GERER LE HACKING AVEC SRA

AVANT-PROPOS

La matrice n'est pas toujours simple à appréhender, que ce soit en termes de règles ou de possibilités et jusqu'à la sortie du futur supplément SRA, les règles de ce dernier sont assez succinctes, de quoi suscité beaucoup d'interrogation quant à la façon de gérer un hacker dans une partie de Shadowrun.

Le document que vous parcourez actuellement concerne la façon de gérer le hacking : ce qu'il est possible de faire et comment le faire. Vous trouverez sur le site daegann.fr un autre document concernant des notions que j'espère assez complètes et générales sur ma vision de la matrice, comment se la représenter au quotidien et comment elle fonctionne (dans les grandes lignes).

Si la présente aide est avant tout destinée à Shadowrun Anarchy, elle contient des indications pouvant être utiles dans les autres éditions. Ces règles sont également faciles à adapter pour jouer une matrice simplifiée dans les autres éditions de Shadowrun.

⚠ Ces règles s'inspirent des règles de matrice de différentes éditions (en les simplifiant pas mal) et ne correspondent pas à une image fidèle des règles/background de la matrice à SR6, en particulier en ce qui concerne la sécurité matricielle et le GOD. Sur ces points, ces règles se rapprochent plus de l'esprit des premières éditions, simplement parce que je trouve cela plus intéressant.

RÉSUMÉ

Pour faire bref, voici les quelques points à retenir concernant les règles de hacking pour SRA développées ci-dessous. Bien sûr chacun de ces points comporte des subtilités, aussi ne vous contentez pas du résumé pour bien comprendre le fonctionnement du hacking.

- Utiliser la matrice en RA permet d'agir dans le monde physique en parallèle. Se connecter en VR impose de laisser son corps inerte, mais permet d'obtenir un modificateur de +1 dé à tous ses tests matriciels.

- Les actions matricielles légales (percevoir la matrice ou effectuer une recherche) s'effectuent avec Logique + Électronique (spécialité adaptée). Le seuil peut être ouvert (plus on obtient de succès, plus on obtient de détails), fixe si on cherche une information précise ou opposé à Logique + Hacking (discrétion) lorsqu'on tente de repérer un hacker.

- Pour pirater un appareil ou un serveur/réseau, il faut connaître son adresse matricielle. Il faut donc être soit à proximité de sa cible pour établir une connexion directe, soit avoir découvert cette adresse pour pouvoir établir une connexion distante.

- Toute action illégale contre un appareil ou un serveur/réseau (imiter un ordre, s'introduire dans un système, contrôler un système, se cacher, brouillage, cybercombat, etc.) se fait via un test de Logique + Hacking (spécialité adaptée).
  - Le seuil de ce test dépend du code couleur du système cible : 1 pour un code Bleu, 2 pour un code Vert, 3 pour un code Orange, 4 pour un code Rouge. Tout appareil asservi à un réseau/serveur utilise le code le plus élevé entre le sien et celui de son "maître".
  - Si le hacker a été détecté et qu'un decker de sécurité est présent, celui-ci peut utiliser son action (s'il ne l'a pas déjà utilisée) pour tenter de s'opposer à l'action via un test de Logique + Hacking. Les succès obtenus constituent le nouveau seuil pour réussir le piratage (seulement s'ils sont plus nombreux que le code couleur du serveur, autrement ce dernier s'applique toujours).

- Chaque fois qu'une action illégale est tentée, le système fait un test de détection. La réserve de dé de ce test est le plus élevé entre la réserve du système (4 pour un code Bleu, 8 pour un code Vert, 12 pour un code Orange, 16 pour un code Rouge) et la Logique + Électronique de toute personne qui surveille ce système (s'il y en a… si cette personne est occupée en parallèle, un malus peut être appliqué à sa réserve).
  - Le seuil pour détecter une action illégale correspond au nombre de succès obtenus pour réaliser cette action.
  - Si le test de détection est réussi, le système passe en alerte passive (s'il n'y avait pas d'alerte) ou en alerte active (s'il y avait déjà une alerte passive).

- Lors d'une alerte passive, la cible n'est encore sûre de rien et aura tendance à activer une CI Sonde. Celle-ci effectuera des tests de perceptions matricielles (action légale telle que décrite ci-dessus) jusqu'à réussir à détecter le hacker (ce qui déclenche une alerte active s'il n'y en avait pas déjà et permet de cibler le hacker). Ce test de perception peut également être réalisé par un éventuel hacker de sécurité.

- Lors d'une alerte active, le système déclenche une ou plusieurs CI (nombre limité par son code couleur), avertit la sécurité et, en cas de dernier recours, peut rebooter le système.

- Lorsqu'un persona est détecté (le savoir présent n'est pas suffisant), toute action contre ce dernier (trace, verrouillage de connexion, cybercombat, etc.) se fait via un test de Logique + Hacking (cybercombat). La cible se défend ici avec Logique + Firewall.

- Le cybercombat vise à infliger des dégâts matériel ou cérébral à un persona, un programme (CI notamment) ou un appareil.
  - Les dégâts de base pour un hacker sont de (Logique/2) E, ceux pour une CI dépend de la couleur du système (2E pour un code Bleu, 3E pour un code vert, 4E pour un code orange et 5E pour un code rouge). Des atouts tels que les programmes marteau ou biofeedback peuvent modifier le type ou la valeur de ces dégâts.
  - Les dommages étourdissants sont toujours appliqués au matériel
  - Les dommages physiques sont appliqués au moniteur physique (en ignorant l'armure) si la cible est un personnage connecté en VR ou au matériel dans les autres cas.
  - Si le moniteur d'un cyberdeck, d'un appareil ou d'un serveur auquel est connecté un personnage en VR est rempli, alors ces personnages subissent un choc d'éjection (dégât de 3E pour les personnages en RA, 3P s'ils étaient en VR)

- Les moniteurs de conditions courants sont :
  - Cyberdeck : 6 à 15 cases
  - CI : 8 cases
  - Système Bleu : 4 cases
  - Système Vert : 8 cases
  - Système Orange : 12 cases
  - Système Rouge : 16 cases

- Les actions du hacker sont :
  - Percevoir la matrice (légal)
  - Effectuer une recherche (légal)
  - Imiter un ordre
  - Accéder à un système
  - Contrôler un système
  - Attaquer une icône
  - Se cacher

- Les actions de sécurité sont :
  - Surveiller un système (Hacker de sécurité – légal)
  - Percevoir la matrice (Hacker de sécurité/CI – légal)
  - Protéger un système (Hacker de sécurité)
  - Attaquer une icône (Hacker de sécurité/CI)
  - Déclencher une CI (système)
  - Remplacer une CI par une autre (système)
  - Nettoyer une CI planté en cybercombat (système)

LES BASES

Connexion à la matrice

C'est la base, mais ça va mieux en le disant : s'il suffit d'un commlink pour surfer, percevoir la matrice et y faire des recherches matricielles, un cyberdeck est nécessaire pour pirater un système ou entrer en cybercombat.

