROS DE TRÁFICO Y NIEBLA

Las redes de la Malla y la RA están saturadas con yottabytes[3] de información. Aunque los injertos de malla y los ectos pueden lidiar con un montón de tráfico de datos en términos de ancho de banda y potencia de procesado, usar filtros para separar el tráfico no deseado es simplemente una necesidad. Esto es especialmente cierto con la RA, donde las entópticas no deseadas pueden confundir tu visión y distraerte. No en vano, el spam entóptico de diferentes tipos (anuncios, arengas políticas, porno, estafas…) hacen todo cuanto pueden para superar estos filtros y en muchas áreas la cantidad de entópticas sin filtrar puede ser abrumadora, fenómeno conocido como “niebla” o “bruma”

A discreción del Director de Juego, la niebla puede interferir con las percepciones sensoriales de un usuario. Este modificador puede variar desde –10 a –30 y en algunos casos puede resultar tan perturbador como afectar a todas las acciones del personaje. Para disolver la niebla de datos, la musa de un personaje debe ajustar sus parámetros de filtros con un éxito en una prueba de Interfasar modificada por el penalizador de niebla. De manera alternativa, el personaje puede deshabilitar completamente la entrada de RA, pero esto seguramente le va a perjudicar de otras formas.

ESCLAVIZANDO DISPOSITIVOS

Tanto por facilidad de uso como por motives de privacidad y seguridad, uno o más dispositivos pueden ser esclavizados a otro. Un dispositivo (normalmente los injertos de malla o el ecto del personaje) toma el rol de maestro, mientras los otros toman el rol de esclavos. Todo el tráfico desde y hacia los dispositivos esclavos es enrutado a través del maestro. Esto permite a los dispositivos esclavos confiar en las características de seguridad y monitorización activa del maestro. Cualquier que quiera conectar o hackear un dispositivo esclavo, es enrutado al maestro para su autenticación y escrutinio de seguridad. Los dispositivos esclavos automáticamente aceptan comandos de su dispositivo maestro. Esto significa que un hacker que penetra en un sistema maestro puede acceder legítimamente y enviar comandos a uno esclavo, asumiendo que sus privilegios de acceso se lo permiten.

Las PAN’s (Personal Area Networks) se conforman típicamente al esclavizar todos los dispositivos del personaje a su ecto o injertos de malla. De manera similar, los componentes individuales de un sistema de seguridad (puertas, sensores, etc.) son esclavizados normalmente a un nodo central de seguridad que sirve como cuello de botella para cualqueira que aspire a hackear el sistema. Lo mismo suele ser cierto para otras redes e instalaciones.

EJECUTANDO COMANDOS

Los personajes pueden ejecutar o enviar comandos a cualquier dispositivo esclago o bot teleoperado (ver Control Remoto de Carcasas) con una Acción Rápida. Cada comando cuenta separadamente a menos que el personaje envíe el mismo a múltiples dispositivos/drones.

RETARDOS POR DISTANCIA (LAG)

En cuanto extiendes tus comunicaciones sobre grandes distancias. Aparece el riesto de los retardos temporales o lag. La mayoría de las comunicaciones quedan restringidas al ámbito local por esta razón, lo que generalmente significa tu hábitat y cualquier otro en 50.000km. en cuerpos planetarios como Marte, Venus, Luna o Titán, “local” implica todos los hábitats y redes enmalladas en dicho cuerpo planetario.

Si un personajeestá buscando en la malla más allá de su área local, la manera más eficaz es transmitira una IA de búsqueda (normalmente una copia de su musa) o un bifurcado al área no local, que entonces ejeutará su

[3] Nota del T.: Un Yottabyte = 10^{24} bytes = 1000.000.000.000 (1Billón) Terabytes = 1000 Billones de Megabytes.

búsqueda y devolverá resultados completos. Este proceso, sin embargo, suma el tiempo de transmisión al de búsqueda (pej.: buscando en la malla de una estación a 10 minutos–luz, añade 20 minutos a la búsqueda ya que la misma es transmitida y los resultados enviados de vuelta). Dado que las comunicaciones de larga distancia son a veces interfericas o relegadas en pos de elementos de más alta prioridad, el Director de Juego puede incrementar este tiempo a su discreción. Si la búsqueda implica correlación y finos ajustes de los parámetros basándose en los datos acumulados de diferentes zonas locales, el período de búsqueda puede incrementarse exponencialmente debido a la necesidad de interacción bidireccional.
Si el personaje simplemente está comunicándose o accediendo a redes no locales, un retardo apropiado debe introducirse entre la comunicación y las acciones. Los efectos de este lag quedan a discreción del Director de Juego para ajustarse a las distancias y otros factores.

ACCEDIENDO A MÚLTIPLES DISPOSITIVOS

Los personajes enmallados pueden conectarse e interactuar con numerosos dispositivos, redes y servicios simultáneamente. No hay penalización por hacer esto, pero un personaje sólo se puede centrar en un sistema a la vez. En otras palabras, puedes interactuar con un sistema en cada momento, aunque también puedes cambiar entre ellos libremente, incluso durante la misma Fase de Acción. Podrías por ejemplo, gastar unas cuantas acciones rápidas para enviar un mensaje con tu ecto, decirle a tu spime en casa que te empiece a cocinar la cena, y mirar el perfil actualizado de un amigo en una red social. No puedes, sin embargo, hackear en sistemas separados simultáneamente. Hay que destacar que puedes enviar el mismo omando a múltiples dispositivos esclavos o drones teleoperados con la misma Acción Rápida como ya se ha expuesto.

BÚSQUEDAS ONLINE

La habilidad Búsqueda representa la capacidad de un personaje de encontrar información en la malla.Tal información incluye cualquier tipo de datos digitalizados: texto, imágenes, vídeo, RX, capturas de sensor, datos en bruto, software, etc. Estos datos recabados de todo tipo de fuentes: blogs, archivos, bases de datos, directorios, redes sociales, redes Rep, servicios en línea, foros, salas de chat, cachés de torrent y sitios de malla de todo tipo. Las búsquedas son llevadas a cabo usando varios motores de búsqueda públicos y privados, tanto genéricos como especializados así como índices de datos e IA's de búsqueda.
Búsqueda tiene además otros usos. Los hackers la usan cuando necesitan información específica en una red o dispositivo en el que han irrumpido. De igual forma, dado que inevitablemente todo el mundo usa e interactúa con la malla, la habilidad de Búsqueda es también una manera de identificar, seguir y/o conseguir información de personas mientras no hayan escondido su identidad, trabajen anónimamente o cubran sus ID con un velo de desinformación.

DESAFÍOS DE BÚSQUEDA

Debido a la abrumadora cantidad de datos disponible, encontrar lo que estás buscando puede parecer a veces una tarea dantesca.
Afortunadamente, la información está aceptablemente bien organizada, gracias al duro trabajo de las IA's "araña", que navegan por la mañña y actualizan constantemente los datos y los índices de búsqueda. De forma adicional, la información en la malla está etiquetada con semántica, lo que significa que se presenta con código que permite a una máquina entender el cotnexto de la misma así como lo haría un lector humano. Esto ayuda a las IA's y el software de búsqueda a correlacionar datos más eficientemente. Por lo que encontrar información no es habitualmente tan difícil como entenderla. Encontrar información especializada, escondida o correlacionar datos de múltiples fuentes es habitualmente el auténtico desafío. Puede que un problema mayor sea la cantidad de datos incorrectos o desinformación en línea. Algunos datos simplemente están mal (los errores pasan) o desactualizada, pero la naturaleza de la malla implica que tales cosas pueden persistir durante años e incluso propagarse ampliamente mientras circulan sin una comprobación factual. Igualmente, dada la transparencia de la sociedad actual, algunas entidades se dedican activamente a extender la desinformación con tal de llenar la malla de suficientes falsedades para que la verdad quede escondida. Dos factores ayudan a combatir esto, siendo el primero que las mismas fuentes tienen sus propias puntuaciones de reputación por lo que las fuentes de poca confianza o desacreditadas pueden ser identificadas y puntuadas más bajo en los resultados de búsqueda. Segundo, muchos archivos se aprovechan del crowdsourcing (el aprovechamiento del poder colaborativo de los usuarios de la malla y sus musas por doquier) para verificar la integridad de los datos de manera que tales sitios sean dinámicos y autocorregidos.

