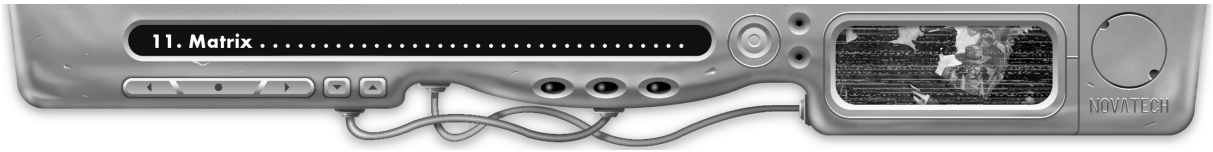


MATRIX

Matrix je rozškatulkovaný systém složený z počítačů zvaných hosty, které jsou vzájemně spojeny souřadnicemi – celosvětovou telekomunikační sítí. Skrze matrix se člověk může dostat prakticky ke všem počítačovým systémům tohoto světa – pokud má správné heslo nebo systém hackne. Uživatel se teoreticky může dostat během několika vteřin k jinému hostu na druhé straně planety. Tento aspekt celosvětové sítě, tj. permanentní aktualizaci dat, vyžadují jak zákony podnikového prostředí, tak absolutní nutnost ve světě, v němž může během pár sekund dojít k nejzávažnějším změnám.

Lidská mysl nemá k proudu dat v matrixu bezprostřední přístup. Kdyby byl uživatel i nadále odkázán na pomoc zastaralé techniky – na příkazové řádky, názvy souborů, programy v programovacích jazycích – nedalo by se s tímto systémem pracovat. Příklad: Pokud chtěl uživatel v roce 1998 pracovat s počítačovým souborem, musel pracně vyťukat příkaz, zpřístupnit si soubor v okně nebo potřebnou informaci hledat jiným, stejně pomalým způsobem. Po krachu v roce 2029 nabídla ovšem technologie ASIST možnost přímého nervového rozhraní (PNR), jež umožnilo přístup k počítačům, a matrix byl na světě. Celý matrix – fyzické komponenty, programy, dokonce i akce jako kopírování souboru – se graficky znázorňuje pomocí *ikon*. Dnes podniká uživatel za nalezením souboru cestu trvající pouze několik mikrosekund počítačově vygenerovanou krajinou. Pokud je oprávněn ke čtení souboru, nalezne ho přesně tam, kde ho očekával. Standardní programy rozhraní, s nimiž pracuje, přitom vypadají pokud možno jako kancelářští zaměstnanci nebo jako obrovské knihovny, možná ale také jako spletené vzory z čisté energie. Uživatel soubor uvidí, dotkne se ho, a to už se data ukládají do jeho kyberterminálu.

Uživatel si už nemusí pamatovat hesla, posloupnost příkazů nebo názvy souborů. Pokud něco chce, jde prostě na věc. Chce-li naprogramovat pracovní proces laboratoře nebo montážního pásu, vytvoří v myšlenkách patřičné schéma nebo pomocí virtuálních komponentů sestaví model. Všechno ostatní už pak zařídí počítač. Například moderní chemici sestavují podle svých vzorců molekuly, jako když si děti hrají se stavebnicí. Počítač pak převede tyto činnosti do programu, který zrealizuje proces ve skutečném světě.

Shadowrunneři, kteří se z jistých vlastních důvodů zdržují v nějakém počítačovém systému, mohou samozřejmě využít tyto technické inovace k vlastnímu prospěchu. Stejná matrixová výbava, jež námezdnímu otroku ulehčuje práci, dává deckerovi moc. Tito nelegální uživatelé se mohou vplížit do počítačového systému a tutéž jednoduchou symboliku použít pro vlastní účely.

MATRIXOVÝ ŽARGON

Technologie systému umělého smyslového vnímání (Artifical Sensory Induction System Technology, ASIST) – hardware a programy, které uživateli umožňují vnímat podstatu matrixu, příp. zprostředkovávají smyslové vjemy někoho jiného (simsens).

Kyberdeck – mikropočítač, který používají deckeři pro ilegální přístup k matrixu; používají ho i bezpečnostní deckeři.

Kyberterminál – počítač používaný pro bezpečný legální přístup k matrixu, daleko pomalejší než kyberdeck.

Decker – hacker; ilegální uživatel matrixu.

Přímé nervové rozhraní (PNR) – technika, s jejíž pomocí vzniká rozhraní mezi nervovými impulsy deckera a počítačovým systémem. Umožňuje uživateli přímé řízení a ovládání počítačového systému prostřednictvím jeho mozku.

Souřadnice – řada propojených počítačových systémů (hostů).

Host – samostatný počítačový systém.

Ikona – objekt, který vidí uživatel v matrixu.

IC (Intrusion Countermeasure, **led)** – druh softwaru, který se instaluje do počítačového systému (hostu), aby ho chránil před neautorizovaným přístupem.

Přípojka – fyzický komponent spojení, který umožňuje přístup k matrixu.

Uzel – část hostu, například subsystém, který je zpravidla představován virtuální krajinou.

Lokální telekomunikační souřadnice (LTS) – souřadnice, které pokrývají určitou oblast (obytné bloky, města). Jistý počet LTS je vždy spojen s jedněmi určitými RTS.

Matrix – celosvětová počítačová telekomunikační síť.

Modelované systémy – hosty, jejichž obzvláště detailní virtuální realita neodpovídá standardní symbolice matrixu; toto znázornění má zvláštní důvody.

HPOP – hlavní program ovládání persony; srdce kyberdecku.

Persona – ikona deckera.
Programy persony – takříkajíc „atributy“ kyberdecku (odolnost, únik, maskování, senzory).
Soukromé lokální telekomunikační souřadnice (SLTS) – jakékoli telekomunikační souřadnice, k nimž nemá veřejnost přístup.
Šnek – slangový výraz pro kyberterminál.
Bezpečnostní decker – decker, který pracuje pro podnik nebo pro vládu a chrání určité oblasti matrixu před deckery.
Simsens – hardware a programy, s jejichž pomocí může člověk zažívat realitu někoho jiného (z nahraných vzpomínek nebo na živo).
Subsystém – jeden z pěti funkčních aspektů všech souřadnic nebo hostů (přístup, ovládání apod.).
Systémový přístupový uzel (SPU) – ikonografické spojení mezi počítačovými systémy nebo souřadnicemi a jiným počítačovými systémy nebo souřadnicemi.
Univerzální matrixový symbolismus (UMS) – grafický standard pro znázorňování ikon v matrixu, který pomalu, ale jistě vychází z módy.
Přístup/ovládání/index/soubor/periférie – formát, v němž se udávají systémové stupně hostu.

Přístup k matrixu

Jako kybernetického rozhraní k matrixu se užívá buď kyberdecku, nebo kyberterminálu. Oba přístroje jsou vybaveny kabelem ze skelných vláken se standardní datovou zástrčkou, kterou lze najít i na každém telekomu pro každodenní použití. Se správným nářadím může decker napíchnout každé existující komunikační spojení (viz **Přípojky**). Spojení mezi deckem a uživatelem je tvořeno buď sítí elektrod, jež se nasazuje na hlavu (metoda zbabělců), nebo přímým nervovým rozhraním přes datajack (jedině tak je možné létat). Někteří deckeři sahají i nadále po klávesnicové podpoře, ale mnozí dávají přednost čistě kybernetickému rozhraní.
Jakmile je deck aktivován, potlačí většinu tělesných smyslových vjemů a nahradí je elektronickou simulací matrixu. Tyto simsensové signály převádějí komplexní strukturu kódování vlastního matrixu do grafické podoby. Po chvilce dezorientace se decker (či spíše jeho konstrukt) ocitne v matrixu na místě, kde je jeho deck připojen k souřadnicím. Jedná-li se při tom například o ilegální připojení v zadním pokoji Matchstickova baru & grilu, vynoří se decker v telekomunikačním vedení tohoto obchodu.
Legální uživatelé používají registrované kyberdecky, které při každé činnosti v matrixu zanechávají datovou stopu (určitý druh otisků prstů uživatele). Kyberdecky deckerů ovšem žádné stopy nezanechávají. Deckeři zůstávají v anonymitě a když se vše dobře daří, mohou protančit mezi tajemstvími matrixu a přitom se vysmívat bezpečnostním opatřením. Pokud samozřejmě něco selže, mohou stejně tak dobře v matrixu zemřít.

Přípojky

Přípojky sestávají z fyzických komponentů spojení, pomocí nichž si decker zjedná přístup k matrixu. Existují dva druhy přípojek: legální a nelegální. Legální přípojka umožňuje deckerovi přístup přes legálně registrovaný trideofon. Přitom se samozřejmě nemusí jednat o tvůj telekom, *čéče*!
Přípojka s nelegálním přístupem představuje buď přístup přes ilegální trideofon (nějaká duše bez skrupulí se vetřela do služeb telekomunikační společnosti) nebo přes nějaké jiné místo, kde je možné přímo napíchnout síť z kabelů ze skelných vláken. Deckeři většinou užívají přípojky s nelegálním přístupem.
Nakonec existují ještě různé přípojky, které jsou buď legální, nebo nelegální – to podle toho, jak k nim decker získal přístup. Příkladem mohou být pracovní stanice (kyberterminály, které jsou spojeny přímo s hostem), periferní přístroje (například bezpečnostní terminál nebo nápojový automat) nebo konzole (vlastní řídící panely hlavního počítače).
Přípojka přes telekom spojí deckera přímo s LTS. Pracovní stanice, konzole nebo periferní přístroje spojí deckera přímo s hostem. Podle toho, s jakým systémem je daný optický kabel spojen, může přípojka, k níž si pomocí nelegálního napíchnutí zjednal přístup, spojit deckera buď s hostem, nebo s LTS.

Ikony

Každý objekt, který uživatel matrixu vnímá, je ikonou. Uživatelé jsou rovněž reprezentováni ikonami, které se nazývají *persony*. Pokud mluvíme o personě deckera, mohli bychom stejně dobře mluvit o jeho ikoně nebo on-line ikoně.
Ať už se deckerovi zdá zkušenost z matrixu jakkoli reálná, ve skutečnosti do něj nevstupuje nikdy fyzicky. Jeho tělo z masa a kostí sedí tam, kde je kyberdeck připojen k matrixu, tedy u takzvané přípojky. Deck krmí deckera

signálem ASIST; to se děje stejným způsobem, jako když simsensový přístroj dovoluje uživateli věřit, že se nachází někde jinde. Tohle jinde je v tomto případě matrix.
Programy persony a užitkové programy, které běží v kyberdecku, jsou hlavní kopie softwaru, které umožňují deckování. Když se decker přihlásí do souřadnic nebo do hostu, vyloží kyberdeck verze těchto programů do matrixu. Krátce řečeno: decker má co do činění se dvěma druhy programů – takzvanými předřazenými programy, které běží v kyberdecku a převádějí deckerovy nervové impulsy na počítačové příkazy, a obslužnými programy v matrixu, jež tyto příkazy konvertují na programové příkazy, které mají vliv na funkce systému.
Tento proces vytváří dva komplexy; deckera z masa a kostí a jeho předřazené programy v decku na straně jedné a on-line ikonu deckera, která běží v počítačích, z nichž je tvořen matrix, na straně druhé. Pokud dojde k odpojení decku, přeruší se komunikační spojení, které oba celky spojuje, nebo se persona zhroutí, potom je decker off-line, odpojen, vyhozen.

Vnímání matrixu

Jak vypadá matrix? Největší část je znatelně vygenerovaná a znázorněná počítačově, ať už jsou detaily jakkoli působivé nebo realistické. Matrix je a zůstává stvořen počítačem. Jistě, některé úseky matrixu jsou doslova a do písmene nerozeznatelné od reálného světa, ovšem tyto oblasti jsou velmi nebezpečnými místy.
Vše v matrixu má symbolický význam. Při pohledu zvenku vypadají počítačové systémy často jako budovy, hory nebo jiné vysoké struktury. Vnitřek systému může vypadat v závislosti na jeho funkci velmi rozdílně. Většina počítačových systémů roku 2060 jsou speciálně navržené „modelované systémy“, které používají náročná a detailní znázornění, jež představují funkce systému. Ústřední znázornění modelovaného systému definuje jeho virtuální realitu. Například pagoda Mitsuhamy sestává z virtuálních vesnic, v nichž se na kybernetických rýžových polích středověkého Japonska dřou do úmoru aplikace. Nejdůležitější data jsou ukryta v hradech, které chrání IC v podobě samurajů. Pokud se decker nachází v modelovaném systému, jsou všechny jeho činnosti a vjemy znázorňovány v obrazech, jež odpovídají ústřednímu znázornění systému.
Data mají rovněž svou vlastní podobu, stejně jako systémy, v nichž jsou uložena a chráněna. Určitá zásobárna dat může například vypadat jako vznášející se krychle nacpaná změtí dat, kterou obtáčí obrovský had (symbolické znázornění IC typu Vír), čekající na neopatrné vetřelce. Totéž platí i pro ostatní druhy programů. Přihlášení se do hostu může být například symbolizováno vstupem do dveří – nebo velkou neonovou trubicí, která do sebe deckera nasaje.
Také programy užívané deckery vykazují taková znázornění. Podoba útočného programu může představovat cokoli, čím lze provést útok, od nože po raketomet. Štítový program se může jevit jako klasický bitevní štít nebo jako silové pole, jež deckera v případě potřeby chrání.
A jak vypadá samotný decker? Tak, jak si sám přeje. Jako člověk v rytířském nebo technizovaném brnění, jako bytost z čirého světla, jako žhnoucí bílá koule, jako démon z jakéhosi koutu pekla – to není podstatné. V matrixu mohou všechny věci vypadat libovolně.
To možná zní pozoruhodně, ale nemělo by se zapomínat, že obrazy, které decker vidí (zvuky, které slyší apod.) jsou vytvářeny samotným kyberdeckem, a sice na základě informací, jež dostane od počítačového systému, s nímž si právě informace vyměňuje. Výše popsaný počítačový systém Mitsuhamy sdělí například kyberdecku, že vypadá jako pagoda. Program Vír vysílá krátký kód, který říká, že vypadá jako velký had. Útočný program sděluje, že vypadá jako velká pistole. A kyberdeck sám oznámí každému, kdo se na to bude ptát, že decker vypadá tak, jak se sám naprogramoval.
Mnohé programy a jejich ikony mohou být před deckerem skryté. Ikona je „zde“, ale decker ji nemůže vidět, protože není aktivní nebo senzorické programy decku nejsou dost dobré, aby ji odhalily. Programy IC jsou například často ukryté nebo vypadají jako neškodné ikony, dokud je decker nespustí. Deckeři mohou tuto hru na schovávanou využít ve svůj prospěch, pokud svou personu zneviditelní maskovacími programy nebo ji budou vydávat za autorizované programy příp. systémové funkce.

Souřadnice a hosty

Matrix sestává z komunikačních sítí (souřadnic) a počítačových systémů (hostů). Souřadnice přenášejí hlasové a datové informace – vše od místního telefonního hovoru přes balíky dat o velikosti několika gigapulsů. Hosty jsou tím, co se dříve nazývalo základní počítačovou jednotkou, ovšem základní jednotky nejsou už v Šestém světě samostatné, silné hardwarové jednotky. Daleko více se u mnoha hostů jedná o zesíťované paralelní procesory v menších sestavách. Poskytují stejný výkon jako jeden jediný superpočítač. Jednoduše řečeno: v *Shadowrunu* je hostem každý počítač, který je sdostatek důležitý, aby do něho deckeři pronikli, a dostatečně odolný, aby se tomu mohl bránit.

V matrixu jsou souřadnice obrovské trojrozměrné prostory, malé světy, v nichž září jako hvězdy ikony četných hostů, datových přenosů, deckerů a ještě mnohem více.

Regionální telekomunikační souřadnice (RTS)

Stupně systému severoamerických RTS jsou shrnuty v tabulce **Stupně systémů RTS: severní Amerika**.
Pokud budete určovat stupně systému pro veřejné souřadnice, jež zde nejsou uvedeny, vycházejte z toho, že jejich vstupní třída je jednoduchá a odečtěte od všech stupňů 2 (pro pásmový rozsah 6 až 8).

STUPNĚ SYSTÉMŮ RTS: SEVERNÍ AMERIKA						
RTS	**Bezpečnost**	**Přístup**	**Ovládání**	**Index**	**Soubor**	**Periférie**
Aztlan	Oranžová-3	8	8	6	7	7
Karibská liga						
Bermudy	Zelená-2	6	6	6	6	6
Kuba	Oranžová-3	8	8	7	8	7
Grenada	Oranžová-4	6	8	8	8	8
Jamajka	Zelená-3	6	7	6	6	6
Jižní Florida	Zelená-2	6	7	6	6	6
Panenské ostrovy	Zelená-2	6	7	6	6	6
KAS	Zelená-3	6	8	7	8	8
SDA						
Algonkinsko-manitouská rada	Zelená-4	7	8	7	6	6
Athabaská rada	Zelená -3	6	8	6	6	6
Korporační rada Pueblo	Oranžová-4	8	8	8	8	8
Seliš-šihíská rada	Zelená-3	6	8	7	6	6
Sioux	Oranžová-3	7	8	8	7	7
Transpolárně-aleutská rada	Zelená-2	6	6	6	6	6
Ute	Oranžová-3	7	8	7	7	7
Svobodný stát Kalifornie	Zelená-4	6	8	6	6	7
Québec	Zelená-2	6	8	8	7	7
Tir Tairngire	Oranžová-5	7	8	8	7	7
Cimšjan	Oranžová-5	8	8	8	8	8
SKAS	Zelená-4	6	8	6	6	6

Lokální telekomunikační souřadnice (LTS)

Pokud se decker na začátku runu přihlásí do matrixu, vyloží deck jeho ikonu nejprve do nějakých LTS. Stupně LTS odpovídají, přinejmenším v severní Americe, stupňům systému mateřských RTS.

Soukromé lokální telekomunikační souřadnice (SLTS)

Soukromé LTS (SLTS) jsou nezávislé uzavřené souřadnice, které jsou veřejnosti nepřístupné. Většina velkých podniků a všechny megakoncerny provozují přinejmenším jedny SLTS. Většina rozvinutých zemí má několik státních SLTS, které mohou sahat až k vojenským nebo diplomatickým zařízením za jejich hranicemi. STLS probíhají přes kabely z optických vláken, které patří buď uživateli, nebo jsou pronajaté od místní telefonní společnosti.
SLTS podléhají zákonům podniku nebo státu, jemuž patří. Z tohoto důvodu mohou vlastníci SLTS nainstalovat jakékoli ochranné zařízení, které chtějí. A protože vybudování SLTS představuje významnou investici, nešetří většina vlastníků na IC.
Pokud chce gamemaster přiřadit stupně systémů SLTS, jež sám navrhl, měl by použít oranžovou až červenou úroveň bezpečnosti a jednoduchou vstupní třídu (viz **Vstupní třídy**).

Určení a vstupní body

Podnikové SLTS obepínají celou zeměkouli. Jedny LTS mohou například spojovat podnikové hosty na celém světě. SLTS disponují pokud možno více vstupními body, jež je spojují s různými veřejnými souřadnicemi. Decker si zjedná přístup k SLTS tak, že buď použije jeden z těchto vstupních bodů, nebo pronikne do některého hostu, který je připojen na tyto STLS.

Obecně řečeno je určení STLS motivováno politicky a neexistují jednotná pravidla. Tak si megapodniky v zemích, jež jim efektivně náleží, ponechávají právo provozovat své vlastní SLTS, zatímco jiným totéž právo upírají. Podobným způsobem dovoluje Japonsko přístup k SLTS těm podnikům, jež jsou v japonském vlastnictví, zatímco zahraničním firmám se tohoto práva nedostává. A překvapí snad někoho, že SLTS Aztechnology jsou jediné SLTS, které jsou provozovány v Aztlanu?

Hosty

Hosty slouží v Šestém světě jako srdce informační společnosti. Těmito systémy proudí denně miliardy nujenů a nepočítaně megapulsů dat. Hosty představují pokladnice, do nichž jsou tyto poklady ukládány. Hosty slouží jako databanky, knihovny, virtuální obchodní domy, chatovací místnosti, virtuální herní haly, místa soukromých schůzek, poštovní schránky, místní sítě, archivy, banky apod.