Pour utiliser la VR (mais aussi pour utiliser plus facilement la RA), un utilisateur a besoin d'une Interface Neural Direct (IND) telle qu'un datajack ou des électrodes. Les électrodes sont des équipements, le datajack est un atout coûtant 1 point (il ne fournit qu'un avantage narratif, le bonus de VR n'est pas lié à l'atout, c'est un modificateur de situation), un cyberjack est un datajack spécialisé offrant des bonus pour les actions matricielles (le datajack du livre de base VF est un cyberjack, certains sont encore plus évolués et offrent plus de bonus).

Les technomanciens sont une exception : ils n'ont besoin ni de commlink, ni de cyberdeck, ni d'IND pour agir dans la matrice.

Hacker en RA

En RA, les utilisateurs peuvent accéder à la matrice tout en continuant d'être actifs à côté. Seul leur matériel est exposé aux dégâts matriciels.

En RA, le hacker utilise plusieurs fenêtres, objets RA et autres représentations graphiques pour visualiser ce qu'il cherche, l'état des processus de sa cible, de son matériel et tout un tas d'autres indicateurs. On est plus proche du hacking tel qu'on le connaît aujourd'hui en quasi-ligne de code que des métaphores 3D de la VR. Lorsqu'il agit dans la matrice, il utilise principalement une IND pour envoyer mentalement des instructions, lancer des programmes et activer ses commandes. De nombreux hackers utilisent aussi leurs mains pour gérer et réorganiser la disposition de leur affichage RA, voire lancer manuellement certaines commandes en parallèle.

Lorsqu'il n'est pas possible d'utiliser une IND (si on utilise un clavier mécanique ou holographique sur un vieux terminal par exemple), le MJ devrait imposer un malus pour les tests de hacking et autres actions matricielles où la réactivité est importante.

Hacker en VR

En VR, l'esprit de l'utilisateur plonge dans la matrice tandis que son corps devient inerte. Il devient plus réactif et obtient un modificateur de +1 sur tous ses jets matriciels. Il s'agit bien d'un modificateur et pas d'un bonus d'atout. En VR, le cerveau de l'utilisateur est exposé aux biofeedbacks sensoriels, l'utilisateur risque aussi d'être blessé.

Là aussi, hacker en VR revient à exploiter son IND pour activer mentalement certains programmes et utiliser mentalement les fonctions intégrées de son deck, la différence c'est qu'en VR, l'utilisateur est baigné par l'iconographie de la matrice et que certains de ses programmes peuvent adopter cette même iconographie (un programme d'attaque chargé dans la mémoire du deck pouvant apparaître comme une arme dans les mains du persona matriciel).

Trouver sa cible

Une action matricielle dirigée contre un système ne peut atteindre ce dernier que si une connexion peut être établie entre le hacker et sa cible.

Cette connexion peut être directe si l'utilisateur se trouve à proximité d'une icône appartenant au système cible. Ce peut être un lien matriciel dans un serveur ou un appareil asservi au réseau ciblé dans le monde physique. La portée d'un signal est d'environ cent mètres en ville, mais tombe à une cinquantaine de mètres dans les zones densément peuplées/spammées ou à moins de dix mètres à travers les murs dotés d'une armature métallique. Une icône cachée ou un appareil opérant en mode furtif doivent d'abord être détectés avant de pouvoir être ciblés.

La connexion peut aussi être distante si l'utilisateur connaît l'adresse matricielle de la cible (soit parce que celle-ci est accessible publiquement depuis la matrice, soit parce que le hacker a eu l'occasion d'examiner une connexion vers cette cible, ou encore s'il a trouvé un moyen d'acheter cette information).

Les personas sont un cas particulier : ils ne peuvent être pris pour cible que si l'on se trouve dans un système où ce persona est actif, que ce soit sur un serveur distant ou directement dans le PAN de cet utilisateur. Il n'est d'ailleurs pas possible de s'introduire dans le PAN d'un utilisateur directement via le persona, il faut d'abord tracer le persona (action de cybercombat) pour découvrir l'adresse matricielle du PAN et pouvoir établir une connexion distante avec celui-ci. Bien sûr, il est aussi possible d'établir une connexion directe avec un PAN si on se trouve physiquement à proximité de celui-ci.

LA SÉCURITÉ MATRICIELLE

Fonctionnement

Le niveau de sécurité d'un système matriciel est défini par un code couleur et un chiffre.

La couleur représente le nombre de succès nécessaire pour qu'une action de piratage soit réussie (Bleu = 1 succès nécessaire, Vert = 2, Orange = 3 et Rouge = 4). Le code couleur est aussi un indicateur (parfois trompeur) du type de sécurité mis en œuvre en cas d'alerte, plus un serveur étant foncé, plus ses CI sont en général efficaces, nombreuses et mortelles.

Le chiffre correspond à la réserve de détection du système : chaque fois qu'une action illégale (tests impliquant la compétence Hacking) est entreprise dans ou contre le système, celui-ci lance sa réserve de détection. S'il obtient plus de succès que l'action qu'il tente de détecter, une alerte est déclenchée : passive dans un premier temps, puis active.

Notez qu'un personnage peut tenter d'améliorer la sécurité d'un système en le surveillant et/ou en le protégeant (voir les deux actions correspondantes dans "les actions du hacker" plus bas dans le document).

Alerte passive

Lorsqu'une alerte passive est déclenchée, c'est que le système a détecté des anomalies, mais qu'il ne peut pas encore être sûr qu'il y a piratage. La réaction la plus fréquente à une alerte passive est l'activation d'une CI sonde pour tenter de détecter un éventuel hacker (test de perception matriciel).

Bien qu'il n'y ait pas de mécanique pour cela, considérez de façon rôleplay que des faux positifs existent et qu'à ce stade le système cherche encore à déterminer s'il y a réellement une anomalie ou s'il ne s'agit que d'un bug ou d'un phénomène matriciel inoffensif.

Alerte active

Lorsqu'une alerte active est déclenchée, c'est que le système sait de façon certaine qu'il est attaqué. La priorité est alors de détecter le responsable pour être en mesure d'agir contre lui (via un test de perception matricielle effectué par une CI sonde et/ou un hacker de sécurité). Les réactions les plus fréquentes sont l'activation de CI offensives, l'envoi de hackers de sécurité et dans les cas extrêmes, la mise offline ou le reboot du système.

Lorsqu'une alerte active est déclenchée, il ne fait aucun doute que les éditions/modifications apportées au système ou à ses données seront tôt ou tard identifiées et réinitialisées.

Niveau de sécurité type

La sécurité matricielle n'est pas qu'une affaire de compétence, elle dépend bien plus du rapport entre le risque lié à la probabilité d'un piratage, du préjudice subi en cas de réalisation de ce risque et du coût de la sécurité (en équipement, entretien et en productivité, car une sécurité accrue à généralement un impact sur l'ergonomie et la performance d'un système). Les configurations de serveurs les plus courantes sont :

Bleu-4 (seuil 1, réserve de détection de 4) : commlinks bas de gamme, la plupart des objets connectés, distributeurs automatiques, supports publicitaires, banque de données publiques, services matriciels gratuits, serveurs d'entreprises indépendantes. Bref, tout ce qui n'a pas les moyens de faire mieux où qui ne nécessite pas mieux.

