

# REALITE VIRTUELLE 3.0

**Texte extrait** du Virtual Realities 3.0, par Tzeentch (mail: tzeentch666@earthlink.net), alias Kenneth Peters. Site web : <http://matrix.dumpshock.com/tzeentch>  
**Traduction:** Namergon, alias Ghislain Bonnotte.

## SE CONNECTER

Pour accéder à la Matrice vous devez avoir un compte chez un Fournisseur de Service Matriciel (FSM). Ce compte dit au RTL qui vous êtes et à quels services vous avez accès (ou pas accès, selon les cas). Le fait d'avoir un compte vous donne un commcode et l'accès aux services Matriciels de base, comme l'accès aux bases de données publiques et les moteurs de recherche. En plus, ce compte est généralement relié à la fois au compte en banque de l'utilisateur et à son SIN. Cela fournit une sécurité à l'utilisateur et aide à relier l'utilisateur à sa piste de données, y compris son domicile d'enregistrement. Lorsqu'un utilisateur se logue sur la Matrice son créditube est souvent utilisé pour l'authentification. Le créditube stocke les particularités de son compte, y compris le SIN, le mot de passe, les conditions spéciales d'accès et toute autre information dont le fournisseur RTL a besoin pour tracer votre accès et s'assurer que vous n'êtes pas un decker déroband de précieuses ressources. Ça protège aussi l'utilisateur, car un créditube est bien plus difficile à falsifier qu'un mot de passe.

Cette information est validée par le RTL et un espace de compte est ouvert pour l'utilisateur. C'est dans cet espace que les utilisateurs ont leur persona chargé. Une fois que c'est fait il a un point d'entrée sur la Matrice et l'information commence à être alimentée sur son système. Du début à la fin le procédé ne prend généralement pas plus de quelques secondes.

Les deckers contournent ces vérifications avec des comptes falsifiés, ou en interceptant ou en piratant des connexions déjà actives. Lq plupart des deckers maintiennent de nombreux comptes actifs sur le RTL. Au fur et à mesure que les faux comptes sont découverts et fermés il passe à un nouveau. Tout decker digne de ce nom aura au moins une douzaine de comptes prêts à un moment donné.

## LE PERSONA

Aucun système ne pourrait gérer la quantité de données traversant la Matrice, littéralement des milliards de mégapulses parcourent les grilles chaque seconde.

Tenter d'accéder à tant d'information à la fois planterait même le plus puissant serveur en quelques secondes. Et c'est là que le programme persona intervient.

Le persona est la "devanture" de l'utilisateur pour traiter avec la Matrice. Le programme persona se charge dans la Matrice et filtre sur la base d'une série incroyablement avancée de programmes et d'utilitaires les données, qui sont ensuite servies à l'interface système des utilisateurs. Mais sans le persona vous ne pouvez pas accéder à la Matrice, même d'autres "bêtes" appareils comme votre tridéo doit avoir au moins des programmes Solidité et Senseur rudimentaires.

Les programmes persona utilisés par les deckers et même les professionnels de l'informatique sont aussi conçus pour être semi-indépendants, s'appuyant sur des modélisations comportementales avancées de l'utilisateur des modifications personnalisées de sorte qu'ils accomplissent beaucoup des interactions avec le serveur par eux-mêmes, sur la base des actions passées et préférences des utilisateurs. L'utilisateur ne fait que guider les actions du persona.

Sans un persona "intelligent", aucun decker ne pourrait comprendre ou répondre aux actions sur la Matrice et rester compétitif avec le software, peu importe ses réflexes et sa compétence. Pour la plupart des utilisateurs les programmes persona servent principalement à accélérer l'accès et à fournir une sécurisation des données. Ils ont toujours des programmes Solidité et Senseurs chargés, mais n'affichent pas nécessairement une quelconque icône ni même n'ont leur système configuré pour visualiser la Matrice comme un environnement tridimensionnel.

## **SOLIDITE**

La Solidité représente la connexion des personas avec la Matrice et la résistance du programme confronté à des effets adverses comme des éjections par le système, des plantages de RTL and des corruptions de pistes d données. Ce n'est pas tant la stabilité que l'adaptabilité des programmes. Des programmes avec des indices de Solidité élevés sont utiles dans des secteurs où le réseau est de mauvaise qualité ou les connexions pas fiables.