Off-line hosty

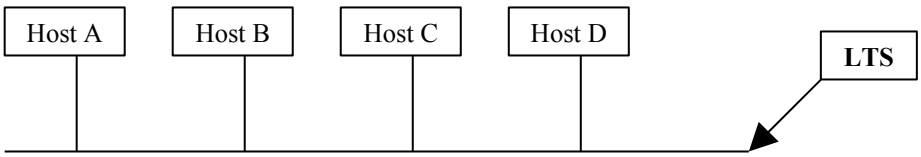
Ne všechny hosty jsou připojeny k matrixu. Mnohé ultrabezpečné hosty, střežené s přímo paranoidní starostlivostí, nejsou na základě nebezpečí vycházejícího z neoprávněných deckerů úmyslně napojeny na matrix. Jediná možnost, jak si decker může k takovému hostu zjednat přístup, je přímo na fyzickém stanovišti hostu. Aby se například decker dostal k nejcitlivějším datům o výzkumu Saeder-Krupp, musel by fyzicky proniknout do výzkumného zařízení a nalézt přípojku, s jejíž pomocí by se dostal přímo k cenným datům.

Matrixová topologie

Spojení mezi souřadnicemi a hosty definují základní topologii matrixu. Jsou známé pouze čtyři druhy těchto spojení: otevřený přístup, úrovňový přístup, sériový přístup a přístup přes soukromé souřadnice. Pokud se ovšem tato spojení vynásobí miliony hostů, které jsou křížem krážem roztroušeny v souřadnicích, dostaneme síť o takové komplexitě, že se do ní může zamilovat pouze decker.

Otevřený přístup

Většina počítačových systémů používá otevřený přístup. Jednoduše řečeno, otevřený přístup má každý host, který je přímo napojen na souřadnice. Všichni uživatelné na celém světě mohou užívat veřejné souřadnice, aby si zjednali přístup k takovému hostu. Všechny čtyři hosty na připojeném diagramu jsou připojeny k týmž LTS. Decker může získat přístup ke každému z nich, pokud pronikne do LTS. Pokud už je v jednom z těchto hostů přihlášen, může se od něj odpoutat a vstoupit do jiného hostu z této skupiny, aniž by musel matrixový run ukončit.

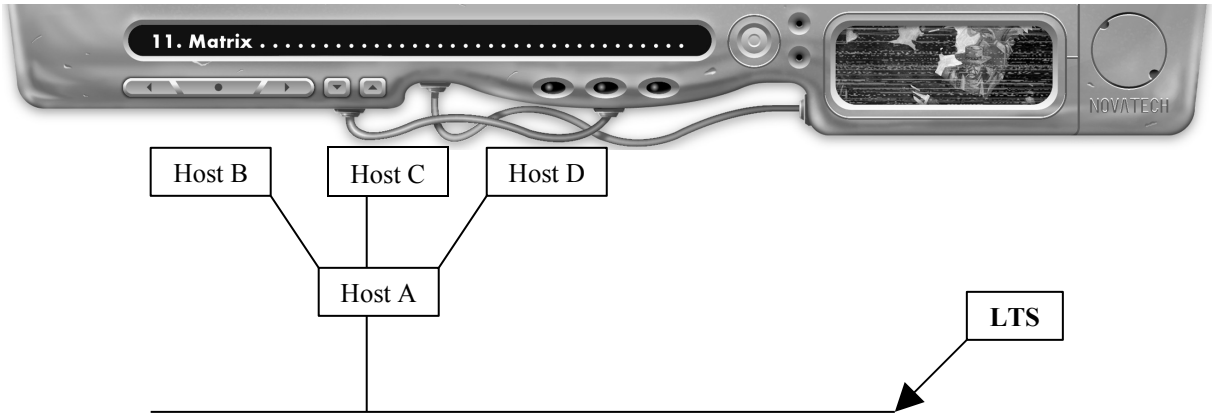


Úrovňový přístup

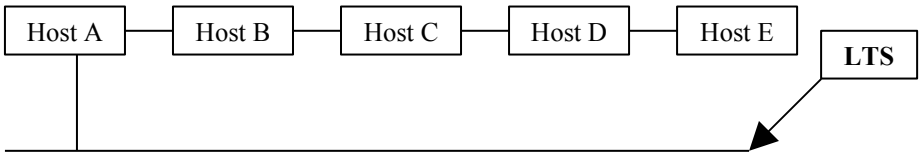
V diagramu pro úrovňový přístup je se souřadnicemi přímo spojen pouze host A. Hosty B, C a D jsou naproti tomu spojeny pouze s hostem A. V tomto uspořádání funguje host A jako systém prvního sledu, zatímco hosty B, C a D pracují jako systémy druhého sledu. Každý uživatel, který se chce dostat do hostu B, C nebo D, musí nejdříve projít hostem A. Aby se decker propracoval z hostu B k hostu C nebo D, musí nejprve znovu do hostu A.

Systémy prvního sledu mohou být nakonfigurovány jako výhybkáři, kteří oprávněné uživatele přesměrují do systémů druhého sledu. Systémy prvního sledu ovšem mohou umožnit uživatelům i přístup k SLTS, které zase poskytují přístup k systémům druhého sledu.

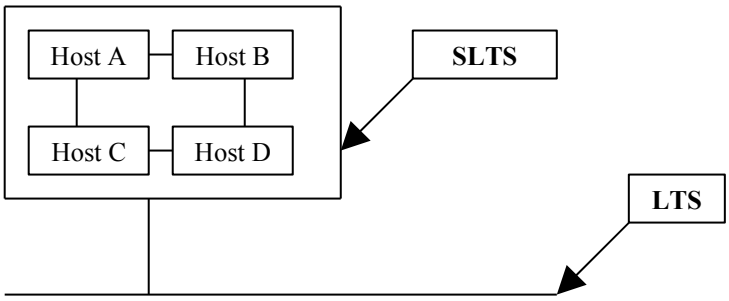
U klasického matrixového bezpečnostního konceptu, takzvaného designu „tlumivých bodů“, se jedná o zvláštní formu úrovňového přístupu. V těchto systémech je host prvního sledu vybaven tím nejvražednějším bezpečnostním softwarem, jaký lze vůbec pořídit, zatímco hosty druhého sledu mají nesrovnatelně nižší bezpečnostní úroveň.



Sériový přístup
Tato konfigurace sestává ze sady hostů, jež jsou všechny spojeny přímo jeden s druhým. Žádný z těchto hostů nemá za úkol chránit ostatní. Každý z nich má specifický úkol, avšak k jeho splnění si musí vyměňovat data s ostatními.
Sériová řazení hostů lze často najít v podnikových systémech. Za normálních okolností je pouze málo hostů připojeno přímo na veřejné souřadnice, zatímco četné komponenty druhého sledu systému jsou navzájem propojené. Deckeři získají k takovým hostům přístup jen tehdy, pokud projdou ostatními počítači, jež jsou s nimi propojeny. Na diagramu sériového přístupu by musel decker, který se zdržuje v LTS, projít hosty A, B, C a D, aby se dostal k hostu E.



Přístup přes soukromé souřadnice
Soukromé souřadnice (SLTS) jsou komunikační sítí, do níž patří výlučně hosty jednoho určitého podniku nebo konsorcia, příp. jedné určité vlády. Přitom se může jednat o malé, místně ohraničené sítě, jimž se říká MPS (místní plošné sítě), nebo o obrovské globální SLTS. Jakmile si decker zjednal přístup k jednomu hostu SLTS, má odtud volnou cestu ke všem hostům, které přísluší daným souřadnicím.
V rámci SLTS mohou být hosty uspořádány úrovňově nebo sériově – a také jsou. V Šestém světě se u designerů matrixových bezpečnostních konceptů nepovažuje paranoia za chorobnou psychózu – jde o základní předpoklad.



Systémové přístupové uzly
Systémové přístupové uzly (SPU) spojují hosty se souřadnicemi a jinými hosty. Pokud decker provádí ze souřadnic nebo speciálního spojení hostů systémovou operaci „přihlášení do hostu“, dostane se do ikony SPU hostu, do nějž chce proniknout. Gamemaster musí v předstihu nebo na místě rozhodnout, k jakým LTS je host s otevřeným přístupem připojen. I když je host dosažitelný pouze přes SLTS nebo sériový přístup, musí gamemaster učinit odpovídající rozhodnutí.

Spojené databanky
Propojení počítačových sítí může vést k opravdovému honu na data matrixem. Informace, které jsou zjevně uloženy v jednom hostu, tam mohou být pouze „zdánlivě“. Pokud se chce decker dostat k danému souboru, nalezne pouze odkaz na jiný spojený host, v němž jsou data opravdu uložena. To může vést k tomu, že decker

bude muset projít celým řetězem vzájemně propojených hostů, než se konečně dostane k tomu, v němž jsou data uložena. Gamemaster může hodit 1k6, aby určil počet takových vzájemných odkazů v daném spojovacím řetězci.

Stupně systému

Každý systém, ať už souřadnice nebo host, vykazuje kód bezpečnosti a pět stupňů subsystémů: přístup, ovládání, index, soubor a periférii. Těmto stupňům se říká stupně systému.
Gamemaster určuje stupně systému na základě takzvané vstupní třídy hostu. K určení těchto stupňů si může buď skrytě hodit, nebo sám rozhodnout, jaké jsou přiměřené hodnoty.

Vstupní třídy

Existují tři různé vstupní třídy: jednoduchá, průměrná a obtížná. Obecně se vstupní třída řídí „přívětivostí k uživatelům“, již musí systém mít, aby plnil svou funkci, a počtem uživatelů, kteří se normálně pokouší v jednom dni získat přístup k hostu. Průměrné systémy používá menší skupina uživatelů než jednoduché; navíc jsou vhodné pro exkluzivnější a bezpečnější transakce. Obtížné systémy obsahují nejutajenější data a přístup k nim má jen několik uživatelů.

Kódy bezpečnosti

Kód (nebo také stupeň) bezpečnosti sestává z úrovně bezpečnosti (barvy) a hodnoty bezpečnosti (čísla).
Čtyři úrovně bezpečnosti jsou modrá (malé nebo vůbec žádné zabezpečení), zelená (průměrné zabezpečení), oranžová (vysoké zabezpečení) a červená (maximální zabezpečení). Podle pověstí mají existovat dokonce systémy s takovou zabijáckou obranou, jejichž stupeň bezpečnosti přesahuje „oficiální“ stupnici barev. V deckerském slangu se jim říká ultrafialové (UV) systémy nebo černé systémy.
Hodnota bezpečnosti sahá obvykle od 4 do 12, někdy i výše. Dvoumístné hodnoty představují extrémně vysoký bezpečnostní systém. Hodnota bezpečnosti udává počet kostek, jimiž gamemaster hází proti systémovým testům deckera (viz **Systémové testy**). Kromě toho udává počet kostek pro testy bezpečnosti.

Úrovně bezpečnosti

Úroveň bezpečnosti hostu udává množství bezpečnostních opatření. Většinou to odráží, jak důležitá jsou uložená data, ale někdy jde jen o výraz paranoie provozovatele systému.

Modré hosty

K modrým hostů patří většinou veřejné databanky, systémy pro zasílání zpravodajství, seznamy komunikačních kódů – tedy skoro vše, co je poskytováno zdarma, ať už ze strany státu, podniku nebo soukromé osoby. Také malé podniky, jejichž prostředky nestačí na lepší zabezpečení jejich systémů, mají zpravidla modré hosty.

Zelené hosty

Zelené hosty jsou relativně průměrné systémy. Ovšem člověk by nikdy neměl udělat tu chybu, aby je považoval za lehkou kořist. Jsou možná vůči vetřelcům trpělivější než oranžové nebo červené systémy, ale mohou být vybaveny jakýmkoli IC, které lze nalézt i v tvrdších hostech.

Oranžové hosty

Oranžové hosty si trochu namlouvají, že jsou bezpečné, dokonce na sebe pohlížejí jako na zabijácké hosty s divokým pohledem. Oranžové hosty obsahují data, jež se obecně označují za „důvěrná“, a provádějí zpracovatelské úkoly, které jsou pro provozovatele důležité, ale nikoli životně nutné. K oranžovým systémům patří běžná výrobní zařízení, stejně jako sítě, jež používají typické podnikové kanceláře středního managementu.

Červené hosty

Červené hosty nabízejí největší míru bezpečnosti, která ještě projde před zákonem jako legální. Obsahují „přísně tajná“ data – často toho druhu, kvůli jejichž ochraně je vlastník schopen jít přes mrtvoly, stejně jako záznamy rozhodující o úspěšnosti projektu (údaje o provozních prostředcích, laboratořích a továrnách značného významu, sítích pro zásobování energií apod.). Obranná opatření jsou většinou smrtícího rázu – decker v červeném systému nemůže počítat s tím, že nejdříve dojde na „varovné výstřely“.

Stupně subsystémů

Pět stupňů subsystémů – přístup, ovládání, index, soubor a periférie – představuje míru odporu subsystémů daného systému proti neautorizovaným pokusům o manipulaci ze strany deckera. Tyto stupně udávají cílová čísla pro všechny testy, které musí decker provést, aby mohl se systémem nelegálně manipulovat. Decker bez oprávnění, který chce například pročítat soubory určitého systému, musí kupříkladu v průběhu jednoho dvojtestu provést pomocí své dovednosti počítače test přístupu a souboru. Tyto testy se nazývají systémové testy (podrobnosti viz dále). Dvojtest proti stupni přístupu zjednává deckerovi přístup k hostu nebo k souřadnicím. Test proti stupni souboru systému mu umožňuje číst soubory.
Přitom byste neměli zapomínat na to, že vysoký stupeň subsystému nebrání v jeho užívání oprávněným osobám. Tedy vysoký stupeň přístupu v žádném případě nepůsobí na přihlášení oprávněného uživatele. Ztěžuje pouze ilegální přihlašování.
Nezapomeňte, že se po spuštění pasivního poplachu zvyšují stupně všech subsystémů o 2.

Přístup
Stupeň přístupu je měřítkem pro intenzitu odporu systému proti neoprávněnému přístupu. K proniknutí do hostu nebo do souřadnic musí decker bez oprávnění uspět v dvojtestu proti odpovídajícímu stupni souřadnic resp. hostu.

Ovládání
Stupeň ovládání udává intenzitu odporu systému vůči neoprávněným administrativním příkazům. Pokud by chtěl například neautorizovaný decker vyhodit z hostu legitimního uživatele, musel by zvítězit v dvojtestu proti stupni ovládání. Jinak řečeno: úspěšné testy ovládání umožňují deckerům přeprogramování systému nebo likvidaci jeho bezpečnostních opatření.

Index
Stupeň indexu udává intenzitu odporu systému vůči nedovoleným pokusům o prohledávání hostu. Neautorizovaný decker, který hledá v hostu nebo souřadnicích systémovou adresu nebo nějaký určitý soubor, musí zvítězit v dvojtestu proti odpovídajícímu stupni souřadnic nebo hostu.

Soubor
Deckeři musí zvítězit v testu proti stupni souboru, pokud chtějí soubory nelegálně číst, vytvářet nebo manipulovat s jejich obsahem. Tento test je nutný i pro rozluštění zakódovaných souborů nebo pro odeslání souboru do výstupního zařízení, jako je tiskárna nebo vypalovačka čipů.

Periférie
Stupeň periférie je určen pro obsluhu dálkově řízených přístrojů, které systém ovládá. Úspěšný dvojtest proti stupni periférie umožňuje neautorizovanému deckerovi například obsluhu hostem řízených bezpečnostních kamer nebo výtahů.

Formát systému

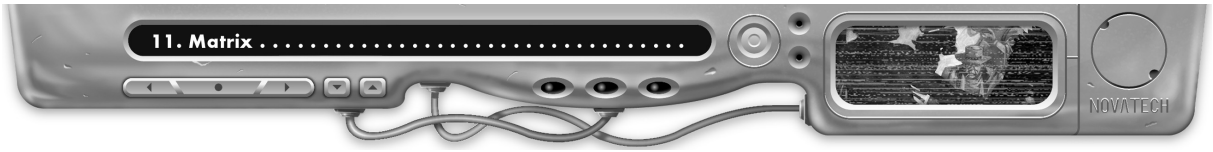
Pro popis stupňů systému se používá následující schéma:

Úroveň bezpečnosti-hodnota bezpečnosti/přístup/ovládání/index/soubor/periférie

Systém červená-6 se stupněm přístupu a indexu 10, stupněm ovládání 12 a stupněm souboru a periférie 9 by měl následující formát zápisu:

Červená-6/10/12/10/9/9

STUPNĚ HOSTŮ		
Vstupní třída	**Hodnota bezpečnosti**	**Stupně subsystémů**
Jednoduchá	1k3 + 3	1k3 + 7
Průměrná	1k3 + 6	2k3 + 9
Obtížná	2k3 + 6	1k6 + 12



Kyberdecky

Kyberdecky jsou klíčem k umění deckera. Kyberdeck představuje rozhraní mezí matrixem a deckerem. Krátce řečeno, kyberdeck je extrémně výkonný mikropočítač s dostatečnou kapacitou zpracování, aby mohl disponovat rozhraním ASIST, jež převádí deckerovy nervové impulsy na holografické příkazy. S nejžhavějšími užitkovými programy z ulice může decker za pomoci svého kyberdecku tančit na elektronovém nebi.
Všechny kyberdecky sestávají z určitých komponentů, které si decker přizpůsobí tak, aby vykouzlil v matrixu co nejlepší ikonu. Tyto komponenty vytvářejí deckerovu personu a definují deckerovy hodnoty v matrixu.
K jednomu kyberdecku může být připojen pouze *jeden* decker. Decker musí pomocí kabelu z optických vláken vytvořit spojení mezi deckem a svým datajackem. Deck musí mít k dispozici přípojku, aby mohl decker vstoupit do matrixu.

Stupně decku

Kvalitu deckerovy persony určuje kapacita zpracování HPOP (hlavního programu ovládání persony) a programů odolnost, senzory, únik a maskování. HPOP reprezentuje operační systém decku a má stupeň, který udává jeho odolnost vůči poškození a schopnost fungovat i nadále po utrpěném poškození. Programy odolnost, senzory, únik a maskování se označují také jako programy persony. Číselné hodnoty těchto programů slouží jako „atributy“ deckerovy persony a používají se ve všech testech persony deckera, pokud se nachází v matrixu. Deckeři používají i užitkové programy, jež mají rovněž takové stupně (viz **Užitkové programy**).
Stupeň HPOP je nejdůležitější hodnota kyberdecku. Trojnásobek stupně HPOP udává maximální celkový stupeň programů persony na daném decku. Žádný ze stupňů persony nemůže překročit stupeň HPOP a nejvyšší stupeň většiny užitkových programů se udává rovněž prostřednictvím stupně HPOP.
Zkrácený formát stupňů kyberdecku je následující:

HPOP-stupeň/odolnost/únik/maskování/senzory

Deck s HPOP 8, jehož programy persony jsou stejnoměrně zvýšeny na maximální celkový stupeň (3 x 8 = 24) by měl následující formát:

HPOP-8/6/6/6/6

Pokud by chtěl decker zvýšit stupeň odolnosti o 2, musely by se ostatní programy persony vzdát celkem 2 bodů. Pokud by se snížily únik a senzory každý o 1 bod, byly by stupně decku následující:

HPOP-8/8/5/6/5

Pevnost

Pevnost představuje vnitřní programy, jež zvyšují odolnost kyberdecku vůči nepřátelským kódům jako počítačovým virům, šedým a černým IC apod.
Za každý bod pevnosti, jejž má deck k dispozici, se snižuje účinnost útoků černých IC na on-line ikonu nebo deckera samotného o 1. Pokud je ikona deckera napadena šedým IC, zvyšuje se cílové číslo útočného testu IC za každý bod pevnosti o 1.
Pevnost pomáhá i proti programům Černé kladivo a Vražednost, ale nikoli proti jiným útočným programům.

Aktivní paměť

Pokud bychom použili starý pojem, pak je aktivní paměť RAM kyberdecku. Tak jako hackeři ve dvacátém století mluvili o tom, že mají v počítači 64 mega, mluví decker Šestého světa například o 100 Mp aktivní paměti na svém decku. Aktivní paměť rozhoduje o tom, kolik aktivních užitkových programů může být současně spuštěno v decku, a tak mohou být deckerovi k dispozici k okamžitému použití. V decku s 200 Mp aktivní paměti mohou běžet současně užitkové programy o celkové velikosti maximálně 200 Mp.

Paměťová banka

Paměťová banka odpovídá pevnému disku starodávných počítačů. Každý program v paměťové bance decku může být pomocí operace „výměna obsahu paměti“ naložen do aktivní paměti decku (viz **Systémové operace**). Všechny programy, jež chce decker při runu použít, musí být v paměťové bance, ať už jsou v dané době naloženy v aktivní paměti nebo ne. Data, jež mají být vyložena nebo naložena, lze skladovat rovněž v paměťové

bance decku nebo v laciné off-line paměťové bance. Celkový počet megapulsů užitkových programů a dalších uložených dat nesmí překročit místo v paměťové bance. Pokud má tedy decker ve své paměťové bance na základě tam uložených užitkových programů k dispozici ještě 500 Mp volného místa, nemůže tam naložit žádná data, jejichž velikost přesahuje 500 Mp.

