

OKTOBER 2012

**TNO** innovation  
for life

**TNO.NL**

CYBER SECURITY EN SERIOUS GAMING:  
VRAAGSTUKKEN UIT HET DIGITALE  
DOMEIN.

TNO VERBINDT MENSEN EN KENNIS OM INNOVATIES TE CREËREN  
DIE DE CONCURRENTIEKRACHT VAN BEDRIJVEN EN HET WELZIJN  
VAN DE SAMENLEVING DUURZAAM VERSTERKEN.

# DE DIGITALE WERELD IS HERE TO STAY

# INLEIDING

De problemen waarmee wij in onze hedendaagse wereld geconfronteerd worden, vragen om innovatieve oplossingen. Deze problemen spelen zich meer en meer af in het digitale domein en raken ons allemaal. Het is dan ook van groot belang dat wij dit soort vraagstukken met elkaar aanpakken. Wij doen dat al 80 jaar lang vanuit onze kennis en expertise, samen met u. Samen werken wij aan een betere wereld, of het nu gaat om het gezamenlijk uitvoeren van projecten of om visievorming op belangrijke strategische onderwerpen. Hiertoe organiseren wij ieder jaar de TNO Round Tables. Voor de TNO Round Tables 2012 hebben wij gekozen voor de onderwerpen cyber security en serious gaming. Immers, beide onderwerpen raken een veelvoud aan maatschappelijke en economische onderwerpen en zijn relevanter dan ooit!

Op een technologisch aansprekende locatie  
– het Louwman Museum in Den Haag

– bespraken wij tijdens een werkdiner het belang en de urgentie van de gekozen onderwerpen: Cyber security gaat om het vergroten van onze weerbaarheid tegen misbruik, criminaliteit en verstoringen in het digitale domein. Bij serious gaming gaat het om de mogelijkheid om in een veilige virtuele omgeving op verleidelijke wijze samen te oefenen en nieuwe concepten te ontwikkelen.

Een samenvatting van de inleidingen en de discussies op basis van stellingen vindt u in deze brochure. Ik wens u veel leesplezier!

Vanaf deze plaats wil ik alle deelnemers aan de Round Tables hartelijk dank zeggen voor hun aanwezigheid en betrokkenheid bij de discussies. Wij hebben ervan genoten en kijken terug op een reeks bijzondere en waardevolle bijeenkomsten.

**Ir. Jan Mengelers**  
**Voorzitter TNO Raad van Bestuur**



# DE DIGITALE WERELD IS HERE TO STAY

## CYBER SECURITY

### VEILIGHEID IS NIET VANZELFSPREKEND

Nederland heeft een percentage van 98% internetgebruik. Online dienstverlening, zaken doen, financiën regelen, informatie delen of ophalen zijn niet meer weg te denken uit ons dagelijks leven. De sociale en de digitale wereld raken steeds meer verknoopt nu apparaten informatie gaan delen. Een steeds groter deel van ons sociale leven en ons werk is afhankelijk van internet. Dat roept de vraag op wat daarvan de risico's zijn en of het daar wel zo veilig is. Het antwoord is niet zonder meer positief. Zo is gebleken dat we in de virtuele wereld meer kans hebben om slachtoffer te worden van criminaliteit dan op straat.

De bedreigingen zijn divers: ze gaan van treiteren tot fraude en van terrorisme tot oorlog. Wat die oorlog betreft, de Chinezen lijken de fase van de ouderwetse kinetisch oorlog over te slaan en zich meteen voor te bereiden op een oorlog in cyber space.

### CYBER SECURITY OP DE AGENDA VAN BESTUURDERS EN BURGERS

Zowel individuen als organisaties en naties moeten werken aan de veiligheid op internet. Dat begint met bewustwording van wat er aan de hand is. De techniek kan helpen met security by design en vroegtijdige detectie van moedwillige verstoringen. Crisismanagement moet zich voorbereiden op digitale rampen. Dit geldt voor overheden, bedrijven en burgers, want ook burgers moeten alert zijn en helpen door het verstrekken van informatie. Het is van essentieel belang daarbij de juiste kennis

en ervaring te hebben. Ervaring zonder kennis is blind, kennis zonder begrip is waardeloos. Bij het nemen van effectieve beveiligingsmaatregelen is expertise een eerste vereiste. Dat vraagt om samenwerking tussen overheid, bedrijfsleven en kennisinstellingen.