Les deckers et autres fâcheux personnages apprécient de bons programmes Solidité car ils sont plus résistants aux tentatives faites pour les mettre hors connexion, généralement par la corruption des programmes persona ou en tuant leurs alimentation d'accès. Les programmes Solidité des deckers, contrairement à ceux de l'utilisateur moyen, sont capables d'installer des connexions multi-homing, chargeant de multiples copies d'eux-mêmes sur un serveur, et faisant varier leurs chemins de données de sorte d'empêcher un serveur de tuer le programme persona qui est en cours d'exécution sur son système.

## **SENSEUR**

Le programmes Senseur est ce qui permet aux utilisateurs de "voir" dans la Matrice. En essence c'est la partie du persona qui dit à la Matrice quel type de système le fait tourner et quelles information il devrait obtenir. Le programme Senseur traduit alors les informations qu'il reçoit et les envoie en code machine au système de l'utilisateur. Plus le programme Senseur est avancé et meilleures sont des capacités de discrimination et de traduction de signal.

Le programme Senseur de l'utilisateur moyen est plutôt limité dans ce qu'il peut accomplir. Généralement il traduit seulement l'imagerie UMS ou sculptée émise vers le deck, où il est soit rendu comme un environnement tridimensionnel soit en une autre forme que le système peut afficher. En essence, un programme Senseur standard ne fera que montrer les bonnes informations se mouvant dans la Matrice, et ne sera pas capable de traduire les données qu'il n'est pas autorisé à voir.

Le decker de son côté utilise un pack de programmes persona très différent de celui de l'utilisateur moyen. Le programme Senseur du decker peut être vu comme une version très évoluée des programmes développés à l'origine pour le projet Echo Mirage et modifiés au fil des années par l'underground decker. Ces programmes ont été développés avant qu'il n'y ait une iconographie standard, donc ils ont un spectre bien plus large de données qu'ils peuvent collecter et traduire.

Ils ne sont pas trompés par les standards superficiels utilisés par l'iconographie UMS ou même sculptée. Un hacker peut être capable de masquer son icône UMS et devenir invisible pour l'utilisateur moyen, mais il laisse néanmoins une piste de données que le programme Senseur du decker peut capter et traduire.

Davantage même que Masque et Evasion, ce sont les programmes Senseur du decker qui le différencient de l'utilisateur moyen. Mais par un malheureux effet secondaire dû au fait de ne pas être limité par les standards courants de la Matrice, il peut être vulnérable du fait que son deck traduise des informations non-standard en signaux simsense potentiellement dangereux. Les CI exploitent ces vides potentiels en injectant des données spécifiquement conçues pour être traduites en signaux ASIST dommageants.

Ce qui ne veut pas dire que l'utilisateur moyen est moins vulnérable

Aux CI Noires s'il utilise l'interface appropriée, mais leur software manque de la sensibilité qui donne plus de "prises" dans le hardware du decker.

## **MASQUE**

Masque est ce qui sépare un decker d'un utilisateur ou même d'un spécialiste en sécurité. Masque est un ensemble de programmes qui falsifient les informations d'un compte valide et analysent le trafic local pour s'assurer que la signature de données du decker ne diffère pas de tout autre utilisateur du système. Lors du log sur la Matrice, c'est le Masque qui génère des fausses informations de login et s'assure que sa signature ne déclenche pas le logiciel de sécurité automatisé utilisé par le RTL. Au moment de se loguer sur un serveur Masque analyse l'espace utilisateur local et "adapte" la signature du persona pour la synchroniser avec celle des autres utilisateurs. Cela rend la tâche des CI beaucoup plus difficile, car elles se fient à l'identification positive du compte persona de l'intrus pour l'attaquer. Masque travaille étroitement avec Solidité pour s'assurer que toutes les connexions du decker sont camouflées.

Masque endommage et falsifie aussi intentionnellement les entrées de log lors de la conduite d'opérations dans la Matrice. Les entrées existent toujours, mais l'information qu'elles contiennent sera en conflit et prêter à confusion pour un relecteur. Il est de pratique courante chez les deckers de faire apparaître ses logs comme ayant été créés par un utilisateur valide – habituellement quelqu'un contre qui ils ont une dent.