Rychlost I/O

Vstup (input) a výstup (output) decku odpovídá starému modemu, který v temných raných časech počítačové techniky spojoval terminály a počítače. Nakládání a vykládání dat probíhá vždy plnou rychlostí I/O decku (v Mp za bojové kolo).

Posílení reakce

Posílení reakce je matrixovým ekvivalentem reflexních vláken. Každý stupeň posílení reakce zvyšuje deckerovu reakci v matrixu o 2 a přidává 1k6 k jeho iniciativě.
Deck mohou podporovat maximálně 3 body posílení reakce. Kromě toho jejich počet nesmí překročit čtvrtinu (zaokrouhleno dolů) stupně jeho HPOP. U decku s HPOP 3 nebo menším tedy není možné vůbec žádné posílení reakce.

KYBERDECKY							
Model	**Stupeň HPOP**	**Pevnost**	**Aktivní paměť**	**Paměťová banka**	**Rychlost I/O**	**Posílení reakce**	**Cena**
Allegiance Sigma	3	1	200	500	100	0	14 000 ¥
Sony CTY-360-D	5	3	300	600	200	1	70 000 ¥
Novatech Hyperdeck-6	6	4	500	1 000	240	1	125 000 ¥
CMT Avatar	7	4	700	1 400	300	1	250 000 ¥
Renraku Kraftwerk-8	8	4	1 000	2 000	360	2	400 000 ¥
Transys Highlander	9	4	1 500	2 500	400	2	600 000 ¥
Novatech Slimcase-10	10	5	2 000	2 500	480	2	960 000 ¥
Fairlight Excalibur	12	6	3 000	5 000	600	3	1 500 000 ¥

Faktor odhalení

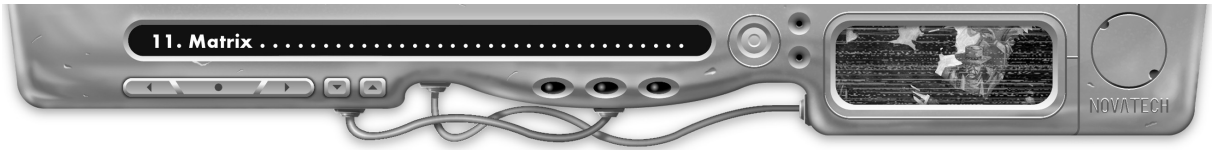
Faktor odhalení slouží gamemasterovi jako cílové číslo pro testy, jimiž má být odhalena přítomnost deckera nebo mu má být zabráněno provádět v matrixu akce (viz **Systémové testy**). Pro určení faktoru odhalení vypočítejte průměr (zaokrouhlený nahoru) stupně maskování decku a stupně užitkového programu Plížení. Deck s HPOP-8/6/8/6/4, v němž běží program Plížení 8, by měl například faktor odhalení 7. Ten tvoří maskování 6 + Plížení 8, děleno 2.
Pokud decker nemá program Plížení vůbec spuštěný, odpovídá faktor odhalení polovině stupně maskování. To činí dobrý program Plížení nutností pro každého deckera s trochou ctižádosti – a s vyvinutým pudem sebezáchovy.

Hackovací rezervy

Hackovací rezervy se řídí pravidly pro rezervy kostek uvedenými v kapitole **Herní mechanismy**, Pro určení hackovacích rezerv sečtěte deckerovu inteligenci a stupeň HPOP jeho decku, vydělte součet 3 a zaokrouhlete výsledek dolů. Jakékoli zvýšení inteligence, ať už kybernetického nebo magického původu, má vliv i na hackovací rezervy. Takové přírůstky jsou kumulativní.
Kostky z hackovacích rezerv mohou být přidány ke všem testům k matrixu – systémovým testům, útočným a obranným testům nebo testům atributů.
Kostky hackovacích rezerv nepomáhají při testech těla nebo vůle při odolávání poškození šedým nebo černým IC, jež se pokoušejí deckerovi způsobit poškození. Za těchto okolností pomáhají pouze kostky karmových rezerv, vylepšení kyberdecku nebo zvýšení těla nebo vůle pomocí magie.

Kyberterminály

Ne každý uživatel matrixu používá při své práci kyberdeck. Naopak, většina z nich se připojuje přes kyberterminál.



Protože decky jsou celkem drahé a podniky je nestrkají do ruky každému ťukači do klávesnice a kancelářskému zaměstnanci, jsou kyberterminály v deckerském slangu nazývány pro svůj nedostatek rychlosti a jemnosti „šneky“.
Kyberterminál je zkrátka klávesnice s obrazovkou a sadou elektrod nebo zástrčkou pro datajack. Některé terminály jsou dokonce vybaveny takovými vykopávkami jako monitory, rukavicemi pro virtuální realitu nebo dokonce myší či joystickem.
Tyto terminály mají přibližně stejné stupně jako kyberdecky, ovšem HPOP žádného kyberterminálu nesmí být větší než 4. Terminály nelze vybavit posílením reakce a stupně všech programů, které jsou na nich spuštěny, se snižují o 1 – to odráží fakt, že kyberterminály jsou ve srovnání s kyberdecky hůře ovladatelné. Šnek má ovšem tu výhodu, že jeho uživatele nemůže zranit černé IC a že ten nemůže utrpět děrový šok. Kromě toho stojí pouze kolem 10 procent obvyklé obchodní ceny odpovídajícího kyberdecku.

Příslušenství

Kyberdecky a terminály jsou často vybaveny příslušenství, jako jsou off-line paměťové banky nebo videoobrazovky, na nichž mohou ostatní sledovat matrixový run z pohledu deckera. Stopařské zástrčky (sítě elektrod nebo zařízení pro připojení přes datajack) umožňují ostatním, aby se rovněž „připojili“ a prožívali run tímto způsobem. Nemají žádný vliv na personu deckera, jsou pouze přítomni jízdě. Kromě toho jsou tito hosté stejně jako uživatelé kyberterminálů chráněni před ošklivými účinky černých IC. Mnozí lidé považují za rušivé, takto deckera doprovázet, protože nemají vliv ani na činnosti, ani na perspektivu deckera. Cenu tohoto příslušenství naleznete v kapitole **Výbava**.

Deckování

Deckování je umění. Jak něco decker dělá, je často přinejmenším stejně důležité jako to, co dělá. Ego deckerů a jejich úsilí být stále o délku nosu před ostatními je legendární dokonce i mimo deckerské kruhy. Tam venku je možné odhalit celou subkulturu točící se kolem matrixu. V mašině existuje úplně jinej svět, kámo.

Pohyb v matrixu

Pohyb v matrixu se děje téměř bezprostředně, pokud se decker nezaplete do matrixového boje, nemusí se vypořádat s IC, neprovádí systémové operace, nepřenáší data nebo nespouští programy. V matrixu se data přenášejí v řádech mega (to je rychlé, lidi) a reakční čas se měří v mikrosekundách. Pouze pokud se decker zabývá něčím, co vyžaduje opravdu pozornost, zpomalí se rychlost runu do té míry, že při něm decker vnímá plynutí času.
Při pohybu v matrixu je vzdálenost *absolutně* relativní. Je to otázka komunikačního spojení, dostupné paměti v subsystémech a střídání systémů a přenosových rychlostí, nikoli metrů nebo kilometrů. Jistě, decker se může procházet klidně od jednoho bodu k druhému – ale proč se plazit, když je možné létat? Pozornost je nade vše.

Subjektivní vnímání času

Nemělo by se zapomínat na to, že postavy v matrixu mají subjektivní vnímání toku času. Čas, který postava stráví v prostředí matrixu, se může zdát o něco delším než skutečný herní čas vyžadovaný pro danou činnost. Decker, který například provádí k nalezení jistého souboru jedinou systémovou operaci, ji může prožívat jako procházku dlouhou, knihami přeplněnou chodbou v knihovně, která skončí teprve tehdy, když nalezne žádanou ikonu. Decker může mít pocit, že hledáním strávil minuty nebo dokonce hodiny, ačkoli ve skutečnosti uplynulo pouze několik vteřin herního času.

Opuštění matrixu

Decker může matrix kdykoli opustit tak, že se odpojí, tj. vytáhne zástrčku, která spojuje jeho datajack s deckem. Myslete na to, že deckerovo vypodobnění v matrixu – persona – je jenom program, který běží v počítačích matrixu. Persona se *ve skutečnosti* nepřesunuje na jiná místa a rovněž nedisponuje samostatným vědomím. Navzdory deckerským legendám nemůže být nikdo v matrixu „uvězněn“. Odpojení se je volná akce, pokud není decker zrovna napaden černým IC.
Je-li decker proti své vůli z matrixu vyhozen, označuje se to jako „pád do díry“. Náhlé přerušení simsensového signálu způsobuje lehkou dezorientaci, které se říká děrový šok (následky jsou popsány v oddílu **Děrový šok**).

Vnímání v matrixu

Uvnitř souřadnic se mohou vzdálenosti jevit jako obrovské, ale v matrixu neexistují žádné „reálné“ vzdálenosti. V závislosti na ústředním znázornění mohou prostory uvnitř hostu vypadat nekonečně rozlehle nebo stísněně. Otázkou však stále zůstává pouze to, zda si persona (je to pouze program) může zjednat přístup k datům jiného programu nebo k hardwarovým komponentům systému. Vzdálenost je pozoruhodným způsobem úměrná relativnímu času (většinou měřenému v nanosekundách), které deck potřebuje, aby se dostal k hardwaru dalšího systému.

Odhalení nové ikony

Pokud do oblasti matrixu, kde se právě decker zdržuje, vstoupí nová ikona, například jiný decker nebo program, může decker provést volný test senzorů (užitkové programy nejsou dovoleny), aby se zjistilo, zda si nové ikony všimne. Cílové číslo pro tento test představuje stupeň maskování plus stupeň užitkového programu Plížení, pokud je novou ikonou decker, nebo stupeň ikony, jedná-li se o IC nebo jiný program. K odhalení ikony stačí deckerovi jediný úspěch (pokud je ikonou IC, pozná při dvou úspěších jeho typ a při třech jeho stupeň), ačkoli decker možná netuší, co ikona zastupuje, dokud neprovede systémovou operaci „analýza ikony“. Jakmile je ikona odhalena, zůstává „viditelnou“, dokud neprovede manévr pro útěk (viz **Bojové manévry**). Tato volná akce představuje schopnost senzorů rozpoznat jiné programy. Pokud není ikona při testu senzorů odhalena, není si jí decker vědom, dokud se mu sama neukáže nebo ho nenapadne.
Pokud má decker podezření na přítomnost jiné ikony, může se pokusit ikonu „lokalizovat“, aby si své podezření ověřil.

Lokalizace IC

Pokud decker spustí IC, nemusí si toho vždy všimnout. Dříve než může zaútočit nebo přijmout jiná opatření, musí IC nejprve „lokalizovat“. Je nabíledni, že lokalizace aktivního IC nečiní žádné potíže, jakmile deckera napadne. Lokalizované IC zůstává viditelné, dokud neprovede nějaký manévr, aby deckerovi uniklo (viz **Bojové manévry**).
Reaktivní IC je zákeřnější, neboť svou přítomnost deckerovi neprozrazuje žádnými akcemi. Jakmile decker spustí reaktivní IC, provede gamemaster skrytý test senzorů decku proti cílovému číslu ve výši stupně IC. Pokud v tomto testu padne alespoň jeden úspěch, informuje deckera, že jeho akce spustily IC. Při dvou úspěších deckerovi sdělí, jaký typ IC spustil. Při třech a více úspěších zjistí decker dokonce i stupeň IC a jeho umístění. Tyto testy senzorů se provádějí pouze jednou, a sice tehdy, když je IC aktivováno. Pokud se decker domnívá, že je přítomno nějaké IC, může se tomuto podezření podívat na zoubek pomocí operace „lokalizování IC“.

Nebojové akce

Decker, který chce takové akce provádět, si za tímto účelem nemusí házet na iniciativu. Místo toho se vydělí jeho reakce 10 (zaokrouhleno nahoru). Výsledek udává počet fází, které může decker provést během tří vteřin (tato doba odpovídá jednomu bojovému kolu). K tomuto výsledku se přidá jedna další fáze za každou kostku iniciativy, kterou má decker k dispozici navíc ke standardní 1k6.
Příklad: Decker se dvěma fázemi za bojové kolo by mohl během svého prvního průběhu iniciativy provést operaci „přihlášení do hostu“ (komplexní akce), stejně jako operaci „analýza ikony“ (volná akce). Během své druhé fáze by poté mohl host analyzovat (komplexní akce). Seznam akcí, jež může decker provádět, je uveden níže. Popis systémových operací následuje.
Reaktivní programy IC, které provádějí své úkoly na konci bojového kola, jednají teprve poté, co všichni deckeři provedli v daném kole všechny své dostupné akce.

Systémové testy

Pokud chce decker v matrixu provést určitý úkol, vyšle hostu nebo souřadnicím příkaz nebo řetěz příkazů. Těmto příkazům se říká systémové operace (podrobný soupis všech systémových operací, jež může decker provádět, najdete dále). Systémový test vyžaduje volnou, jednoduchou nebo komplexní akci a je spojen s určitým subsystémem (přístupem, ovládáním, indexem, souborem nebo periférií), což je vždy uvedeno v popisu.
Kromě toho musí neautorizovaní deckeři provést test (zvaný systémový test), pokud chtějí v matrixu provést systémovou operaci. Důvod tohoto testu spočívá v tom, že decker musí k provedení úkolu systém přinutit, aby mu poskytl procesorový čas a systémové zdroje. Čím větší nároky klade decker na systém, tím pravděpodobněji si systém vetřelce všimne a aktivuje protiopatření.

Systémové testy se vyhodnocují vždy jako dvojtesty mezi deckerem a cílovým hostem nebo souřadnicemi. Decker hází svou dovedností počítače (či jejich specializací deckování). Cílové číslo představuje stupeň subsystému, jímž má daná systémová operace manipulovat. Aby se například decker přihlásil do hostu, musí podstoupit test počítačů proti cílovému číslu ve výši přístupu hostu. Dané cílové číslo je možné modifikovat pomocí užitkových programů, jež má decker spuštěné (užitkové programy potřebné k daným systémovým operacím najdete v oddílu **Systémové operace**). K systémovým testům lze přidat kostky z hackovacích rezerv.
Současně s tím provádí gamemaster za host nebo souřadnice test bezpečnosti. Za tímto účelem hází hodnotou bezpečnosti hostu/souřadnic proti cílovému číslu ve výši faktoru odhalení deckera.
Pokud decker dosáhne více nebo stejně úspěchů jako host, zvítězí v dvojtestu a může úspěšně provést zamýšlený úkol. Dosáhne-li více úspěchů host, decker selže.
Bez ohledu na konečný výsledek testu si ovšem gamemaster poznamená počet úspěchů hostu a přidá je ke všem dřívějším úspěchům, jichž host dosáhl v systémových testech proti tomuto deckerovi. Toto stále aktualizované množství udává stav bezpečnostního konta.
Pro jednoduchost se systémové testy nazývají podle dotyčného subsystému. Příklad: Pojem test přístupu označuje dvojtest, v jehož průběhu se hází deckerovou dovedností počítače proti stupni přístupu a hodnotou bezpečnosti systému proti faktoru odhalení téhož deckera. Stejný postup platí pro testy souboru, indexu, ovládání a periférie.
Následující příklad popisuje první krok, který musí provést každý decker – totiž zjednat si přístup do hostu, do něhož chce vniknout.

HeadCrash má počítače 6 a deck s HPOP-8/6/66/6. Má spuštěné Plížení 5, takže jeho faktor odhalení činí 6 (6 + 5 = 11; děleno 2 dává 5,5; zaokrouhluje se nahoru). Navíc má ještě spuštěno Klamání 4. Head se chce prodeckovat do hostu červená-8 s přístupem 11. Aby se mohl přihlásit, musí uspět v testu přístupu.
HeadCrash si hází na základě své dovednosti počítače 6 kostkami. Cílové číslo se určí následovně: 11 (stupeň přístupu) mínus 4 (stupeň programu Klamání) dávají pro test přístupu konečné cílové číslo 7.
Gamemaster hází osmi kostkami (hodnocení bezpečnosti hostu) proti cílovému číslu 6 (Headův faktor odhalení).
HeadCrashovi padne 2, 2, 3, 4, 5 a 9 – tím má proti cílovému číslu 7 jeden úspěch. Hostu padne 1, 2, 2, 2, 3, 3, 5 a 5, čímž nedosáhl ani jediného úspěchu. HeadCrash se tedy do hostu přihlásí. Má štěstí a měl by doufat, že se ho bude držet.
Zde je nutné podotknout, že kdyby HeadCrash neměl spuštěný žádný program Klamání, bylo by cílové číslo 11 a nikoli 7. V tom případě by nedosáhl žádného úspěchu a nepodařilo by se mu přihlásit se. A poučení z příběhu? Člověk nedosáhne vůbec ničeho, pokud se mu ani nepodaří, aby se do hostu vůbec přihlásil. Dobrý program Klamání je tedy nutností pro každého deckera, který se zajímá o hosty s vysokými hodnotami bezpečnosti.

Systémové testy v souřadnicích

Určitá místa, například fyzická přípojka deckera, mohou omezovat spektrum systémových operací, jež má decker k dispozici. Kromě níže uvedených operací může decker provést kdykoli operaci „elegantní odhlášení“ (viz **Systémové operace**).

Z přípojky

Deckeři, kteří se připojují přes legální nebo nelegální přípojku pro telekom, mohou provádět pouze operaci „přihlášení do LTS“. Následně musejí nalézt host nebo souřadnice, do nichž chtějí proniknout, pokud ještě neznají jejich lokaci. Deckeři, již se připojují přes specializovanou pracovní stanici, periferní přístroje nebo konzolu, mohou provést pouze operaci „přihlášení do hostu“ – a musí vstoupit do hostu, jenž ovládá zařízení, skrze něž si zjednali přístup do systému.

Z LTS

Jakmile je decker přihlášen do LTS, může se dostat k mateřským RTS, provede-li operaci „přihlášení do RTS“. Může se ale také pokusit zjednat si přístup k nějakému hostu, který je připojen k daným LTS, pokud provede operaci „přihlášení do hostu“. Jsou-li s LTS, v nichž se decker právě nalézá, spojeny i nějaké SLTS, může decker provést operaci „přihlášení do LTS“, aby se do daných SLTS dostal.

Z RTS

Pokud se decker nalézá v RTS, může se odtud přesunout buď pomocí „přihlášení do RTS“ do jiných RTS (tedy navázat „dálkové spojení“, aby se dostal do souřadnic na druhém konci světa), nebo vstoupit do libovolných LTS, která jsou součástí daných RTS pomocí operace „přihlášení do LTS“.

Decker v RTS může provést rovněž operaci „lokalizace přístupu“.

Z SLTS
V STLS může decker provést jakoukoli systémovou operaci, jež je proveditelná také ve veřejných LTS a RTS.

Bezpečnostní konto

Gamemaster si poznamená všechny úspěchy, kterých dosáhly host/souřadnice při obraně před deckerem. Na toto konto se zaznamenávají všechny dosažené úspěchy, nejen ty čisté. Jinými slovy: i pokud host/souřadnice v systémovém testu podlehnou, mohou dosáhnout úspěchů, jež zvýší deckerovo bezpečnostní konto. Toto konto je vedeno tak dlouho, dokud je decker v daném hostu nebo daných souřadnicích přihlášen. Jakmile výše konta dosáhne gamemasterem stanovené výše, může to spustit určitou reakci hostu nebo souřadnic, jež sahá od aktivace černých IC až po vůbec nic. Tato pravidla vycházejí z toho, že decker nikdy neví, k čemu dojde v důsledku jeho dalšího testu nebo kolik testů si ještě může dovolit, než na sebe host/souřadnice upozorní a ty budou dělat vše možné, aby jeho personu přivedly ke zhroucení.