BARRA LATERAL: CAPACIDADES DE BÚSQUEDA

La búsqueda en línea en *Eclipse Phase* no es lo mismo que simplemente googlear algo. A continuación hay cinco maneras en las que está vastamente mejorada:

· Reconocimiento de patrones: la biometría y otras formas de reconocimiento de patrones son eficientes e inteligentes. Es posible no solamente ejecutar búsquedas de reconocimiento de imagen (en tiempo real, a través de todos los spimes disponibles e información captada por sensores), sino buscar por patrones tales como los andares, sonidos, colores, muestras de emoción, tráfico, movimientos de multitudes, etc. El análisis de comportamiento y la kinética incluso permiten búsquedas por sensor de personas que exhibin ciertos patrones de comportamiento, como remolonear rondar sospechosamente un lugar, nerviosismo o agitación.

· Metadatos: la información y ficheros online llegan datos ocultos sobre su creación, alteración y acceso. Los metadatos de una foto, por ejemplo, toman nota de con qué aparato se tomó, quién la tomó, cuando y dónde además de quién accedió a ella en línea, aunque tales

metadatos pueden ser fácilmente borrados o anonimizados.

· Correlación de datos: La combinación de computación abundante, datos archivados y sensores públicos ubicuos permite extraer correlaciones intrigantes de los datos cotejados por minería. En el caos de una emergencia de hábtitat, tal como un ataque terrorista por ejemplo, la ID de todos los presentes en la zona puede ser escaneado, comparado con archivos de datos para separar a aquellos que tienen un historial de presencia en dicha zona en esa hora en particular de los restantes y contrastados contra bases de datos con historiales de sospechosos/criminales mientras se analizan sus acciones grabadas en busca de comportamiento inusual.

· Traducción: la traducción en tiempo real de audio y vídeo está disponible a través de bots de traducción de código abierto (open source o código libre que todo el mundo puede corregir).

· Predicciones: un porcentaje significativo de lo que la gente hace cualquier día en respuesta a ciertas situaciones, es conforme a rutinas, habilitando una fácil predicción del comportamiento. Las Musas se aprovechan de esto para anticipar las necesidades y proveer cualquier cosa que se desee en el momento apropiado y el contexto apropiado. La misma lógica se aplica a las acciones de grupos de gente, tales como la economía o el discurso social, haciendo de las predicciones del mercado un gran negocio en el sistema interior.

MANEJAR LAS BÚSQUEDAS

La búsqueda online es a menudo un elemento crucial de los escenarios de *Eclipse Phase* cuando los personajes acuden a la malla para buscar trasfondos y descubrir pistas. Las siguientes sugerencias presentan un método de manejar las búsquedas que no confía sólo en las tiradas de dados y se integra con el flujo de la trama.

Primero, la información común e incosecuente debería estar inmediatamente disponible sin que requiera una tirada en absoluto. La mayoría de los personajes confían en sus musas para manejar por ellos las búsquedas, dándoles los resultados mientras el personaje se centra en otras cosas.

Para las búsquedas son más detalladas, difíciles o importantes para la trama, se debería realizar una Prueba de Búsqueda (realizada bien por el personaje o por la musa). Esta prueba indica el proceso de buscar enlaces y/o acumular todos los datos que pueden ser en realidad relevantes para el tópico de búsqueda. Se debería ajustar la prueba en función de lo obscuro del tema a bucar, variando desde +30 para información común y temas públicos hasta –30 para inteligencia y temas inusuales u oscuros. Esta búsqueda inicial tiene un período de tiempo de un minuto. Si resulta exitosa, devuelve datos suficientes para darle al personaje una visión básica del tema, puede que con detalles superficiales. El DJ debería el MdE para determinar la profundidad de los datos provistos por esta excursión inicial, con un Éxito Excelente fuente de detalles adicionales. De manera similar un Fracaso Severo (MdF 30+) puede resultar en datos que hagan que el personaje trabaje con información incorrecta o directamente malintencionada.

El siguiente paso no es tanto acumular enlaces y datos como analizarlos y entender la información adquirida. Esto requiere otra Prueba de Búsqueda, de nuevo modificada en función de lo oscuro o raro del tema. Si el Director de Juego lo permite, se pueden aplicar habilidades complementarias a esta prueba, aportando modificadores de bonificación (pej.: saber de Académica: Química puede ayudar en la búsqueda de los efectos de una extraña droga). Las musas también hacen esto, aunque sus habilidades son típicamente inferores. Como en el caso anterior, el éxito determina la calidad y profundidad del análisis, con un Éxito Excelente otorgando una historia completa y problemas potenciales relacionados y un Fallo Severo conllevando asunciones totalmente incorrectas. El tiempo dedicado a esta fase de la búsqueda depende en gran medida de dos factores: la cantidad de datos a analizar y la importancia del argumento. Los DJ's necesitan sopesar cuidadosamente la distribución de pistas e información de inteligencia a los jugadores. Si se les dá demasiada y muy pronto, reventarán la trama. Si no se les da bastante, pueden frustrarse o perseguir pistas falsas. El timing lo es todo (información apropiada en el momento apropiado).

BÚSQUEDAS EN TIEMPO REAL

Los personajes pueden poner en marcha escaneos de malla que les alerten si sale a la luz, se actualiza o cambia cualquier información relevante. Esto es una tarea normalmente asignada a las musas de manera continua. Cada vez que tales datos aparecen, el Director de Juego hace en secreto una Prueba de Búsqueda, modificada por lo oscuro o raro del tema. Si tiene éxito, la actualización es detectada. Si no, pasa desapercibida, aunque el Director de Juego puede permitir otra Prueba si el tema alcanza un rango más amplio de circulación o interés.

DATOS ESCONDIDOS

Es importante recorder que no todo puede ser encontrado en línea. Algunos datos pueden ser adquiridos únicamente (o más fácilmente) preguntándole a la gente apropiada. La información que se considera privada, secreta o propietaria, estará seguramente bien guardada tras firewalls VPN, en redes cableadas fuera de la malla o en archivos comerciales privados. Esto requiere que el personaje consiga acceso a tales redes con tal de conseguir los datos que necesita (asumiendo que al menos sabe dónde mirar).

Vale la pena destacar que algunas entidades envían IA's a la malla con la intención de encontrar y borrar datos que preferirían ocultar, incluso si esto requiere hackear sistemas para alterar dicha información.

ESCANEO, SEGUIMIENTO Y MONITORIZACIÓN

La mayoría de los usuarios dejan rastros de su presencia física y digital a través de la malla. Las cuentas a las que

acceden, los dispositivos con los que interaccionan, los servicios que usan y las entópticas que percibem mantienen logs o registros de eventos y algunos de ellos son públicos. Simplemente pasar cerca de algunos dispositivos es suficente para dejar un rastro ya que las interacciones de radio de campo cercano son normalmente registradas. El rastro electrónico puede usarse para seguir a un usaurio, tanto para asegurarse de su posición física como para tomar nota de sus actividades en línea.

ESCANEO INALÁMBRICO

Interfasar con un dispositivo o red inalámbricos, ya sea para establecer una conexión o para otros propósitos, el dispositivo/la red objetivo debe ser localizada primero. Para localizar un nodo activo sus transmisiones de radio inalámbricas deben ser detectadas.

La mayoría de los dispositivos escanean automáticamente en busca de otros dispositivos al alcance (ver Alcances de Radio y Sensores) como procedimiento habitual, por lo que no se requiere ninguna Prueba. Esto significa que es trivial para cualquier usuario conseguir una lista de dispositivos inalámbricos y redes a su alrededor, junto con las ID's de malla asociadas. De igual manera, se puede instruír a una musa o dispositivo para que alerte al usuario cuando una nueva señal (o un usuario específico) entra en el rango de alcance.