Vert-8 (seuil 2, réserve de détection de 8) : commlink moyen et haut de gamme, cyberdecks, serveurs corpo non sensibles, serveur de sécurité des sites de faible importance, plupart des serveurs pirates gérés par des gangs ou par le crime organisé, serveurs des universités, hôpitaux publics, serveurs de jeux matriciels. Bref tout ce qui n'est pas sensible ou n'a pas les moyens de faire mieux.

Orange-12 (seuil 3, réserve de détection de 12) : serveurs corpo traitant de données sensibles, serveurs de sécurité des sites de moyenne importance, serveurs pirates gérés par les pointures du milieu criminel. Bref, tout ce qui commence à demander de sérieuses mesures de sécurité quitte à dégrader l'expérience utilisateur par l'ajout de certaines mesures de sécurité, mais sans pour autant nécessiter les mesures les plus contraignantes ou le top du top (qui reste coûteux à mettre en place et à maintenir).

Rouge-16 (seuil 4, réserve de détection de 16) : serveurs corpo ou gouvernementaux traitant de données top secrètes ou d'installation d'importance cruciale (site militaire, centrale nucléaire, clinique delta, etc.). Bref tout ce qui justifie l'emploi des mesures de sécurité les plus fortes.

Notez que la réserve de détection des systèmes peut être ajustée de +/-2 pour montrer que le système matriciel est plus ou moins robuste que la moyenne, sans pour autant aller jusqu'à changer son code couleur.

Contre-mesure d'Intrusion (CI)

Un serveur peut activer ou remplacer une CI par tour (la CI ainsi chargée pourra agir au prochain tour) et maintenir actif simultanément un nombre de CI correspondant à son code couleur (1 pour un serveur bleu, 2 pour un serveur vert, 3 pour un orange et 4 pour un rouge).

Une CI possède un moniteur de condition de 8 cases. Une fois ce moniteur rempli, la CI est plantée. Elle devra être effacée

avant qu'une copie puisse être relancée par le système (chacune de ces actions nécessite un tour).

Une CI possède également un indice : il s'agit de sa réserve de dés pour toutes ses actions (certaines CI évolué peuvent posséder l'équivalent d'atouts lui procurant des bonus pour certaines actions). Cet indice est généralement égal à la réserve de détection du serveur sur lequel la CI tourne.

Le type d'une CI détermine les actions que celle-ci peut mener. On distingue les types de CI suivantes :

- CI Sonde : ce type de CI peut effectuer des tests de perception matricielle (contre Logique + Hacking (discrétion)) pour tenter de détecter un hacker et/ou déclencher une alerte active.

- CI Trace : ce type de CI cherche à remonter la connexion d'un hacker pour géolocaliser celui-ci afin de lui envoyer une équipe de sécurité ou permettre à un hacker de sécurité de pirater son commlink. Pour tracer une cible, la CI effectue un test contre Logique + Hacking (discrétion). Si la CI à plus de succès que sa cible, divisez 10 par le nombre de succès excédentaire pour obtenir le nombre de tours (arrondis au supérieur) nécessaire à la CI pour localiser sa cible.

- CI Pot de colle : la seule fonction de cette CI est de verrouiller la connexion de sa cible (pour laisser le temps aux autres CI de faire un maximum de dégâts ou à une CI trace de localiser sa cible). Cette action étant une attaque contre un persona, il s'agit d'un test contre Logique + Firewall. En cas de succès, la cible est verrouillée (voir ci-dessous).

- CI Kamikaze : ces CI sont conçus pour tenter de faire planter les programmes et processus de leur cible. En cas de réussite d'un test opposé à Logique + Firewall (discrétion) de la cible, elle impose un malus aux actions matricielles de sa cible égale au nombre de succès excédentaire (max -3). Ces malus disparaissent après un reboot.

- CI Blaster : ces CI grises infligent des dégâts matériels (toujours appliqués au matériel) en cybercombat. Les dégâts de base de cette CI dépendent du code couleur du serveur sur lequel elles tournent : 2E pour les serveurs bleus, 3E pour les serveurs verts, 4E pour les serveurs oranges et 5E pour les serveurs rouges. En cas de succès, la connexion de la cible est verrouillée (voir ci-dessous).

- CI Noire : les CI noires fonctionnent comme les CI blaster, mais en utilisant l'interface simsens de la cible pour lui infliger des dégâts de biofeedback (appliqués au moniteur physique des hackers connectés en VR).

- CI Psychotrope : ce type de CI est une variante non létale, mais plus vicieuse, des CI noires : elles utilisent le biofeedback simsens pour affecter psychologiquement la cible plutôt que de lui infliger des dégâts. Lorsqu'elle attaque une cible connectée en VR, la cible se défend cette fois avec Volonté + Firewall. En cas d'échec, la CI inflige des séquelles psychologiques mineures pour les (succès excédentaires x 2) prochaines heures. Ces effets peuvent varier de l'envie irrépressible d'acheter certains produits, de se rendre aux autorités (ou d'appeler un numéro surveillé par les propriétaires de la CI) à l'aversion pour certaines actions en passant par un sentiment de culpabilité ou même des pertes de mémoire à court terme. Si la cible est connectée en RA, cette CI inflige simplement des dégâts matériels.

Notez que les CI peuvent toucher autant de cibles que leur indice en une action (un seul jet peut affecter indépendamment plusieurs cibles, typiquement lorsque plusieurs hackers s'en prennent à un système).

Verrouillage de connexion

Lorsqu'une cible subit un verrouillage de connexion, elle ne peut plus se déconnecter proprement du serveur sans d'abord faire planter la CI verrouillant sa connexion. Si la cible tente malgré tout de se déconnecter, elle devra passer son tour à cela et réussir un test de Volonté + Logique contre un seuil correspondant au code couleur du système hébergeant la CI. En cas de réussite, la cible parvient à se déconnecter, mais subit un choc d'éjection causant des dégâts de biofeedback de 3 P.

Systèmes imbriqués ou interconnectés

Parfois un serveur n'est accessible qu'en passant par l'intermédiaire d'un autre serveur.

C'est par exemple le cas lorsqu'on ignore l'adresse matricielle d'un serveur et qu'en pirater un premier permet de découvrir l'adresse du second (qui peut alors être piraté indépendamment du premier). Il est ainsi possible de passer de serveur en serveur en explorant les multiples connexions liant les systèmes les uns aux autres.

C'est aussi le cas lorsque le second serveur fait partie d'un système segmenté plus vaste. Par exemple, le serveur des archives d'une corpo peut n'être accessible qu'en passant par un serveur de travail. Dans ce cas, le hacker devra s'introduire successivement dans les deux serveurs et y maintenir une connexion s'il souhaite fouiller les archives.