Bezpečnostní tabulky

Na základě bezpečnostní tabulky se pozná, k jakým bezpečnostním opatřením dojde v hostu nebo souřadnicích a jak budou host/souřadnice na vetřelce reagovat. Jednoduše řečeno, taková tabulka představuje seznam různých aktivačních kroků, kterým se říká aktivační prahy (nebo spouštěcí kroky). Tyto kroky odpovídají prahovým hodnotám bezpečnostního konta. Pokud deckerovo bezpečnostní konto dosáhne určitého spouštěcího kroku, aktivuje systém jeden nebo více programů IC. Aktivační prahy spouštějí rovněž různé systémové stupně poplachu. Poplachový status systému ovlivňuje rovněž druh aktivovaných IC.
Úroveň bezpečnosti hostu/souřadnic udává, jak blízko jsou tyto aktivační prahy systému u sebe. Gamemaster určí, jakou reakci spustí ten který aktivační práh. Může tak učinit s rozmyslem nebo na základě náhody.

Aktivační prahy
Jak již bylo zmíněno, sestávají aktivační prahy z určitých hodnot bezpečnostního konta. Vždy, když deckerovo bezpečnostní konto dosáhne nebo překročí daný aktivační práh, aktivuje systém jedno nebo více bezpečnostních opatření, například programy IC nebo poplachové stavy. Systémy s nízkou úrovní bezpečnosti mají méně aktivačních prahů – a tím pádem i méně programů IC a dalších bezpečnostních opatření. Vysoce zabezpečené systémy (například červené hosty) jsou charakteristické aktivačními prahy blízko u sebe a disponují větším množstvím programů IC a dalších bezpečnostních opatření.
Bezpečnostní rozptyl systému udává různé spouštěcí kroky a poukazuje na události, které každý krok spouští. Tabulka **Jednoduchý bezpečnostní rozptyl (příklad)** představuje systém, který aktivuje IC Sonda-5, pokud deckerovo bezpečností konto dosáhne hodnoty 3. Dosáhne-li konto 7, aktivuje systém IC Sonda-7 atd.
Gamemaster může určit aktivační prahy buď podle vlastního uvážení, nebo na základě náhody. V tom případě hodí 1k6 a vydělí výsledek 2 (zaokrouhleno nahoru). K výsledku pak přičte modifikátor z tabulky **Aktivační prahy systému**, který vychází z úrovně bezpečnosti. Každý výsledek hodu se přičítá k hodnotě předchozího aktivačního prahu.
Pokud se tvoří vysoce zabezpečený systém, používá se k určení aktivačních prahů prostě ta nejnižší hodnota ze spektra úrovně bezpečnosti. U slabších systémů se pro určení aktivačních prahů berou nejvyšší hodnoty.
Tak by mohl mít modrý host s minimální bezpečností následující aktivační prahy: 6, 12, 19, 24, 31, 36, 42 atd.

JEDNODUCHÝ BEZPEČNOSTNÍ ROZPTYL (PŘÍKLAD)

Aktivační práh	Událost
3	Sonda-5
7	Sonda-7
10	Zabiják-8/pasivní poplach
13	Zabiják-10/aktivní poplach

AKTIVAČNÍ PRAHY SYSTÉMU	
Úroveň bezpečnosti	**Modifikátor hodu/rozsah aktivačního prahu**
Modrá	+4 / 5 až 7
Zelená	+3 / 4 až 6
Oranžová	+2 / 3 až 5
Červená	+1 / 2 až 4

Několikanásobné spuštění
Pokud decker provádí v systému více akcí, které dohromady přidávají na jeho bezpečnostní konto více bodů, je možné, že dojde k dosažení dvou nebo více aktivačních prahů najednou. V tomto případě nastanou současně VŠECHNY události spojené s dosaženými nebo překročenými aktivačními prahy (říká se tomu rovněž „hodit lejno do ventilátoru“).

Souřadnice a bezpečnostní konta

Následkem změny LTS v rámci týchž RTS se deckerovo bezpečnostní konto nemaže. Pokud se například decker přihlásí do SKAS-SEA-2206 a získá tam stav konta 2, pak přejde do centrální systému SKAS-SEA-RTS, kde se konto zvýší na 3, aby konečně pronikl do SKAS-SEA-4206 a nabral na své konto další 2 body, bude jeho konto činit 5 a takto bude vedeno dál, dokud se bude zdržovat v nějakých souřadnicích SKAS-SEA. Pokud ovšem přejde do jiných RTS, jeho konto ho následovat nebude.

SLTS a bezpečnostní konta
Protože SLTS mají spuštěné velmi aktivní standardní bezpečnostní programy, zůstává bezpečnostní konto získané v určitých RTS v platnosti, pokud se decker z těchto RTS přihlásí do SLTS. To se děje proto, že když SLTS potvrzují proces přihlášení, přebírají od RTS takzvané „bezpečnostní značky“. To může vést k tomu, že decker nahromadí tučné konto, zatímco si zjednává cestu veřejnými souřadnicemi, a poté spustí IC, sotva vstoupí do soukromého datového prostoru.
Decker z našeho příkladu by si podržel bezpečnostní konto 5, pokud by se chtěl prodrat z pochybných RTS do SLTS. Pokud by již tento stav konta stačil ke spuštění určitých bezpečnostních reakcí, dojde k tomu, jakmile se dokončí proces přihlašování. Ať už bezprostřední výsledek dopadne jakkoli, stav deckerova konta z uvedeného příkladu bude na začátku jeho runu v daných SLTS na 5 a možná začne zase stoupat jíž během přihlašování.

Poplachové stavy

Poté, co gamemaster určí aktivační prahy pro daný systém, si vybere programy IC a bezpečnostní opatření, které se spustí po dosažení každého aktivačního prahu. Aby však určil vhodnou míru reakce pro daný práh, musí si nejdříve rozmyslet časové rozvržení systémového poplachu. Každý systém zná tři poplachové stavy – nulový poplach, pasivní poplach a aktivní poplach. Normální stav všech systémů je „nulový poplach“. Určité aktivační prahy spouští pasivní a aktivní poplach. Poplachový stav systému zase určuje druhy programů IC, které budou při dosažení jistého aktivačního prahu spuštěny.

Nulový poplach
Při dosažení aktivačního prahu ve stavu nulového poplachu spouští systém obvykle reaktivní IC.

Pasivní poplach
V typickém bezpečnostním rozptylu se pasivní poplach spouští po dosažení třetího nebo čtvrtého aktivačního prahu.
Pasivní poplach znamená, že systém tuší přítomnost vetřelce, není si ale ještě stoprocentně jistý. Za tohoto poplašného stavu spouštějí aktivační prahy zpravidla bílá nebo šedá aktivní IC.
Pokud se systém přepne do pasivního poplachu, vzrůstají stupně všech subsystémů o 2.

Aktivní poplach
Typický systém se přepíná do stavu aktivního poplachu při dosažení druhého nebo třetího aktivačního prahu poté, co již došlo ke spuštění pasivního poplachu. Aktivní poplach znamená, že systém potvrdil přítomnost neoprávněné ikony.
Při aktivním poplachu se při dosažení dalších aktivačních prahů zpravidla spouští aktivní a někdy dokonce černá IC. Kromě toho je navýsost možné, že do systému vstoupí podnikový nebo policejní decker.

Pokud se již systém přepnul do stavu aktivního poplachu, bude pro neoprávněného deckera daleko obtížnější ze systému zmizet a později se do něj zase proplížit zpět. Bezpečnostní personál má nyní avízo, že zde někdo čmuchal, a systémoví administrátoři budou ještě nějaký čas obzvlášť ostražití.

Reset hostu/souřadnic

Pokud se decker přihlásí do hostu nebo do souřadnic, obrátí tam všechno vzhůru nohama, dožene systém k tomu, že se jen tak-tak sám nevypne, a potom se odhlásí, nemůže počítat s tím, že se za pět minut do toho samého systému vrátí a že tam bude vše odpuštěno a zapomenuto. Bezpochyby budou v hostu nebo souřadnicích nadále aktivní programy IC a další bezpečnostní opatření. Dříve než se decker znovu připojí, měl by raději počkat, dokud se systém „nerozhodne“ odvolat poplachový stav, ukončit běžící programy IC a zcela se vrátit ke svým běžným úkolům. Tomuto procesu se říká reset hostu resp. souřadnic.
Modré systémy provedou úplný reset za 2k6 minut. Za tuto dobu deaktivuje systém bezpečnostní opatření a bezpečnostní konto klesne znovu na 0. U bezpečnějších systémů zabere tento proces více času. Zelené, oranžové a červené systémy začnou s resetem teprve po 3k6 minutách za předpokladu, že decker nespustil v systému pasivní nebo aktivní poplach.
Pokud ovšem decker v zeleném, oranžovém nebo červeném systému poplach spustil, trvá systémový reset ještě déle. U zeleného systému si hází gamemaster 1k6 každých 5 minut, u oranžového každých 10 minut a u červeného každých 15 minut. Bezpečnostní konto systému se snižuje o výsledek tohoto hodu. Každý program IC, který ještě běží, zůstane aktivní tak dlouho, dokud bezpečnostní konto neklesne pod hodnotu, při níž byl nastartován.
Pokud se do systému přihlásí jakýkoli decker ještě předtím, než je reset ukončen, přebírá zbývající bezpečnostní konto s tou hodnotou, na níž se nacházelo v době tohoto nového přihlášení.

Selena pronikla do oranžového hostu a než se zase odhlásila, navýšila jeho bezpečnostní konto na 18, a navíc měla v té době v patách IC Zabiják a jeden konstrukt. Následně začal systém s resetem hostu.
O půl hodiny později se do tohoto hostu přihlásí Kybersuši – reset však ještě není ukončen. V dané chvíli je bezpečnostní konto na 6. Při Selenině runu spustil systém při stavu konta 5 (jeden z aktivačních prahů) pasivní poplach, takže se systém tak jako předtím nachází ve stavu pasivního poplachu. IC Zabiják se aktivoval při 12 a konstrukt při 16, takže oba programy jsou zatím znovu neaktivní.

Spuštění IC

IC znamená *Intrusion Countermeasures* (opatření proti vniknutí; pro vás všechny neposkvrněné matrixem: čte se to jako „led“). Některá IC pouze deckerovi zabrání (nebo se jen pokusí) v neoprávněném vstupu do sítě. Jiná byla vyvinuta za tím účelem, aby dokázala přivést jeho ikonu ke zhroucení. Další jsou zase celé žhavé na jeho deck. A pak existují ještě černá IC – ta ho chtějí prostě a jednoduše připravit o život.

Aktivní versus reaktivní

IC je buď aktivní, nebo reaktivní. Aktivní IC na deckera zaútočí, jakmile obdrží informaci o jeho přítomnosti (viz **Boj v matrixu**). Aktivní IC jedná jako nepřátelská NP. Hází si na iniciativu, pokouší se pomocí různých manévrů dostat se do výhodné pozice a používá své zbraně a další triky.
Naproti tomu reaktivní IC „jen tak posedává“. Může se stát aktivním, pokud bezpečnostní konto dosáhne určitého aktivačního prahu; možná ho decker spustí určitou akcí; možná se také zdržuje na určitém místě nebo v určitém zdroji daného hostu, například v souboru, periferním zařízení nebo dokonce v celém kompletním subsystému. V tomto případě se aktivuje, jakmile si decker zjedná přístup k onomu chráněnému místu nebo zdroji. Jakmile decker spustí reaktivní IC, to má vliv na jeho další akce, dokud není zničeno, oklamáno nebo jinak přesvědčeno, aby se stáhlo. Reaktivní IC má iniciativu jen zřídka.

Přivést IC ke zhroucení

Kdykoli decker v matrixovém boji IC „sejme“ resp. přivede ke zhroucení, přidává se stupeň zhrouceného programu IC k jeho bezpečnostnímu kontu. Důvod zní: Zhroucení IC je srovnatelné s nezřízenou palbou z autokanónu na hlídku v předsunuté pozici – hlídka zemře, ale zároveň varuje své kolegy, že je nepřítel na postupu.

Potlačení IC
Decker se může nevýhodám spojeným se zhroucením programu IC vyhnout tak, že IC zároveň potlačí. Potlačení IC ovšem snižuje deckerův faktor odhalení, a sice o 1 za každý potlačený program IC. Toto snížení trvá tak dlouho, dokud se decker zdržuje v daném systému a potlačené IC znovu neuvolní. Decker musí svůj úmysl potlačit IC oznámit ve chvíli, kdy ho přivede ke zhroucení. Poté ho může kdykoli uvolnit. Za každý uvolněný program IC obdrží decker zpět 1 bod svého faktoru odhalení. Jeho bezpečnostní konto se ovšem zvýší za každé uvolněné IC o odpovídající hodnotu. Decker nemůže potlačit žádný program IC v systému, který opustil.

Stupně IC
Každý program IC má svůj vlastní stupeň. Tento stupeň je měřítkem poškození, které IC způsobuje. Slouží také jako cílové číslo pro testy, jimiž chce decker uniknout jeho účinkům. Kromě toho se používá pro některé vlastní testy, například pro test IC Vír, jež chce smazat soubor, nebo pro test IC, jež se pokouší zvýšit deckerovo bezpečnostní konto. Viz **Opatření proti vniknutí** níže.
V matrixovém boji provádí IC svůj útočný test pomocí hodnoty bezpečnosti hostu, která jakožto „dovednost“ udává počet dostupných kostek. Jinými slovy: host útočí na deckera a při tom používá IC jako zbraň.
Úroveň bezpečnosti hostu/souřadnic rovněž udává, kolik kostek má program IC k dispozici při testech odolnosti vůči poškození.

Kategorie IC
Existují tři rozdílné kategorie opatření proti vniknutí. Níže se nachází jejich stručný popis. Další informace pak obsahuje oddíl **Opatření proti vniknutí**.

Bílá
Bílé IC je naprogramováno k útokům na on-line ikonu deckera. Nemůže způsobit trvalé poškození ani deckerovi,ani jeho decku.

Šedá
Šedé IC má za úkol napadat deckerův kyberdeck a jeho užitkové programy. Tyto útoky mohou trvale poškodit příslušné komponenty.

Černá
Černé IC je speciálně naprogramováno k tomu, aby útočilo na samotného deckera tak, že způsobí nebezpečné zostření zpětné vazby mezi deckerem a jeho kyberdeckem. To může vést k trvalým tělesným nebo psychickým poškozením nebo dokonce ke smrti.

Systémové operace
Skoro každý úkol, který chce decker provést v kyberprostoru, se označuje jako systémová operace. Následující podkapitola pojednává o většině z nich. Pokud by decker chtěl vyzkoušet nějakou akci, která není v uvedeném seznamu obsažena, může gamemaster vytvořit vlastní systémové operace a již existující použít jako směrnice.
Z hlediska herních mechanismů není systémový test program ani dovednost, nýbrž prostě pravidlová procedura, s jejíž pomocí se určuje, zda se deckerovi úspěšně podaří provést zamýšlenou činnost. Každá systémová operace sestává ze tří částí: systémového testu, vhodného užitkového programu a určité herní akce.
Systémový test udává, v jakém dvojtestu musí decker obstát, aby mohl danou činnost vykonat: testu přístupu, ovládání, indexu, souboru nebo periférie. Pro každý z těchto testů se jako cílové číslo použije stupeň daného subsystému hostu nebo souřadnic. Všechny popisy užitkových programů udávají vhodné užitkové programy, jež mohou snížit cílové číslo v daném testu subsystému. V rámci dvojtestu hází gamemaster za host/souřadnice hodnotou bezpečnosti proti faktoru odhalení deckera (viz **Systémové testy**). V popisech je také vždy uveden požadovaný druh herní akce, nutný k provedení operace. Při tom se může jednat o volné, jednoduché nebo komplexní akce. Zcela jednoduché operace – jako zjištění jedné jediné informace, jedno jediné ovládání na virtuálním přeřazovacím panelu nějakého stroje apod. – jsou vesměs volné akce. Jedná se při nich o matrixové ekvivalenty takových činností, jako je otevření dveří nebo pohled z okna. U náročnějších operací jde o řídící proces určitého programu nebo ikony. Pro tento druh operací jsou zapotřebí zpravidla jednoduché akce. Každý úkol, při němž jde o vyhledávání, analýzu nebo ovládání mnohostranného nebo precizního procesu, je komplexní akcí.
Většinu operací lze rozdělit do tří kategorií: na dotazování, déletrvající operace a kontrolované operace.

Dotazování

U většiny systémových operací udělí decker hostu/souřadnicím příkaz, jejž systém okamžitě provede. Při dotazovacích operacích ovšem vstupuje decker se systémem do „dialogu“, aby se dozvěděl určitou informaci. Někdy musí decker takové dotazování provést více než jednou, aby nalezl požadovaný soubor nebo periferní přístroj. Je třeba si udržovat přehled o počtu úspěchů dosažených při dotazování. Jakmile decker získá pět nebo více úspěchů, podařilo se mu najít objekt svého pátrání. Gamemaster ale může posuzovat úspěchy při hledání určitých dat odděleně nebo dokonce vytvořit celý seznam dat, které decker postupně nalezne, jakmile vždy dosáhne určitého počtu úspěchů.

Čím precizněji si decker stanoví kritéria pro dotazování, tím větší je jeho naděje na úspěch. Postava by se měla cíleně vyptávat na jména, události nebo funkce, aby dosáhla úspěchu. Dotazování se v principu podobá pochůzkám ve fyzickém světě *Shadowrunu* – postava musí klást otázky tak dlouho, dokud neobdrží hledanou odpověď nebo se neukáže, že hledané informace jsou zcela nedostupné.

Pokud postava při dotazování bude pokládat vágní nebo všeobecné otázky, zvýší se cílové číslo o 1. Pokud je otázka extrémně vágní nebo obzvláště neurčitá, stoupne cílové číslo dokonce o 2. Za dobře zformulované, velmi věcné nebo prostě velmi jednoznačné otázky může cílové číslo klesnout o 1 nebo 2. Ale nezapomeňte: Počítač lze naprogramovat tak, že bude ukrývat data, ale nedovede lhát – a proto by měl mít decker, jenž sbírá v průběhu dobrodružství indicie, aby mohl položit šikovnou otázku, větší šanci než někdo, kdo stále tápe ve tmě.

Pokud se v daném hostu nebo souřadnicích hledané informace nenacházejí, měl by se to decker dozvědět, jakmile dosáhne alespoň tří úspěchů.

Kromě toho se deckerovi může klidně stát, že se po úspěšném dotazování dozví pouze adresu souboru nebo jiného hostu. Je dokonce možné, že bude muset takovéto odkazy sledovat přes vícero hostů, než konečně nalezne hledaná data (viz **Spojené databanky**).

O dotazování se jedná u následujících operací: lokalizace přístupu, lokalizace souboru, lokalizace periférie.

Grid Reaper a jeho přátele podnikají run na jisté podnikové zařízení. Reaper střeží matrix. Přes vysílačku se dozví, že jeho přátelé jsou lapeni v místnosti, do níž proudí uspávací plyn. Pokud rychle něco nepodnikne, bude z nich žrádlo pro pekelné psy.

Aby mohl Reaper deaktivovat plynovou past, musí nejprve nalézt periferní subsystém, který ji ovládá, což je dotazovací operace. Provede operaci „lokalizace periférie“. Protože zná přesnou polohu periferního zařízení a ví, jaký má účel, sníží gamemaster cílové číslo o 1. Reaper dosáhne sice jen jednoho úspěchu, má však alespoň stopu, po níž může jít. Jeho přátelé brzy upadnou do bezvědomí, takže pokračuje v dotazování. Při svém dalším testu dosáhne čtyř úspěchů a periferní přístroj nalezne. Bohužel nemá čas, aby ho vypnul, jelikož spustil IC. Reaper (a jeho přátelé) mají smůlu…

Déletrvající operace

Některé operace jsou uzavřené ve chvíli, kdy decker provede svůj systémový test. Jiné operace, jako nakládání nebo vykládání dat, potřebují čas. Takovéto déletrvající operace decker spustí a pak je nechá běžet, aniž by musel udílet další pokyny.

Čas nutný pro déletrvající operaci se měří ve vteřinách a určí se podle pravidel pro danou operaci. Pokud se operace děje v interakci s jinými událostmi, měl by gamemaster vypočítat přesný moment v průběhu bojového kola, kdy dojde k jejímu ukončení.

K převodu sekund na bojová kola vydělte počet vteřin 3. Příklad: John nakládá užitkový program a potřebuje na to 6 vteřin. Tento čas odpovídá dvěma bojovým kolům. Pokud začne s nakládáním užitkového programu na počátku třetího bojového kola, může ho od začátku pátého kola používat. Pokud by nakládání trvalo 7 vteřin, odpovídalo by dvěma bojovým kolům se zbytkem 1 vteřiny. V tomto případě by John nemohl daný program použít před svou druhou bojovou fází v pátém kole. Nakládací čas 8 vteřin odpovídá dvěma bojovým kolům se zbytkem dvou vteřin, což znamená, že John bude moci svůj program použít až ve své třetí bojové fázi v pátém kole.

