Storebror ser dig – en artikel om register och registrering i Neotech

Har du någonsin undrat vilka organisationer och myndigheter som bevakar dig? Vad de registrerar, hur många register som finns och hur säkra är de? Finns det något sätt att förbli osedd? Denna artikeln skall svara på dessa frågor, och även om den främst behandlar Neotechs värld så går den utan problem att inspireras av till andra spel med liknande stämning.

Jag kommer att måla upp en ganska mörk bild av världen, åtminstone ur rollpersonernas perspektiv. Om myndigheterna alltid kan registrera vad en individ gör medför detta avsevärda svårigheter att röra sig utanför lagens ramar. Ju mer ”Storebrorskänsla”, desto svårare för rollpersonerna att agera fritt. Vad jag försöker säga är att artikeln endast kommer att beskriva en av alla version av Neotechvärlden, och jag uppmanar alla spelledare att modifiera den efter sin spelgrupps behov, för det finns risk att spelare som är vana att låta karaktärerna röja runt lite väl mycket kan bli aningen besvikna om man skulle följa denna artikel.

Historik

Runt millennieskiftet höjdes allt fler röster mot den ökade övervakningen i samhället. Folk kände att myndigheter och organisationer kränkte deras integritet allt mer. I Storbritannien bevakade övervakningskameror allt från vägnäten och officiella byggnader till torg och affärer. Ingenstans på stan kunde man undgå att bli filmad. Fler och fler rykten dök upp om USA och Storbritanniens avlyssningssystem Echelon, som sades kunde uppsnappa enskilda ord i all tele- och Internettrafik i världen. Allt fler företag och organisationer upprättade egna register, och staterna började sälja ut registerposter från bland annat adressregister till hugande företag, som ämnade använda uppgifterna i sin direktmarknadsföring. På Internet registrerades varje litet klick och musrörelse, surfarnas vanor kartlades för att kunna visa upp den mest lukrativa reklamen för rätt personer.

Kampen om människans integritet fortsatte under det nya årtusendet, men människorätts-organisationerna kämpade i motvind. Få orkade engagera sig i integritetsfrågor när världen skakades av katastrofer och krig, och de kommersiella krafterna blev allt starkare. Så småningom gav idealisterna upp, en efter en. Den personliga integriteten hade försvunnit för gott. Det blev allmänt accepterat att filmas, registreras och kartläggas. De vinnande argumenten var att övervakningen behövdes för att hålla brottsligheten nere, och att den kommersiella kartläggningen bara ledde till bättre riktad reklam.

Echelonsystemet glömdes bort, och stora delar försvann med USA:s kollaps. Efterträdaren var ett ännu hemligare system som byggdes upp av Europeiska Federationen, ett system vars existens fortfarande inte erkänts. Samtidigt skaffade sig de växande företagen allt mer sofistikerade övervakningssystem, och en öppen marknad för registeruppgifter började dyka upp. En ny bransch föddes (även om den legat i sin linda under flera decennier), och nya företag gjorde kometkarriärer. De profiterade på att köpa in uppgifter från andra företag, från statliga register och på den svarta marknaden, för att sedan sälja uppgifterna vidare, smakfullt paketerade. De började även samla in sina egna uppgifter.

Under en period runt 2030-talet hade utvecklingen på något sätt gått för långt. Det fanns så många register att det blev omöjligt att få heltäckande uppgifter. Olika register sade mot varandra, och företagen och myndigheterna fick svårt att lita på de uppgifter de köpte in. Förr i tiden visste man att uppgifterna i statens adressregister var korrekta, men nu kunde man inte vara säker längre. Alla köpte uppgifter från alla, och ingen visste vart uppgiftskällan var. Flera megaföretag och stater gick år 2039 samman i en koalition, kallad International Register- and Surveillance Organisation (IRSO). I början försökte man skapa ett eget, internationell ”överregister”, men planerna gavs snabbt upp när de insåg uppgiftens komplexitet, och i stället ställde de krav på bättre kvalité och enhetlighet på

registermarknaden. Detta resulterade så småningom i en djup kris i branschen, där många företag lades ner. Ur denna krisen växte den pånyttfödda registerbranschen som gällt sedan dess.

De kommersiella registren flyttades i någon mån över till de riktigt stora megaföretagen, även om flera helt registerinriktade företag kvarstod. Världens olika statliga register började slå samman i olika samarbeten, främst kriminalregistren, och när FN återigen blev starkare fick de överta flera stora system. Detta ledde slutligen till att FN fick ett internationellt ansvar för folkräkning, demografi och kriminalstatistik, och allt detta samordnades i FN:s registerenhet, som formellt lyder under Interpol. År 2059 innehar FN de i särklass största och mest omfattande registren; de anses även vara de mest pålitliga. Detta är ett av få områden där man verkligen ser upp till och tar efter FN:s agerande.