## **EVASION**

Evasion est une modification et une amélioration des programmes de Solidité et de Masque de l'utilisateur. Evasion donne au persona du decker un certain niveau "d'intelligence" lors des tentatives de maintien de sa connexion. Evasion analyse les CI et méthodes de sécurité adverses et tente d'exploiter des trous connus dans la sécurité dans l'espoir d'obtenir un accès non-standard. Dans les faits cela rend encore plus difficile la tâche pour les programmes adverses de localiser le persona intrus puisqu'il n'est même plus situé au "bon" endroit.

## **EN FRANCAIS**

Pour utiliser une analogie on pourrait voir les divers programmes persona comme suit:

La Matrice peut être considérée comme une rue affairée d'une ville, don't les divers immeubles sont les serveurs. La Solidité du persona représente sa connexion avec la Matrice, et prend forme dans cet exemple comme son corps. S'il est assommé cela correspond au fait que son compte a été détruit, l'éjectant de la grille. Les Senseurs représentent sa vue et sa capacité à discerner les détails. L'utilisateur moyen verrait les objets principaux, les immeubles, d'autres gens, mais ne verrait pas les petits détails comme le programme de maintenance travaillant sur une connexion en bas de la rue ou le decker qui a hacké son icône UMS pour être invisible. Les deckers, d'un autre côté, auraient les yeux d'un faucon, discernant même les process et signatures subtils.

S'il tente d'entrer dans un immeuble le garde lui demandera pour quel motif et s'il est autorisé à entrer. Le programme Masque analysera les autres personas entrant dans l'immeuble, modifiant sa signature et commençant alors à exécuter des programmes de commande et de manipulation contre le garde pour le convaincre qu'il est effectivement un utilisateur valide.

A l'intérieur de l'immeuble serveur il y a une zone où tous les personas vont s'interfacer avec les données passant sur le serveur. Généralement il n'y a qu'une connexion par persona, mais si la Solidité du decker est suffisamment bonne alors de multiples "copies" de cette connexion se formeront et seront placées en divers endroits de la pièce.

Quand une CI attaque le decker elle inspecte essentiellement la salle à la recherche de signatures anormales et attaque alors le programme persona, soit directement en tentant de détruire la connexion du persona ou indirectement en fournissant de fausses informations au Senseurs du persona. Dans ce cas Evasion pourrait signifier que le persona du decker est situé dans le plafond. Si l'utilisateur du persona dans un serveur pouvait être comparée à une salle avec des milliers de gens dedans, et les CI devait regarder chaque personne pour repérer le decker, alors Evasion signifie que son persona se cache dans le plafond.

## CHARGER DES PROGRAMMES

Presque tout logiciel en 2060 est développé pour opérer dans des architectures client-serveur. Pour être exact, quand un utilisateur charge un programme sur son système, une partie de l'utilitaire est placé dans le même espace utilisateur qu'où réside son persona. Cela présente de nombreux avantages, don't le moindre n'est pas en fait une sécurité (aussi dur que ce soit à croire). Tout utilitaire chargé est lié au persona qui l'a uploadé. Dans un monde parfait si un programme violait des protocoles de sécurité il serait pisté jusqu'au persona aux commandes et serait pris en charge de cet endroit. Et dans la plupart des cas, c'est exactement ce qui se passe. Les deckers utilisent des utilitaires supplémentaires qui empêchent le système de localiser précisément le propriétaire des programmes intrus, outrepassant effectivement le schéma entier de vérification de programme.

Un autre avantage est la vitesse. La portion serveur du programme (typiquement seulement un petit bloc du programme complet) peut accomplir des opérations directement sur le serveur, une considération importante quand on traite potentiellement avec des gigapulses d'information. Les portions du programme peuvent interagir directement avec le persona, et comme il a été remarqué plus haut, le persona est capable d'opérer à une vitesse bien supérieure qu'un opérateur métahumain. Ainsi l'utilisateur dirait au persona d'accomplir une opération et le chargerait alors de tout le travail, l'utilisateur vérifiant occasionnellement la progression et lançant des mises à jour.

L'autre bout de la chaîne est un programme serveur-client. Ce sont des programmes qui résident complètement sur le serveur, chargeant de plus petits modules sur des machines utilisateur qui leur permettent d'utiliser les ressources du programme complet. C'est la façon la plus courante de distribuer un logiciel dans un environnement corporatiste. Cela empêche les travailleurs de potentiellement charger sur leurs terminaux de bureau des logiciels non autorisés car les machines serveur peuvent avoir des ressources diminuées et cependant opérer efficacement dans l'environnement de bureau. Cela maintient aussi les prix à un niveau bas car les machines serveur sont moins chères et la gestion de license est bien plus facile à gérer.