Detectar señales, sin embargo, es un poco más difícil. Para detectar una señal oculta, la parte que escanea debe buscar activamente dichas señales, comando una Acción Compleja y haciendo una Prueba de Interfasar con un modificador de –30. Si tiene éxito, detecta las emisiones ocultas. Si el personaje intentando conseguir la ocultación toma medidas contramedidas activas, también requiere de una Acción Compleja y una Prueba Enfrentada de Interfasar (con el –30 aplicado a quien escanea).

Para los dispositivos encubiertos que sólo transmiten en cortas ráfagas, la detección inalámbrica es sólo posible durante el breve período en el que se realiza la transmisión de ráfaga.

SEGUIMIENTO FÍSICO

Muchos usuarios permiten voluntariamente su seguimiento a través de la malla. Para ellos esto es una característica útil (permite a sus amigos encontrarles, que sus seres queridos sepan dónde están y que las autoridades puedan acudir en su ayuda en caso de emergencia). Encontrar su localización es cuestión simplemente de buscarles en el directorio local, sin que requiera tirada (asumiendo que sepas dónde estás). El posicionamiento en mall tiene una precisión de hasta 5 metros. Una vez localizado, la posición del objetivo puede ser monitorizada mientras se mueve siempre que mantenga activa una conexión inalámbrica a la malla.

Localización por ID de malla

La posición física de un usuario desconocido puede también localizarse a través de su actividad en línea en la malla (o más específicamente por su ID de malla). La seguridad de red a menudo traza las intrusiones de esta manera y despacha equipos de operaciones a por los intrusos. Para localizar a un usuario desconocido únicamente por su ID de malla se requiere una Prueba de Búsqueda. Si se tiene éxito, será localizada su posición física actual (si todavía sigue en línea) o el último punto de interacción con la malla. Si el el personaje está en modo privado, se aplica un modificador de –30.

Localización por biometría

Dada la existencia de tantos spimes, cámaras y sensores públicos, la gente también puede ser localizada incluso por su perfil usando software de reconocimiento facial. Este software accede a los registros de vídeo y busca coincidencias con una imagen o foto del objetivo. Sin embargo, dado el abromador volumen de cámaras y el típico rango de falsos positivos y falsos negativos, encontrar al objetivo a menudo es una cuestión de suerte. Se les puede dar prioridad a las cámaras que monitorizan vías públicas para reducir la búsqueda, pero se corre el riesgo de perder al objetivo si evita las áreas con tráfico denso. El éxito de las búsquedas de este tipo es mejor dejarlo al criterio del Director de Juego, pero también se puede pedir una Prueba de Búsqueda, modificada apropiadamente por el tamaño del área observada, que es dondequiera que haya oportunidad de que el objetivo sea visto.

Otras firmas biométricas se pueden usar para este tipo de búsqueda, aunque están habitualmente menos disponibles que las cámaras: firmas térmicas (requieren cámaras infrarrojas), andares y tipo de paso, olor (requiere sensores olfativos), ADN (requiere escáneres genéticos), etc. Cada escaneo biométrico requiere de un tipo diferente de software.

Seguimiento de la actividad digital

Seguir las actividades en línea de alguien (navegar la malla, interacciones entópticas, uso de servicios, mensajería, etc.) es ligeramente más difícil, dependiendo de lo que estés buscando exactamente. Recopilar información de la actividad de malla pública de un usuario (perfiles de redes sociales, posts en foros públicos, etc.) se maneja igual que una búsqueda en línea estándar.

Seguimiento por ID de malla

Una búsqueda más refinada puede intentar usar la ID de malla del usuario, usándolo como una clase de huella dactilar digital para encontrar dónde ha estado en línea. Esto implica en primer lugar comprobar los logs o registros de acceso/transacciones, que no siempre son accesibles públicamente. Este tipo de búsqueda requiere una Prueba de Búsqueda, manejada como una Acción de Tarea con un tiempo de ejecución de una hora.

SNIFFING

El tráfico de red inalámbrico es emitido al aire (o espacio), lo que significa que pude ser interceptado por otros dispositivos inalámbricos. "Sniffar" o hacer sniffing, implica capturar y analizar el tráfico de datos que fluye a través de la malla. Para irrumpir en la comunicación inalámbrica, se necesita un programa de captura de paquetes o sniffer y estar dentro del radio de alcance del objetivo (o alternativamente, acceder a un dispositivo

que lo esté desde el que snifar). Para capturar la información se debe tener éxito en una Prueba de Infosec. Si se tiene éxito, se captura tráfico de datos de cualquier dispositivo localizado en el alcance. Hay que denotar que snifar no funciona con el tráfico encriptado (incluyendo VPN's y cualquier otra cosa que use encriptación de clave pública) ya que los resultados son ininteligibles. Las comunicaciones cuánticas encriptadas no pueden ser snifadas. Una vez tienes los datos, encontrar la información que estás buscando puede ser un desafío. Manejar esto requiere una Prueba de Búsqueda estándar.

Snifado remoto vía ID de malla
Por último, una ID de malla puede ser monitorizado activamente para ver en qué actividad de malla se involucra. Esto requiere software especial de snifado y una Prueba de Búsqueda. Si se tiene éxito, la monitorización provee información de las actividades públicas de dicho usuario (cuánta, está en función del MdE y del criterio del Director de Juego), tal como a qué sitios ha accedido, con quien intercambia mensajes, etc. Sin embargo, no despatapará nada encriptado (a menos que se rompa la encriptación) o cualquier cosa que se tunele vía VPN (a menos que la VPN se hackee primero), aunque sí mostrará que hay comunicaciones encriptadas en curso o que está teniendo lugar el uso de VPN.

PRIVACIDAD Y ANONIMIZACIÓN

Dado lo fácil que es monitorizar las actividades en la malla, muchos usuarios buscan opciones para su privacidad y anonimización.

MODO PRIVADO

Los personajes que pasan a modo privado, esconden su presencia en línea y actividades de otros hasta cierto grado.
Los parámetros exactos son ajustables, pero típicamente consisten en enmascarar sus perfiles sociales y presencia a otros usuarios en las proximidades inmediatas, como tener un número de teléfono sin listar. El Modo Privado puede ser usado para limitar la firma de ID's de malla en los accesos a datos y logs de transacciones, aplicando un modificador de –30 a los intentos de búsqueda o seguimiento a través de la actividad en línea.

Señales encubiertas
Otra táctica que se puede usar en pos de la privacidad es encubrir las señales inalámbricas de radio que emites. Este método usa una combinación de señales de amplio espectro, saltos de frecuencia y modulación para hacer las emisiones de radio más difíciles de detectar con un escaneo. Encubrir tus señales es o bien una actividad pasiva (Acción Automática, modificador de –30 a Pruebas de Interfasar para localizar la señal) o una activa (Acción Compleja, requiere Prueba Enfrentada para localizar).

ANONIMIZACIÓN

La anonimización lleva el problema de la privacidad un poco más allá. El usuario no sólo oculta su ID de malla, sino que usa activamente ID's de malla falsas y otras medidas para reenrutar y ofuscar su rastro de datos. La anonimización es una necesidad tanto para los operativos clandestinos como para aquellos implicados en actividades ilícitas en la malla.

ID's de malla falsas
El método más sencillo de hacer anónimas las actividades de malla es configurar tu musa para que provea una ID de malla falsa en las transacciones en línea. Aunque ilegal en muchas jurisdicciones, esta es una tarea fácil de hacer para cualquier personaje o musa. Se usan múltiples ID's haciendo extremadamente difícil para cualquiera vincular todas las actividades del usuario. Alguien intentando seguir al personaje a través de estos ID's de malla falsos, debe vencerle en una Prueba Enfrentada, penalizando la tirada de Búsqueda con un modificador de –30 contra la habilidad Infosec del personaje buscado (o de su musa). Es una Acción de Tarea con un tiempo base de 1 hora, ajustado al alza en función de la cantidad de actividad que se espera escanear. Si tiene éxito, el perseguidor consigue acumular suficientes evidencias correlacionadas y registros de ID's falsas como para hacerse una imagen de las actividades del personaje (como de ajustada es esta imagen depende de su MdE). Si falla, el personaje anónimo se ha camuflado eficazmente en la malla.
Monitorizar activamente a un personaje que fluctúa su ID de malla con un programa de snifado o el seguimiento físico es casi imposible, dado el continuo cambio de ID's y los señuelos que pueda dispensar hacen demasiado difícil mantener el rastro.