O déletrvající operace se jedná v následujících případech: vykládání souboru, výměna obsahu paměti, nakládání souboru.

Kontrolované operace

Na kontrolované operace je po jejich započetí nutno pečlivě dohlížet. Poté, co je decker úvodním systémovým testem uvede do chodu, musí v každém průběhu iniciativy použít jednu volnou akci, aby v nich pokračoval.

Opomene-li byť i jen jednou tuto volnou akci investovat, operace se přeruší; v tomto případě musí decker systémový test zopakovat, aby danou operaci znovu spustil.
V některých případech může přerušení kontrolované operace vést k nevratným následkům v reálném světě. Vezměme si příklad deckera, který pomocí operace „editování periférie“ brání tomu, aby živé stráže spatřily v bezpečnostní kameře, jak se jeho druhové vloupávají do jejich objektu. Pokud by decker dopustil, aby se operace přerušila, stráže jeho přátele s velkou pravděpodobností odhalí a jejich run selže, ne-li něco horšího.
O kontrolované operace se jedná u následujících: řízení periférie, editování periférie, vedení rozhovoru, dohlížení na periférii, napíchnutí rozhovoru.

Popis operací

Následující text nabízí podrobné informace o doposud dostupných systémových operacích. Gamemaster by měl mít dostatek volnosti, aby mohl navrhovat dodatečné systémové operace, pokud to vyžadují zamýšlené akce hráče deckera.

Editování souboru
Test: soubor
Užitkový program: Pročítač/zapisovač
Akce: jednoduchá
S pomocí této operace může decker vytvořit, změnit nebo vymazat určitý soubor. Malé změny (např. „korektura“ tiskové řádky) je možné pomocí této operace provést přímo na hostu. V případě, že má dojít k větší změně dat, je však třeba nový materiál nejprve připravit off-line, následně ho vyložit a poté provést operaci „editování souboru“, kterou se soubor umístí na zamýšlenou pozici. Vyložené informace mohou být – bez ohledu na velikost – umístěny pomocí jediné operace „editování souboru“.
Nové soubory se vytvářejí pomocí úspěšného testu souboru. Protože však tyto soubory nemají legální zápis, může je systém kdykoli zase smazat.
Tato operace rovněž umožňuje deckerovi ukládat na tom samém hostu kopie souborů. Tak je tedy možné zkopírovat soubor z obzvláště zabezpečené databanky, tuto kopii následně uložit na nějaké méně zabezpečené místo v tomtéž hostu a později si ji vyzvednout. Za tímto účelem je třeba provést dva systémové testy: nejprve test souboru, poté test subsystému, do nějž chce decker zkopírovaný soubor ukrýt.
Po změně, manipulaci nebo smazaní souboru musí decker podstoupit test ovládání proti cílovému číslu, jež je sníženo o stupeň jeho programu Pročítač/zapisovač. Tímto způsobem je potvrzena hlavička souboru jako originál. Pokud decker v tomto testu neuspěje, musí podstoupit test maskování proti stupni souboru. Počet úspěchů udává, kolik hodin uplyne, než si host povšimne nedovolených změn v souboru a upozorní dohlížejícího na tuto manipulaci.
Decker může také zjistit, zda host nebo jiný decker nemanipulovali s určitým souborem. Pokud se souborem manipuloval bez oprávnění decker, jehož test ovládání na opravu hlavičky selhal, stačí k všimnutí si manipulace pouze úspěšný test souboru. Pokud byla hlavička úspěšně verifikována, musí při testu souboru padnout více úspěchů než při testu ovládání deckera, který se souborem manipuloval.
Ale pozor: Vždy, když decker smaže nějaký soubor, musí gamemaster zvážit dopad tohoto procesu na dobrodružství; neboť na tom závisí zase rozhodnutí, zda existují eventuelní záložní kopie tohoto souboru.

Dekódovaní souboru
Test: soubor
Užitkový program: Dekodér
Akce: jednoduchá
Operace dekódování souboru má za cíl porazit IC Vír, které střeží nějaký soubor. Aby bylo možné u takto zabezpečeného souboru provést nějakou další operaci, je třeba nejprve uspět v „dekódování souboru“. Před dekódování není možné takový soubor ani naložit.

Lokalizace souboru
Test: index
Užitkový program: Prohlížeč
Akce: komplexní
U této operace se jedná o dotazování: jako cíl hledání figurují určité soubory. Pro provedení této operace musí mít decker určitou představu o tom, co vlastně hledá – „cenná data“ nestačí.
Pokud tato operace proběhne úspěšně, dozví se decker systémovou adresu souboru.

Naložení souboru
Test: soubor
Užitkový program: Pročítač/zapisovač
Akce: jednoduchá
Tato operace umožňuje deckerovi zkopírovat soubor z hostu do jeho kyberdecku. Data se přesunují rychlostí, která je dána deckerem nastavenou rychlostí I/O. Je možné je přenášet do aktivní paměti, paměťové banky nebo do off-line paměťové banky.
„Nakládání dat“ je déletrvající operace, která trvá tak dlouho, dokud není přenos dat ukončen, decker se neodhlásí nebo se jeho ikona nezhroutí či proces nakládání není předčasně přerušen. Pokud dojde k zastavení operace před ukončením přenosu, vznikne poškozená a neužitečná kopie daného souboru.
Pokud ovšem soubor obsahuje informace obzvláštního významu pro dobrodružství, může gamemaster stanovit, že díky neúplnému nakládání vznikla poškozená, ale čitelná kopie. Základní čas pro rekonstrukci poškozeného souboru se určí následovně:
(Úplná velikost dat v Mp, dělená množstvím naložených dat v Mp) x 2
Výsledek udává základní čas ve dnech. Jakmile je poškozený soubor rekonstruován, určí gamemaster, zda obsahuje hledané informace tak, že vydělí velikost naloženého souboru velikostí originálního souboru.
Příklad: Deckerovi se podaří naložit 10 Mp dat ze souboru o velikosti 100 Mp. Základní čas pro rekonstrukci souboru činí (100 : 10) x 2 = 20 dní. Když se 10 vydělí 100, dostaneme 0,1 – takže existuje desetiprocentní pravděpodobnost, že zkopírovaná data obsahují požadované informace.

Vyložení souboru
Test: soubor
Užitkový program: Pročítač/zapisovač
Akce: jednoduchá
Tato operace deckerovi umožňuje přenést data ze svého kyberdecku do matrixu. Tato data vycházejí přímo z paměťové banky decku a nemají vliv na aktivní paměť.
Pokud decker ukládá nový soubor do hostu, ten se automaticky zapíše. Pokud by chtěl modifikovat již existující soubor hostu – například doplnit databanku o falešné údaje – musí provést po ukončení vykládání operaci „editování souboru“.
Nezapomeňte, že operace „vyložení souboru“ neslouží k vykládání užitkových programů. K této funkci je určená operace „výměna obsahu paměti“.
Operace „vyložení souboru“ je déletrvající operace.

Lokalizace deckera
Test: index
Užitkový program: Skener
Akce: komplexní
Operace „lokalizace deckera“ zahrnuje dva kroky. Decker hází běžný systémový test a následně otevřený test senzorů. Decker lokalizuje všechny deckery, jejichž stupeň maskování je nižší nebo roven výsledku jeho testu senzorů. Navíc se dozví, když se tito odhlásí nebo odpojí. Pokud má cílový decker spuštěný užitkový program Plížení, přidává se jeho stupeň k jeho hodnotě maskování pro určení toho, zda ho decker provádějící operaci „lokalizace deckera“ odhalí.
Lokalizovaní deckeři mohou kontakt přerušit, provedou-li jistý manévr (viz **Bojové manévry**).
Spřátelení deckeři, kteří se chtějí navzájem informovat o své přítomnosti, tak mohou učinit automaticky.

Elegantní odhlášení
Test: přístup
Užitkový program: Klamání
Akce: komplexní
Operace „elegantní odhlášení“ umožňuje deckerovi ukončit bez rizika děrového šoku spojení s hostem nebo souřadnicemi, přes něž se připojil do matrixu.
Úspěšné provedení této operace dále smaže veškeré stopy deckera a jeho činnosti v bezpečnostních systémech a databankách hostu. Pokud se v lokalizačním cyklu nachází užitkový program Stopař, přičítá se jeho stupeň k cílovému číslu pro test na „elegantní odhlášení“.

Napíchnutí rozhovoru
Test: zvláštní
Užitkový program: Komunikátor
Akce: komplexní
Tato operace deckerovi umožňuje lokalizovat v daných LTS komunikační kódy a vystopovat a napíchnout rozhovory. Pro všechny testy, jež přicházejí pro tuto kontrolovanou operaci v úvahu, lze použít užitkový program Komunikátor.
Aby mohl decker lokalizovat aktivní komunikační kód nějakých LTS, musí se nacházet v RTS, jež dané LTS ovládají. Provádí test indexu, aby se zjistilo, zda nějaké komunikační kódy v daných LTS právě vytvářejí nějaké aktivní spojení, případně se o takové spojení s nimi někdo pokouší. Pokud decker prověřuje nějaký určitý komunikační kód, musí se nejprve vydat do mateřských RTS tohoto komunikačního kódu a obdrží modifikátor –2 k cílovému číslu pro test indexu. Pokud decker nalezne aktivní kód, může provést test ovládání, aby mohl sledovat hovor do místa jeho původu nebo na místo určení. Pokud je komunikačním kódem spojeno v konferenčním modu více účastníků, dozví se decker za každý úspěch v tomto testu komunikační kód jednoho z účastníků.
Pokud je spojení navázáno jiným deckerem pomocí operace „vedení rozhovoru“, test ovládání tohoto deckera lokalizuje. Decker, jenž chce rozhovor napíchnout, musí vyhledat RTS volajícího deckera a použít proti němu užitkový program Stopař; použití Stopaře se považuje za útok a odhalí přítomnost deckera, který tento užitkový program používá. Pokud se Stopař úspěšně prosadí, vyhledá poté všechny ostatní komunikační kódy, které se na spojení podílejí.
Pokud se chce decker na rozhovor napíchnout a nahrát ho do paměťové banky decku nebo off-line paměťové banky, musí provést test souboru. Každá minuta nahrávání zabere 1 Mp paměti.
Pokud je spojení zakódováno, musí ho decker nejprve dekódovat tak, že provede srovnávací test svou dovedností počítače proti stupni systému kódování dat. Užitkový program Dekodér snižuje deckerovo cílové číslo. Počet připojení a kódovacích přístrojů nemá vliv na deckerovo cílové číslo. Pokud první test dekódování selže, může to decker zkusit znovu; cílové číslo ovšem vzrůstá po každém neúspěšném pokusu o 2. Žádný z deckerových testů zaměřených proti zakódování nemá vliv na jeho bezpečnostní konto v daných RTS.
Pokud má některá z přípojek účastnících se rozhovoru k dispozici snímač datových linek, může ho decker spustit, i když samotný poplach v RTS neaktivuje. Snímače datových linek mají stupně mezi 1 a 10. Jakmile decker rozhovor napíchne, musí provést srovnávací test počítačů proti stupni snímače datových linek (užitkový program Komunikátor snižuje jeho cílové číslo). Zvítězí-li decker, podařilo se mu synchronizovat nepatrné fluktuace integrity signálu, jež byly způsobeny napíchnutím rozhovoru, a snímač oklame. Pokud se při rozhovoru používá více snímačů datových linek, používá se pro test stupeň nejvyššího z nich. V tomto případě potřebuje decker jeden úspěch za každý použitý snímač, jinak některé přístroje (patrně ty dražší) místo jeho napíchnutí odhalí. Ať už se tento test zdaří nebo ne, deckerovo bezpečnostní konto v RTS zůstane beze změny.
Jakmile decker nějaký rozhovor napíchne a dekóduje, může ho odposlouchávat a nahrávat. Když je rozhovor ukončen, může zůstat nadále napojen v některém komunikačním kódu – buď v tom prvním, který původně hledal, nebo v jednom z vystopovaných. Pak se může pokusit sledovat další hovory, které budou z tohoto kódu vycházet. Jestliže bude decker sledovat již napíchnuté připojení, nemusí házet žádný test indexu, aby zjistil, kdy bude toto číslo znovu aktivní. Musí ovšem podstoupit nový test, pokud chce vysledovat nebo napíchnout nové hovory, stejně jako se vypořádat se snímači datových linek nebo zakódovanými hovory.
Decker může svou přítomnost rovněž zveřejnit a do napíchnutého rozhovoru se připojit, příp. některému z účastníků rozhovoru přerušit spojení. Za tímto účelem musí provést operaci „vedení rozhovoru“ (test souboru modifikovaný užitkovým programem komunikátor).
„Napíchnutí rozhovoru“ je kontrolovaná operace.

Vedení rozhovoru
Test: soubor
Užitkový program: Komunikátor
Akce: komplexní
Touto operací může decker, který se nachází v jedněch určitých RTS, zavolat na jakýkoli komunikační kód podřízených LTS. Tato operace ovšem neslouží pouze k převezení zpoplatněných přípojek. Decker může uskutečnit hovor, pokračovat do jiných RTS, pak zavolat na číslo pod jejich kontrolou a obě přípojky spojit dohromady. Tímto způsoben je možné pro vytvoření zajištěného konferenčního modu vybrat více RTS. Za každou přípojku, kterou decker zařadí do spojení, musí provést další test souboru.

Deckeři mohou také získat licenci pro poskytování těchto služeb různým RTS. V tomto případě obdrží od provozovatele RTS heslo, které je k tomu zplnomocňuje. V tomto případě nejsou pro výběr spojení a vytváření konferencí nutné žádné testy. Tyto licence však obvykle dostávají pouze podnikoví deckeři. Proti takovým rozhovorům nemá operace „napíchnutí rozhovoru“ žádný účinek, ovšem jiný decker může použít užitkový program Stopař, aby lokalizoval komunikační kódy účastníků (další informace viz **Napíchnutí rozhovoru**).
Dále může vytvářející decker odhalit všechny datové štěnice nebo stopovací přístroje, pokud provede svými senzory srovnávací test proti stupni přístroje. Pomocí dalšího srovnávacího testu (stupeň úniku versus stupeň přístroje) je může neutralizovat. Deckeři často vyvářejí rozhovory zajištěné proti odposlechu – přitom se jedná o lukrativní vedlejší zaměstnání: běžný poplatek za takovéto služby činí 100 ¥ za volajícího a minutu.
„Vedení rozhovoru“ je kontrolovaná operace.

Analýza hostu
Test: ovládání
Užitkový program: Analyzátor
Akce: komplexní
Touto operací může decker analyzovat stupně hostu. Za každý čistý úspěch v testu ovládání se decker dozví jednu z následujících informací:

- stupeň bezpečnosti hostu (úroveň a hodnotu)
- stupeň jednoho ze subsystému hostu

Při sedmi nebo více úspěších získá decker všechny informace. Je třeba připomenout, že se musí zdržovat v hostu, aby mohl proti systému provést operaci „analýza hostu“; není možné pouze trochu zavětřit ze souřadnic.

Analýza IC
Test: ovládání
Užitkový program: Analyzátor
Akce: volná
Operace „analýza IC“ deckerovi umožňuje analyzovat určitý program IC, který již předtím lokalizoval (deckeři IC lokalizují provedením operace „lokalizace IC“ nebo pokud je program IC napadne). Pokud se deckerovi operace zdaří, dozví se typ, stupeň a všechny možnosti obrany daného programu IC.

Analýza ikony
Test: ovládání
Užitkový program: Analyzátor
Akce: volná
Operace „analýza ikony“ prozkoumá ikonu a odhalí její obecné zařazení: IC, persona, užitkový program apod. cílové číslo pro test je stupeň ovládání, snížený o stupeň senzorů a případně užitkový program Analyzátor. I v tomto případě však nesmí cílové číslo nikdy klesnout po dvě.

Lokalizace IC
Test: index
Užitkový program: Skener
Akce: komplexní
Tato operace se řídí stejnými pravidly jako operace „lokalizace deckera“. Úspěšný systémový test vede ovšem automaticky k lokalizaci IC – decker nepotřebuje žádný dodatečný test senzorů. Decker je o poloze IC informován tak dlouho, dokud IC neprovede manévr, aby odhalení uniklo.

Přihlášení do hostu
Test: přístup
Užitkový program: Klamání
Akce: komplexní
Operace „přihlášení do hostu“ sestává zkrátka z normálního systémového testu. Při tom se zohledňují všechny vhodné modifikátory a neměli byste zapomenout okamžitě přidat k bezpečnostnímu kontu deckera všechny úspěchy, které hostu padnou v testu bezpečnosti.
Decker nezná stupeň přístupu hostu do té doby, dokud nepodnikne svůj první pokus o přihlášení. V tu chvíli se stupeň ukáže velmi rychle a není důvod s tím dělat nějaké velké tajnosti.

Jakmile se deckerovi zdaří test přístupu, spatří virtuální prostředí hostu. Pokud si decker zjednal přes pracovní stanici přímý přístup do systému, může se jeho ikona vynořit přímo ve scenérii, jež odpovídá vstupnímu/výstupnímu portu. S přihlédnutím k dnešním převládajícím modelovaným systémům může tato scenérie vypadat samozřejmě zcela jedinečně.
Pokud se decker dostane do systému skrze periferní přístroj, vstoupí jeho ikona do ovladače periférie; přístup přes konzolu zavede deckera přímo do srdce uzlu centrální procesorové jednotky. Tato virtuální místa nemají žádný účinek na deckerovy testy, poskytují ovšem gamemasterovi náměty pro popis okolí.
Jakmile se decker nachází v hostu, může provádět všechny operace, které jsou v jeho profesi běžné – například analýzu hostu a jeho obranných zařízení, vyhledávání hodnotných dat, předělávání souborů apod.

Přihlášení do LTS
Test: přístup
Užitkový program: Klamání
Akce: komplexní
Tato operace sestává z prostého systémového testu proti stupni přístupu LTS. Nezapomeňte hned otevřít deckerovo bezpečnostní konto všemi úspěchy, jichž souřadnice dosáhnou ve svém testu bezpečnosti. Dopadne-li test neúspěšně, deckerův pokus o přihlášení do LTS selže. Může to zkusit znovu, ale neměl by zapomínat, že jeho bezpečnostní konto zůstane po určitou dobu v souřadnicích zachováno (za normálních okolností si veřejné LTS „pamatují“ neoprávněné pokusy o přihlášení 1k3 x 5 minut). Další pokus o přístup se samozřejmě může odehrát na jiné přípojce, což znamená, že souřadnice musí pro deckera zřídit nové bezpečnostní konto.
Jakmile decker v dvojtestu uspěje, objeví se jeho ikona v důvěrně známém prostředí LTS. Z LTS se může přihlásit do RTS nebo do SLTS, jež jsou spojeny s těmito LTS (za předpokladu, že zná adresu) nebo do nějakého hostu, jenž je s těmito LTS spojen (také v tomto případě musí znát adresu hostu).

Připojení do RTS
Test: přístup
Užitkový program: Klamání
Akce: komplexní
Jakmile se decker přihlásí do LTS, může se pomocí této operace přihlásit do nadřazených RTS. Tuto operaci musí provést, pokud chce navázat spojení s jinými LTS ve stejných RTS nebo se chce dostat přímo do jiných RTS.
Při provádění této operace podstupuje decker systémový test proti stupni přístupu RTS. Myslete na to, že „místní“ výkyvy stupňů systémů LTS nemají vliv na RTS. Gamemaster může samozřejmě použít přechodné kolísání stupňů RTS.
Nezapomeňte také, že RTS vedou pro deckera jednotné bezpečnostní konto za všechny deckerovy akce v podřízených LTS, stejně jako v RTS samotných.
Jakmile se decker nachází v RTS, může se přihlásit do všech podřízených LTS nebo do jiných RTS kdekoli na světě.