## LOGIN ET PISTAGE

Comme l'ensemble persona de l'utilisateur est chargé sur le réseau et qu'une "adresse" lui est assignée, il peut alors être pisté. L'utilisateur moyen ne s'inquiète pas outre mesure de ça. En fait c'est souvent pratique, car il est plus facilement trouvable par des amis ou la famille. Quand il entre dans un centre commercial virtuel cette "signature" est vérifiée s'il est déjà venu auparavant il a peut-être pu configurer un affichage interactif personnalisé qui est à ses goûts. La signature est aussi son authentification lorsqu'il passe des appels et conduit des transactions dans la Matrice. C'est à la fois une sécurité et une commodité pour l'utilisateur moyen.

Mais pour le decker cela peut être un handicap mortel. Là où l'utilisateur trouverait pratique d'être identifié par un serveur, cela peut potentiellement menacer la vie du decker. La même information codée dans la piste de données qui est utilisée pour diagnostiquer des problèmes réseau peut être utilisée pour situer la localisation physique exacte du decker; l'information enregistrée pour maintenir des fichiers de préférences personnelles peut alerter des systèmes de sécurité si sa signature a été "flaguée".

Donc les deckers enfreignent les règles. Les deckers utilisent des programmes qui exploitent les inévitables trous dans la sécurité qui seront trouvés dans tout système aussi immensément complexe que la Matrice. Dans ce cas la commodité de l'utilisateur moyen de la Matrice marche à son avantage. Dans la plupart des cas combler les trous dans la sécurité que les deckers utilisent interrompraient le service vers des milliers, voire des millions d'utilisateurs. Donc les deckers

continuent d'exploiter des erreurs dans la configuration de la Matrice tandis que les compagnies de communications continuent d'implémenter des patches pour combler les trous. Mais comme elles ne peuvent vraiment corriger les problèmes sous-jacents ces patches exposent souvent d'autres trous dans la sécurité que les deckers exploitent rapidement.

C'est une course sans fin don't les deckers doivent garder la tête ou perdre leur avantage ... ou leur vie.

## LA PISTE DE DONNEES

Lorsque l'utilisateur quitte son RTL d'origine il convient de remarquer qu'une partie de son persona est toujours présent dans sa grille native, routant des informations à l'utilisateur sur la localisation actuelle du persona dans la Matrice. Ce chemin est généralement référencé comme la " piste de données" et représente les liaisons de communication que les programmes comme trace et pistage remontent dans l'espoir de localiser la position originale du persona.

Quand l'utilisateur accomplit une opération de Connexion à un RTR sa signature est authentifiée et son persona est chargé sur le système RTR, laissant une partie du persona original toujours chargé sur le système d'origine. C'est nécessaire car le persona est ce qui permet à l'utilisateur de recevoir des données du système dans lequel il est logué. Ces données sont analysées puis routées vers le original du login où elles sont renvoyées à l'utilisateur. Pour des utilisateurs légitimes ce processus est transparent et n'est même pas remarqué, les deckers d'un autre côté doivent hacker la vérification de compte et le routage des sous-systèmes de sorte de passer au travers.

Lorsque l'utilisateur se connecte sur un autre RTR ou RTL il décharge tout sauf un pointeur de redirection, et son persona est alors chargé par le système vers lequel il va. S'il se déconnecte du RTL de destination alors son persona est complètement déchargé. S'il se déconnectait alors du RTR et retournait à son RTL original son pointeur de redirection serait effacé du RTR.

Pour illustrer davantage, si l'utilisateur se connectait sur un RTR puis passait dans un autre RTR son persona serait déchargé du RTR original aussitôt qu'il serait authentifié et une nouvelle copie serait chargée sur le nouveau RTR. Seule une redirection serait présente sur le RTR original.

Si l'utilisateur se connectait alors sur un RTL depuis le nouveau RTR il serait de nouveau authentifié, et si cela se passe bien le RTR déchargerait son persona, le remplacerait par un drapeau de redirection et le RTL chargerait alors son programme persona.