Servicios de cuentas anónimas
Un gran número de personas (no sólo criminales, hackers y agentes secretos) tienen interés en mantener algunos de sus asuntos en el anonimato. Para satisfacer esta demanda, varios proveedores de servicios en línea ofrecen cuentas anónimas para mensajería y transferencia de crédito. Algunos de estos proveedores son negocios legítimos (en lugares donde es legal), otros son criminales operando ilegalmente, otros son hacktivistas promoviendo el meme de la privacidad e incluso otros son hipercorporaciones y otras organizaciones que ofrecen tales servicios internamente a su propio personal o miembros.
La interacción entre el proveedor y el usuario es encriptada y anonimizada, sin que se mantengan logs, por lo que incluso si los servidores del proveedor son hackeados, un intruso no encontrará ninguna pista. Mientras que algunas cuentas anónimas están establecidas para su uso habitual, los auténticos paranoicos usan (múltiples) cuentas de un solo uso para obtener la máxima seguridad. Las cuentas de uno solo uso sirven para un único mensaje (entrante o saliente) o transacción de crédito tras lo que son borradas.
Hacer seguimiento de cuentas anónimas e prácticamente imposible y algo que sólo una organización con vastos recursos podría intentar empleando un esfuerzo sistemático y muy caro.

Ectos desechables
Otra opción para aquellos que buscan privacidad y seguridad es simplemente usar ectos desechables. Usando este método, todo el tráfico es enrutado a través de un ecto específico (usando su ID de malla) durante un tiempo limitado (hasta que está demasiado expuesto o "caliente") y entonces simplemente se descarta o destruye.

INTRUSION 254

PRECONDITIONS 254

CIRCUMVENTING AUTHENTICATION 255

INTRUSION TESTS 255

INTRUDER STATUS 256

CHANGING STATUS 257

BRUTE-FORCE HACKING 257

INTRUSION COUNTERMEASURES 257

SECURITY ALERTS 257

PASSIVE COUNTERMEASURES 257

ACTIVE COUNTERMEASURES 258

JOINT HACKING/SECURING 258

SUBVERSIÓN

Una vez que un intruso ha invadido un dispositivo o red, puede llevar a cabo cualquier tarea en la que esté interesado, tal como le permite dicho sistema. Dependiendo del tipo de cuenta que el intruso haya hackeado, puede tener o no privilegios de acceso a lo que quiere hacer. Si sus derechos de acceso se lo permiten, la actividad es tomada como la de un usuario legítimo y no hace falta Prueba alguna (a menos que la propia actividad lo requiera, tal como una Búsqueda). Por ejemplo, un hacker que se infiltra en el sistema de seguridad de un hábitat con una cuenta de seguridad, puede monitorizar cámaras, desactivar sensores, revisar grabaciones de seguridad y demás, como cualquier usuario legítimo con derechos de seguridad sería autorizado a realizar.
Iniciar cualquier tipo de actividad para la cual no tienes permisos de acceso es mucho más difícil y requiere hacker el sistema. Esto típicamente requiere una Prueba Existosa de Infose, modificada por la dificultad de la acción tal como se especifica en la tabla Dificultades de Subversión. En la mayoría de los casos no se trata de una Prueba Enfrentada incluso si el sistema está siendo activamente monitorizado a menos que se indique específicamente lo contrario. Sin embargo, fallar dichas Pruebas, resultará en un cambio del estado del intruso (ver Fallar Pruebas).
Se dan ejemplos de diferentes tipos de subversiones de sistema en la barra lateral. No es una lista exhaustiva, sin embargo y se anima a DJ's y jugadores a improvisar efectos de juego en caso de que una acción no haya sido explícitamente descrita.

Ejemplos de Subversión
Adicionalmente a las areas anotadas en la table de Dificultades de Suversión, estos modificadores presentan algunos ejemplos de acciones extra.

Mod	Tarea
Hackear Bots/Vehículos	
–0	Dar órdenes a drones
–10	Alterar parámetros de sistemas sensors, deshabilitar sensors o sistemas de armas.
–20	Alterar entradas de smartlink, enviar datos falsos a una IA o teleoperador
–30	Bloquear a una IA o a un teleoperator, tomar el control vía puppet sock.
Hackear Ectos/Injertos de Malla	
–0	Interaccionar con entópticas, hacer amigo en línea a cualqueira en alcance, hacer compras usando el crédito del usaurio, interceptar comunicaciones, registrar en un log la actividad.
–10	Alterar el perfil social/status de la red, ajustar los filtros RA, modificar la interfaz sensorial, cambiar el skin de la RA, cambiar el avatar, acceder a la VPN.
–20	Bloquear o confundir sentidos, injector ilusiones RA, falsificar commandos a drones/dispositivos esclavo.
–30	Explusar al usuario fuera de su RA.
Hackear Sistemas de Hábitats	
–0	Abrir/cerrar puertas, parar/arrancar elevadores, operar el intercom.
–10	Ajustar la temperature/iluminación, deshabilitar avisos de seguridad, reemplazar el skin entóptico, bloquear puertas, cambiar los temporizadores de tráfico.
–20	Deshabilitar subsistemas (desagüe, reciclaje, etc.), deshabilitar enlaces wifi, enviar patrullas de reparación.
–30	Anular los cierres de seguridad.
Hakear Sistemas de Seguridad	
–0	Mover/manipular cámaras/sensors, localizar sistemas de seguridad/guardias/bots.
–10	Ajustar patrones de barrido de sensors, ver los logs de seguridad, deshabilitar sistemas de armas.
–20	Borrar logs de seguridad, despachar equipos de seguridad.
–30	Deshabilitar alertas.
Hackear Sistemas Simulspace	
–0	Ver el estado actual del simulspace, simulmorfos y egos con acceso.
–10	Cambiar reglas del dominio, añadir trucos, alterar

	parámetros de la historia, alterar los simulmorfos, cambiar la dilatación temporal.
–20	Eyectar simulmorfo, alterar/borrar las IA's personaje
–30	Abortar la simulación
Hackear Spimes	
–0	Obtener informe de estado, usar las funciones del dispositivo
–10	Ajustar la IA/parámetros de voz y personalidad, ajustar los parámetros de funcionamiento programado.
–20	Deshabilitar sensors, deshabilitar funciones del dispositivo.

Dificultades deSubversión Modificadores de dificultad para tareas comunes.	
Mod	**Tarea**
–0	Execute commands, view restricted information, run restricted software, open/close connections to other systems, read/write/copy/delete files, access sensor feeds, access slaved devices
–10	Change system settings, alter logs/restricted files
–20	Interfere with system operations, alter sensor/AR input
–30	Shut system down, lockout user/muse, launch countermeasures at others

ILUSIONES RA

Un harcker que se ha infiltrado en un ecto, injerto de malla o algún otro dispositivo con una interfaz RA, puede inyectar diferentes tipos de ilusiones visuales, auditivas, táctiles e incluso emocionales en la realidad aumentada del usuario del dispositivo dependiendo del tipo de interfaz usada. Cómo responderá el usuario hackeado a la ilusión depende de un número de factores, tales como si está al tanto de la intrusión (el hacker está en estado Descubierto o Bloqueado), qué tipo de interfaz está usando (entóptica o háptica) y cómo es de realista la ilusión.