Olika register

Trots trenden mot större och mer samlade register finns det ett otal olika kvar. Praktiskt taget all registrering sker fortfarande på lokal basis, men uppgifterna skickas sedan direkt vidare till högre ort. En normal invånare i västvärlden står förmodligen med i ett tiotal större register och förmodligen tusentals mindre. Rent allmänt kan man dela upp registren i tre olika typer; demografiska, säkerhetsmässiga och kommersiella.

Den första typen av register är de som oftast kontrolleras av statliga eller överstatliga organisationer. De finns till för att kunna bidra med beslutsgrundande statistik (både för statlig och kommersiell användning), göra prognoser och samordna en mängd statliga system, exempelvis skatter.

De säkerhetsmässiga registren finns till för att lättare kunna lösa och förhindra alla typer av brott och säkerhetsproblem. Dessa register är alltid mycket hemligare än de demografiska, men det är ungefär samma typ av organisationer som innehar registren. Säkerhetsregistren används tillsammans med olika övervakningssystem för att upptäcka brottslingar.

Det flesta registren finns dock av kommersiella skäl. Det kan vara kundregister, medlemsregister i olika typer av organisationer, marknadsföringsregister (ett register för ”potentiella” kunder, det vill säga folk som skall bli dränkta i reklam) och många andra. De större företagen har även egna demografiska och säkerhetsmässiga register, av samma anledningar som olika nationer har det.

Övervakningssystem

År 2059 har övervakningen gått så långt att det i praktiken är fullständigt omöjligt att undvika att bli ”sedd”. Både företag, organisationer och stater håller sig med egna övervakningssystem, och de motiverar detta med att de behöver bevaka sina tillgångar, hålla koll på ”sitt folk” samt ha ett öga på fienden.

Det kryllar av tekniska lösningar och metoder för övervakning, och branschen är som alltid näst intill överhettad. För att nämna några: videoövervakning, transpondrar, biometrisk analys, datatrafiköverväkning, satellitfotografering, fjärrljudsupptagning, DNA-spårning, serienummersspårning och ”medborgarplikt” (regler som säger att individer är skyldiga att rapportera alla oegentligheter som de kan tänkas bevittna).

Fotografering, videoinspelning och ljudupptagning, både i de vanliga spektrumen och i de osynliga (och ohörbara), är fortfarande den absolut vanligaste metoden för vanlig övervakning, även om den inte är den effektivaste. Det finns i stort sett ingen byggnad som inte är försedd med en videokamera eller motsvarande. Allt från små kiosker till köpcenter, personbilar och kollektivtrafik, villor och lägenheter. Allt lagras digitalt och sparas en viss tidsrymd, för att sedan återigen skrivas över av nya inspelningar. En mycket liten del av det som spelas in övervakas av människor. Alla typer av videoinspelningar väger

tungt i rätten, och för att en kriminalteknisk bevisning skall vara trovärdiga krävs nästan någon videoupptagningar med samband till brottet.

En ny teknologi som gett videoinspelningen ett uppsving är den biometriska analysen. Den bygger på att det filmade materialet analyseras av en dator, som letar efter exempelvis speciella personer, handlingsmönster, utrustning eller liknande. Det innebär att man inte behöver anställa folk som tittar på bildskärmar, utan kan låta datorn analysera hundratals inspelningar samtidigt. Tekniken kräver mycket datakraft, och måste oftast verifieras av människor, men den är en stark konkurrent till en annan, äldre, identifieringsteknik som bygger på radiotranspondrar.

Transpondrarna är mycket små radiosändare, som sänder ut identifikationssignaler till ett omgivande radionät. Det vanligaste är att människor får bära transpondrar, i exempelvis identitetsbrickor, men även fordon och olika föremål förses med transpondrar. Detta gör att ett datorsystem alltid kan ha full kontroll över vilka som är i en byggnad, exakt vart de är, vart viktiga föremål är, etc. Det kräver inte heller någon större beräkningskapacitet.

Den nästan mytiska satellittekniken bygger också på videoupptagningar eller fotografering (dock ej ljudupptagning, av naturliga skäl). Tekniken är oerhört avancerad, men samtidigt minst lika dyr. De kraftfullaste satellitsystemen, som dessutom är utrustade med biometrisk analys, kan finna en individ med signalement, oavsett vart i världen denne befinner sig, på så kort tid som några minuter. Vistas personen inomhus används en infraröd kamera, eller röntgen, som klarar av att se igenom många våningsplan. Upplösningen, det vill säga största detaljrikedomen, kan vara bara några millimeter. Enda säkra sätten att undfly satelliterna är att i alla ljusets spektra ha samma färg som omgivningen, vilket antingen uppnås genom mycket avancerade kameleontdräkter eller genom att befinna sig mycket långt under jorden.