### Altérer la Piste de Données

Les deckers altèrent généralement leur piste de données d'une quelconque façon. La pratique la plus commune est d'avoir de multiples connexions ouvertes et de basculer des unes aux autres, ce qu'on appelle généralement faire de la redirection. L'autre méthode consiste à simplement rendre la connexion plus difficile à trouver, généralement via l'utilisation du programme Masque sur le persona. Cet utilitaire fait en sorte que les systèmes au travers desquels il passe mettent les pointeurs de redirection vers des endroits farfelus, ou qu'ils créent de faux pointeurs qui ne mènent nulle part ou bouclent.

### Déconnexion en Douceur

Quand un utilisateur se déconnecte sa piste de données est retirée de sa position courante après coup. Le système retire avec application les fragments de mémoire et redirige les drapeaux aussi bien qu'il accomplit d'autres soit-disant " collectes de déchets". Pour l'utilisateur moyen cela ne prend virtuellement pas de temps. Si cette collecte n'est pas faite alors les pistes de données de l'utilisateur pourraient rester pendant de nombreuses minutes avant que les serveurs remarquent le temps de latence de la communication et lancent un nettoyage eux-mêmes. C'est ce délai qui est si mortel pour les deckers qui se déconnectent sans accomplir une opération de Déconnexion

en Douceur. En effet, leur " chemin " continue d'exister dans la Matrice et les programmes Trace peuvent toujours le remonter.

## **VISIBILITE**

Ce qu'un utilisateur ou decker voit en réalité dans la Matrice est entièrement dépendant de son interface. Bien que les interfaces ASIST ont généralement le plus de presse et sont ce à quoi la plupart des gens pensent lorsqu'ils parlent de " La Matrice " , elles sont de loin la méthode la moins commune d'accéder à la Matrice.

### **Interface Basique**

C'est le niveau auquel la plupart des gens accèdent la Matrice. Sous cette forme la Matrice a généralement l'apparence de l'Internet de la fin du 20ème siècle. Il y a des différences, bien sûr, mais en règle générale il y a peu de différences notables. Les principales différences entre les deux réseaux sont la forte augmentation dans la vitesse et dans l'interactivité rendue possible par les avancées dans l'infrastructure et l'utilisation des programmes persona. Dans ce cas les données UMS sont soit pas utilisées du tout ou sont simplement des " aides " pour le programme Senseur pour déterminer le type d'information.

Selon l'interface spécifique, la plupart des process bas niveau comme se déplacer de commcodes locaux aux RTL sont entièrement transparents, pas plus visibles que de changer de chaîne ou de surfer de sitea en sites sur le vieil Internet.

### **Interface Avancée**

Un utilisateur avec une interface avancée voit généralement la Matrice pratiquement de la même façon qu'un utilisateur avec une interface ASIST – au moins du point de vue de la visualisation. Les interfaces avancées manquent des systèmes de feedback simsense qui permettent aux utilisateurs d'ASIST de se débrouiller avec de plus grandes quantités de données. Certaines interface avancées de bas niveau utilisent du matériel de réalité virtuelle plutôt primitif, mais l'effet reste cependant remarquable.

Si nécessaire les interfaces avancées peuvent afficher la Matrice comme un système d'interface basique, ou même en un mode "hybride" qui restitue la Matrice comme un espace tridimensionnel mais utilise aussi divers menus déroulants et des commandes gestuelles.

### **Interface ASIST**

Alors que voit un persona avec une interface ASIST? A peu près tout ce qui est configuré pour être vu. Evidemment un utilisateur (ou même un decker selon le cas) ne verra pas chaque paquet de données flottant ici et là. Il verra plutôt une représentation de ces données, généralement comme un rayon de lumière, plus la lumière est brillante plus il y a de données. Généralement la plupart des objets ont ancré à "l'émission" Matricielle leur existence au moyen de données UMS qui sont rendues comme icônes.

Les autres utilisateurs, serveurs et de nombreux programmes sont aussi " visibles " dans la Matrice, bien que leur position dans la Matrice ne représente en aucune façon leur position dans le monde réel.

Les utilisateurs d'interface ASIST ne voient pas non plus les transactions bas niveau ni les mouvements de données comme les appels téléphoniques ou les données déplacées de système en système. Il serait nécessaire de contrôler individuellement des commcodes pour voir un réel trafic entre deux d'entre eux. Cette information n'est même pas passée dans le même espace de données comme là où le persona obtient ses informations, comme un utilisateur d'internet du 20ème siècle n'est pas conscient de la manière don't circule les données entre les eerveurs sans

utiliser des outils spéciaux. Seul un decker a la capacité de hacker dans d'autres couches de données et voir ce qui se passe réellement dans la Matrice.