Las mejores ilusiones son, por supuesto, fabricadas con antelación, usando las mejores herramientas disponibles de manipulación sensorial y de imagen. Tales ilusiones son hiperrealistas. Cualquiera que haga una Prueba de Percepción para identificarlas, sufre un modificador de –10 a –30 (a discreción del Director de Juego). Una colección ecléctica de programas de software, ofrece un rango diverso de ilusiones RA. Los hackers pueden también improvisar ilusiones "on the fly", normalmente parcheando datos sensoriales desde otras Fuentes, auqnue esto es más difícil y más fácilmente detectado (túpicamente añade desde un +10 a un +30 a la Prueba de Percepción). La ventaja es que el hacker puede modificar la ilusión en respuesta a las acciones del personaje o a factores ambientales en el momento. El software de ilusiones RA, sin embargo, también ofrece plantillas que pueden ser modificadas y controladas en tiempo real a través de una interfaz conectada.

Cuandoquiera que un usuario es bombardeado con ilusiones RA, el Director de Juego debería hacer una Prueba de Percepción secreta para ver si detecta el engaño. Incluso si lo hace, el personaje aún puede reaccionar a ellas. Prácticamente todo el mundo se agacha cuando ve un objeto volar de repente hacia su cabeza, ya que su cuerpo reacciona por su cuenta antes de que el cerebro se de cuenta de que es una ilusión y no una amenaza.

A parte de su valor de engaño, las ilusiones pueden ser usadas para distraer a los usuarios o limitar sus facultades perceptivas. Por ejemplo, nubes oscuras ilusorias pueden oscurecer la visión, ruidos desgarradores a alto volumen pueden hacer que la gente se encoja y una sensación de cosquilleo persistente puede volver loco a cualquiera. Tales efectos pueden aplicar un modificador de –10 a –30 a Pruebas de Percepción y otras acciones, pero el usuario puede ajustar sus filtros y/o apagar su AR si es necesario.

PUERTAS TRASERAS

Una puerta trasera es un método de evitarlas características normales de autenticación y seguridad de un sistema. Habilita a un hacker para colarse en un sistema explotando una debilidad (que puede tomar la forma de un programa instalado o una modificación de uno existente o del harware) que ha sido integrada previamente en el sistema, ya sea por él mismo o por otro hacker (que comparte la puerta).

Para instalar una puerta trasera, el hacker deber infiltrarse con éxito en el sistema y superar una Prueba de Programación y otra de Infosec (o una Prueba Enfrentada de Infosec si el sistema está siendo monitorizado activamente). La Prueba de programación determina coo está de bien construida y escondida la puerta trasera entre los procesos del sistema, mientras que la de Infosec representa la incorporación de privilegios al uso de la misma (–30 para admin.)

Una vez instalada, usar una puerta trasera, no requiere Pruebas para acceder al sistema, el hacker simplemente hace log in como si fuera un usuario legítimo, obteniendo estado Encubierto. Cualquiera que esté al tanto de los detalles de la puerta, puede usarla. Lo que durará operativa una puerta depende de muchos factores y está en manos del Director de Juego. Las puertas traseras sólo serán evidentes durante una auditoría de seguridad completa, por lo que los sistemas más paranoicos serán más propensos a encontrarlas antes. Las auditorías de seguridad suelen también realizarse cuando un hacker es Descubierto pero nunca Bloqueado. Una auditoría de seguridad es una Acción de Tarea con un tiempo de 24 horas. El personaje que dirige la auditoría hace una Prueba de Infosec para buscar la puerta trasera. Si quien la instaló consiguió un MdE Excelente en su tirada de Programación, esta tirada sufre un modificador de –30.

CRASH DE SOFTWARE

Los intrusos pueden intentar causar un "crash" o fallo de software matando los procesos en ejecución. Esto requiere una Acción Compleja y una Prueba de Infosec. Hay que denotar que cierto software está configurado para reiniciarse inmediatamente, pero esto puede tardar desde 1 Acción completa a 1 minuto, dependiendo del sistema. Los hackers puede cascar IA's, IAG's e incluso informorfos de esta manera, pero el proceso es más difícil. En estos casos, se hace una Prueba Enfrentada de Infosec contra el objetivo, quien inmediatamente sabe

que está bajo ataque. Para causar un crash a una IA hacen falta dos éxitos consecutivos. Tres para tumbar una IAG o infomorfo. Si se tiene éxito, la IA/informorfo, inmediatamente se reinicia, lo que generalmente cuesta 3 Turnos de Acción, más si el Director de Juego así lo decide.

ELIMINANDO HUELLAS DE INTRUSIÓN

Los hackers que han evitado ser Bloqueados, pueden intentar limpiar todas las trazas de su intrusíon antes de salir del sistema. Esto implica borrar datos incriminatorios en los logs de seguridad y acceso o por el contrario esconder cualquier prueba de trasteo con el sistema. Requiere una Acción Compleja y una Prueba de Infosec, o una Prueba Enfrentada de Infosec si el sistema está siendo monitorizado. Si tiene éxito, el intruso borra cualquier cosa que pueda ser usada para rastrearle más tarde, tales como ID de malla, etc.

HACKEO DE VPN'S

Las redes privadas virtuales (Virtual Private Networks) son un desafío mayor que los demás dispositivos a la hora de hackear. Dado que existen como redes encriptadas dentro de la malla, acceder a los canales de comunicación dentro de una VPN es poco menos que imposible sin la clave de encriptación. Esto significa que cualquier intento de snifar el tráfico VPN es también inútil sin la clave. Los paquetes capturaros serán un galimatías.

La única manera de hackear una VPN es hackear un dispositivo que sea parte de dicha VPN y esté ejecutando el software de encriptación. Una vez el intruso tiene acceso a tal dispositivo, puede intentar acceder a la VPN. La cuenta que el hacker ha comprometido puede tener privilegios VPN, en cuayo caso ya está dentro. Si no, debe hackear el acceso, requiriendo una Prueba de Infosec con un modificador menor (–10).

Una vez que se ha adquirido acceso a la VPN, el hacker puede tratarla como cualquier otra red. Puede hackear otros dispositivos en la VPN, snifar tráfico, rastrear a otros usuarios en la VPN, buscar datos escondidos en ella y demás.

SCRIPTS

Un script es un programa simple (un lote o paquete de instrucciones) que un hacker puede embeber en un sistema para que sea ejecutado en un momento posterior preestablecido o cuando se cumpla cierto evento que lo dispare, incluso sin que el hacker esté presente. Cuando se activa, el script se encargará de un cierto número de operaciones del sistema limitado por las propias capacidades del mismo y los derechos de acceso que el hacker tenía cuando implementó el script en el sistema. Los scripts son para el hacker una manera estupenda de subvertir un sistema sin estar necesariamente en peligro mientras lo hace. Los scripts pueden ser programados en el momento o estar preprogramados. Cuando compone un script, el personaje debe detallar qué operaciones del sistema llamará, en qué orden y a qué hora (o bajo qué circunstancias se disparará). El script no puede contener más pasos/tareas que la puntuación de Programción de usuario dividia entre 10 (redondeando hacia abajo). Para programar un script, debe tener éxito en una Prueba de Programación con un tiempo determinado por el Director de Juego.

Para cargar el script, el personaje debe haberse introducido en en sistema y superar una Prueba de Infosec (o una Prueb Enfrentada si el sistema está siendo monitorizado). Si tiene éxito, el script es cargado en el sistema y se ejecutará según está programado. Una vez se activa, lleva a cabo la secuencia de acciones preprogramada. La habilidad Infosec del programador se usa para cualquier prueba que esas acciones impliquen. Los scripts aún sin activar pueden ser detectados en una auditoría de seguridad de la misma forma que las puertas traseras.

HACKEO CIBERCEREBRAL

Las vainas y los sintemorfos (incluyendo algunos bots y vehículos) están equipados con cerebros cibernéticos. Mientras que esta tecnología permite a un ego transhumano enfundarse y controlarlos, también padece la desventaja de ser vulnerable al hackeo, como cualquier otro dispositivo electrónico.