En lite annan typ av övervakning är den som inriktar sig datatrafiken. Den behandlar sådana enorma informationsmängder att den spelar i en helt egen liga när det gäller datakraft. Tekniken kan snappa upp i teorin all information som sänds över alla typ av datanät, främst det världsomspännande Nätet. De flesta som använder dessa kanaler vet dock om att de är övervakade, och i stort sett all datatrafik krypteras eller försöker döljas på annat sätt. Kampen är fortsatt jämn mellan dem som försöker finna information och dem som försöker dölja densamma.

Det är viktigt att påpeka att även om alla dessa övervakningssystem faktiskt finns så sker oftast inget större samarbete mellan dem. Ingen har laglig tillgång till mer än en bråkdel av dem, utom möjligtvis Interpol. Det finns ingen officiell myndighet som sammanställer informationen. Detta faktum gör att det inte är så extremt svårt som det verkar att undkomma ”storebror”. Fast å andra sidan är det ingen som vet vilka resurser Europa eller Interpol verkligen har till förfogande.

Ett världsomspännande ”Big Brother”

Kanske behövs det ett litet exempel på hur mycket Neotechs befolkning faktiskt blir övervakad. Det går inte riktigt att försöka resonera vart det behöver övervakas, för de flesta är eniga om att *allt* behöver övervakas.

Föreställ er Norman, en datakonsult i BAMA. När han stiger upp på morgonen i sin lägenhet ute i förorten är han förmodligen inte övervakad. Men när han går utanför dörren filmas han av korridorskameror, och när han lämnar byggnaden är det mycket möjligt att han registreras via ID-transponder på väg ut ur byggnaden. Under den korta promenaden till maglevstationen filmas han av flera trafikövervakningskameror. Hade han tagit bilen hade TransNet loggat varje liten rörelse bilen hade tagit. Inne på stationen filmas han av säkerhetsskäl, och när han går genom spärrarna loggas detta i

transportföretagets register. Ombord på tåget filmas han ur flera vinklar, för det gäller att förebygga brott på dessa dyrbara och sårbara tåg.

När han ankommer till stationen kontrollerar datorn när han passerar spärrarna och debiterar honom för det. I hissen upp till arbetsplatsen filmas han, och för att komma in på kontoret krävs en scanning av hans retina, samt förstås kontroll av ID-kortet. Väl inne plirar flera diskreta kameraögon mot honom, som rapporterar till chefen om de anställda gör något otillbörligt. Så fort han loggar in på sin dator skickas tusentals informationspaket ut, som uppsnappas av brandväggar hos företaget han jobbar hos, av operatören för nätet, av den lokala dataroteln och kanske även av någon underrättelsetjänst. Hans vanor på Nätet registreras av sajterna han besöker, samtidigt som loggar matas iväg till styrelsen för att undersöka att de anställda jobbar som de skall.

På lunchen går Norman ner i lobbyn (loggar ut ur byggnaden) och tar en taxi. Där sparas hans identitet på datorn och han filmas, med hänsyn till taxichaufförens (eller den automatiska taxibilens) säkerhet. Via taxibolagets datanätverk kan man se exakt vilken väg Norman tog till köpcentret. Inne i köpcentret kollar varje butik att kunderna inte stjäl något, och inne på den offentliga toaletten förebygger man skadegörelse; med kameror. När han ringer till sin sambo under lunchen spelas samtalet in och sparas hos teleoperatören, samtidigt som båda telefonerna lagrar information om samtalet. Den välbehövliga lunchen intar Norman ute i parken. Kameror övervakar de grusade gångarna, för att förhindra att våldtäktsmän och annat pack drar omkring, men Norman sätter sig ute på gräset, och det enda som övervakar honom är kanske en satellit, som scannar de öppna områdena efter en efterlyst brottsling.

Resten av dagen förflyter som vanligt. Skulle Norman misstänkas för något brott skulle polisen kunna se vart han har varit hela dagen. De kan konfirmera detta med analys av DNA-fragment på plats, samt förhöra ett otal personer som säkerligen sett Norman (förmodligen har någon dessutom reagerat på att han verkade suspekt när han satte sig alldeles ensam mitt ute på gräset). Norman skulle inte veta att polisen var efter honom förrän han var gripen. Hade han försökt att fly från sitt brott hade alla offentliga transportsystem blockerat honom och rapporterat hans position. Ett otal polispatruller skulle ha bäring på honom med bara några decimeters felmarginal.

Ett registrerat liv

FN:s mål är att ha full registrering av alla människor i hela världen. Det skall inte finnas en enda individ som inte finns i deras databas. Det kommer förmodligen aldrig att ske, men de är på god väg. I västvärlden räknar man med att mer än 99,9 % av befolkningen är registrerad hos FN. Siffrorna är dock betydligt lägre i andra områden.