Un serveur raccordé à une Grille de Télécommunication Locale Privé (GTLP) agit de la même façon : le hacker doit d'abord pirater la GTLP (et y maintenir une connexion) avant de pouvoir s'introduire sur les serveurs qui y sont raccordés.

Le MJ ne devrait pas abuser de ces imbrications, car l'intérêt en termes d'amusement et de gameplay est limité. Mieux vaut faire certaines abstractions et limiter ces imbrications à deux niveaux au maximum (au moins dans les jets de dé, rien n'empêche d'en mentionner plus dans la narration de la partie).

Appareils connectés et réseaux, quel niveau de sécurité choisir ?

Lorsqu'un appareil est asservi à un maître, il devient une partie de celui-ci : une caméra de sécurité ou un maglock est un périphérique commandé (et surveillé) par un serveur de sécurité, une montre connectée ou un pistolet smartlinké fait partie du réseau personnel (PAN) géré par un commlink, etc.

Dès qu'un appareil doit se défendre, il utilise l'indice le plus élevé entre le sien ou celui de son maître. Cependant, en raison de la connexion privilégiée existant entre maître et esclaves, accéder à l'un revient à accéder à l'ensemble du réseau.

Juridictions

La sécurité matérielle d'un réseau, d'un serveur ou d'une Grille de Télécommunication Locale est sous la responsabilité de son administrateur ou de la corporation détenant le contrat de sécurité matricielle de ce système. C'est lui qui définit la réaction du système en cas d'attaque.

Sauf s'il s'agit d'une entité extraterritoriale, cet administrateur doit respecter le cadre légal correspondant à la GTL auquel ce système est raccordé : un serveur connecté à la grille de Seattle doit respecter les lois du métroplexe, qui mentionnent par exemple que les CI noires ne sont pas légales et que les CI blaster sont soumises à un permis.

Lorsqu'un hacker est géolocalisé en dehors de la juridiction de l'entité assurant la sécurité matricielle, celle-ci doit théoriquement faire appel au GOD/DIEU, une sorte d'Interpol matriciel : un accord entre les principaux acteurs de la sécurité leur permet en effet de collaborer pour signaler une activité matricielle illicite. L'entité gérant la police locale sera alors mandatée pour intervenir physiquement et, au besoin, extrader les coupables. Bien sûr, certaines corpos préfèrent parfois régler le problème par eux-mêmes en envoyant leurs propres équipes lorsqu'elles le peuvent, plutôt que de prévenir le GOD/DIEU.

Le GOD/DIEU possède également ses propres membres, les G-mens (en fait, des agents des corpos membres placés sous sa direction et agissant en son nom) capables de mener des investigations multijuridictionnelles.

LES ACTIONS DU HACKER

Il y a 9 types d'action nécessitant un test qu'un personnage peut entreprendre dans la matrice, trois sont légales (test de Logique + Électronique) et six sont des actions illégales (Logique + Hacking) :

- Percevoir la matrice (légal)
- Effectuer une recherche (légal)
- Surveiller un système (légal)

- Imiter un ordre
- Accéder à un système
- Contrôler un système
- Attaquer une icône
- Se cacher
- Protéger un système

Perception matricielle

Les tests de perception matricielle permettent de détecter des icônes cachées et appareils opérant en mode furtif, ainsi que d'obtenir des informations sur son environnement matriciel. Cela nécessite la réussite d'un test de Logique + Électronique (perception matricielle). Le nombre de succès détermine la quantité et la précision des informations recueillies (en fonction de ce que l'on cherche à percevoir).

Scanner et analyser son environnement matriciel consiste principalement à jouer avec le paramétrage de son appareil pour être en mesure de détecter et d'analyser les icônes et les signaux environnants.

Utilité de percevoir la matrice en RA

Un test de perception matriciel en RA permet de scanner son environnement pour, entre autres :

- Chercher l'icône d'un appareil furtif que l'on sait présent (ce qui permettra de cibler cet appareil matriciellement et donc de le hacker). Les appareils n'opérant pas en mode furtif sont considérés comme pouvant être ciblés sans test préalable.

- Vérifier (et localiser) la présence (ou l'absence) dans les environs d'une signature matricielle connue, y compris si l'appareil opère en mode furtif.

- Sonder la présence (types et nombre) d'appareils connectés à un endroit donné (et ainsi savoir que trois commlinks, dont un en mode furtif, se trouvent dans la pièce d'à côté).

- Voir quels tags un individu porte sur lui, ou avoir conscience de la présence de certains tags dans les environs (et ainsi savoir que la personne en face de vous porte un pistolet lourd non détagué sous son manteau long). Un test n'est pas nécessaire, mais une action doit être utilisée pour cela.

- Analyser une icône (tag, comlink, objet connecté, etc.) pour y récupérer les métadonnées (numéro de série, fabricant, géoloc, etc.) s'il y en a et/ou déterminer sa signature matricielle (fingerprinting) afin de pouvoir la reconnaître ultérieurement.

- Analyser une icône permet également de déterminer à quel réseau éventuel l'appareil est asservi ou connecté (et identifier les autres appareils du réseau qui se trouvent à porter).

- Ou encore vérifié si un appareil/tag est resté présent dans votre environnement au cours de ces vingt dernières minutes alors que vous vous déplaciez (et si c'est le cas, tirez-en les conclusions que vous voulez).

Utilité de percevoir la matrice en VR

En VR, le test de perception matriciel permet entre autres de :

- Sonder un serveur pour y détecter des icônes cachées, que ce soit des personas, des fichiers ou même des liens vers d'autres serveurs (ce qui permettra ensuite d'agir dessus). Les CI et hackers de sécurité effectuent ce type d'action pour détecter la présence d'un hacker.

- Analyser un serveur pour savoir si celui-ci est en état d'alerte.

- Scanner un fichier pour savoir s'il est protégé par une databomb ou tout autre mécanisme.

- Analyser une CI pour connaître son type (et en déduire ses effets).

- Plus généralement, analyser n'importe quelle icône pour comprendre de quoi il s'agit (à noter que les technomanciens, leurs formes complexes et leurs sprites sont difficiles à vraiment identifier comme tel).

Commlinks et appareils en mode furtif

Les commlinks et autres appareils connectés peuvent fonctionner en mode furtif : leurs échanges d'information avec la matrice sont alors réduits au maximum et ils deviennent plus difficiles à repérer. De nombreuses juridictions interdisent l'utilisation de ce mode de connexion. Considérez qu'un appareil furtif ne peut être détecté que via un test de perception matriciel.

Recherche matricielle

La recherche matricielle est utilisée lorsque l'on cherche une information (chercher un fichier dans un serveur sera plus de

la perception matricielle). Il s'agit d'un test de Logique + Électronique (recherche matricielle) contre un seuil de réussite basé sur la complexité de la recherche : est-ce que l'information est disponible dans un tas d'articles récents de grands médias ou uniquement dans une vieille archive payante d'un obscur forum matriciel spécialisé ? Notez qu'on ne peut pas toujours tout trouver via une recherche, certaines informations sont simplement introuvables dans la matrice.