### WAT MOET ER GEBEUREN?

Er is maar één conclusie: het moet veiligert! Laten we zorgen voor een 'secure economy' net zoals we streven naar een 'green economy'. Hoe doen we dat? In de eerste plaats zorgen dat iedereen weet dat cyber security niet over incidenten gaat, maar over iets veel fundamentele. Dus bewustwording is het eerste.

Het tweede is dat we moeten zorgen dat onze apparaten zijn ontworpen met veiligheid als voorwaarde: 'security by design'. Dus geen pacemakers en insulinepompen met een IP-adres dat simpel gehackt kan worden.

Het derde is dat er maatregelen moeten worden getroffen om moedwillige verstoringen vroegtijdig te detecteren en je daartegen te beveiligen.

Tot slot moet het crisismanagement op een nieuwe leest worden geschoeid: hoe krijg je een goed operationeel plaatje van de gebeurtenissen als er een digitale ramp uitbreekt ('common operational picture')? Hoe kun je informatie van burgers gebruiken voor een goede informatiepositie? Hoe kun je internet inzetten voor tegenmaatregelen, voor digitale 'crowd control' en hoe kun je zo snel mogelijk weer herstellen naar de normale situatie? Hiervoor is expertise is nodig.

### VANDAAG AAN DE SLAG VOOR TOEKOMSTIGE VEILIGHEID

Cyber crime is here to stay. We kunnen er niet omheen, we moeten er mee aan de slag. Cyber crime is zich aan het ontwikkelen en daarom moeten we meegaan. Om preventieve maatregelen te kunnen nemen, om in te springen en correctieve maatregelen te nemen, maar bovenal om bewustwording op basis van kennis en ervaring te realiseren. Expertise is nodig, maar iedereen moet een bijdrage leveren. Producenten om producten veilig te ontwerpen en consumenten om producten veilig te gebruiken. Veiligheid is tenslotte te belangrijk om alleen aan professionals over te laten.

**Drs. Henk Geveke, algemeen directeur  
Integrale Veiligheid**

# ROUND TABLES

## DISCUSSIE ROUND TABLE I

### STELLING CYBER SECURITY: ICT HEEFT ONS VEEL GEBRACHT MAAR NEEMT ONS NOG MEER AF

Cyber security kun je omschrijven als het vergroten van de weerbaarheid tegen misbruik, criminaliteit en verstoringen van het digitale domein. Cyber security is geen luxe, daarover waren de dinergasten het eens: "Het zijn bedreigingen die je serieus moet nemen." Of zij dat zelf wel deden, was de vraag. Het viel op dat we met elkaar snel de telefoon inzetten voor gebruik van allerlei toepassingen zoals mobiel stemmen, zonder ons de vraag te stellen of dit veilig is! En dat terwijl veel gasten aangaven ervaring te hebben met cyber crime. De belangrijkste conclusie paste daarbij: het ontbreekt nog aan voldoende awareness.

### PROBLEEM OF NIET?

Over de omvang van de bedreigingen waren drie meningen te onderscheiden. De eerste: die zijn serieus, maar laten we het niet overdrijven. De tweede: we weten niet goed wat er aan de hand is. En de derde: de bedreigingen zijn acuut en ernstig.

De tafels waar de eerste mening overheerste, concludeerden dat criminaliteit van alle tijden is: "Het verschil is de schaal, die bij cybercrime groot kan zijn." Beveiliging is nodig, maar die mag gewone transacties niet bemoeilijken.

Andere tafels vonden dat er te weinig bekend is over cyber security. Veel organisaties houden aanvallen op hun computersystemen geheim en soms weten ze niet eens dat ze zijn aangevallen: "Zelfs de echte deskundigen kunnen een goede hack volledig missen." De omvang en impact van het probleem is te onbekend.