När en västlänning föds på ett statligt eller privat sjukhus förs detta genast in i datasystemet. Det finns ett fåtal mindre nogräknade privata kliniker och andra mycket nedgångna statliga sjukhus som inte är fullt så noggranna med detta, men föräldrarna uppmanas att kontrollera att deras barn registrerats. Exakt födelsetid, DNA-nummer, blodgrupp, födelseort, nationalitet och liknande uppgifter förs då in i registret. DNA-numret är en lång siffersträng som beräknas ur positionen på en mängd stabila gener. Det anses vara en mycket säker metod, även om fall har visat att muteringar under livet kan ändra DNA-numret. Sådana muteringar är dock extremt ovanliga. Desto vanligare är att fel görs vid provtagningarna, så de flesta sjukhus tar ett flertal prov för att säkerhetsställa barnets nummer. DNA-numret har ersatt personnumret i många stater.

Exempel på register:
Adressregister
Diverse vårdregister
Fastighetsregister
Fordonsregister
Föreningsregister
Kreditupplysningscentraler
Kriminalregister
Kundregister
Kyrkoregister
Licensregister
Medlemsregister
Migrationsregister
Passregister
Personregister
Sjukhusregister
Skatteregister
Socialregister
Äktenskapsregister
Övervakningsloggar

De första uppgifterna vid födseln vidarebefordras till folkbokföringsregistret och adressregistret. När barnet skall börja dagis registreras detta, och skolan gör detsamma. Betyg förs in i ett betygsregister, olika sjukhusregister registrerar löpande individens möten med sjukvården och vid en passande ålder registreras individen som arbetsför och skattepliktig. Då finns förmodligen individen redan i ett hundratal register hos företag. Individen kan sedan registreras för militärtjänstgöring, betygen från universiteten registreras, socialregister listar individens behov av bidrag. När individen kanske begår något brott eller på något sätt blir delaktig i en utredning registreras detta i kriminalregistret. Skulle individen köpa vapen eller ammunition registreras även detta, likväl som andra typer av licenser, som körkort, medför registrering. Även när individen köper fastigheter, mark, fordon eller vissa typer av djur registreras denne som ägare till dessa.

Alla dessa nya register eller registerändringar loggas av FN (även om uppgifter ibland uteblir på grund av datafel, kompatibilitetsfel eller lata tjänstemän). Detta gör att FN:s register har en listning över alla viktigare händelser i en persons liv, från födelse till död.

Ett världsomspännande register

Om FN fick bestämma skulle det bara finnas ett enda register, deras. Men den verkliga situationen är en helt annan. Olika myndigheter och organisationer registrerar olika saker, och ofta varken vill eller kan de samarbeta med varandra, av en mängd orsaker. All den kommunikation som dessutom sker mellan register bäddar dessutom för datafel, mänskliga misstag och annat. Systemen blir så komplexa att de omöjligt kan överblickas.

FN:s lösning på detta är en akt som säger att Interpol har rätt med omedelbar verkan granska alla register i alla FN-anslutna länder (med några få undantag). Interpol har tolkat denna akt som att de skall ha full tillgång till alla register hela tiden, och de flesta regeringar har mer eller mindre villigt accepterat detta.

För att kunna upprätthålla ett uppdaterat och världsomspännande register har Interpol valt att införa en godkännandeprocedur för olika register. Ett godkännande från Interpol innebär att allt som registreras i det registret per automatik förs in i Interpol:s register, samtidigt som relevanta uppgifter hos Interpol förs in i det godkända registret, vid behov. Detta garanterar att båda parter alltid har uppdaterade register. Kraven från Interpol för ett godkännande är dock hårda. De ställer höga krav på säkerheten, för att ingen skall kunna missbruka registret. Ju viktigare uppgifter registret handhar, desto säkrare måste registret vara. Trots detta dubbelkollar ibland Interpol de uppgifter de får in från godkända register. De flesta större statliga register är godkända. Även kundregister för viktiga varor som vapen är ofta Interpolgodkända. Interpol hävdar också att deras godkända register medför en mycket större personlig integritet och säkerhet än andra register, och de gör således reklam till privatpersoner för att påverka dem att välja godkända register om möjligt.

Majoriteten av alla register blir dock inte godkända, men Interpol vill fortfarande ha den information som de kan innehålla. Lösningen på detta blir att de kontinuerligt kräver att få avläsa registren. De kopierar helt sonika registren och för över den information som visar sig vara pålitlig. Detta sker ofta automatiskt via olika datasystem, men det är inte alltid det hela går smärtfritt till. Många företag delar inte gärna med sig av registren, och andra har svårt att på ett passande sätt överföra informationen. Interpol har sällan råd att manuellt gå in och avläsa ett register, och de har inte heller så stora möjligheter att konstant argumentera med företagen, så dessa register utelämnas ofta, även om Interpol givetvis inte erkänner detta.

En relativt ny ”lösning” för företagen att slippa Interpol är att inhysa sina register i icke-Interpolanslutna länder (exempelvis Brunei och Liberia), samma länder som man gärna registrerar både sina fartyg, flygplan och högkvarter i, för att minimera insynen och maximera profiten.