Ajouter un peu de rôleplay (optionnelle)
N'hésitez pas ajoutez un peu de rôleplay en offrant quelques choix lorsque la situation s'y prête (en particulier si le résultat du test de recherche ne permet pas de donner des infos qui rendraient la suite du scénario plus intéressante, où pour avoir l'opportunité de révéler des infos annexes à la recherche). Voici pour cela quelques exemples :

- En épluchant les résultats de sa recherche, le personnage est parvenu à identifier une personne qui pourrait avoir accès à des informations intéressantes. Peut-être que cette personne s'est vantée sur un forum (public ou des ombres) ou bien plusieurs articles font référence à ses travaux. Quoi qu'il en soit, la contacter directement pourrait être instructif, mais il faudra peut-être trouver un moyen de convaincre ce PNJ, peut-être que le contacter alertera les mauvaises personnes ou peut-être que suivre cette piste ne sera qu'une perte de temps précieux. Aux PJs de voir s'ils veulent explorer cette piste et de quelle manière.

- Peut-être que poser des questions sur quelques forums spécialisés permettra d'obtenir des réponses, mais cela risque aussi mettre la puce à l'oreille des mauvaises personnes. En conséquence, des prix peuvent monter, des sécurités être renforcées, des PNJs se méfier ou commencer à faire profil bas. Peut-être aussi qu'un PNJ essayera de pigeonner les PJs ou de profiter de leur besoin d'information pour qu'on lui rende service…

- Des informations prometteuses semblent se trouver dans une base de données payante ou sont vendues aux enchères. Les PJs accepteront-ils de débourser quelques nuyens, tenteront-ils de dérober l'information en piratant la source d'information ou chercheront-ils ailleurs ?

Surveiller un système

Lorsqu'un personnage surveille un système (par exemple un spider, ou le propriétaire d'un commlink), celui-ci peut choisir (sans obligation) de remplacer la réserve de détection du système par sa Logique + Électronique.

Cette surveillance ne coûte aucune action au personnage, qui peut agir normalement en parallèle. Cependant, si le personnage est distrait (parce qu'il est occupé à faire autre chose à côté), le MJ devrait imposer un malus à cette réserve. Autrement dit, un personnage surveillant activement un système aura droit à toute sa réserve et pourra, en cas d'alerte, effectuer immédiatement un test de perception matriciel, tandis qu'un personnage vacant à ses occupations sera plus susceptible de passer à côté des bugs, anomalies et indice permettant de comprendre que le système est compromis.

Imiter un ordre

Parfois, on n'a ni le temps ni l'envie de s'introduire dans un système matriciel alors qu'on souhaite juste déverrouiller un maglock, réorienter l'angle d'une caméra ou éjecter le chargeur du type qui nous braque. Dans ce cas, le spoofing est votre solution.

Il s'agit ici de tromper un appareil pour le forcer à exécuter un ordre qu'il croit légitime. Cela revient à prendre le contrôle de l'appareil le temps d'une unique action.

Notez que seuls les appareils sont concernés et qu'il n'est possible de leur faire faire que ce pour quoi ils sont conçus : on peut donner l'ordre à une caméra de se mettre en pause, mais pas de se mettre en pause uniquement pour les cinq prochaines minutes (pour ça il faudra imiter l'ordre de mise en pause, puis celui de remise en marche au moment voulu, ou bien carrément pirater le système pour reprogrammer la caméra).

Imiter un ordre nécessite un test de Logique + Hacking (guerre électronique) contre un seuil dépendant de la couleur du système ciblé (voir sécurité matricielle plus haut). De son côté, le système lancera sa réserve de détection pour déterminer si l'action déclenche une alerte (là aussi, voir sécurité matricielle plus haut).

S'introduire dans le système

Il existe deux grandes façons de s'introduire illégalement dans un système matriciel : sans préparation à la volée (à l'arrache diraient certains) ou en prenant le temps de sonder sa cible pour y trouver des failles à exploiter le moment venu.

Utiliser cette seconde façon devrait apporter, le moment venu, un modificateur positif au test d'intrusion dépendant du temps passé à sonder la cible (de quelques minutes à quelques heures). Alternativement, si vous jugez la préparation suffisante, vous pouvez plutôt choisir de donner un point d'Anarchy utilisable jusqu'à la prochaine scène, à dépenser en rapport avec le piratage (ou cybercombat) de la cible sondée.

Dans les deux cas, s'introduire dans un système nécessite un test de Logique + Hacking (intrusion) contre un seuil dépendant de la couleur du système ciblé (voir sécurité matricielle plus haut).

Contrôler un système

Une fois dans un système, toute action qui ne relève pas d'une recherche, de la perception ou du cybercombat est considérée comme une action de contrôle. Cela couvre donc entre autres le téléchargement ou l'édition de données (fichiers, streaming de flux vidéo, etc.), l'effacement de log et autres signatures matricielles, la prise de contrôle totale d'un appareil (plonger dans l'appareil pour le contrôler sans nécessiter de test de piratage ultérieur), la mise sur écoute d'un appareil, etc.

Comme toute action illégale, contrôler un système se fait via un test de Logique + Hacking contre un seuil dépendant de la couleur du système ciblé.

Contrôler un appareil contrôlé par un utilisateur en plongée

Un hacker ne peut pas plonger dans un appareil déjà contrôlé par un utilisateur plongé dedans (cela vaut pour un rigger pilotant un véhicule en plongée, pour le possesseur d'un cyberware, mais pas pour un rigger donnant des ordres à distance à un drone).

S'il veut malgré tout plonger dans l'appareil, le hacker devra préalablement éjecter l'utilisateur légitime qui s'y trouve plongé. Pour cela, il doit attaquer le persona de cet utilisateur en cybercombat, soit à l'aide d'un programme biofeedback (si l'utilisateur meurt ou tombe inconscient, la place devient libre), soit à l'aide d'un programme psychotrope spécifique influençant la cible pour qu'elle se déconnecte lorsque c'est possible (voir CI Psychotrope pour les règles associées).

Autrement, un hacker peut toujours tenter de contrôler l'appareil en piratant celui-ci pour qu'il effectue certaines actions, mais la présence d'un utilisateur en plongée complique chacune de ces actions : chaque fois qu'une tentative de donner un ordre ou de contrôler un appareil est réussie, l'utilisateur en plongée a droit à un test de Volonté + Logique pour réagir et contrer cet ordre, le seuil étant le nombre de succès obtenus par le hacker. À la discrétion du MJ ces tentatives de contrôle, qu'elles soient ou non réussies, peuvent gêner le personnage en plongée pour ses propres actions et donc lui imposer un malus.