Los cibercerebros no están habilitados inalámbricamente por razones de seguridad, pero sí tienen puertos de acceso y están directamente conectados a injertos de malla. Esto significa que con tal de hackear un cibercerebro, el hacker debe tener acceso físico al morfo para conectarse o bien debe primero hackear los injertos de malla y luego entrar en el cibercerebro desde ahí.

Debido a su importancia, los cibercerebroes están equipados con numerosas características de seguridad por hardware para hacer la intrusión realmente difícil. Se aplica un modificador de –30 a todos los intentos de infiltrarse y subvertir un cibercerebro. Hay que denotar que el modificador de –30 para hackear una cuenta admin no se aplica a cibercerebros.

Los cibercerebros son tratados como cualquier otro sistema en lo que a intrusión y subversión se refiere, pero dado que alojan al ego que controla el morfo, representan varias oportunidades de hackeo únicas.

ATRAPAMIENTO

Un personaje intruso puede intentar bloqeuar un ego, previniendo que evacúe el cibercerebro. El hacker (con el modificador de –30 indicado anteriormente) debe superar al personaje defensor o musa en una Prueba Enfrentada de Infosec. Si tiene éxito, el ego no puede transferirse a otro sistema.

Para atrapar totalmente a un personaje, tanto su ego como su musa protectora deben ser bloqueados de todo acceso y control del sistema cibercerebral, de otra manera el ego podría escapar ser liberado.

Los egos atrabados son bastante vulnerables. Podrían ser, por ejemplo, sujetos a carga forzada, bifurcación a la fuerza o psicocirugía.

HACKEO DE MEMORIA

Todos los cibercerebros incorporan aumentos mnemónicos o recuerdos grabados digitalmente. Un

hacker que haya accedido al cibercerebro, puede leer, alterar o borrar estos recuerdos con una Prueba de Búsqueda o Interfasar exitosa (el modificador de –30 se aplica).

TÍTERES

La mayoría de los cibercerebros incorporan también un puppet sock o enlace de marioneta, que permite a usuarios remotos controlar la vaina o el cuerpo del sintemorfo vía teleoperación o interferencia. Esto permite a un hacker tomar control del cuerpo y manipularlo remotamente. Para hacerlo el hacker debe tomarse una Acción Compleja y superar al personaje defensor o musa en una Prueba Enfrentada de Infosec con el modificador de –30 aplicado.

Un defensor que no está atrapado puede continuar luchando por el control del morfo usando cada turno una Acción Compleja. En este caso, se hace otra Prueba Enfrentada de Infosec. Esto puede resultar en una situación en la que el morfo cambia de manos repetidamente o puede que entre en estado catatónico mientras ambos bandos pelean.

ABRASAR

Tener acceso directo al cibercerebro abre la posibilidad de ciertos tipos de ataque que son normalmente irrelizables dado el estricto control de contenido que ocurre en el enlace entre cibercerebro e injertos de malla. Una de las posibilidades es “abrasar” (el uso de algoritmos de impulso neural dañinos para dañar la mente de la víctima).

Para llevar a cabo un ataque de abrase o quemadura como también se puede llamar, el intruso debe desplegar un programa dedicado. Para utilizarlo, el intruso debe superar al ego defensor en una Prueba Enfrentada de Infosec con el modificador de –30 aplicado. Existen varios tipos de programas de abrasado, con efectos diferentes: cauterizadores (daño), manicomios (stress, espasmos (dolor), pesadillas (miedo) y cerrojos (deprivación sensorial). Son descritos en detalle en la sección de Equipamiento.

APAGAR

Si un cibercerebro es apagado, el morfo inmediatamente cesa toda actividad, probablemente colapsándose o parándose. Las vainas parecerán estar en coma. El ego, sin embargo, será reiniciado junto al cibercerebro.

FINALIZAR LA ALIMENTACIÓN DE LA PILA CORTICAL

El cibercerebro alimenta la pila cortical con datos para su respaldo como copia de seguridad o backup. Es una conexión de una sola dirección, por lo que la pila cortical no se puede hackear, per la transferencia de datos se puede cortar. Esta acción de finalización requiere una Prueba Enfrentada de Infosec entre el hacker (con el modificador de –30) y el defensor. La copia de seguridad del ego no será actualizada mientras la conexión permanezca apagada.

INTERFERIR SEÑALES DE RADIO

Interferir es un método de transmitir señales de radio que deliberadamente se solapen con otras para desorganizar la coherencia de la comunicación. En el altamente conectado mundo de Eclipse Phase, la interferencia intencionada es a menudo ilegal, por no mencionar grosera. La interferncia de radio no requiere ningún equipo especial más que un dispositivo inalámbrico estándar, tal como un ecto o injertos de malla. La interferencia puede ser selectiva o universal. La selectiva apunta a un dispositivo o conjunto de dispositivos en concreto. Para interferir selectivamente, el personaje debe haber escaneado el dispositivo objetivo. Los dispositivos universales apuntan a todos los equipos de radio indiscriminadamente.

Interferir requiere simplemente una Acción Compleja y una Prueba de Interfasar. Si se tiene éxito, los dispositivos afectados dentro del alcance tienen interrumpidas sus comunicaciones (son desconectados de la malla y no se pueden comunicar inalámbricamente). Los dispositivos cableados no resultan afectados. Los dispositivos equipados con IA’s autmáticamente intentarán superar la interferencia, lo que requiere una Acción Compleja (los usuarios transhumanos puede intentar lo mismo). En este caso, una Prueba Enfrentada Variable se lleva a cabo entre el emisor de la interferencia y el defensor. Si el interferente gana, todas las comunicaciones son bloqueadas. Si gana el defensor, no resultan afectadas. Si ambas partes tienen éxito, las comunicaciones resultan afectadas, pero no interrumpidas totalmente. El DJ decide cuánta información puede conseguir hacer pasar el defensor a través de la interferencia y cómo afecta esta situación al uso de la malla.

INTERFERIR RADARES

También se puede usar la interferencia contra dispositivos radar. En estos casos, se hace una Prueba de Interfasar. Si se tiene éxito el radar sufre la interferencia que le impone un modificador de –30 en todas las pruebas de sensores relacionadas. La entidad que maneje el radar puede intentar superar esta interferencia superando al interferente en una Prueba Enfrentada de Interfasar.

ESPACIOS SIMULADOS

Los espacios simulados o simulspaces son entornos de RV donde la resolución va más allá de la alta definición realista hasta lo hiperreal. Los ambientes que crean son ilusiones exhaustivas y auténticas, desde aspectos tales com la iluminación, los ciclos diurnos o lunares y el clima y a un nivel minucioso de detalle y sensación. Enchufarse a un espacio simulado es como entrar en otra realidad o mundo alternativa, razón por la que los espacios simulados se han ido haciendo cada vez más populares como entretenimiento.

Mientras que los espacios simulados normalmente no pueden dañar a los personajes inmersos en ellos dado que los algoritmos sensoriales no están diseñados para ser programas o rutinas ofensivas, las experiencias en ellos pueden tener un fuerte impacto psicológico en un ego, ya que la simulación es lo más parecido a la realidad que puedes tener. Un personaje que es "físicamente" torturado en un espacio simulado no resultará físicamente dañado, pero el estrés mental de la experiencia puede resultar suficiente para causarle traumas permanentes.

SIMULMORFOS

Los personajes acceden a un espacio simulado usando una personificación de tipo avatar llamado simulmorfo. Este simulmorfo es creado por el espacio, basándose en las reglas del dominio y ciertas características del morfo o ego que accede a la simulación. Dependiendo de la simulación, el simulmorfo puede ser personalizable hasta cierto punto. Mientras se interactúa con la simulación, se tratan los simulmorfos como infomorfos básicos para propósitos de reglas, incluso si los egos poseen otro cuerpo en en la realidad.

Cuando se accede al espacio, las musas no suelen ser transferidas dentro de la simulación, aunque pueden acceder si las reglas del dominio lo permiten. En tal caso, las musas son tratadas como personajes separados dentro del espacio simulado con su propio simulmorfo.