Registren i praktiken

Den vanligaste användningen av registren inbegriper dock ingen skrivning till eller ändring i registren. Interpol ger de flesta viktigare statliga och korporativa inrättningar möjligheter att läsa av FN:s register. När en kund exempelvis köper ett vapen kontrolleras att kundens uppgifter stämmer med registrets. Gör de inte det så vidtas åtgärder, som att tillkalla polis. Dessa registerläsningar sköts via kraftigt krypterad trafik, och det finns ingen möjlighet för användarna av systemen att kolla i registren fritt. Oftast krävs det att ett ID-kort registreras av kassamaskinen, som sedan automatiskt kontrollerar mot registren. Detta minimerar risken att information kommer ut i onödan.

Automatiken och säkerheten är ledorden i utbyggnaden av det globala registernätverket, men det finns många glipor i systemet. Därför utför Interpol ett omfattande kontrollarbete där de ser till att inga obehöriga använder registren. Direkt koppling till FN:s register ges i stort sett bara till viktigare myndigheter, globala banker, de största vapenförsäljningsföretagen och andra megaföretag. Övriga organisationer får nöja sig med koppling till statliga person- eller polisregister, även om dessa register i sin tur är kopplade till Interpol.

Registeruppgifter går alltid att sälja, och på Nätet finns en omfattande marknad för sådana. Interpol:s register läcker inte mycket, men de flesta andra register gör det, och effekten blir ungefär densamma. För rätt pris kan man hitta information om de flesta av jordens människor.

Icke-personer

Trots alla ansträngningar av FN är många människor inte registrerade. I de minst utvecklade länderna är stora andelar av befolkningen inte registrerad, speciellt de som bor på landsbygden. Det saknas både pengar och vilja att inrätta de system och myndigheter som krävs för att kunna registrera medborgarna korrekt. Även i de mest utvecklade länderna finns det dock många oregistrerade personer. Det kan vara nomader som bor ute i ödemarkerna, gatubarn, invånare i de mest nedgångna och farliga stadsdelarna. Det finns även ett fåtal personer som ”fallit mellan stolarna”, så kallade icke-personer. Deras registeruppgifter har försvunnit eller aldrig förts in korrekt. Termen icke-personer, eller non-persons, används dock om alla oregistrerade individer.

Hade dessa icke-personer aldrig kommit i kontakt med samhället hade det inte varit särskilt intressant att finna dem, men många av de oregistrerade invånarna i slummen är grova brottslingar, och utgör därför enligt polisen ett hot mot samhället (även om de sällan lämnar sina hemkvarter). För att råda bot på dessa icke-personer använder Interpol och polisen två metoder, så kallade registerrazzior och sambandsspaningar.

Registerrazzior går helt enkelt ut på att polisen ingriper och tvångsregistrerar folk. Denna medför dock stora risker för både poliser och medborgare, så de brukar främst användas i kombination med andra, mer motiverade, upprensningar av slummen. Sambandsspaningar är desto mer avancerade, och är främst till för att upptäcka folk som på olagliga sätt raderat eller manipulerat med sin identitet. Genom att låta AI:er eller andra kraftfulla program granska ett otal övervakningssystem och register kan de upptäcka oegentligheter, som exempelvis personer som dykt upp på flera videoupptagningar men aldrig synts till i några register. Felprocenten för dessa spaningar är dock stor, så Interpol tvingas utreda varje fall manuellt.

Att lura systemet

I takt med att FN och världens olika myndigheter försöker utvidga och förbättra sina registersystem så jobbar den globala undre världen på att finna kryphål, motmetoder och andra mer eller mindre kreativa lösningar. Det ligger stora och mäktiga intressen bakom förmågan att försvinna spårlöst från både övervakningssystem och register, och den som kommer på ett bra sätt att knäcka ett system kan se fram emot stora anonyma kontanta bidrag.

Det skall dock klargöras att det inte finns några patentlösningar, vare sig för myndigheterna eller den undre världen. Det pågår ständigt en kamp om att ligga först. Lanserar myndigheterna ett säkrare system så kommer det snart därefter en metod att hacka det. Det är som alltid, relativt lätt att lura de lägsta instanserna av systemet, likväl som det är extremt svårt att lura de högsta nivåerna. Endast ett fåtal organisationer eller personer i världen har möjlighet att hacka Interpol:s system, medan man kan köpa fejkade ID-kort på gatan.

När man skall redogöra för de olika lösningarna är det viktigt att tänka på en sak. Den största inbyggda säkerheten i Interpol och andra myndigheters registersystem är att registren i sig är oerhört säkra och svåra att manipulera. Men långt ifrån alla organisationer har råd eller möjlighet att via krypterad datatrafik ständigt kolla upp folk mot registren. Det kräver ofta dyr utrustning, licenser och tillåtelser från olika myndigheter. Även om så enkla rörelser som videouthyrare kontrollerar identiteten hos sina kunder så gör de inte en sökning mot ett register, utan nöjer sig med att kolla att ID-kortet verkar stämma. Behövs ytterligare säkerhet så görs en ytterligare kontroll, där själva individen i fråga testas för exempelvis DNA-nummer (med en DNA-avläsare). Därför skiljer man på systemen med en nivåbeteckning. Ett system med en första gradens kontrollnivå kollar bara att ID-handlingen stämmer. Ett andra gradens system kopplar upp sig mot ett register och kontrollerar. Ett tredje gradens system testar även individen i fråga, exempelvis med DNA-avläsning.