Attaquer une icône

Attaquer une icône vise à affecter directement le fonctionnement de celle-ci, que ce soit en brouillant un appareil, en faisant planter les processus d'un serveur ou d'un persona ou encore en tentant d'infliger des dégâts logiciels et matériels à sa cible pour la rendre aussi utile qu'une brique (d'où le fait que l'on parle de "briquer" un appareil) ou cérébraux (via l'envoi de dangereux biofeedbacks sensoriels). C'est également en attaquant l'icône d'un persona que l'on peut tracer l'origine physique et matricielle de celui-ci (il n'est par contre pas possible de géolocaliser un serveur de cette façon).

Pour attaquer un persona, celui-ci doit avoir été préalablement détecté (le savoir présent ne suffit pas). Il faut ensuite réussir un test de Logique + Hacking (cybercombat) tandis que la cible se défend avec Logique + Firewall.

Attaquer un appareil, une CI ou un serveur demande aussi un test de Logique + Hacking (cybercombat) contre l'habituel seuil dépendant de la couleur du système auquel appartient la cible.

Dégâts en cybercombat

Les dégâts de base des attaques en cybercombat sont de (Logique/2) E, éventuellement modifiés par des programmes tels que marteau ou biofeedback.

Les dommages étourdissants causent des dégâts logiciels et matériels affectant uniquement le matériel, quel que soit la cible ou le type de connexion employé.

Les utilisateurs en VR ayant désactivé la plupart des sécurités pour gagner en performance (hot sim), les dégâts causés par l'envoi de pics sensoriels générant un biofeedback (CI Noire, programme biofeedback) sont susceptibles de leur causer lésions cérébrales, ruptures d'anévrisme et autres blessures. Ces dégâts Physiques sont appliqués au moniteur de condition physique du personnage concerné sans tenir compte de son armure.

Lorsqu'un pic de biofeedback cible un appareil ou un utilisateur connecté en RA, les sécurités de l'équipement encaissent ces dégâts qui sont donc appliqués au moniteur de l'appareil.

Si le moniteur d'un cyberdeck, d'un appareil ou d'un serveur auquel est connecté un personnage en VR est rempli, alors ces personnages subissent un choc d'éjection (dégât de 3E pour les personnages en RA, 3P s'ils étaient en VR)

Les principaux moniteurs de conditions sont :

- Cyberdeck : 6 à 15 cases
- CI : 8 cases
- Serveur Bleu : 4 cases
- Serveur Vert : 8 cases
- Serveur Orange : 12 cases
- Serveur Rouge : 16 cases

Se cacher

Lorsqu'un hacker est repéré (via un test de perception matricielle), hacker de sécurité et CI peuvent agir directement contre son persona. Pour éviter cela, un hacker peut tenter de masquer ses traces via un test de Logique + Hacking

(discrétion) contre un seuil dépendant de la couleur du système où a lieu l'action.

En cas de réussite le hacker semble s'être déconnecté et est de nouveau furtif, ce qui veut dire qu'une CI Sonde ou qu'un hacker de sécurité va devoir à nouveau réussir un test de perception matricielle pour pouvoir agir contre lui.

À noter que si le hacker ne fait pas de vagues pendant plusieurs tours/minutes et parvient à rester cacher, il est probable que la sécurité matricielle pense qu'il s'est effectivement déconnecté. Le serveur retombera alors en alerte passive et les éventuelles CI Sonde arrêteront d'effectuer des tests de perception matricielle (mais resteront active un temps, au cas où).

Protéger un système

Un personnage peut consacrer son action à protéger activement un système pour tenter de contrer une action d'un hacker adverse (sous réserve que celui-ci ait été détecté). Dans ce cas, le seuil nécessaire pour pirater le système est le plus élevé entre le code couleur du système et le résultat d'un test de Logique + Hacking effectué par le personnage souhaitant s'opposer au piratage.

EN PRATIQUE

La théorie, c'est bien, mais en jeu on a parfois un peu plus de mal à voir comment les choses fonctionnent ou peuvent être utilisées. Voici quelques exemples permettant d'avoir un aperçu un peu plus concret de l'organisation matricielle de système auxquels les joueurs sont fréquemment confrontés.

Pirater un serveur R&D

Tout d'abord une évidence : l'adresse matricielle d'un serveur R&D n'est pas publique.

Avec de bons contacts, on peut peut-être la découvrir, ce qui permet de faire une passe matricielle dessus à distance (notez tout de même que cette information a généralement une durée de vie limitée, les serveurs pouvant changer d'adresse plus ou moins régulièrement par sécurité. Notez aussi que c'est une information qui devrait bien se monnayer). Si le serveur se trouve sur une Grille de Télécommunication Locale Privée, il peut être nécessaire de se frayer d'abord un chemin à travers cette GTLP avant de pouvoir atteindre le serveur.

Si on ne peut pas découvrir ainsi son adresse (ou si le serveur est purement et simplement coupé de la matrice), il faudra établir une connexion directe, c'est-à-dire infiltrer physiquement un site de la corpo (à supposer qu'on sache quel site runner) pour se retrouver à proximité d'un appareil asservit au serveur R&D (tel qu'un équipement de laboratoire par exemple) ou se connecter avec un câble à un terminal de télétravail n'acceptant pas de connexion sans-fil (dans le cas de site vraiment sécurisé).

Le serveur en lui-même est probablement un serveur Rouge-16 si les données qui se trouvent dessus sont vraiment sensibles. Considérant l'importance des informations, peut-être qu'un hacker de sécurité surveille ce serveur. Dans ce cas, celui-ci pourra utiliser Logique + Électronique éventuellement modifiée par les circonstances (si par exemple des fichiers sont massivement supprimés, des archives remontées en dehors des heures de bureau, si un fichier piège est téléchargé au milieu d'autres données, etc.) si cette réserve dépasse l'indice du serveur.

Dans le cas où une alerte passive serait déclenchée, une CI sonde-16 sera activée. Celle-ci (ainsi que le spider) effectuera des tests de perception matricielle à chaque tour durant de longues minutes avant que l'alerte soit levée. Et si une alerte active est déclenchée, des CI Kamikaze-16, Trace-16 et Noire-16 seront certainement activées. Elles agiront contre l'intrus dès que celui-ci sera détecté par la CI Sonde ou par le hacker de sécurité (qui pourra à son tour utiliser ses programmes contre l'intrus ou tenter de protéger le serveur une fois le hacker détecté).

Pirater un service de streaming

Un service de streaming est un serveur public (un nombre important de clients s'y connectent directement ou via des applications pour profiter du service). Son adresse matricielle est donc connue (ou du moins accessible) et le serveur peut être piraté à distance à tout moment.

Le nombre de connexions et son caractère public limitent l'efficacité du firewall et des autres sécurités pouvant être installées sur ce type de serveur. Par ailleurs, il est toujours possible de rapidement mettre en ligne une copie du serveur pour assurer une continuité de service même en cas d'attaque. Sa sécurité n'est donc au mieux qu'un Vert-8, même s'il s'agit d'un service de streaming appartenant à une grosse filiale d'une mégacorp.