Volgens de derde opvatting is er iets ernstigs gaande. De beveiliging tegen cyber crime kan niet alle acties van criminelen voorkomen en

loopt per definitie achter op de ontwikkelingen. Whizzkids van tussen de 16 en 19 jaar verdienen op de zwarte markt goud geld als ze zwakke plekken in beveiligingen opsporen. Een nieuwe uitdaging vormen de gecoördineerde acties van grote aantallen via internet gebundelde computers. De bedreigingen vormen overigens wel een voedingsbodempot voor innovaties. Bedreigend is het feit dat organisaties en consumenten onvoldoende voorbereid op en bekend zijn met acties die een ieder kunnen overkomen.

### VERTROUWEN

Tegelijkertijd zijn er ontwikkelingen die vertrouwen geven. Het internet is stevig genoeg om uitval van delen van het systeem op te vangen. Dat gaat wel ten koste van het vertrouwen van het grote publiek en mag dus niet te vaak gebeuren. En uiteindelijk, zei een gespreksdeelnemer, overleven bedrijven die slecht zijn beveiligd het gewoon niet.

### CONSUMENTEN

Consumenten ondervinden gemak van internet, maar zijn wantrouwend. Individuele gebruikers zijn kwetsbaar: "Voor hen zijn de problemen amper te overzien." Ze moeten accepteren dat hun privacy afneemt en dat manipulatie van persoonsgegevens niet valt uit te sluiten. Wantrouwen is er ook vanwege de schaal en de ongrijpbaarheid van internet. Sommige bedreigingen zijn bijzonder reëel: "Stuxnet, het virus dat is ingezet tegen het nucleaire programma van Iran, is vermoedelijk in handen van criminelen gevallen." Het wantrouwen heeft ook een positieve kant: "Het zet aan tot actie."

### BOARDROOM

Op de vraag over het niveau in de organisatie waar cyber security thuishoort, kwamen verschillende antwoorden. "In de lijn" zei de één, "het is een zaak voor de Raad van Bestuur" zei een ander. De constatering dat het op het hoogste niveau aan kennis over automatisering en ict ontbreekt, kreeg algemeen bijval. Maar dat probleem lost zich vanzelf op: "Jongeren beschikken over ruime kennis en ervaring." Wat weer tot een relativering leidde: "Jongeren raken zonder digitale hulpmiddelen voor navigeren snel de weg kwijt."

### OPLOSSINGEN

De zoektocht naar oplossingen begint bij awareness. Daarnaast klonk de roep om meer normen en waarden op het net, ook bij downloaden. De relletjes in Haren lieten zien wat er mis kan gaan op de sociale media, maar dat daar ook een tegenbeweging kan ontstaan. Grotere transparantie kan helpen, onder andere om de omvang van de problemen duidelijk te maken. Uiteindelijk dragen we met elkaar de verantwoordelijkheid en moeten we die bewustwording vergroten, zowel voor burgers als voor organisaties en maatschappij. Keuzes moeten we bewuster maken en de consequenties transparanter delen. Zo kunnen we met elkaar veel werk verrichten en veel bereiken, om de cyber security te vergroten. Dan bereik je met elkaar een andere aanpak. Andere concrete ideeën waren regelmatige veiligheidstests door betrouwbare hackers, onderzoek naar gedrag in cyberspace en een krachtige opsporing plus een stevige strafmaat. De techniek kan helpen met security by design en slimme versleutelingen.

En dan was er de suggestie om serious gaming in te zetten: "Serious gaming kan een belangrijk instrument zijn om cyber crime na te spelen en te oefenen met beveiliging." Daarmee zijn we bij het tweede deel van de Round Tables.



# SERIOUS GAMING

## SPELEND LEREN EN EXPLOREREN

Serious games zijn een middel om het leren en ervaren, het zoeken naar oplossingen en het nemen van besluiten te versnellen. Ze kunnen ook cultuur en gedrag veranderen. Serious games zijn effectief omdat ze spelers verbinden in een gemeenschappelijk doel, bestaande kennis op intuïtieve wijze laten zien, horen of voelen, en mensen zelf achter het stuur te zetten. Bovendien stimuleren ze out-of-the-box-denken en zetten ze aan tot creativiteit. Tenslotte wordt er door serious gaming brainpower bij elkaar gebracht welke tot bijzondere uitkomsten kan leiden. Uitkomsten die voordien niet tot de mogelijkheden werden geacht. Kortom mensen gaan het pas geloven en doen als ze het zelf beleven.