De vanliga ID-kontrollerna är förhållandevis enkla att lura. Normala ID-kort ges ut av en statlig kontrollmyndighet och är krypterade, samt kräver ibland en PIN-kod eller annan identifikation (exempelvis en fingeravtrycksläsning). Trots detta har ett otal hackers genom åren lyckats knäcka systemen. Känner man rätt personer kan man köpa skräddarsydda ID-kort som visar upp den identitet man vill ha. Det finns även olika sätt att mer eller mindre felfritt modifiera ett existerande ID-kort. En annan, mer handfast lösning är att använda någon annans ID-kort. En ansiktsbild medföljer i ID-informationen på ett kort, men de flesta butiksbiträden tittar inte på bilderna. Rent allmänt ses ansiktsbilder som mycket opålitliga för identifiering. Det är lätt att modifiera sitt utseende, både temporärt och permanent. Att använda andras ID-kort försvåras ju dock om ID-kortet kräver kod eller fingeravtryck.

Exempel på system:

Ingen ID-kontroll
Gatuförsäljare, vanliga butiker, restauranger.

1:a nivåns kontroll
Butiker med exklusivare varor eller med behov av kundregister (ex. videouthyrare), rörelser som delvis använder nätet (ex. bokningssystem), enklare kollektivtrafik, taxibilar.

2:a nivåns kontroll
Handlare med licensierade varor , statliga myndigheter, resebolag, exklusivare passagerartrafik, banker, posten, andra finansiella institutioner.

3:e nivåns kontroll
Sjukhus, polis, andra vårdinrättningar, finansiella institutioner och myndigheter med större krav på säkerhet.

Alla dessa modifikationer av ett ID-kort räcker dock inte långt om det kontrollerande systemet är registeranslutet. Är man registrerad korrekt men använder ett ID-kort som ger felaktiga uppgifter larmar systemet omgående. Man kan då vänta sig bli uppsökt av polis inom kort. Det skall dock sägas att mindre betydande skillnader inte behöver leda till polisingripande, då det faktiskt finns möjlighet att ID-kortet har äldre uppgifter än registret.

Att lura registret är alltså desto svårare, och framförallt dyrare. Det finns många alternativ, men inget av dem är riktigt bra. Många tror att det bästa vore att bara ändra i registeruppgifterna, men detta är förmodligen den svåraste vägen. Att hacka ett register är ofta bland det svåraste man kan göra, för även om man lyckas bryta sig in i exempelvis det lokala polisregistret så kommer felet upptäckas så fort registret synkroniseras med ett annat register. Kan man ändra i Interpolregistret så betraktas de nya uppgifterna som korrekta gentemot andra registers uppgifter, men det är i praktiken omöjligt att ändra på Interpol:s register (åtminstone med hjälp av hackning).

Således måste man gå runt problemet. Den enklaste grejen är förstås att stjäla någon annans ID-handling. När systemet kontrollerar i registret så stämmer ju ID-kortet överens med registret. Denna metod fallerar ju dock helt om någon form av ID-kontroll görs direkt på personen. Det skall även tilläggas att så fort ett ID-kort anmäls stulet så är det livsfarligt att använda med system som kollar mot registret, då polisen och expediten genast uppmärksammas på att ett stulet ID-kort används. Stulna ID-kort är alltså bara ett val för desperata, även om det finns ligor som inriktar sig på att stjäla ID-kort från folk som inte är så benägna att anmälda dem stulna, exempelvis pensionärer, ungdomar och andra brottslingar.

En annan lösning är att kopiera någon annans ID-kort, och sedan utge sig för att vara denne. Återigen är det populärt att anta identiteter av pensionärer eller andra brottslingar. Pensionärernas identitet drar ingen uppmärksamhet till sig, och polisen brukar inte tveka att gripa andra brottslingar, vilket gör att man själv har sitt på det torra. Denna metoden, kallad ”shadowing”, är den mest använda. Svårigheterna ligger i att få tag på någon annans ID-kort och kopiera det, utan att ägaren märker något. Sådant ordnas oftast via olika mindre nogräknade butiker, som har olagligt modifierade (men dyra) ID-kontrollenheter som kan läsa av och spara andras ID-kort. På grund av sådan så kallad ”skimming” har folk börjat bli mycket misstänksamma mot firmor som kräver ID-kort utan uppenbar anledning (likaväl som de inte gärna betalar med kontokort).