En cas d'alerte passive, une CI Sonde-8 sera activée. En cas d'alerte active, c'est généralement une CI Trace-8 qui est lancée (afin d'envoyer la police locale chez le hacker), éventuellement secondée par une CI Pot de colle-8 en remplacement de la CI Sonde lorsque celle-ci a détecté le hacker. Un hacker de sécurité peut également être appelé en cas d'alerte active.

Pirater ce type de service offre la possibilité de profiter gratuitement du service, rendre un contenu inaccessible (voir le supprimer du catalogue), ajouter un contenu au catalogue, forcer les utilisateurs à consulter un contenu donné, envoyer une mailing list aux clients, consulter l'historique de connexion d'un client particulier, etc. Si une altération du service est particulièrement visible (ou si une alerte active est déclenchée), celle-ci sera rapidement rectifiée. Une altération plus subtile durera plus longtemps (dépendant du sérieux et des compétences du fournisseur de service). Toutes ces actions sont des actions de type "contrôler un système".

Architecture matricielle d'une enclave corpo

La plupart des enclaves et bureaux corporatistes (même AAA) ne possèdent pas de service de sécurité propre et font appel à des sociétés de sécurité privée. Bien sûr, il est tout à fait possible que cette société appartienne à la même megacorp au final (les filiales d'Ares sont, sans surprise, sécurisées par Knight Errant), mais cette distinction signifie que les serveurs de sécurité (et toutes les alarmes, drones et caméras associés) se trouvent sur des serveurs distincts des serveurs de travail de l'enclave (ce qui n'est pas forcément le cas du bar à runner du coin qui assure sa propre sécurité et gère sa comptabilité sur un même serveur). Généralement le serveur de sécurité d'une enclave corporatiste sera un code Orange-12 (plus s'il s'agit d'une enclave vraiment sensible).

Il en va souvent de même pour le réseau domotique de l'enclave. Il peut en effet s'agir d'étages, d'immeubles ou d'un complexe entier possédé par un tiers (là encore peu importe que ce tiers ait les mêmes actionnaires) et loué à la corpo. Il

se peut aussi qu'un contrat d'entretien ait été signé avec une autre société et même si ce n'est pas le cas, la domotique (donc la gestion de la température de l'immeuble, des drones ménagers, l'affichage des plans d'évacuation RA, les alarmes incendie, les ascenseurs, etc.) est gérée par un serveur distinct auquel les employés n'ont généralement pas accès (ou n'ont qu'un accès limité à quelques paramètres concernant leur bureau ou la machine à café de l'étage). La sécurité matricielle du serveur domotique d'une enclave sera généralement un code Orange-12.

Suivant la taille de l'enclave, il est possible que les serveurs de travail et administratifs soient distincts. Peut-être même que le serveur administratif n'est pas propre à l'enclave, mais concerne plusieurs sites en ville ou dans le pays (le pirater donne alors accès aux informations de chacun de ces sites). Les données du personnel hébergées dans le serveur administratif étant plutôt sensibles, il s'agira là encore d'un code Orange-12, quant au serveur de travail, si les données sont basiques, il peut s'agir d'un simple code Vert-8, mais si des données relatives au secret des affaires se trouvent dessus, alors on peut à nouveau compter sur un code Orange-12.

Tous ces serveurs sont interconnectés : la sécurité a des droits sur les commandes des ascenseurs du serveur domotique, les drones de maintenance ont des autorisations sur le serveur de sécurité pour accéder à certaines parties de l'enclave, le serveur de travail doit vérifier sur le serveur administratif que l'employé travaille toujours dans le service, etc.

Le PAN d'un employé sera également interconnecté avec l'ensemble des serveurs de l'enclave : le serveur de sécurité lui donnera l'accès à certaines zones de l'enclave, le serveur domotique lui permettra de gérer la lumière et la température de son bureau ainsi que la possibilité d'ouvrir un ticket pour signaler une zone à nettoyer. Il aura aussi accès à ses fiches de paye et à son compte employé sur le serveur administratif et bien sûr à son espace de travail virtuel dans le serveur de travail.

De façon stricte, chacun de ces serveurs et réseaux est distinct : en pirater un ne permet d'agir que sur celui-ci. Leur interconnexion permet cependant de trouver simplement l'adresse des autres serveurs qui peuvent ensuite être piratés à leur tour. Par simplicité et pour limiter les jets de dés, vous pouvez cependant définir un unique code de sécurité matriciel (le plus élevé) et estimer que l'interconnexion des serveurs permet au hacker d'agir sur l'ensemble des systèmes informatiques de l'enclave une fois dans l'un de ces serveurs.

Serveur du stuffer shack au coin de la rue

Comme pour l'enclave, le réseau de sécurité, le système domotique et le serveur de service et logistique (gérant les prix, le stock, les commandes, le scan des produits à facturer, la liste des promotions, les publicités diffusées dans le magasin, etc.) peuvent être aussi bien séparés que réuni dans un unique serveur. Considérant la faible criticité (le montant des fraudes reste assez anecdotique et le coût de la sécurité ne doit pas trop rogner sur les marges), il s'agit probablement d'un code Vert-8. Il est cependant possible, suivant l'enseigne, que les CI chargées en cas d'alerte active incluent des CI Blaster, voir Psychotrope.

À noter que les serveurs d'un magasin donné seront interconnectés avec les serveurs régionaux de l'enseigne (permettant notamment de gérer la logistique à une échelle plus grande). Il s'agit alors d'un serveur distinct certainement un peu plus stratégique et donc protégé par un code Orange-12.

Pirater le PAN d'un cadre corpo

Le commlink d'un cadre corpo est sécurisé, mais ça reste un commlink. Son code sera donc vraisemblablement du Vert-8. Cela dit, à part quelques fichiers d'ordre personnel, les commlinks contiennent assez peu d'informations (mais toujours utile pour dénicher de quoi mieux connaître une cible ou pour en apprendre plus sur son emploi du temps). Les travaux et autres ressources sensibles sont vraisemblablement plutôt hébergés vers des serveurs corpo probablement mieux sécurisés (mais dont l'adresse matricielle est révélée par le piratage du commlink).

À noter que l'emploi du temps professionnel du cadre (ainsi que d'autres outils) peut être hébergé sur le serveur de sa corpo, alors que le commlink possède des droits dessus. Dans ce cas, il est possible de lire et d'utiliser l'emploi du temps (pour modifier ou ajouter un rendez-vous par exemple) depuis le commlink comme le ferait l'utilisateur légitime. Cela reste du piratage et requiert donc un test de type "contrôler un système", mais c'est faisable. En revanche, aller au-delà des autorisations de l'utilisateur (en supprimant l'agenda sur le serveur corpo ou en en essayant de consulter l'agenda d'un autre employé par exemple) nécessitera plutôt un accès sur le serveur hébergeant l'agenda.

Hacker un PAN en passant de serveur en serveur

L'adresse matricielle d'un commlink est rarement publique (sauf victime d'un hacker qui l'aurait trouvé puis posté sur un forum) et peut changer sur demande après un reboot. Le plus simple pour hacker un PAN est donc généralement d'établir une connexion directe. Alors que faire lorsqu'on ne se trouve pas à proximité de sa cible, ou lorsqu'on cherche justement à la localiser ?