Nulová operace
Test: ovládání
Užitkový program: Klamání
Akce: komplexní
Gamemaster může od deckera vyžadovat provedení jedné nebo více nulových operací, a sice pokaždé, když postava na něco čeká – ať už na událost v matrixu, konec déletrvající operace nebo něco jiného, co deckera nutí k tomu, aby nečinně (tj. bez provádění systémových operací) pobýval v matrixu. Gamemaster může nulovou operaci vyžadovat tehdy, pokud decker dělá něco, k čemu sice potřebuje akce, ale nikoli systémové testy – například pokud udržuje operaci „editování periférie“. Pokud gamemaster chce, může provádět nulové operace místo deckera, a sice skrytě.
Jestliže decker zůstane v hostu neaktivní méně než deset vteřin, hází se dvojtest proti běžné hodnotě bezpečnosti hostu. Je-li nečinný více než deset vteřin, ale méně než minutu, vzrůstá hodnota bezpečnosti o 1. Pokud je tato doba kratší než jedna hodina, ale delší než minuta, stoupá hodnota bezpečnosti o 2. Je-li to méně než dvanáct hodin, ale více než hodina, vzrůstá hodnota bezpečnosti o 4. Každých dalších dvanáct hodin zvyšuje hodnotu bezpečnosti o další bod. Gamemaster může stanovit maximální hranici nečinnosti a při tom se orientovat podle schopnosti deckera bojovat během takto nerozumně dlouhé doby se spánkem.

Selena začíná s procesem nakládání, který zabere dvanáct vteřin. Nic dalšího nemá v plánu, takže prostě vyčkává. Gamemaster od ní požaduje nulovou operaci a přidá k hodnotě bezpečnosti hostu +1.
Při jednom z dalších runů čeká Selena na to, až její pozemní tým překoná zamčené dveře (nejsou tyto dveře na kliku bez počítačového ovládání zámku prostě otravné?). Gamemaster rozhodne, že rozlousknutí magnetického zámku zabere sedm minut. Hází si za Selenu skrytou nulovou operaci a pro tento dvojtest zvýší hodnotu bezpečnosti hostu o 2. Při testu bezpečnosti padne více úspěchů, které Selenino bezpečnostní konto zvýší nad další aktivační práh, čímž se aktivuje jeden opravdu zlomyslný program IC. Gamemaster rozhodne, že se toto IC objeví teprve po třech minutách čekání.

Pokud test bezpečnosti zvýší deckerovo bezpečnostní konto a spustí reakci hostu, měl by gamemaster určit reakční čas podle vlastního uvážení – třeba po určité části vyčkávacího testu deckera.

Editování periférie
Test: periférie
Užitkový program: Podvodník
Akce: komplexní
Pomocí kontrolované operace „editování periférie“ může decker modifikovat data, která jsou vysílána k perifernímu přístroji nebo která tento přijímá. Decker může tuto operaci například provést, aby upravil videosignály nebo senzorická data počítačem řízeného bezpečnostního systému nebo data zasílaná konzole nebo simulátoru.

Dekódování periférie
Test: periférie
Užitkový program: Dekodér
Akce: jednoduchá
Tato operace slouží k porážce IC Vír na periferním subsystému. Decker může provádět testy proti zakódovanému systému periférie až poté, co úspěšně provede tuto operaci.

Lokalizace periférie
Test: index
Užitkový program: Prohlížeč
Akce: komplexní
Dotazovací operace „lokalizace periférie“ se řídí stejnými pravidly jako operace „lokalizace souboru“ (viz **Lokalizace souboru**). Tato operace se používá ke zjištění systémové adresy určitého periferního přístroje, který host řídí. Vágní dotaz by zněl: „Najdi všechny bezpečnostní kamery, které tento počítač řídí.“ Přesně formulovaná otázka by zněla: „Najdi kamery, jež střeží dveře, které vedou ve třetím patře k východnímu schodišti.“
Na druhé straně spravuje většina hostů pravděpodobně daleko méně periferních přístrojů než souborů; z tohoto důvodu potřebuje decker při testu indexu k lokalizaci žádaného systému pouze tři úspěchy. Jakmile je periferní přístroj nalezen, může s ním decker provádět operace jako „řízení periférie“ nebo „editování periférie“.

Řízení periférie
Test: periférie
Užitkový program: Podvodník
Akce: komplexní
Operace „řízení periférie“ deckerovi umožňuje převzít řízení periferního přístroje, jenž je podřízen subsystému periférie daného hostu. Při tom se může jednat o všechno možné, od prostých automatických bezpečnostních dveří a výtahů po celé autonomní továrny plné automatických výrobních zařízení.
Pokud se decker pokouší převzít řízení průmyslového nebo vědeckého procesu, který subsystém periférie ovládá, musí provést test periférie s dovedností, rovnající se průměru stupňů jeho dovednosti počítače a K/O dovednosti nebo vědomosti, jež přiměřeně odpovídá danému procesu (zaokrouhleno dolů). Pokud by chtěl například převzít automatizovanou lékařskou laboratoř, musel by použít průměr svých počítačů a biotechniky, počítačů a medicíny, příp. počítačů a nějaké jiné podobné dovednosti. Gamemaster by měl v tomto případě stanovit přísná měřítka, jaké dovednosti jsou relevantní, obzvláště pokud se decker pokouší o něco, co volá po nějaké obskurní specializaci.
„Řízení periferie“ je kontrolovaná operace.

Sledování periférie
Test: periférie
Užitkový program: Podvodník
Akce: jednoduchá
Pomocí této kontrolované operace může decker číst data, která jsou vysílána nějakým periferním přístrojem. Takto může odposlouchávat zachycené akustické signály, prohlížet si nahrávky z bezpečnostních kamer, prozkoumat záznamy počítačového skeneru, který je propojen s hostem, apod. Dokud tuto operaci udržuje, dostává od přístroje nepřetržitě aktualizovaná data.

Analýza zabezpečení
Test: ovládání
Užitkový program: Analyzátor
Akce: jednoduchá
Je-li tato operace úspěšně provedená, dozví se decker aktuální stupeň bezpečnosti hostu, stav vlastního bezpečnostního konta v tomto hostu (včetně všech bodů, které získá teprve při operaci „analýza zabezpečení“), stejně jako poplachový stav hostu.

Výměna obsahu paměti
Test: žádný
Užitkový program: žádný
Akce: jednoduchá
Pomocí této operace může decker naložit do aktivní paměti decku nový užitkový program a následně ho naložit do své on-line ikony. Naložení užitkového programu do aktivní paměti je jednoduchá akce – decker prostě decku nařídí, aby tuto činnost provedl. Pokud v aktivní paměti není dostatek místa pro nový program, musí decker nejprve použít volnou akci, aby nějaký program z aktivní paměti odstranil. Tyto akce nevyžadují žádné testy.
Jakmile je užitkový program naložen v aktivní paměti, začíná deck automaticky s jeho vykládáním do on-line ikony. Podrobnosti o tom, kdy přesně je užitkový program pro personu dostupný, naleznete v oddílu **Udržované operace**.

Analýza subsystému
Test: odpovídající subsystém
Užitkový program: Analyzátor
Akce: jednoduchá
Tato operace analyzuje všechno možné, co se vyskytuje v daném subsystému vedle běžných parametrů. Touto operací může decker zjistit, zda jsou v analyzovaném subsystému padací dveře, červi, program IC Vír nebo jiné obranné nebo systémové triky.

Dekódování přístupu
Test: přístup
Užitkový program: Dekodér
Akce: jednoduchá
Tato operace slouží k poražení IC Vír, které střeží přístup do hostu. Programy IC v zakódovaném SPU je třeba nejprve vyřadit operací „dekódování přístupu“, než bude decker vůbec moci v takovém SPU provést operaci „přihlášení do hostu“.

Lokalizace přístupu
Test: index
Užitkový program: Prohlížeč
Akce: komplexní
Operace „lokalizace přístupu“ je jistým druhem „informací po telefonu“ ve stylu Šestého světa. Umožňuje deckerovi nalézt kódy LTS, které mu zjednají přístup k zamýšlenému hostu. Touto operací lze najít i komunikační kódy pro běžné telefonní rozhovory.
K cílovému číslu testu indexu se přidává modifikátor, který závisí na ohlášeném cíli deckerova snažení. Pokud například zná pouze jméno podniku nebo jednotlivce („Hledám systém Mitsuhamy.“), platí modifikátor +1. Pokud svůj záměr dokáže formulovat konkrétněji („Hledám systém oddělení pro styk s veřejností Mitsuhamy.“),

zůstává cílové číslo beze změn. Pokud dokáže jednoznačně určit daný cíl („Hledám systém oddělení pro styk s veřejností pobočky Mitsuhamy v Bellevue na LTS SEA-5029.“), snižuje se cílové číslo dokonce o 1.
Jakmile decker odhalí kód LTS, nemusí už v budoucnu provádět operaci „lokalizace přístupu“, aby tento host znovu nalezl – samozřejmě jen tehdy, pokud vlastník nezmění adresu.
„Lokalizace přístupu“ je dotazovací operace.

Užitkové programy

Teoreticky by mohl dostatečně inteligentní decker manipulovat matrixem pouze pomocí své persony a své dovednosti. Méně nadaní síťaři musí ovšem své skromné schopnosti podpořit užitkovými programy. Užitkové programy existují ve čtyřech formách: operační, speciální, útočné a obranné. Operační užitkové programy podporují deckerovy systémové testy. Jako obzvláště užitečné se ukazují být u systémových operací; odtud také jejich jméno. Speciální užitkové programy jsou vhodné pro zvláštní matrixové úkoly. Útočné užitkové programy slouží k způsobování poškození nepřátelským deckerům, programům IC apod. Obranné užitkové programy mají zcela zabránit nebo alespoň snížit vlastní poškození v boji v matrixu.
Násobitel uvedený u každého programu se používá k určení velikosti programu (viz tabulka **Velikost programů**). Popis rovněž udává, pro jaké systémové operace je daný užitkový program použitelný (popisy a pravidla pro systémové operace viz **Systémové operace** výše).
Užitkové programy existují ve dvou formátech: jako originály nebo jako kopie. Aby bylo možné program upgradovat nebo modifikovat, musí decker vlastnit zdrojový kód programu (viz také **Zdrojový a objektový kód**).
Pokud není uvedeno jinak, musí mít decker užitkový program naložen v aktivní paměti, aby ho mohl používat.

Operační užitkové programy

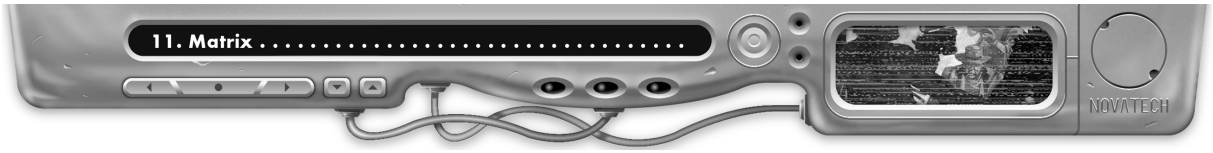
Tyto programy pomáhají deckerovi při provádění systémových operací, tak jako samurajův smartspoj činí ze zbraně efektivní náčiní nebo jako podkožní pancíř podporuje jeho pancéřovanou bundu. Operační užitkové programy snižují cílové číslo systémových testů o svůj stupeň (viz **Systémové testy**). Deckeři mohou samozřejmě provádět své systémové operace i bez užitkových programů (viz **Systémové operace**) – pokud člověk nemá ten správný program, není díky tomu operace nenožná, ale pouze těžší.

Analyzátor
Násobitel: 3
Systémové operace: analýza IC, analýza hostu, analýza ikony, analýza zabezpečení, analýza subsystému
Užitkový program Analyzátor snižuje cílová čísla operací, při nichž jde o identifikaci IC, programů a dalších prostředků nebo událostí, které daný host řídí.

Dekodér
Násobitel: 1
Systémové operace: dekódování přístupu, dekódování souboru, dekódování periférie
Užitkový program Dekodér snižuje cílová čísla všech systémových testů, v nichž jde o překonání IC Vír.

Komunikátor
Násobitel: 1
Systémové operace: vedení rozhovoru, napíchnutí rozhovoru
Užitkový program Komunikátor snižuje cílová čísla u všech testů, jež se vztahují na komunikační spojení deckera.

Pročítač/zapisovač
Násobitel: 2
Systémové operace: naložení souboru, editování souboru, vyložení souboru
Užitkový program Pročítač/zapisovač snižuje cílová čísla všech systémových testů, které jsou nutné pro přenos souborů, a všech ostatních systémových testů, které připadají v úvahu při matrixovém získání přístupu k souboru, jeho editování nebo vytvoření.



Skener
Násobitel: 3
Systémové operace: lokalizace deckera, lokalizace IC
Užitkový program Skener snižuje cílové čísla všech systémových testů, jež slouží k pátrání po deckerech nebo IC.

Prohlížeč
Násobitel: 1
Systémové operace: lokalizace přístupu, lokalizace souboru, lokalizace periférie
Užitkový program Prohlížeč snižuje cílová čísla testů indexu, které slouží k lokalizaci určitých dat nebo systémových adres. Na rozdíl od Analyzátoru a Skeneru, jež pátrají po matrixových aktivitách, působí Prohlížeč na obsah nebo funkce datových uzlů v reálném světě.

Podvodník
Násobitel: 3
Systémové operace: řízení periférie, editování periférie, sledování periférie
Užitkový program Podvodník snižuje cílová čísla všech testů, při nichž jde o ovlivnění systému a subsystému periférie.

Klamání
Násobitel: 2
Systémové operace: elegantní odhlášení, přihlášení do hostu/LTS/RTS, nulová operace
Pokud není uvedeno jinak, slouží Klamání ke snižování cílových čísel při všech testech přístupu.

Odbočka
Násobitel: 2
Tento užitkový program se používá proti programu Stopař, jenž je zapojen do lokalizačního cyklu. Unikající a stopující decker provádějí vzájemný dvojtest. Decker se spuštěnou Odbočkou provádí test počítačů proti cílovému číslu ve výši protivníkových senzorů mínus stupeň svého užitkového programu Odbočka. Decker používající Stopaře provádí test HPOP proti stupni odbočky. Zvítězí-li unikající decker, stopovací program při hledání totálně selže. Útočník musí cílového deckera znovu napadnout, než bude smět použít svůj užitkový program Stopař.

Speciální užitkové programy

Speciální užitkové programy provádějí zvláštní úkoly, jež není možné zařadit do následujících kategorií (útočné a obranné programy).

Stopař
Násobitel: 8
Stopař je vyhledávací program, který se používá jako bojový program proti nepřátelským deckerům. Po každém úspěšném útoku si poznamenejte počet úspěchů, kterých dosáhl útočící decker. Cílový decker hází test úniku s cílovým číslem ve výši stupně Stopaře. Pokud při tomto testu nedosáhne alespoň tolika úspěchů jako útočník, přilepí se Stopař na jeho datovou stopu a zahájí svůj lokalizační cyklus. Vydělte 10 počtem čistých úspěchů, abyste určili počet bojových kol, které potřebuje Stopař k nalezení deckerovy přípojky. Při měření lokalizačního cyklu se počítají pouze celá bojová kola, zbytky se ignorují. Pokud decker dokáže tento program zničit před posledním průběhem iniciativy bojového kola, toto kolo se nezapočítává.
Cílový decker se může pokusit útočícímu deckerovi uniknout, pokud se odhlásí nebo odpojí. Program Stopař ztěžuje operaci odpojení.
Proti Stopaři může cílový decker použít užitkový program Odbočka (viz **Odbočka**).
Cílový decker má samozřejmě stále možnost přivést útočící personu a tím také všechny její nepříjemné programy ke zhroucení.

Plížení
Násobitel: 3
Užitkový program Plížení určuje spolu se stupněm maskování decku deckerův faktor odhalení: (maskování + Plížení) : 2 (zaokrouhleno nahoru).

Útočné užitkové programy

Útočné užitkové programy poškozují ikony deckerů, programy IC, spuštěné programy, soubory dat – tedy skoro všechno. Některé útočné užitkové programy – například Úder – jsou brutální a destruktivní viry. Jiné jsou jemnější a ve svých možnostech omezenější. Následující popisy útočných užitkových programů udávají cíle, na než daný program může útočit.
Úder
Násobitel: lehká 2, střední 3, vážná 4, smrtelná 5
Cíle: persony, IC
Tento nejtvrdší útočný program lze naprogramovat na určitou úroveň poškození – od lehké po smrtelnou. Sonduje příkazové algoritmy cílové ikony a pokouší se implantovat opravdu velké paměťové chyby do kódových segmentů, které jsou nejčastěji používané. V boji v matrixu se tento proces zaznamenává jako přímý útok do kondičního záznamníku persony nebo ikony IC.
Užitkový program úder má vliv výhradně na on-line ikony a nemá žádný účinek na fyzické tělo deckera nebo jeho kyberdeck. Účinnost tohoto programu snižuje užitkový program Pancíř.

Brzda
Násobitel: 4
Cíle: IC
Užitkový program Brzda snižuje operační rychlost aktivního IC. Vždy, když decker tímto programem zaútočí, musí cílové IC provést srovnávací test odolnosti pomocí bezpečnostní hodnoty hostu proti stupni Brzdy. Pokud IC dosáhne většího počtu úspěchů než útočník, nestane se mu nic. Pokud však při útočném testu padne více úspěchů, ztratí IC za každé dva čisté úspěchy programu Brzda jednu bojovou fázi. Pokud už IC nezbudou v daném bojovém kole žádné fáze, zabalí to a ustrne.
Ale pozor: Pokud člověk takto vyřadí IC dočasně z provozu, zabrání se současně zvýšení bezpečnostního konta deckera. Potlačení IC ovšem stojí jeden bod faktoru odhalení (viz **Potlačení IC**). Pokud není IC na začátku dalšího kola potlačeno, určí se jeho iniciativa jako obvykle a IC bude pokračovat tam, kde bylo zastaveno.
Reaktivní IC je vůči brzdě imunní.

Vražednost
Násobitel: 10
Cíle: deckeři
Užitkový program Vražednost imituje účinky nesmrtícího černého IC. Způsobuje deckerovu fyzickému tělu omráčení. Jinak je tento program identický s užitkovým programem Černé kladivo.

Černé kladivo
Násobitel: 20
Cíle: deckeři
Před pěti lety to byla jen pověst, před čtyřmi lety extrémně nebezpečná zbraň ve výbavě elity GridSec Lone Star. Před třemi lety se takzvaný užitkový program Černé kladivo dostal poprvé do rukou stínů a dnes je to běžný útočný užitkový program, který skoro všichni deckeři považují za samozřejmost.
Černé kladivo je černé IC, jehož cílem je decker, nikoli jeho deck. Může deckera usmrtit, aniž by jeho kyberdeck odpojilo. Bude tedy nadále možné vystopovat jeho přípojku. Černému kladivu se nedostává výbušných schopností černého IC, ale jinak jeho působení odpovídá účinkům smrtícího černého IC (viz **Černá IC**).

Obranné užitkové programy

Tyto programy slouží k zabránění poškození v matrixovém boji, k jeho snížení nebo k opravení.

Zaměřovač
Násobitel: 3
Užitkový program Zaměřovač snižuje cílová čísla ve všech srovnávacích testech senzorů při provádění bojových manévrů (viz **Bojové manévry**).

Plášť
Násobitel: 3
Užitkový program Plášť snižuje cílová čísla všech testů úniku při provádění bojových manévrů (viz **Bojové manévry**).

Medik
Násobitel: 4
Užitkový program Medik může snížit počet čtverců na kondičním záznamníku on-line ikony. Pro použití tohoto programu musí decker vynaložit komplexní akci a provést test s počtem kostek rovným stupni Medika. Cílové číslo vychází z celkové úrovně poškození, jíž už bylo na kondičním záznamníku on-line ikony dosaženo a která je uvedena v tabulce **Medik – cílová čísla**.
Každý úspěch z tohoto testu regeneruje jeden vyplněný čtverec na kondičním záznamníku ikony. Vždy, když je použit, ztrácí tento program jeden bod svého stupně, ať už dosáhne nějakých úspěchů nebo ne. Decker může naložit novou kopii s plným stupněm, pokud provede operaci „výměna obsahu paměti“.

MEDIK – CÍLOVÁ ČÍSLA	
Úroveň poškození	**Cílové číslo**
Lehká	4
Mírná	5
Vážná	6

Pancíř
Násobitel: 3
Užitkový program Pancíř snižuje účinnost útoků vedených na ikonu o svůj stupeň. Snižuje například všechna poškození, jež způsobuje IC Zabiják nebo útočný program Úder. V případě černého IC ovšem snižuje pouze poškození, kterému musí čelit deckerova ikona, nikoli ale poškození jeho fyzického těla. Krátce řečeno: Užitkový program pancíř je při standardním poškození na kondičním záznamníku ikony stále efektivní, ale nemá pražádný účinek na poškození, kterému jsou vystaveni decker nebo jeho deck; při nich pomáhá pouze pevnost decku.
Pancíř ztrácí vždy, když decker utrpí poškození, jeden bod svého stupně – tedy vždy, když nedokáže zcela absorbovat zásahem způsobené poškození. Decker může opotřebovaný Pancíř nahradit pomocí operace „výměna obsahu paměti“ „čerstvou“ kopií.