För att ytterligare vara på säkra sidan kan man skydda sig mot den tredje nivåns kontroller, om man har ett stulet eller kopierat ID-kort. Det finns nämligen olika metoder att lura DNA-, retina-, röst- och fingeravtrycksscanners. DNA och fingeravtryck kan man fejka med ett artificiellt eller äkta hudlager som fästs ovanpå det vanliga. Sådana ”double-skins” är dock dyra och mycket olagliga att tillverka, och de bästa DNA-scannrarna luras vanligtvis inte av sådana metoder. Speciella linser eller cybernetiska implantat kan lura retinascannrar, och i den mån röstidentifiering används så kan den luras med specialsamplingar i ljudinspelare.

De mest luxuösa alternativen för de professionella registerbedragarna är att antingen skapa en ny registrerad identitet, eller att ta bort sin förra identitet (eller en kombination av de båda). Att skapa en identitet kan man göra på olika sätt, där det säkraste men dyraste sättet är att skaffa sig en ny identitet i ett icke-Interpolanslutet land, och sedan begära medborgarskap i ett Interpolland. Detta kräver dock att ens gamla identitet inte ligger kvar i registren, då ett DNA-prov ju skulle visa att det rörde sig om samma person. Skall man temporärt använda en ny identitet räcker det oftast med att begära olika typer av visum (behövs alltid vid inresa från ett icke-Interpolland), och dessa kräver inte alltid DNA-prov. Då skapas oftast en temporär identitet i registren, där man registreras som tillfällig besökare i landet. Lagstiftningen kring visum, medborgarskap och tillfälliga vistelser är en gråzon, och det finns alltid ett sätt att slippa undan kontroller. Ibland räcker det med att visa upp papper på att man är utlänning (utanför Interpolsfären, vill säga) för att slippa ha med registren att göra.

Att ta bort sin identitet är lite svårare. Det går inte att helt radera sina uppgifter, eftersom all data arkiveras och aldrig raderas; dör en individ så tas man inte bort från registret, däremot skrivs man in som avliden. Vissa register tar dock bort sin information då, exempelvis adressregister, så att fejka sin

död kan i vissa fall hjälpa. Det kräver endast lite finess och kunskap om kriminalteknik (så att man inte blir påkommen med att ha undsluppit sin ”död”). Man kan även begära utträde ur staten och flytta utanför Interpol:s sfär, men likväl står ens information kvar i registren.

Vissa personer har lyckan att inte vara registrerade (icke-personerna, ovan), och vissa har lyckats radera sina poster i registren. Dessa människor är mycket svårspårade, men samtidigt kan de omöjligt leva ett vanligt liv, eftersom registreringar krävs överallt. Sådana personer kan tjäna stora pengar som yrkesmördare.

Den sista, och kraftfullaste metoden att ändra sin identitet är att rikta sig direkt mot registren. Som tidigare nämnts är våld (läs ”hackning”) ingen bra metod. Förvisso har försök gjorts och lyckats, mot mindre register händer detta ofta, men Interpol är så gott som vattentätt. Genom att med olika hackerattacker belasta systemen så mycket att fel börjar dyka upp kan man skapa oegentligheter i registren som är svåra att spåra. Detta gör att man lättare kan använda sin identitet i verkliga sammanhang till olagligheter, medan registerägarna fortfarande tror att det är felen som spökar. Att hacka sig direkt in i registren för att ändra är det ingen som gör. Det är förmodligen enklare att muta eller lura sig till en ändring. Detta motverkas av Interpol genom flerdubbla kontrollsystem över registerändringar, genom angiverisystem bland de anställda och genom frekventa kontroller på de anställda, så att de inte har samröre med suspekta element. Trots detta kan de allra bäst bemedlade manipulera identiteterna, men priserna är astronomiska, och resulterar även i ständigt höjd säkerhetsnivå på Interpol när ändringarna eventuellt uppdagas.

Den riktiga eliten bland registerbedragarna har en egen gräddfil. Genom mycket goda kontakter och mycket pengar har de ett flertal, felfria identiteter registrerade, och kan komma och gå som de vill. De är dessutom medborgare i Brunei eller motsvarande, eller har skaffat sig diplomatpass. Det ryktas även att Interpol tillåter ”fria” identiteter åt vissa samarbetspartners. Exempelvis sägs Europol ha ett frikostigt avtal med Interpol, som garanterar Europol fri tillgång på nya identiteter, i utbyte mot hemligt material. De allra mäktigaste brottsorganisationerna sägs även ha dessa avtal, där ledarna erbjuds ”flexibla” identiteter i utbyte mot några läckor på lägre nivåer. Om allt detta vore sant så skulle inte Interpol vara lika moraliska och rättfärdiga som de hävdar.