## IMPACT

Serious games maken gebruik van de menselijke neiging tot spelen en worden al ingezet in het onderwijs, bij sociale veranderingenprocessen, de training van professionals en in de zorg. Een succesvol voorbeeld is de online game Foldit, waarin 240.000 spelers gezamenlijk de structuur ontrafelden van een enzym dat een HIV-gerelateerd virus in staat stelt om zich te vermenigvuldigen. En met succes.

## PLAY IT BEFORE YOU LIVE IT

Serious games lenen zich ook om te oefenen voor echte situaties. Militaire spelers van de war game Nimble Titan krijgen politieke en militair-strategische dilemma's voorgelegd tijdens oefeningen in luchtverdediging. Stel, land A dreigt een raket af te schieten op land B. Land C kan met afweergeschut een inslag

voorkomen, maar dan zal een deel van de raketlading neerwarrelen op land D. Wat moet het leger van land C doen? In Nimble Titan is alle denkbare kennis op dit gebied gemodelleerd in een volledige gesimuleerde wereld. Spelers uit diverse landen werden al meermalen bij elkaar gebracht om dilemma's door te spelen, culturen te overbruggen om uiteindelijk tot oplossingen te komen. De militairen die het spelen, worden er betere beslissers van en het leidt tot betere geopolitieke samenwerking. Slimme strategieën en tactieken die de militairen ontwikkelen tijdens dit spel, worden daarna in reële situaties gebruikt. Deze serious game vormt een krachtige combinatie van het bundelen van bestaande kennis in modellen, een doeltreffend game design om die kennisikbaar te maken in 'what-if' scenario's, en dit te laten doen in een samenspel van belanghebbenden zodat groepsdynamiek en commitment ontstaat. 'Play it before you live it!'

## INTEGRATIE WERKELIJKHEID EN DIGITALE WERKELIJKHEID

Serious games zullen in de toekomst steeds vaker worden ingezet bij het oplossen van grootschalige en complexe problemen. Goed ontworpen games maken gebruik van het collectieve denkvermogen van grote groepen burgers waardoor verrassende oplossingen ontstaan.

Werkelijkheid en digitale werkelijkheid zullen ook in elkaar gaan overlopen. Games zullen via mobile devices integreren met de werkelijkheid. Omgekeerd zullen sensoren de werkelijkheid in games gaan weergeven.

Straks loop je op een virtueel voetbalveld tussen de spelers en kijk jij of je die strafschop wél had gestopt.

**Prof. dr. Peter Werkhoven, algemeen directeur Technical Sciences**

## DISCUSSIE ROUND TABLE II

### STELLING SERIOUS GAMING: REALITY IS BROKEN BUT SERIOUS GAMING CAN FIX IT

Veel dinergasten hadden al serious games gespeeld. Ze maakten een onderscheid tussen simulaties die dienen om vaardigheden te oefenen en de echte games die mensen leren om betere beslissingen te nemen in complexe situaties. TNO kiest een brede definitie, waarin beide passen. De mogelijkheden van serious games zijn volgens de dinergasten groot, maar er zijn ook beperkingen. Hier volgt eerst een samenvatting van de mogelijkheden, daarna een aantal relativeringen.

#### POSITIEVE ERVARINGEN

Serious gaming is een uitstekende manier om competenties en vaardigheden te trainen, om wisdom of the crowds in te zetten bij complexe problemen en om de gevolgen van mogelijke oplossingen te verkennen. De vraag of serious gaming bijdraagt aan productiviteitsverhoging kreeg geen eenduidig antwoord.