Même avec qu'une tranche des données déplacées dans la Matrice visible cela peut déborder. Pour cette raison la plupart des gens désenclenche leur visibilité de certains objets dans la Matrice (sur la base de leur type de données UMS). La plupart du temps cela inclut les icônes des autres utilisateurs, car dans des RTL bondés rien que le nombre d'icônes d'utilisateurs peut mettre un sous-système d'affichage du système sur les genoux. Même les deckers restreignent généralement leur vision des icônes d'autres personnes à des points abstraits ou à d'autres méthodes facilement affichables. Il est aussi possible de configurer une "distance de vue", au-delà de laquelle seules certaines données sont affichées – c'est une alternative populaire pour visiter le forum local par exemple.

## **TECHNOLOGIE DE BASE**

Les technologies de base se divisent en quatre catégories, décrites ci-dessous:

### **SILICONE**

Le silicium est la moins chère des technologies de base. Mais bien que ce soit une technologie très mature, elle ne peut tout simplement pas rivaliser avec les capacités de ses successeurs. Il est principalement employé dans des solutions de moindre coût où une grande puissance n'est pas indispensable. Ainsi, le silicium est encore très courant dans les simples ordinateurs embarqués, jouets, et même des biens de consommation électroniques bas de gamme.

Malgré son avantage de simplicité et de coût, les systèmes optiques continuent d'éroder les parts de marché du silicium même en bas de gamme. Ce ne sera pas long avant que les systèmes optiques relèguent les systèmes en silicium au placard.

Les principaux désavantages des systèmes à base de silicium sont leur comparativement haute consommation d'énergie, leur grande taille (les systèmes à silicium comparables aux systèmes optiques nécessitent un refroidissement intensif et consistent souvent en un amas de multiple processeurs).

Mais ils sont TRES bon marché.

### **Remarques Technologiques:**

Les systèmes à base de silicium en 2060 sont très différents de leurs équivalents du 20ème siècle. Dans de nombreux cas, la conception n'a de silicium que le nom, la véritable fabrication étant des matrices de cristaux vaporisés utilisant des nanites comme graveurs. Le terme "silicium" est resté, cependant, même si la technologie employée est devenue bien distincte.

De toute façon, les principes généraux sont les mêmes. Des couches de matériaux non-conducteurs sont superposées, avec des rainures gravées pour permettre à des matériaux conducteurs d'y être posés. La technologie silicium actuelle tend à être massivement miniaturisée, avec des noyaux silicium arrangés en matrices tridimensionnelles de sorte de maximiser la densité du transistor.

Malheureusement, malgré que la technologie ait fait de grandes percées, elle a toujours tendance à avoir des problèmes de dissipation de la chaleur, d'effets quantum qui limitent effectivement leurs capacités maximales, et un plateau de développement technologique avec le passage aux systèmes optiques.

### **HYBRIDE**

Les systèmes hybrides ont pour origine les premières technologies optiques à être intégrées avec des systèmes silicium. Dans la plupart des cas ils utilisent la logique silicium mais les bascules et bus de données optiques de sorte d'améliorer l'efficacité et la bande passante du système.

Ils n'ont pas les mêmes capacités que des systèmes complètement optiques, mais sont moins chers. Ils ne possèdent pas non plus toutes les limitations des systèmes silicium.

Les systèmes hybrides perdent rapidement leur popularité dans le monde moderne. Bien que supérieurs aux systèmes silicium, ils sont plus onéreux et dans de nombreux cas des systèmes complètement optiques sont mieux adaptés pour des applications modernes. Leur plus grande niche se trouve dans les cyberterminaux de grande consommation et les jouets "intelligents" ciblés pour la classe moyenne supérieure.

#### **Remarques Technologiques:**

Les systèmes hybrides sont généralement composés de processeurs en silicium liés à un bus de données optique. Libéré des limitations des vitesses des bus standard, les systèmes hybrides représentèrent un pas en avant décisif dans la conception d'ordinateur au moment de leur introduction, particulièrement pour les stations qui utilisaient les interconnexions optiques pour construire de puissants systèmes en paquets.

### **OPTIQUE**

La grande majorité des produits informatiques haut de gamme sont passés à des systèmes complètement électro-optique (ou "optronique") dans la dernière décennie. En particulier il n'y a pas eu un super-ordinateur construit depuis 20 ans qui repose sur des processeurs à base de transistors. A mesure que la technologie mûrit, le prix baisse et il devient disponible pour des gammes de plus en plus basses.