VELIKOST PROGRAMŮ										
Stupeň programu	**Násobitel**									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	1	2	3	4	5	6	7	8	9	10
2	4	8	12	16	20	24	28	32	36	40
3	9	18	27	36	45	54	63	72	81	90
4	16	32	48	64	80	96	112	128	144	160
5	25	50	75	100	125	150	175	200	225	250
6	36	72	108	144	180	216	252	288	324	360
7	49	98	147	196	245	294	343	392	441	490
8	64	128	192	256	320	384	448	512	576	640
9	81	162	243	324	405	486	567	648	729	810
10	100	200	300	400	500	600	700	800	900	1 000
11	121	242	363	484	605	726	847	968	1 089	1 210
12	144	288	432	576	720	864	1 008	1 152	1 296	1 440
13	169	338	507	676	845	1 014	1 183	1 352	1 521	1 690
14	196	392	588	784	980	1 176	1 372	1 568	1 764	1 960

Boj v matrixu

Deckeři a programy IC se mohou navzájem zaplést do matrixového boje. Ikony, jež zastupují systémové zdroje a uživatelské programy, nemohou tímto způsobem útočit ani být napadeny. Deckeři ovšem mohou provádět systémové operace, jimiž takové ikony mohou napadnout.

Sekvence boje v matrixu

Kyberboj v matrixu se řídí velmi podobnými pravidly jako běžný boj v *Shadowrunu*. Nejprve si určí soupeřící postavy a ikony iniciativu; následně ohlásí své akce a provedou je. Bojové kolo v matrixu trvá tři vteřiny, stejně jako v normálním boji v *Shadowrunu*. (Ačkoli tři vteřiny mohou při skutečném používání počítačů představovat nekonečně dlouhou dobu, třívteřinové bojové kolo umožňuje gamemasterovi lépe koordinovat matrixové akce s fyzickými akcemi, jež se ve hře odehrávají na jiném místě.) Všechny současně probíhající akce v jednom průběhu iniciativy se vyhodnocují v následujícím pořadí: astrální akce, matrixové akce a fyzické akce – platí ovšem následující výjimky.

Pokud decker ohlásí odložení akcí, protože čeká na událost ve fyzickém světě, provedou se tyto akce současně s běžnými fyzickými akcemi v tomto kole. Příklad: John má v bojové fázi 9 čtvrtého průběhu iniciativy k dispozici akce. Odloží si je a vyčká s nimi, než se jeho kolegové ve fyzickém světě dostanou přes bezpečnostní dveře. Náhle na něho v bojové fázi 8 vyskočí program IC. Program IC provede své akce spolu s ostatními matrixovými akcemi bojové fáze 8, zatímco John musí naproti tomu čekat, než dojde na fyzické akce této fáze. Bude tedy na řadě až po IC. Takže, síťaři, dobře si rozmyslete, zda s něčím budete otálet – v boji přežije zpravidla ten nejrychlejší!

Také deckeři, kteří komunikují s materiálním světem prostřednictvím hlasu nebo obrazovky, provádějí své akce spolu s fyzickými akcemi dané bojové fáze, i když mají k dispozici akce již z dřívějška. Toto ztížení neplatí pro komunikaci přes stopovací zástrčky, s nimiž někdo „spolusurfuje“ přes deckerův terminál, ani pro komunikaci s jinými personami, jež se zdržují ve stejném systému.

Zahájení boje

Decker může zahájit boj s ikonou, která je pro něho „viditelná“ nebo kterou lokalizoval, pokud tato neprovede úspěšný bojový manévr, aby se před ním skryla (viz **Bojové manévry**). Decker může lokalizovat reaktivní programy IC, pokud provede patřičnou analytickou operaci, a jiné deckery, pokud provede operaci „lokalizace deckera“ (viz **Systémové operace**). Kromě toho se mu mohou jiní deckeři zviditelnit tak, že s ním budou komunikovat, napadnou ho nebo se úmyslně ukáží nějakým jiným způsobem. Jakmile je decker „viditelný“ nebo lokalizovaný, zůstává tento stav nezměněn, pokud nějakým úspěšným manévrem odhalení znovu neunikne. Aktivní programy IC se mohou pustit do boje s každým deckerem, jehož bezpečnostní konto IC spustí. Program IC může v útocích pokračovat, dokud decker systém neopustí nebo pomocí bojového manévru pronásledování neunikne.

Iniciativa

Všechny ikony s atributem reakce si určují svou iniciativu podle obvyklých pravidel *SR3*.

Iniciativa deckerů

Iniciativa deckera je založena na reakci jeho persony. Pokud není tato reakce nějakým způsobem posílena, hází decker 1k6 a výsledek přičte ke své reakci, a tak zjistí svou iniciativu. Každý stupeň posílené reakce kyberdecku zvyšuje deckerovu reakci o 2 a zvyšuje jeho iniciativu o 1k6.

Reflexní vlákna, magická posílení, kontrolní rigy a další zlepšení deckerovy reakce ve fyzickém světě nemají vliv na jeho iniciativu v matrixu.

Iniciativa a fyzický svět: Pokud decker přímo komunikuje s fyzickým světem (hlasem, přes tiskárnu, obrazovku apod.), ztrácí 1k6 ze své iniciativy, dokud toto spojení neukončí. Tento postih neplatí pro komunikaci přes stopařské zástrčky a pro uživatele šneků.

Iniciativa IC

Pro určení iniciativy programů IC použijte vzorec z tabulky **Iniciativa IC**.

Pokud je IC spuštěno v průběhu bojového kola, snižuje se jeho vypočítaná iniciativa o 10 za každý průběh iniciativy, který již kompletně proběhl. Svou bojovou fázi bude mít IC až v následujícím průběhu iniciativy. Příklad: Pokud bylo IC spuštěno ve třetím průběhu iniciativy (dva průběhy iniciativy jsou už zcela uzavřeny) a

padne mu na iniciativu 29, bude mít své první akce v bojové fázi 9. Pokud by ho decker spustil v bojové fázi 7, bylo by IC na řadě až v příštím bojovém kole (naštěstí pro deckera).

INICIATIVA IC	
Úroveň bezpečnosti hostu	**Iniciativa**
Modrá	1k6 + stupeň IC
Zelená	2k6 + stupeň IC
Oranžová	3k6 + stupeň IC
Červená	4k6 + stupeň IC

Akce

Ikona může v jedné bojové fázi provést jednu volnou akci a buď dvě jednoduché, nebo jednu komplexní.
Vedle dále uvedených akcí mohou deckeři rovněž provádět systémové operace (viz **Systémové operace**). Pro každou z těchto operací musí decker použít odpovídající druh akce.

Volné akce

Volné akce jsou jednoduché, téměř mechanicky proveditelné činnosti, které nevyžadují prakticky žádné úsilí nebo koncentraci.
Následující systémové operace jsou volné akce: analýza IC, analýza ikony.
Odložení akcí: Deckeři si mohou podle běžných pravidel *SR3* odložit akce. Pravidla pro provádění odložených akcí naleznete v oddílu **Sekvence boje v matrixu**.
Odpojení: Decker se může kdykoli pomocí volné akce odpojit z matrixu, pokud nebyl úspěšně napaden černým IC (viz **Černá IC**). Pokud decker před odpojením neprovede operaci „elegantní odhlášení“, vystavuje se možnému děrovému šoku (viz **Děrový šok**).
Pronesení slova: Platí běžná pravidla *SR3* pro komunikaci. Bezprostřední komunikace s postavami ve fyzickém světě se projeví na iniciativě deckera, jak je popsáno v oddílu **Iniciativa** výše.
Deckeři mohou svá sdělení také „napufrovat“. Tímto způsobem napíše decker zprávu až o 100 slovech a předá ji jiné postavě, která je s ním ve spojení přes stopovací zástrčky, vysílačku, obrazovku nebo jiný přístroj. Druhá osoba obdrží napufrovanou zprávu na konci bojového kola.
Ukončení nakládání/vykládání: Decker může kdykoli ukončit nebo přerušit přenos dat.
Smazaní programu: Decker může kdykoli odstranit nějaký program z aktivní paměti decku. Tím získá místo pro operaci „výměna obsahu paměti“.
Uvolnění potlačovaného IC: Decker může kdykoli uvolnit potlačované IC, a tak znovu zvýšit svůj faktor odhalení o tolik bodů, kolik jich vynaložil k potlačení IC. Pokud mělo potlačení zabránit tomu, aby zhroucené IC zvýšilo deckerovo bezpečnostní konto, okamžitě dojde k jeho zvýšení. Pokud mělo potlačení podvázat akce IC, to se okamžitě znovu aktivuje (viz **Potlačení IC**).

Jednoduché akce

Jednoduchá akce vyžaduje o trochu více soustředění než volná a může probíhat poněkud komplikovaněji.
Následující systémové operace jsou jednoduché akce: analýza zabezpečení, dekódování periferie, analýza subsystému, dekódování přístupu, dekódování souboru, nakládání dat, editování souboru, sledování periférie, výměna obsahu paměti, vykládání dat.
Útok: Decker může napadnout jinou ikonu libovolným útočným programem, který má naložen ve svém decku. Programy IC a další ikony útočí podle toho, jak jsou naprogramovány.
Bojový manévr: Deckeři mohou jako jednoduché akce provádět níže uvedené bojové manévry (viz **Bojové manévry**).

Komplexní akce

Provedení komplexní akce vyžaduje intenzivní soustředění na daný úkol. Komplexní akci vyžadují určité systémové operace, stejně jako pokusy o odpojení po útoku černého IC (viz **Černá IC**).
Následující systémové operace jsou komplexní akce: analýza hostu, řízení periférie, editování periférie, elegantní odhlášení, lokalizace přístupu, lokalizace deckera, lokalizace souboru, lokalizace IC, přihlášení do hostu/LTS/RTS, vedení rozhovoru, nulová operace, napíchnutí rozhovoru.

Bojové manévry

Deckeři, aktivní IC a všechny ostatní samostatně jednající ikony mohou provádět bojové manévry, aby unikli odhalení, parírovali útoky nebo získali výhodnější pozici pro preciznější útoky. Všechny bojové manévry jsou jednoduché akce.
Každý bojový manévr vyžaduje srovnávací test, a sice mezi ikonou, jež ho provádí, a ikonou, která mu čelí. Manévrující ikona provádí test úniku proti protivníkovým senzorům a opačně. Pokud se u jedné z ikon jedná o program IC, hází gamemaster hodnotou bezpečnosti hostu namísto odpovídajícího stupně persony. (Programy nepatřící mezi IC nemají atribut únik, a proto nemohou provádět žádné bojové manévry. Rovněž tak se jim nemohou aktivně bránit, protože nemají žádné senzory. Manévr ovšem může i přesto selhat, totiž pokud manévrující ikona nedosáhne žádného úspěchu.)
Pokud manévrující ikona dosáhne více úspěchů, její čisté úspěchy se zaznamenají – tj. počet úspěchu, o něž má více než vzdorující ikona. Tyto úspěchy určují, jak je manévr úspěšný. Pokud má bránící se ikona stejně nebo více úspěchů, bojový manévr se nezdaří.
Pokud má manévrující ikona k dispozici užitkový program Plášť, snižuje se její cílové číslo o jeho stupeň. Pokud má vzdorující ikona k dispozici užitkový program Zaměřovač, klesá její cílové číslo o jeho stupeň.
K těmto testům je možné přidat kostky z hackovacích rezerv.

Uniknutí odhalení

Tento manévr provádí ikona, jež chce uniknout nepřátelské ikoně, která ji odhalila.
Decker musí provést operaci „lokalizace IC“, aby znovu odhalil program, který mu pomocí tohoto manévru unikl. K znovuodhalení persony, jež se mu ztratila, musí provést operaci „lokalizace deckera“.
Programy IC naleznou opětovně ikony, jež jim unikly, za tolik bojových kol, kolik činí počet čistých úspěchů ikony v testu úniku. Tento čas se zkracuje o jedno kolo za každý bod, o nějž se bezpečnostní konto za tuto dobu zvýší. Program IC se objeví na konci posledního kola únikové periody – připraven na měření iniciativy v dalším bojovém kole.

Kybersuši se nachází v hostu oranžová-8, když je napaden IC Zabijákem. Potřebuje pauzu k nadechnutí, aby mohl naložit silnější útočný program, takže se pokusí o únikový manévr.
Nejprve hází Suši svůj test úniku proti hodnotě bezpečnosti hostu. Má únik 6, takže hází šesti kostkami. Kromě toho má spuštěný užitkový program Plášť 4, takže jeho cílové číslo činí 4 (hodnota bezpečnosti hostu – stupeň Pláště). Dosáhne tří úspěchů. Mezitím hází gamemaster test bezpečnosti hostu proti Sušiho stupni úniku. Hází si tedy osmi kostkami a dosáhne jednoho úspěchu.
Suši tedy vychází se dvěma úspěchy ze srovnávacího testu jako vítěz; může tedy IC Zabijákovi uniknout na dvě kola.
Host ovšem Kybersušiho odhalí v dalším kole, kdy decker provádí operaci „výměna obsahu paměti“. Sušiho bezpečnostní konto vzroste o dva body, což jeho únikovou periodu kompletně anuluje – IC Zabiják ho tedy na konci tohoto kola znovu objeví.

Parírování útoku

Tento manévr umožňuje manévrující ikoně zlepšit její obranu v matrixovém boji. Pokud manévrující ikona ve srovnávacím testu zvítězí, zvýší se cílová čísla všech útoků na tuto ikonu o počet čistých úspěchů.
Tento bonus platí do následujícího útoku ikony čelící manévru. Pokud nepřátelská ikona provede manévr „útočná pozice“ (viz níže), manévrující ikona si svůj bonus zachovává. Pokud některá z ikon unikne odhalení, bonus je ztracen.

Útočná pozice

Tento manévr pomáhá ikoně, aby se ve srovnání se svým protivníkem dostala do výhodnější útočné pozice. Jedná se o nebezpečný manévr, který se může obrátit proti ikoně. Pokud manévrující ikona uspěje ve srovnávacím testu, může o počet svých čistých úspěchů snížit své cílové číslo pro další útok nebo o tutéž hodnotu zvýšit účinnost svého následujícího útoku. Pokud ikona čelící manévru zvítězí, dostane toto zvýhodnění ona.
Tento bonus platí pouze do následujícího útoku.

Kybersuši má únik 6 a právě má spuštěný užitkový program Plášť 2, když tu náhle narazí na podnikového deckera se senzory 5 a užitkovým programem Zaměřovač 3. Suši se pokusí o manévr „útočná pozice“, aby získal oproti protivníkovi výhodu. Hází test úniku proti cílovému číslu 3 (senzory soupeřovy ikony mínus Sušiho Plášť).

Jeho protivník hází test senzorů s cílovým číslem 3 (Sušiho únik mínus jeho Zaměřovač). Sušimu padnou čtyři úspěchy, jeho soupeři ovšem pět. Tím pádem smí podnikový decker snížit o 1 cílové číslo svého dalšího útoku nebo o 1 zvýšit jeho účinnost.
Suši použije svou zbývající jednoduchou akci v této fázi k manévru „parírování útoku". Testy zůstávají stejně, ale tentokrát zvítězí Suši s jedním čistým úspěchem. Tím se cílové číslo pro útok podnikového deckera zvýší o 1. Ten se rozhodne toto zvýšení cílového čísla akceptovat a připočte svůj bonus k účinnosti vlastního útoku.

Provádění útoků

Všechny útoky v matrixovém boji jsou jednoduché akce. Při provádění útoku hází útočník tolika kostkami, kolik činí stupeň jeho útočného programu (k tomuto testu lze přidat kostky z hackovacích rezerv). Cílové číslo pro tento test závisí na dvou faktorech: statutu cílové ikony – oprávněná nebo ilegální –, stejně jako na úrovni bezpečnosti hostu, v němž se boj odehrává. Každá ikona deckera nebo program IC, jež se do systému přihlásily s platným heslem, se považují za oprávněné. Všechny ostatní ikony jsou považovány za vetřelce. Tabulka **Cílová čísla pro boj v matrixu** udává cílová čísla ikon, založená na těchto faktorech. K nim se přičítají všechny modifikátory cílového čísla založené na užitkových programech, poškození apod.
Pokud si decker nějakým způsobem obstaral platné heslo nebo mohl na hostu již předtím nějaké heslo zřídit, může se pomocí něho přihlásit. Pokud získá decker prostřednictvím tohoto hesla v boji s bezpečnostními programy hostu výhodu, host takové heslo většinou smaže poté, co se decker odhlásí nebo odpojí. Dalo by se říci, že se jeho kamufláž provalila. Decker ale může takové heslo používat v boji s nelegálními deckery, aniž by tím svou kamufláž ohrozil.
Poznamenejte si počet úspěchů, jež padnou při útočném testu, protože určují účinek útoku. Rozličné útočné užitkové programy mají na své cíle různé účinky, ovšem většina z nich způsobuje poškození deckerovu tělu. Všechny zvláštní efekty a testy, které musí cíl podstoupit, jsou uvedeny v popisu útočných programů (viz **Útočné užitkové programy**). Informace o útočných programech, které nemají za následek žádné zvláštní poškození, naleznete dále v oddílu **Poškození ikony**.

CÍLOVÁ ČÍSLA PRO BOJ V MATRIXU

Úroveň bezpečnosti hostu	Cílové číslo pro ilegální ikony	Cílové číslo pro oprávněné ikony
Modrá	6	3
Zelená	5	4
Oranžová	4	5
Červená	3	6

Poškození ikony
Mnohé programy – například útočný užitkový program Úder a IC Zabiják – způsobují poškození podle běžných pravidel *Shadowrunu*. Každý z těchto programů má kód poškození, sestávající z číselně vyjádřené účinnosti a úrovně poškození: lehké, mírné, vážné, smrtelné. Účinnost takovýchto programů odpovídá jejich stupni. Úroveň poškození těchto programů je založena na úrovni bezpečnosti hostu a je uvedena v tabulce **Poškození IC**.
Zasažená ikona provádí test odolnosti vůči poškození na základě svého stupně odolnosti proti cílovému číslu ve výši účinnosti útoku. Pokud utrpí poškození program IC, udává hodnota bezpečnosti počet kostek, které jsou k dispozici pro test odolnosti vůči poškození. Užitkový program Pancíř snižuje účinnost útoku.
Srovnejte počty úspěchů útočníka a obránce. Dosáhne-li více úspěchů útočník, zvyšuje se za každé dva čisté úspěchy úroveň poškození o jeden stupeň. Dosáhne-li více úspěchů obránce, za každé dva čisté úspěchy se úroveň poškození naopak o jeden stupeň snižuje.

POŠKOZENÍ IC

Úroveň bezpečnosti hostu	Úroveň poškození IC
Modrá	Mírné
Zelená	Mírné
Oranžová	Vážné
Červená	Vážné

Cassie je v oranžovém hostu napadena IC Zabijákem-6, takže se musí vypořádat s kódem poškození 6V. IC dosáhne ve svém útočném testu tří úspěchů. Cassie má spuštěný užitkový program Pancíř 4, čímž se účinnost útoku snižuje na 2. Provede tedy test odolnosti a dosáhne čtyř úspěchů. V konečném důsledku tak dosáhla jednoho čistého úspěchu, takže se poškození nesníží a její ikona utrpí vážné poškození.

Kondiční záznamníky
Všechny ikony používají běžný kondiční záznamník *Shadowrunu*; sestává ovšem pouze z jednoho řádku – u ikon neexistuje žádné omráčení. Modifikátory cílového čísla a iniciativy naleznete přímo tam. Pokud je vyplněno všech deset čtverců, ikona se zhroutí. Pokud se jedná o personu, je decker vyhozen z matrixu. Poté obvykle následuje děrový šok (viz **Děrový šok**) i možné další efekty (pokud černé IC zlikviduje ikonu, spojení deckera s matrixem se nepřeruší – neboť nyní může ještě o to snáze usmažit jeho mozek).

Simsensové přetížení
Vždy, když deckerova ikona utrpí poškození od bílého nebo šedého IC, může deckerovo fyzické tělo utrpět omráčení na základě rezonančního efektu rozhraní ASIST.
Pro určení, zda decker utrpěl díky simsensovému přetížení poškození, musí podstoupit test vůle proti cílovému číslu, které vychází z výše utrpěného poškození ikony. Tato cílová čísla shrnuje tabulka **Cílová čísla pro poškození z přetížení**. Každá ikona, jež utrpí smrtelné poškození, se automaticky zhroutí a vystaví deckera děrovému šoku. Pokud test vůle selže, utrpí decker lehké omráčení a musí vyplnit jeden čtverec ve svém řádku omráčení. Poškození v důsledku simsensového přetížení není třeba řešit, pokud má decker co do činění s černým IC. Veškeré poškození, jež decker v takovém případě utrpí, není v žádném případě pouhý vedlejší efekt!