Poliskontroller

De som har bäst identifikationsmöjligheter är polisen. Alla polisbilar, och ibland alla poliser, har tillgång till en portabel identifikationsenhet, som läser av ID-kort, kollar upp mot registret och tar DNA-prov. Dessa enheter massproduceras, och patchas så snart nya metoder för att lura dem dyker upp. I många föreskrifter står det att polisen skall göra en 3:e gradens ID-kontroll vid alla typer av poliskontroller (vägkontroller, brottsspaning, vid vittnesförhör på plats, etc.). I realiteten följs detta inte till punkt och pricka. När polisen har bråttom och det inte rör sig om någon viktigare kontroll brukar de nöja sig med en 2:a gradens ID-kontroll, eftersom det tar någon minut att avläsa och analysera ett DNA-prov. Detta kan betyda liv och död för en person som inte utger sig för att vara någon annan.

Det kan vara av speciellt intresse att veta hur en poliskontroll kan luras. Det finns en mängd sätt, varav flera kräver vissa yttre omständigheter. Här följer några förslag:

Snacka sig förbi: Oftast inte särskilt lätt. Poliser är cyniska och mycket trötta på mänskligheten, och har sällan runt att lyssna på annat än exakt det de vill veta. Har man inte något mycket bra att säga som riktar deras uppmärksamhet åt annat håll (som att få dem att tro att de är avskedade) brukar man bara sätta sig i en svårare sits med för mycket snack.
Mutor: Mutor går alltid, och även om poliser ofta är mindre benägna att ta emot mutor (speciellt företagspoliserna och olika specialpoliser) så finns det ett pris för alla. För att muta sig förbi en

poliskontroll gäller det att säga rätt pris på en gång. Har man otur tar man en för låg summa och löper stor risk att åka dit ordentligt. Det gäller även att vara diskret och snabb, så att inte poliserna får någon större möjlighet att tänka över saken.

Störa ut utrustningen: En väl fungerande metod, som polisen dock är utrustad för att klara av. Exempelvis kan man ha en störsändare kapabel att störa ut IR-kommunikationen mellan ID-enheten och Nätet. Man kan även använda en mer drastisk metod, att bära en kraftig elektromagnetisk ”bomb” eller motsvarande. Polisens elektroniska utrustning är dock EMP-skyddad, så det gäller att ha tillräckligt kraftfull spole.

Hackning: Är man ett geni när det gäller datorer kan man lyckas blockera ID-enhetens signaler när de kommer in på Nätet, och byta ut dem mot egna. Är det skickligt gjort skulle varken polisen eller registret märka annat än en kort fördröjning. Observera att detta inte görs i realtid, det hinns omöjligt med, man måste förprogrammera ett program som är kapabel att göra det. Metoden går i detalj ut på att man hackar sig in på den närmsta Nät-noden (trådlös sändare och mottagare uppkopplad mot stamnätet). Där installerar man sedan mjukvara som ”plockar upp” ID-enhetens signal, dekrypterar den, modifierar den till ”rätt” ID-uppgifter, krypterar den och sedan skickar den till sin ursprungliga destination.

Diversion: Om man kan leda bort uppmärksamheten har man en god möjlighet att bli bortglömd eller kunna fly. Återigen är poliserna anno 2059 mycket härdade, och det krävs något spektakulärt för att bringa dem ur fattning. Exempelvis skulle en rejäl bombkrevad i närheten förmodligen duga.

Våld: Lösningen för den desperata, och tyvärr, den vanligaste valda lösningen. Polisen är mycket medveten om detta och är beredd. Som exempel kan nämnas att de ofta i praktiken har dragna vapen när de kontrollerar suspekta personer. Finns det risk för att personen i fråga skulle fly med bil brukar det finnas en polis i bilen för att ta upp jakten vid behov. Visserligen kan ett par välutrustade brottslingar nedgöra poliserna, men då har de gjort det dummaste man kan göra i Neotech. Polisen lägger tiodubbla resurser på polismördare, och risken är mycket liten att man ens överlever, om man inte har en god flyktplan eller mycket inflytelserika kontakter.

Summering

Som alltid går vågorna fram och tillbaka i kampen mellan den ”rättfärdiga” världen och den undre världen. Så kommer det alltid att fortgå. Vissa perioder har ena sidan ett övertag, vissa perioder den andra. Som typisk rollperson mitt i denna smet finns bara en regel: ”Ingenting är omöjligt, bara du har pengar.” Den här artikeln har förhoppningsvis gett en klarare bild av hur de olika systemen integreras. Det är viktigt för spelledaren att veta hur det kan fungera bakom kulisserna, men spelarna bör inte vara allt för underrättade om detta. I själva verket är ju systemen oändligt mycket komplexare, och för att kunna motverka dem bra måste man vara expert på ett mycket specialiserat område. Det är just så olika hackers och andra av Interpol:s antagonister arbetar. De söker reda på expertisen, betalar den och sätter samman en möjlig lösning. Strax därefter påbörjar Interpol i praktiken samma jobb, bara för att täta hålet.

Känner du nu en olust av alla hindrande register och övervakningssystem? Spela inte i västvärlden, håll kampanjerna i slummen eller syssla inte med brottslig verksamhet. Fast ännu bättre, gör om, gör bättre (för din spelgrupp)!