Bien qu'il lui reste encore à détruire complètement la main mise du silicium sur les biens de consommation électroniques les moins chers, on considère généralement que ce n'est qu'une question de temps avant des avancées rendent la technologie économique même à ce niveau. Les systèmes optiques sont renommés pour leur faible consommation d'énergie (très important pour le haut de gamme) et leur incroyable possibilité de miniaturisation. Même des cyberdecks bas de gamme possèdent souvent de multiples processeurs optiques travaillant en parallèle.

#### **Remarques Technologiques:**

Comme son nom l'indique, le système optique est basé sur la manipulation de la lumière. Aussi simple que cela puisse paraître, cela peut prendre de nombreuses formes.

Les systèmes de stockage optique sont basés autour de l'injection sur des treillis de cristal des protéines photosensibles dérivées de la bactériorhodopsine. La structure de ces protéines peut être altérée par des longueurs d'onde laser spéciales, et conserve leur structure jusqu'à être altérées à nouveau. Un autre laser peut alors lire la structure de la protéine. Les protéines simples utilisées dans les systèmes optiques n'ont généralement que deux états, mais de récentes avancées dans la biochimie moléculaire ont produit des protéines avec des niveaux variés de discrimination de longueurs d'onde. Ce qui signifie qu'une "cellule" protéinique peut avoir de multiples états, dépendant de la longueur d'onde des lasers utilisés pour lire et écrire leur état.

Les processeurs optiques, d'autre part, utilisent des protéines similaires qui ont des qualités conductrices variant avec leur structure courante. D'autres protéines fonctionnent comme des portes logiques, passant ou ne passant pas des impulsions lumineuses de certaines longueurs d'onde. Ainsi, manipuler les chaînes de protéines dans différentes configurations peut modifier les chemins logiques des puces. Ces structures sont généralement arrangées dans un format d'hypercube qui fournit une densité maximale de connexions possibles. De grandes installations sont généralement requises pour modifier des processeurs optiques à cause de techniques spéciales utilisées dans leur formatage, mais des processeurs optiques plus simples peuvent être reformatés au moyen d'encodeurs optiques couramment disponibles.

La recherche des futurs systèmes optiques est principalement concentrée dans la recherche de nouvelles protéines photosensibles, en particulier celles qui présentent des changements de phase stables en réaction de longueurs d'onde variables. D'autres axes de recherche sont des

formateurs laser plus rapides (les vitesses de lecture et d'écriture sont limitées par le mouvement l'ouverture du laser) et des modèles plus efficaces pour les processeurs optiques.

## **BIOTEK**

Les systèmes Biotek représente ce qui est à la pointe de la technologie informatique. Ces systèmes sont modélisés autour de réseaux neuronaux organiques pour leur construction et leur mode d'opération.

Les circuits sont littéralement cultivés selon des schémas prédéterminés puis leur logique leur est "imprimée". La science exacte derrière cette nouvelle technologie n'a pas été révélée, et jusque là seules Renraku et Maas-Neotek sont connues pour posséder cette technologie.

### **Remarques Technologiques:**

Les systèmes Biotek utilisent les technologies développées à la fois pour l'augmentation humaine et l'intégration système. Des fibres neuronales cultivées sont manipulées pour créer des structures à haute densité de traitement avec d'incroyables capacités d'auto-organisation et de densités de connexion. Toutes les biopuces sont cultivées à partir d'une masse "mère" centrale, puis des sections sont extraites et mises en croissance forcées selon des schémas précis. Les masses neuronales dans la puce n'ont pas individuellement suffisamment de matériel génétique pour cloner complètement une mère, une touche intentionnelle de "protection contre la copie". Chaque génération d'extrait de mère est devenue davantage complexe et capable, sans limite en vue pour sa capacité future.

Les processeurs Biotek requierent un niveau minimum d'équipement de maintien en vie, et peuvent être endommagés par une radiation intense ou des champs magnétiques. Pour cette raison, les biopuces ont tendance à être plutôt grandes de sorte d'incorporer les systèmes de nutrition appropriés et de protection. De petits connecteurs sur la puce procurent des canaux d'alimentation pour les nutriments nécessaires qui baignent les structures neuronales.