Serious gaming is breed toepasbaar, van planologie tot training van piloten en van het onderwijs tot de voorbereiding van militaire operaties. Een concreet voorbeeld dat de revue passeerde was een game die aanbieders van producten en diensten doorlicht op betrouwbaarheid. Plannen voor de herontwikkeling van Vliegveld Twente werden dankzij Serious games ongewoon snel gerealiseerd.

#### PROCEDURES

Serious gaming kan onzekerheden bij bestuurders wegnemen en hen de weg wijzen naar effectieve en creatieve oplossingen. Als zij de gevolgen van hun beslissingen beter overzien, zullen zij en hun medewerkers minder gaan vasthouden aan knellende procedures en beter inspelen op de vereisten van een

specifieke situatie. De Burgemeestersgame, waarmee gemeentelijke bestuurders crisismanagement kunnen oefenen, kreeg een zeer positieve beoordeling. Een groot voordeel van serious gaming is de Reset-knop: "In het gewone leven kun je dingen uitproberen, maar die hebben onomkeerbare gevolgen." Serious games-spelers moeten dan wel in een veilige omgeving spelen en niet bang zijn dat collega's hen op fouten afrekenen.

#### IRRATIONEEL GEDRAG

Veel dinergasten verwachtten dat serious gaming een grote toekomst tegemoet gaat, maar ze maakten ook kanttekeningen. De belangrijkste is, dat de sociale werkelijkheid moeilijk in een game te vatten is: "Emoties en irrationeel gedrag vallen moeilijk te simuleren." Een oplossing is, dat de tegenstander in een serious game niet door de computer, maar door een ander mens wordt gespeeld.

Een game vervangt niet de werkelijkheid: 'Het is een verkennend instrument, meer niet.' Als serious games worden ingezet om opvattingen te peilen bij mensen die zijn betrokken bij een beslissing, dan moet manipulatie door de belanghebbenden worden uitgesloten. Ook mogen uitkomsten geen absolute waarde krijgen: "Je moet niet zeggen: we hebben een spel gespeeld over de aanleg van de nieuwe snelweg en uw huis moet gesloopt worden."

#### BOARDROOM

In de boardroom ontbreekt het nog aan kennis over de gebruiksmogelijkheden. "Daar moet je met chaos omgaan. Het gaat

er niet om dat je de oplossing weet, maar dat je die organiseert. Serious gaming kan daarin ondersteunen."

In het onderwijs kan serious gaming een effectieve manier van kennisoverdracht zijn, al moeten docenten van rol veranderen en meer begeleider worden. Net als bij cyber security zijn jongeren al veel beter op de hoogte van mogelijkheden.

## CONCLUSIE

De uitdagingen van vandaag zijn omvangrijk en worden steeds complexer. Zeker als we beseffen wat de impact van cyber crime op onze welvaart en welzijn kan zijn. Cyber security is een onderwerp waar we met elkaar aan moeten werken. De snelheid waarmee wij in staat zijn de problemen op te pakken en op te lossen, wordt bepaald door de wijze waarop wij in staat zijn met elkaar samen te werken: de wijze waarop wij onze denkkraft, ervaring en expertise combineren ten behoeve van een snelle en integrale aanpak. Een aanpak die gekenmerkt wordt door creativiteit, inzet en openheid, de bereidheid tot delen en samen bouwen. Hulpmiddelen kunnen de wijze waarop wij dit doen en de ervaring die wij ermee hebben veel effectiever maken. Serious games zijn daar een voorbeeld van en de mogelijkheden ongekend groot.

Zo'n aanpak resulteert in ongewone en verrassende oplossingen, gekozen vanuit nieuwe dimensies en ervaringen. Zo'n aanpak is voorwaarde voor het daadwerkelijk oplossen van grote maatschappelijke vragen. Zo'n aanpak brengt innovaties en vernieuwingen!

Deze TNO Round Tables waren opnieuw een mooi voorbeeld van het bij elkaar brengen van verschillende ervaringen en kennis, van het vermengen van ingrediënten tot een smakelijke maaltijd die naar meer smaakt. Van ons allen en voor ons allen, of het nu over cyber security of serious gaming gaat, het gaat vooral om Innovation for Life!