Avec de bonnes compétences, il est possible de pirater le fournisseur d'accès matriciel de l'utilisateur, mais il s'agira probablement d'un code Orange-12 et encore faut-il connaître le FAM de sa cible.

Si vous disposez de l'adresse de son logement en revanche, il est possible de remonter sa piste en piratant une série de serveurs normalement moins sécurisés : rendez-vous en face de l'immeuble où habite la cible et établissez une connexion directe avec le réseau domotique de l'immeuble (ou recherchez le site matriciel corporate du syndic, piratez-le et accédez aux réseaux domotiques de l'immeuble, si vous préférez ne pas vous déplacer) qui devrait être un code Vert-8. De là, il sera facile de trouver la liste des appartements et leur sous-réseau dédié (sinon vous pouvez toujours "imiter un ordre" ou deux pour ouvrir un maglock ici et détourner une caméra là-bas afin de finir par vous trouver à portée de signal du réseau de l'appartement). Le réseau de l'appartement étant peu exposé (puisqu'il faut avoir accès à l'immeuble ou à son réseau), il ne s'agit probablement que d'un code Bleu-4. Et puisque le commlink de la cible possède très certainement une connexion permanente avec son réseau domotique (sinon envoyez une alerte quelconque pour forcer l'utilisateur à se connecter voir ce qui se passe), il sera possible de récupérer l'adresse matricielle du commlink-cible… que vous pourrez à son tour pirater.

Il est donc possible de remonter une piste en hackant différents serveurs sur la route… Ce qui peut générer un certain nombre de jets de dés pas vraiment intéressant, d'autant que le hacker ne fera probablement que passer et se déconnectera de chaque serveur après avoir récupéré l'adresse de sa prochaine cible. Dans ce cas, même s'il venait à déclencher des alertes, celles-ci ne devraient pas avoir beaucoup d'incidence. Vous pouvez donc ne demander qu'un seul test d'intrusion correspondant au code de sécurité le plus élevé rencontré sur le chemin emprunté (les tests suivants correspondront au code de sécurité du serveur/réseau dans lequel le hacker compte réellement agir).

À la discrétion du MJ, si la piste est longue, vous pouvez également jeter un dé de complication par serveur traversé (en incluant le serveur-cible), si le PJ obtient deux 1, c'est qu'il a déclenché l'équivalent d'une alerte passive sur la GTL à laquelle il se trouve connecté : le GOD ou le gestionnaire de la grille a détecté une activité anormale. Une CI Sonde-16 est activée. Si le PJ à eu au moins trois 1 ou si la CI Sonde finie par détecter le hacker, la GTL passe en alerte active : une CI Trace-16 est activé et des deckers du GOD sont mis sur le coup.

Hacker le PAN ou le cyber d'un runner

Lorsque l'on souhaite contrôler ou donner un ordre à l'équipement d'un runner (tel que dérégler un smartlink pour qu'il impose un malus au lieu d'un bonus, éjecter le chargeur d'une arme connecté ou désactiver la vision nocturne de cyberyeux), il faut comme toujours être en mesure de se connecter à sa cible, ce qui signifie la plupart du temps être à proximité de celle-ci.

L'équipement du runner est la plupart du temps asservi à un commlink (code Vert-8), pouvant lui-même être asservi et surveillé par le hacker du groupe (code Vert-8 également, mais bénéficiant de bonus de firewall et de relance d'échec dans le cas d'un cyberdeck – et la réserve de détection du réseau peut être égale à la Logique + Électronique du hacker si celui-ci surveille le réseau de PAN).

Notez qu'un personnage peut comprendre qu'il a été piraté même sans alerte : l'éjection d'un chargeur sans qu'il en ait donné l'ordre ou toute autre activité "visible" peut faire douter le personnage, qui peut ensuite légitimement choisir de rebooter son commlink, alerter son decker ou tenter de détecter l'intrusion lui-même via un test actif de perception matricielle (d'où parfois l'intérêt de solution plus subtile comme de légèrement dérégler la mire d'un smartlink).

Concernant les possibilités offertes, il faut garder en tête que l'action "imiter un ordre" ne permet d'imposer que des actions pouvant être normalement effectuées par l'utilisateur (exemple : désactiver sa vision nocturne). Reprogrammer les fonctions d'origine d'un appareil pour lui faire faire quelque chose qui n'est normalement pas prévu dans sa programmation de base (exemple : afficher une image psychédélique dans les cyberyeux de sa cible ou rediriger le flux vidéo des yeux vers un commlink sans afficher de notification) n'est possible qu'en ayant préalablement piraté le PAN de l'utilisateur.

Il est aussi raisonnable de penser qu'un certain nombre d'équipements, à commencer par le cyberware, sont utilisés en mode offline (les mises à jour et la maintenance en ligne ne sont effectuées qu'à des moments choisis, hors opération). Dans de nombreux cas, cela ne changera rien à l'utilisation qui peut être faite de l'équipement (bras, griffes, etc.), mais il arrive que certains équipements doivent être adaptés à une utilisation offline (comme le smartlink, qui nécessite alors l'utilisation d'un câble reliant l'arme à un datajack ou à des électrodes) et d'autres n'ont pas le choix et doivent être connecté pour fonctionner (dès lors qu'on souhaite afficher des informations RA sur des cyberyeux, ceux-ci utilisent de fait le sans-fil, même si c'est en étant (inutilement) câblé à un commlink, puisque lui est connecté en sans-fil).

Notez cependant que les équipements et cyber ne sont, par design, pas censés pouvoir être coupés de la matrice. Une équipe de runner sans compétences techniques, des gangers ou des agents de sécurité basiques auront tout leur matériel connecté (il sera ainsi possible donner l'ordre à un bras cyber de viser et tirer sur un allié… le porteur, étant "en plongée" dans son bras, a tout de même avoir droit à un test de Logique + Volonté pour résister/réagir à l'ordre, avec un bonus à son jet, car celui-ci est complexe et particulièrement préjudiciable).

Organisation matricielle des gardes corpo

Les équipements et PAN des gardes d'un complexe sont généralement tous reliés au serveur de sécurité. Les sites sensibles seront par ailleurs surveillés en permanence par un spider, tandis que des sites moins sensibles ne seront pas surveillés en permanence (un spider pouvant n'intervenir qu'en cas d'alerte ou surveiller plusieurs serveurs et n'être donc présent que par intermittence.

Les unités d'intervention possèdent quant à elles un réseau (furtif dans le cas d'opérations clandestines) reliant tous leurs membres à un poste de commandement (un serveur de sécurité qui peut être soit hébergé dans un centre de commandement mobile (pour les opérations clandestines nécessitant de grands moyens ou en cas de risque de brouillage), soit dans la matrice). Parfois, ces unités opèrent sans poste de commandement à la façon d'un groupe de runners. Ce type d'unité est normalement toujours accompagnée d'un hacker surveillant le réseau de l'unité.