CÍLOVÁ ČÍSLA PRO POŠKOZENÍ Z PŘETÍŽENÍ	
Úroveň poškození ikony	**Cílové číslo**
Lehké	2
Mírné	3
Vážné	5

Děrový šok
Pokud je decker v důsledku zhroucení své ikony vyhozen z matrixu nebo se odpojí, aniž by předtím provedl operaci „elegantní odhlášení“, riskuje omráčení v důsledku děrového šoku. Účinnost závisí na hodnotě bezpečnosti hostu a představuje měřítko šoku, který je způsoben náhlým přechodem z virtuální do fyzické reality. Úroveň poškození je založena na úrovni bezpečnosti hostu, jak udává tabulka **Poškození při děrovém šoku**. Každé dva úspěchy v testu vůle snižují úroveň poškození o jeden stupeň.

POŠKOZENÍ PŘI DĚROVÉM ŠOKU	
Úroveň bezpečnosti hostu	**Úroveň poškození**
Modrá	Lehké
Zelená	Mírné
Oranžová	Vážné
Červená	Smrtelné

Opatření proti vniknutí
V následujícím textu budou popsány různé druhy bílých, šedých a černých IC, včetně jejich efektů. Další informace o tom, jak IC zapojit do hry, naleznete v oddílu **Spuštění IC**.

Bílá IC
Bílé IC ovlivňuje pouze on-line ikonu, ale nikoli permanentní stupně kyberdecku nebo užitkových programů. V nejhorším případě vyhodí bílé IC deckera z matrixu nebo zakóduje data, která chce decker číst nebo napsat.

Drtič
Drtiče jsou aktivní programy IC, které vždy útočí na jeden z atributů ikony deckera. Drtiče existují ve čtyřech formách: Kyselina, Tmel, Rušič a Značkovač. IC Kyselina napadá odolnost ikony, Tmel únik, Rušič senzory a Značkovač maskování.
Pokaždé, když IC Drtič napadne ikonu, hází si gamemaster útočný test za host a poznamená si počet úspěchů (podrobnosti o útočních testech naleznete v oddílu **Boj v matrixu**). Současně s tím podstupuje deckerova ikona test postiženého atributu proti cílovému číslu ve výši stupně programu Drtič. Pokud deckerovi padne alespoň tolik úspěchů jako hostu, nezpůsobí IC žádné poškození. V opačném případě se daný atribut snižuje o jeden bod

za každé dva čisté úspěchy, kterých IC dosáhne. Ano, to znamená, že jeden čistý úspěch IC nezpůsobí žádné škody. Dva úspěchy vedou k jednomu bodu poškození, čtyři úspěchy ke dvěma bodům atd.
Před programy Drtič nechrání Pancíř ani pevnost.
Drtič nemůže nikdy snížit žádný atribut ikony pod hodnotu 1.

Selena se nachází v systému oranžová-6, když tu je náhle napadena IC Drtičem Kyselina-4. Gamemaster hází za IC útočný test a dosáhne při něm čtyř úspěchů.
Selenina ikona má odolnost 6, takže na obranu před IC má k dispozici šest kostek pro svůj test odolnosti s cílovým číslem 4. Padnou jí dva úspěchy – to je o dva méně, než kolik padlo IC Kyselina. Následkem toho se odolnost Seleniny ikony sníží na 5.

Zabiják
Zabiják je aktivní IC, které způsobuje ikoně poškození v matrixovém boji. Každé IC Zabiják má kód poškození, jeho účinnost se rovná stupni IC. Úroveň poškození je založena na úrovni bezpečnosti hostu. IC Zabiják v modrých a zelených systémech způsobuje mírné poškození; IC Zabiják v oranžových nebo červených systémech způsobuje vážné poškození. IC Zabiják-6 v oranžovém hostu by mělo například kód poškození 6V. Úroveň poškození se zvyšuje za každé dva čisté úspěchy v útočném testu o jeden stupeň – tak jako v normálním boji.
Pokud se IC Zabiják postará o kompletní vyplnění kondičního záznamníku persony, je decker vyhozen z matrixu. Užitkový program Pancíř snižuje účinnost útoku IC Zabiják.

Sonda
IC Sonda je reaktivní IC, které provádí dodatečné prověřování balíků dat a požadavků programů na počítačové zdroje. Tím pomáhá při odhalování operací ze strany neautorizovaných programů.
U systému, v němž se nachází spuštěné IC Sonda, hází gamemaster test Sondy proti faktoru odhalení deckera – a to pokaždé, když tento provádí systémový test. Každý úspěch, jehož se v tomto testu Sondy docílí, se přičítá k bezpečnostnímu kontu dotyčného deckera.

Vír
Vír je reaktivní IC, které chrání prvky subsystémů přístup, soubor nebo periférie. IC Vír může být naprogramováno tak, aby střežilo buď určité komponenty subsystému, nebo celý subsystém. Může například chránit jediný soubor, databanku nebo veškeré datové funkce hostu (včetně faxových výstupů a specializovaných terminálů). Podobně brání v přístupovém subsystému přihlášení z určitých vstupních bodů (například z veřejných souřadnic a z určitých pracovních stanic) nebo všem pokusům o přístup. V periferním subsystému střeží buď určité periferní přístroje, nebo prostě všechny přístroje, jež jsou s tímto subsystémem spojeny.
Dokud není IC Vír dekódováno, brání v přístupu k hostu nebo periferním přístrojům. Navíc IC Vír zničí chráněná data dříve, než se dostanou do neoprávněných rukou. Pokud deckerův pokus o dekódování selže, hází gamemaster test Víru s počtem kostek rovným stupni IC proti cílovému číslu ve výši stupně deckerovy dovednosti počítače. Pokud v testu neuspěje, podařilo se deckerovi destrukční kód IC Vír potlačit. Pokud test uspěje, jsou data zničena.
Deckeři mohou pro likvidaci IC vír provádět určité systémové operace, a každou z nich je možné podpořit užitkovým programem Dekodér (viz **Systémové operace**). Dekódování IC Vír nezvyšuje deckerovo bezpečnostní konto. Decker může také pomocí programu Úder přivést IC vír ke zhroucení; tím se ovšem jeho bezpečnostní konto zvýší, pokud toto IC nepotlačí.

Asfaltové děťátko
Asfaltové děťátko je reaktivní IC, které se pokouší zlikvidovat užitkové programy deckera. Každé Asfaltové děťátko je naprogramováno na určitý druh užitkových programů: operační, útočné, obranné nebo speciální (podle rozhodnutí gamemastera). Výlučně pasivní programy (jako Pancíř a Plížení) nemůže Asfaltové děťátko napadnout.
Vždy, když decker použije jeden ze spouštějících užitkových programů, hází gamemaster srovnávací test mezi oběma programy. Test Asfaltového děťátka se hází proti cílovému číslu ve výši stupně užitkového programu. Cílové číslo užitkového programu odpovídá stupni Asfaltového děťátka.
Pokud Asfaltové děťátko tento srovnávací test vyhraje, přivede ke zhroucení jak sebe, tak daný užitkový program. Asfaltové děťátko zhroucené tímto způsobem nezvyšuje deckerovo bezpečnostní konto. Decker musí následně provést operaci „výměna obsahu paměti“, aby mohl naložit novou kopii daného programu. Pokud ve

srovnávacím testu zvítězí užitkový program, zůstane zachován. Gamemaster hází skrytý test senzorů, aby zjistil, zda decker Asfaltové děťátko objeví (viz **Lokalizace IC**).

Během jednoho runu provádí Selena systémovou operaci, během níž má spuštěný Analyzátor 6. Tento užitkový program spustí IC Asfaltové děťátko-6, které jde rovnou na věc. Gamemaster hází za IC test Asfaltového děťátka a za užitkový program test Analyzátoru. Oba mají cílové číslo 6. Asfaltové děťátko dosáhne více úspěchů, takže se zhroutí jak IC, tak užitkový program.

Šedá IC

Šedé programy IC napadají přímo kyberdeck a deckerovy užitkové programy. Poškození způsobené šedým IC se projeví *trvale* na stupních decku. K dosažení původních stupňů decku je třeba poškozené čipy a další součástky nahradit.

Výbuch

IC Výbuch je aktivní IC, které provádí matrixové útoky stejným způsobem jako IC Zabiják (viz **Zabiják** výše). Účinnost výbuchu je možné snížit Pancířem.
Navíc může IC Výbuch permanentně poškodit HPOP kyberdecku, pokud přivede deckerovu ikonu ke zhroucení. Pokud Výbuch deckera vyhodí z matrixu, hází se test Výbuchu proti cílovému číslu ve výši HPOP decku. Cílové číslo zvyšuje pevnost, Pancíř zde nemá žádný účinek. Za každé dva úspěchy z testu výbuchu se snižuje stupeň HPOP o 1. Zde je třeba podotknout, že decker bude možná donucen k tomu, že bude muset snížit stupně svých programů persony, pokud deck utrpí takové poškození, že součet jejich stupňů přesáhne trojnásobek zredukovaného stupně HPOP (viz **Kyberdecky**).

Selena dnes nějak nemá šťastný den. Program, který se na ni z matrixu vrhl, nebyl pouze (jak doufala) Zabiják, byl to program IC Výbuch-6.
Selenin deck má HPOP 6 a pevnost 2, takže gamemaster hází test Výbuchu s cílovým číslem 8. Při tomto testu padnou dva úspěchy – stupeň Selenina HPOP tedy permanentně klesne na 5. Pokud se vydá zase na nějaký run, aniž by tuto škodu opravila, bude nucena tomu přizpůsobit své programy persony – aby se ujistila, že součet jejich stupňů nepřekročí 15.

Trhač

IC Trhač je šedou verzí IC Drtič. Tyto aktivní programy útočí stejným způsobem (viz **Drtič**), ale vždy, když Trhač sníží některý stupeň ikony na 0, provádí se test IC Trhač proti stupni HPOP kyberdecku (k cílovému číslu se přičítá pevnost decku). Každé dva úspěchy, které v tomto testu padnou, snižují daný stupeň persony trvale o 1. K odstranění těchto škod je nutná výměna čipu persony.
Existují čtyři rozdílné formy IC Trhač: Kyselina, Tmel, Rušič a Značkovač. Kyselinový Trhač (zvaný též „trhač těla“, „stahovač“ nebo „smažička“) napadá odolnost. Tmelový Trhač („koňské kopyto“, „mumie“ nebo také „mucholapka“) napadá únik. Trhač Rušič (rovněž zvaný „oslepovač“, „majzlík“ nebo „špíz“) útočí na senzory. Značkovací Trhač (jinak „světluška“, „vlajka“ nebo „vřešťan“) útočí na maskování.

Jiskra

Toto aktivní IC útočí stejně jako Zabiják (viz **Zabiják**), pokud ovšem přivede deckerovu ikonu ke zhroucení, dojde k přetížení dodávky proudu do decku, což má za následek řadu náhodných elektrických výbojů v HPOP decku a deckerově mozku. Výsledky kolísají mezi malou improvizovanou elektrošokovou terapií a smrtícím úderem.
Toto je tedy skutečně tmavošedé IC, jež hraničí již s černým; protože ovšem nezpůsobuje fyzické poškození cíleně, z technického hlediska se neřadí mezi smrtící.
Pokaždé, když Jiskra způsobí zhroucení ikony, hází se test Jiskry proti cílovému číslu ve výši HPOP decku + 2. K cílovému číslu se navíc přičítá pevnost. Za každé dva úspěchy dosažené v tomto testu klesá HPOP o jeden bod. Navíc samotnému deckerovi způsobí útok poškození ve výši (stupeň IC)M. Účinnost útoku lze snížit Pancířem. Tomuto poškození odolává decker běžným způsobem. Za každé dva čisté úspěchy se úroveň poškození o jeden stupeň zvýší (dosáhne-li jich IC) nebo sníží (když padnou deckerovi).

HeadCrashe vyšoupl z matrixu program Jiskra-8. Při testu Jiskry padnou tři úspěchy, což v konečném důsledku zničí jeden bod stupně HPOP. Navíc musí HeadCrash čelit poškození se základním kódem 8M. Jeho fyzické tělo je na stupni 4 a navíc má jeho deck pevnost 1. Hází si svůj test odolnosti vůči poškození: čtyřmi kostkami (jeho

tělo) proti cílovému číslu 7 (stupeň Jiskry 8 mínus pevnost 1). Dosáhne jednoho úspěchu. Při porovnání obou testů vyjde najevo, že IC dosáhlo dvou čistých úspěchů, takže HeadCrash utrpí vážné poškození. JAU!

Asfaltová jáma
Toto reaktivní IC jedná a útočí stejně jako Asfaltové děťátko (viz). Ovšem pokud se IC Asfaltová jáma podaří přivést on-line užitkový program ke zhroucení, vpustí současně do kyberdecku virus, který zničí *všechny* kopie tohoto programu v aktivní paměti a paměťové bance decku. Pokud decker nemá momentálně záložní kopii v nějaké off-line paměťové bance, o daný program přijde. A i kdyby ji měl, nemá ho k dispozici pro zbytek probíhajícího runu.
Jakmile IC Asfaltová jáma způsobí zhroucení programu, hází se test Asfaltové jámy proti cílovému číslu ve výši stupně HPOP decku, k němuž se přičítá jeho pevnost. Pokud v tomto testu nepadnou žádné úspěchy, byl virus zlikvidován a Asfaltová jáma má stejný účinek jako Asfaltové děťátko, tj. decker může daný užitkový program naložit z paměťové banky pomocí operace „výměna obsahu paměti“. Pokud však Asfaltové jámě padne byť jen jeden jediný úspěch, znehodnotí veškeré kopie daného programu v decku. Decker může takový program znovu používat až tehdy, pokud se odpojí a nahraje ho ze zdroje mimo deck (pravděpodobně z paměťového čipu).

Černá IC
Černé IC je aktivní formou IC, jež prověřuje přenos příkazů mezi deckerem a deckem, aby potom mohlo infikovat rozhraní ASIST decku nebezpečně zostřenou biologickou zpětnou vazbou. Tyto zostřené zpětné vazby zvyšují simsensový signál decku na takovou výši, jaká je charakteristická pro čipy BTL s nadměrnou intenzitou. Tímto způsobem může signál přetížit nervové dráhy deckera a přivést ho do bezvědomí, způsobit psychické poruchy, vyvolat vymývání mozku nebo přivodit smrt prostřednictvím mrtvice, selhání srdce, ochromeného dýchaní, rozšíření artérií nebo neurotransmiterního sebeotrávení. A to je pouze malý výběr z možných efektů.

Černá IC v boji
Jakmile černé IC provede úspěšný útok na deckera, začíná deformovat rozhraní ASIST kyberdecku – dokonce i když daný útok nezpůsobil žádné poškození. Až do doby, kdy se IC podaří tento první útok, se odpojení od matrixu počítá jako volná akce.
Po zásahu od černého IC musí decker vynaložit komplexní akci a uspět v testu vůle s cílovým číslem ve výši stupně černého IC, aby se ještě vůbec mohl odpojit. Pokud se mu test zdaří, může se odpojit, ovšem černé IC i přesto provede ještě jeden útok, dříve než se přeruší spojení. Černé IC provede jeden automatický útok i tehdy, pokud nějaký deckerův přítel u přípojky vytáhne zástrčku, jakmile deck oznámí aktivitu černého IC.

Smrtící černá IC
Smrtící černé IC se v matrixovém boji chová stejně jako IC Zabiják. Úspěšný útok ovšem způsobí poškození deckerovi i jeho ikoně. Kód poškození IC je založen na úrovni bezpečnosti hostu: (stupeň IC)M v modrých a zelených systémech, a (stupeň IC)V v oranžových a červených systémech. Tento kód poškození platí jak pro deckera samotného, tak pro jeho ikonu.
Vždy, když černé IC deckera zasáhne, podstupuje tento dva testy odolnosti vůči poškození. Pevnost snižuje při těchto testech účinnost obou útoků. Test odolnosti vůči poškození pomocí těla umožňuje deckerovi snížit fyzické poškození. Při tomto testu není možné použít hackovací rezervy, karmové ovšem ano. Jako další krok hází decker test odolnosti vůči poškození odolností svého decku, aby snížil poškození své ikony. Ikona odolává poškození stejným způsobem jako při útoku IC Zabiják (viz **Zabiják**). Ikona je chráněná Pancířem jako obvykle. Po provedení všech testů se srovnají počty úspěchů. Černé IC může zvýšit úroveň poškození o 1 stupeň za každé dva čisté úspěchy, zatímco decker může poškození sebe sama či své ikony za každé dva své čisté úspěchy o 1 stupeň snížit.
Deckerovo spojení s matrixem zůstává nedotčeno i tehdy, je-li ikona zničena dříve, než se decker mohl odpojit nebo dokud nezemře. V tomto případě získává IC úplnou kontrolu nad všemi funkcemi ikony deckera. Tím se zvyšuje efektivní stupeň IC o 2. Decker se už samozřejmě nemůže vůbec bránit, pokud se jeho ikona zhroutila. Může se stále ještě pokoušet o odpojení, než ho IC připraví o život. Spojení s matrixem se automaticky zhroutí, pokud se černému IC podaří deckera zabít. Ovšem ještě předtím, než deck vypadne ze sítě, provede černé IC ještě poslední ránu na HPOP; tento útok provádí stejně jako IC Výbuch, jeho stupeň se však považuje za *dvojnásobný*. Pokud se IC podaří HPOP kompletně zničit, smažou se tím také veškerá data, která byla naložena během tohoto runu. To platí pro všechna data, i ta v databankách spojených s deckem. Stupeň HPOP klesá na nulu.

Permanentní efekty: Smrtící černé IC může rovněž způsobit nadměrné fyzické poškození, stejně jako jiné události. Smrtelné poškození může i zde vést k permanentnímu poškození (viz). Nadměrné poškození způsobené smrtícím černým IC představuje zvýšenou úroveň poškození mozku. Navíc k permanentnímu poškození může dojít následným poškozením neurologické povahy, jež mohou vést ke ztrátě paměti, halucinacím, epilepsii, přízračným bolestem, migréně nebo jiným poruchám. V případě neurologického poškození si může gamemaster vymyslet vlastní pravidla pro chronické poruchy. Pokud se ovšem podaří deckera znovu přivést k životu, platí všechna obvyklá pravidla pro smrtelné poškození.

Kybersuši (tělo 4, pevnost decku 1) právě šmejdí v systému červená-8, když tu mu najednou vstoupí do cesty černé IC na stupni 10. IC útočí a v útočném testu mu padnou dva úspěchy. Na tomto místě se už nebudeme zabývat ikonou – Kybersuši sám má problémů až dost.
Kybersuši dostane od IC úder s kódem poškození 10V. Pevnost jeho decku snižuje účinnost na 9, ovšem vzhledem k ubohým čtyřem kostkám těla nedostává Kybersuši z tohoto bonusu zrovna záchvaty nekontrolovatelného nadšení. Svůj tělesný test podpoří čtyřmi kostkami z karmových rezerv a docílí při něm dvou úspěchů. Ani jedna strana nemá žádné čisté úspěchy, takže poškození zůstává na vážné úrovni. To bylo o fous!
Kybersuši vyplní šest čtverců v řádce pro fyzické poškození ve svém kondičním záznamníku. Mezitím nadělá IC z jeho ikony sekanou a získá úplnou kontrolu nad všemi jejími funkcemi.
Ve své další akci se IC znovu opře do Kybersušiho. Jeho ikona se nachází ve věčných lovištích matrixu, takže efektivní stupeň IC se zvedá o dva body na 12! Tentokrát mu padne pouze jeden úspěch, ale i přesto musí Kybersuši čelit poškození 12V, jež je díky pevnosti jeho decku sníženo na 11V. Hodně štěstí, Suši!

Nesmrtící černá IC
Nesmrtící černé IC funguje stejně jako smrtící černé IC, s následujícími výjimkami: Nesmrtící černé IC nezpůsobuje fyzické poškození, ale omráčení. Decker těmto útokům odolává pomocí vůle. Pokud decker ztratí díky takovému útoku vědomí, jeho spojení s matrixem se automaticky přeruší a deck vypadne ze sítě. Přesto však má nesmrtící černé IC nárok na poslední úder na HPOP kyberdecku a na data naložená během runu.
Nadměrné omráčení, jež nesmrtící černé IC způsobí, se zaznamenává do kondičního záznamníku do řádku fyzického poškození.