Dependiendo del rol que espacio simulado está destinado a jugar en la historia, el Director de Juego puede querer inventar "valores físicos" para los cuerpos simulmorfo, especialmente si los personajes van a invertir un montón de tiempo en la simulación. Estas estadísticas pueden ser literalmente inventadas (es una realidad virtual después de todo, cualquier cosa vale). Alternativamente, el Director de Juego puede simplemente improvisar e inventar las estadísticas necesarias al vuelo a medida que surge la necesidad.

INMERSIÓN

Cuando un personaje se sumerge en un espacio simulado, se "convierte" en el simulmorfo. El cuerpo físico del personaje, típicamente aislado en una vaina o asiento especial, permanece inerte. Mientras está inmerso, sufre un –60 a todas las Pruebas de Percepción o intentos de llevar a cabo cualquier acción con su morfo físico. Los personajes pueden entrar y salir del espacio simulado a volutad pero conectar o desconectar cuesta una Acción Compleja.

Si la simulación falla o el personaje es de alguna otra forma expulsado de ella, retoma el control normal de su morfo de inmediato. Salir volcado de una RV es extremadamente desagradable y causa 1d10 ÷ 2 de Estrés mental al personaje.

INTERACCIÓN CON LA MALLA EXTERNA

Un personaje que accede a un espacio simulado puede aún interactuar con la malla (y a través de ella con el mundo exterior) asumiendo que las reglas del dominio lo permitan. Sin embargo, cualquier interacción con el exterior está sujeta a problemas de dilatación temporal. Por ejemplo, en un espacio con simulación de tiempo acelerada que el tiempo real, mantener un chat con alguien en el exterior es insoportablemente lento, ya que los segundos del tiempo real se convierten en minutos en la RV. Si el personaje decide acceder directamente a otros nodos de malla, debe desconectarse o salir del espacio simulado.

REGLAS DE ESPACIOS SIMULADOS

Dado que un espacio simulado es un mundo alternativo cuyo realismo iguala a la realidad, los personajes utilizan sus habilidades físicas y aptitudes como si estuvieran actuando en el mundo real, con unas pocas excepciones:

Aunque la intrusion y el hackeo pueden ser representadas como otra capa de la simulación, no hay auténtico hackeo en el espacio simulado (ver Hackeando Espacios Simulados).

Los Asíncronos no pueden usar sus habilidades Psi en un espacio simulado, aunque tales habilidades se pueden simular.

Cualquier daño "físico" recibido en RV es tratado como daño "virtual". Aunque las heridas y lesiones virtuales usan la misma mecánica, los personajes que mueren en un espacio simulado normalmente son simplemente eyectados de la simulación. En algunos casos, los personajes "muertos" son volcados en una habitación blanca desde donde pueden reentrar o simplemente observar la simulación, dependiendo de las reglas del dominio.

El estrés mental o traumas infligidos durante una simulación afecta al ego como daño de Lucidez real. A discreción del Director de Juego, algún estrés mental puede ser reducido si los personajes son conscientes de que están en una simulación.

REGLAS DE DOMINIO

Cualquier cosa vale en un espacio simulado, según dicten las reglas de dominio. Un espacio puede ser una aproximación muy cercana a la realidad o diferir drásticamente. La gravedad puede fluctuar, la luz en el espectro visible puede no existir, los personajes pueden curarse el daño virtual sin esfuerzo, los simulmorfos pueden ser capaces de transfigurarse en otras criaturas, todo puede estar bajo el agua (las posibilidades son inacabables, limitadas sólo por la imaginación). En términos de juego, esto permite al DJ inventar reglas al vuelo.

HACER TRAMPAS

Como con cualquier buen juego, los espacios simulados proveen de formas de hacer trampas. Los trucos están o bien incorporados en el software de la RV o programados (externamente) e incorporados por un hacker. Los trucos permiten a los personajes romper las reglas del dominio de algún modo. Éste puede ser un poder especial, una manera de alterar algún factor ambiental (com volar), alterar la dilatación temporal, alguna forma de aumentar el poder de las habilidades, un método de conseguir otros simulmorfos, o un atajo a través de una parte de la simulación. En términos de juego, las trampas y trucos pueden proporcionar modificadores a ciertas Pruebas de habilidades o atributos hechos por el simulmorfo. Hacer trampas está normalmente prohibido. Los jugadores que hacen trampa

en un juego RV y son pillados pueden tener que afrontar la expulsión del espacio simulado.

HACKEAR ESPACIOS SIMULADOS

Dado que los espacios simulados son entornos virtuales complejo y a menudo se ejecutan con dilatación de tiempo, los hackers no pueden atacarlos de una manera normal cuando participan en la simulación. Hay maneras de afectar e influenciar la simulación desde dentro, pero el grado de subversión que se puede conseguir es limitado. Por esta razón los hackers raramente entran en RV para hackear. Hacker el sistema externo que ejecuta el espacio simulado es exactamente igual que irrumpir en cualquier otro sistema. Usa todas las reglas estándar para la intrusión y la subversión.

Trasteando desde el interior

Desde dentro de un espacio simulado, la única opcioón de interactuar con los controles RV que tiene un hacker es a través de la interfaz estándar que todo simulmorfo puede operar. Usada típicamente para características estándar de usuario como ajustar el simulmorfo, chatear o comprobar el estado de otros usuarios, un hacker espabilado puede encontrar vías de de usarla para subvertir el sistema. Sin embargo, tales opciones son normalmente limitadas dado que gran número de controles y procesos del sistema no pueden ser accedidos ni manipulados desde dentro.

La mayoría da las opciones del hacker van a implicar trastear con la simulación y sus reglas específicas de dominio o posiblemente conseguir acceso a trucos y trampas. Realizar un cambio requiere una Prueba exitosa de Interfase. En última instancia, el Director de Juego decide lo que puede y no puede conseguir el hacker, basándose en las limitaciones del espacio simulado concreto.

La mayoría de los espacios son monitorizados para evitar las trampas y abusos, aunque los monitores están típicamente preocupados con mantener el espacio como un todo, lidiando con otros usuarios, etc. A discreción del Director de Juego, tales monitores pueden tener que superar una Prueba de Interfase (posiblemente con un modificador de distracción) para percatarse de los esfuerzos del hacker.

Hackeando Espacios Simulados desde dentro

Modificador	Tarea
–0	Analizar parámetros de simulación, ver reglas del dominio, cambiar la apariencia del simulmorfo, cambiar de simulmorfo o su tipo
–10	Cambiar la probabilidad de los resultados de Pruebas, hacerse invisible para otros (“salir de juego”)
–20	Interferir con la simulación (pej.: hacer llover, generar terremotos…), generar objetos, ignorer las reglas del dominio, matar o bloquear a otros simulmorfos
–30	Pasar a Modo Dios, manejar los personajes simulados, tomar control de la simulación

IA’S Y MUSAS

Las IA’s son programas conscientes pero especializados. Como otros tipos de software, deben operar en un sistema computerizado. La mayoría de las IA’s se ejecutan en bots, vehículos y otros dispositivos donde pueden ayudar a los usuarios transhumanos u operar las máquinas por sí mismas. También son usadas comúnmente para monitorizar sistemas activamente contra intentos de intrusión. Las Musas son IA’s que se especializan como compañeros personales, siempre virtualmente junto al personaje desde que era un niño. Se pueden encontrar IA’s y Musas de ejemplo en el apartado de Equipo.

LIMITACIONES IA

Las IA’s poseen una serie de restricciones y limitaciones incorporadas. Para empezar, pueden ser cargadas sólo en los cibercerebros de vainas y sintemorfos, pero no pueden ser descargadas en cerebros de biomorfos. Como software, usan las mismas reglas que cualquier software y pueden ser apagadas, reseteadas, copiadas, borradas, almacenadas como datos inertes, infectadas por virus y reprogramadas. Debido a su tamaño y complejidad, sólo una IA (o infomorfo) puede ejecutarse en una computadora personal al mismo tiempo y no pueden ejecutarse en dispositivos periféricos.

Si bien poseen consciencia e inteligencia, son incapaces de automejora y no pueden expandir sus habilidades y programación por su propia cuenta. Aunque no son capaces de aprender, sí poseen gran capacidad de almacenaje que les otorga la habilidad de recordar y una limitada forma de adaptación. Las IA’s no ganan Puntos Rez ni tienen Moxie.

Las IA’s tienen Aptitudes que no superan los 20 puntos y son incapaces de Basar sus Habilidades. Si no poseen una Habilidad, no sabe cómo hacerlo (a discreción del Director de Juego pueden Basar en otras habilidades similares con un modificador de –10 o –30). Pueden usar Habilidades como cualquier personaje en *Eclipse Phase*, sin embargo no pueden poseer ninguna Habilidad Activa con una puntuación mayor de 40 o ninguna Habilidad de Conocimiento superior a 90 (el máximo nivel de pericia que su software les permite).

A pesar de que las IA’s son programadas con plantillas de personalidad y empatía, son generalmente menos emotivas y difíciles de interpretar (se aplica un modificador de –30 a cualquier Prueba de Kinésia hecha contra ellas cuando están en cuerpos vaina). Si se combinan con un morfo sintético inexpresivo, son incluso más difíciles de interpretar (modificador de –60). Algunas IA’s carecen totalmente de capacidades emotivas y son imposibles de interpretar con la Habilidad de Kinesia

Barra Lateral: Interpretando Musas

Las musas no deberían ser vistas como una mera herramienta para conseguir habilidades extra, sino como una oportunidad de profundizar en el juego de rol. Aunque una musa IA típica no es una inteligencia incompleta (pero pueden serlo, ver Infomorfos como Musas), su matriz de personalidad es a menudo bastante

sofisticada y pueden ser muy buenas adaptándose a las rarezas de la personalidad de sus usuarios. Por otra parte, comparten la misma Ingenuidad por el Mundo Real que los personajes IAG cuando se trata de entender todas las facetas del comportamiento transhumano, la interacción social, el lenguaje corporal o la emoción. Sus personalidades son más no–humanas, abstractas, extrañas y menos apasionadas que las formas de vida transhumanas, a menudo llevando a interpretaciones copceptuales erróneas y malentendidos. Igualmente, sus capacidades creativas son limitadas, reforzadas en su lugar por la habilidad de calcular probabilidades, ejecutar simulaciones y evaluar sus resultados y hacer predicciones basadas en experiencias previas.

Dependiendo de la psotura del usuario sobre los programas sintientes, las musas pueden ser vistas como juguetes inteligentes, seguidores, sirvientes, esclavos, amigos o mascotas, lo que debería verse reflejado de alguna manera en el juego. La mayoría de los transhumanos han adquirido también la tendencia a sentirse unidos mentalmente con su musa debido a su omnipresencia y devoción por el usuario (como el vínculo emocional que se puede tener con un niño o perro que crece para convertirse en adulto). Por tanto la subversión o incluso la destrucción de la personalidad de una musa es a veces equiparado a la violación o el asesinado.

DIRIGIR IA'S

Las IA's y Musas están progrmadas para aceptar órdenes de usuarios autorizados. En algunas circunstancias, pueden ser programadas para cumplir la ley o algún código ético. Sin embargo, la programación nunca es perfecta y las IA's pueden ser bastante listas en lo que a interpretar órdenes y cumplirlas se refiere. En la mayoría de los casos, una IA difícilmente rechazará cumplir una petición u obedecer una órden. Dado que normalente tienen también el deber de proteger a la persona que las dirige, la IA puede ser reticente a a seguir órdenes construidas como peligrosas o que tengan un impacto negativo en el usuario. Bajo ciertas cirunstancias, los imperativos preprogramados pueden forzar a una IA a ignorar o desobedecer las órdenes de su propietario (a discreción del Director de Juego).

AGI'S E INFOMORFOS

El término "infomorfo" se usa para referirse a cualquier ego en un cuerpo digital, ya sea una IAG o la emulación digital de una mente biológica (incluyendo copias de seguridad y bifurcados). Las siguientes reglas aplican a personajes e IAG's infomorfos.

MENTES DE SOFTWARE

En el fondo, los infomorfos sólo son programas y por tanto son tratados como cualquier otro software en términos de reglas. Deben correr sobre un computador personal o un servidor. Si el dispositivo es apagado, el infomorfo también se apaga en un estado de inconsciencia, reiniciándose junto con el dispositivo (los infomorfos también pueden apagarse a sí mismos, aunque es raro que lo hagan). Si el dispositivo es destruido, el infomorfo muere con él (a menos que sus datos puedan ser de alguna manera extraídos de los componentes supervivientes, a lo mejor resultando en un Vapor).

Los infomorfos se copian a sí mismos, aunque en algunos lugares esto es ilegal y muchos otros está muy mal visto ya que levanta numerosas cuestiones éticas y legales. Por esta razón muchos infomorfos que se copian y transfieren a sí mismos para correr sobre un nuevo dispositivo, se borrarán a sí mismos completamente del viejo.

Como seres digitales, los infomorfos no tienen mente física, pero es una cuestión muy simple para ellos poseer un sintemorfo inhabitado, tomando residencia en el cibercerebro. Se pueden descargar también en cuerpos biomórficos siguiendo las reglas de reenfundado estándar. Incluso cuando no tienen cuerpo, pueden interactuar con el mundo físico a través de la malla, viendo a través de sensores, proveyendo flujos de RX, comunicándose con los personajes, dirigiendo dispositivos esclavo y teleoperando o interfiriendo drones.

Los infomorfos tienen una Velocidad de 3, reflejando así su naturaleza digital y su habilidad de actuar a velocidades electrónicas. Sin embargo, si un infomorfo se reenfunda en un cuerpo, adquiere la velocidad de dicho cuerpo.

PERSONAJES IAG

Aunque las IAG's no nacieron en un cuerpo biológico, su programación abarca el espectro completo de la personalidad, aspecto, emociones y estados mentales humanos. Las IAG's son, de hecho, criadas en cierto sentido de manera similar a los niños humanos, por lo que están socializadas tanto como lo están los humanos. No en vano, a un nivel fundamental, son no–humanos programados para actuar como humanos. Hay puntos inevitables donde la programación no enmascara o altera el hecho de que las IAG's suelen poseer o desarrollar rasgos de personalidad e idiosincrasias que son bastante diferentes de la norma humana y a a menudo directamente ajenas a ésta.

A diferencia de las IA's estándar limitadas, las IAG's son capaces de afinada creatividad, aprendizaje y automejora (a un ritmo lento y estable equivalente al humano). Igual que otros personajes, obtienen puntos Rez y pueden mejorar sus Habilidades y Aptitudes. Las IAG's no sufren ninguna de las limitaciones impuestas en las IA's débiles, usándolas como cualquier otro personaje.

A nivel emocional, las IAG's ejecutan subrutinas emocionales que son comparables a las emociones biológicas humanas. Las IAG's están, de hecho, programadas para tener empatía y compartir un interés por los asuntos y la prosperidad humanos y darle una gran importancia a la vida en todo tipo de formas. En términos de juego, las IAG's se emocionan como los humanos (y por tanto la Kinésica se puede usar en su contra) y son vulnerables a efectosde manipulación emocional, miedo, etc.

Barra Lateral: Infomorfos como Musas

En lugar de confiar en musas subdesarrolladas para ayuda y compañía, los personajes pueden preferir tener una inteligencia totalmente madura a su lado, ya sea una IAG, un ego biológico respaldado (a partir de un backup o copia de seguridad) o un bifurcado de la propia personalidad del usuario. Alternativamente, un personaje con un módulo “Jinete Fantasma” podría tener ambos, llevando una musa en sus injertos de malla y un infomorfo en el módulo Fantasma.

Esta posibilidad es muy útil para los personajes infomorfos, ya que pueden acompañar y participar en los asuntos del grupo sin necesidad de un morfo propio.