Drs. Vincent Hoek
Enterprise Architect (EA), I-Interimrijk.nl, onderdeel van de Uitvoeringsorganisatie Bedrijfsvoering Rijk

NOG NET NIET WAAR GEBEURD...

CODE EN ZWARTE THEE

Kijk Dmitri, zei Vlad en hij verdunde zijn zwarte thee uit de samovar, zwakkeren doen het alleen goed, als alles gaat zoals zij verwachten. Die Nederlanders zijn een stuk zwakker dan ze denken én zij hebben geen historisch besef meer. Vroeger leidden alle wegen naar Rome. Wegen die symbool stonden voor Romes economische, militaire en culturele macht.

Die wegen werden haar achilleshiel en vormden de heirweg van Hunnen, Goten en Vandalen. De Romeinse weg is het internet van vandaag: een ideaal infiltratiepad voor 'zachte' cyber operaties: cyberspionage, digitale diefstal van publieke en private geheimen; informatieoperaties en – zeker rond verkiezingstijd – doxing[1], de diefstal en onwelgevallige publicatie van privé-informatie. Combineer dat met lage cyberverstoringen zoals denial-of-service en ransomware attacks en... we leggen een prima basis voor Code War.

Neem nou hun scheiding van machten, vrijheid van meningsuiting, privacy, legalisme en relatief ongereguleerde markten. Eén kluwen van diepe digitale afhankelijkheden! Juist de stabiliteit van hun instituties maakt Nederland asymmetrisch kwetsbaar. Hun besluitvormingskosten om samenhangend beleid te ontwikkelen, uit te voeren en blijvend te verbeteren zijn enorm. Ze zijn kwetsbaar in hun wereldwijde gedataficeerde economische verbondenheid, in hun open media, in de transparantie van hun overheden, in hun engagement met de rechtsstaat en in het scepticisme van hun eigen regelgeving. Data zitten tegenwoordig tot in de haarvaten van hun samenleving en de binnenzak van hun burgers. Gewoon de natte droom van elke totalitaire ideologie. De ironie!
De beste Westerse vrijdenkers bedachten het internet dat zij zelf hebben gesubsidieerd, benaamd en benummerd. Google, Apple, Microsoft, Amazon en Facebook domineren hun industrie. Wij hoeven slechts slim gebruik te maken van hun digitale kwetsbaarheden om hun eigen data tegen henzelf te gebruiken. Al hun economische, inlichtingen-, militaire en culturele activa liggen digitaal opgeslagen! De meeste assets en resources zijn in handen van particulieren en hangen aan open communicatiekanalen

[1] Doxing is het verzamelen van informatie over een doelpersoon of -organisatie en het openbaar maken ervan.

met hard- en software vol kwetsbaarheden.

Wie heeft portfolio management, beveiliging en compliance verificatie op orde? Hun rechtsstaat kan zo slecht omgaan met het grensoverschrijdende karakter van cyberoperaties. Terwijl voor ons het internet afstand als barrière elimineert. Wij kunnen praktisch overal komen met cyberwapens die maar een fractie kosten van militaire platforms. Anonimiteit en spoofing blijven eenvoudig, zolang het Westen geen gefedereerde registers van legale organisaties (ROLO's) inzet om illegitieme entiteiten te kunnen herkennen. Elke organisatie is wel ergens aan het internet verbonden, dus een organisatie identificeren zou toch een van de belangrijkste pijlers moeten zijn om digitaal vertrouwen op te bouwen. Voor een correct functionerende overheid en een sluitende bedrijfshoedanigheid zou je toch verwachten dat zij nieuwe digitale eisen zouden stellen die online, internationaal en in real time sluitend beantwoord zouden moeten kunnen worden.
Wie vertegenwoordigt de organisatie en met welke bevoegdheden *(entitlement)*? Wie geeft identificatiemiddel en/of claims uit en hoe betrouwbaar zijn deze? Is informatie correct, niet misbruikt en actueel? Hoe ga je om met veranderende omstandigheden, nieuwe technologie en zaken als *dynamic logging*? Hoe worden fouten hersteld? Zijn er alternatieve bronnen beschikbaar? Wat zijn de consequenties wanneer het fout gaat? Zolang landen als Nederland geen ernst maken met het opzetten van *Digital Twins* van hun kritische infrastructuur, ketensamenwerking en gedataficeerde procesaansturing, elektriciteitsopwekking en verkeersleiding, is alles wat gehackt kan worden in potentie van ons. Met een *Digital Twin* zouden zij de systeempunten waar data elkaar beïnvloeden helder kunnen maken en risicosimulaties kunnen draaien. Tot die tijd is digitalisering een goudmijn voor uitbuiting, afpersing, data kopiëren, valse berichten verspreiding en gerichte aanvallen.

Wij zijn de slimme parasiet die de Gouden Eieren van een naïeve kip uitzuigt. Hun particuliere bedrijven bezitten het grootste deel van hun intellectuele eigendom, (onder)handel(ing)sgeheimen, posities, deal nieuws... allemaal digitaal en lang niet altijd versleuteld. Internet en genetwerkte apparaten genoeg.

Voorlopig legt Nederland nauwelijks een formele link tussen de bescherming van intellectueel eigendom, de kwetsbaarheid van kritische infrastructuur en de eigen nationale veiligheid. Kopen zij strategische infra met digitale componenten in het buitenland. Terwijl Nederland toch draaipunt is voor exportcontrole gevoelige handel, voor de beoordeling van buitenlandse investeringen, voor militaire aannemers (JSF onderhoud) en voor voedselveiligheid.

Wij stelen om onze eigen industrieën te helpen, maar omgekeerd? Wat valt er te halen dan? Ooit van Russische Nobelprijzen gehoord? Wij krijgen nog geen aardappel door de winter.

Hun digitale represailles hebben weinig zin. Hun traditionele economische sancties of juridische aanklachten maken nauwelijks indruk. Intussen infiltreren onze hackers steeds dieper in hun digitale netwerken en dagelijks leven. Makkelijk zat, zolang vertrouwelijke installaties aan 'goedkope installateurs' gegund worden, zonder te tellen hoeveel man er feitelijk komt werken en wat zij komen installeren. Nederland is een van de meest digitaal verbonden samenlevingen ter wereld; vol doelen waar wij makkelijk bij kunnen komen.

Omgekeerd heeft het Westen nauwelijks (legale) toegangsmogelijkheden en bij ons kan ook veel minder stuk. De cyberwereld is een op maat gemaakt machtsinstrument met lage toegangskosten, grotendeels asymmetrisch, behoorlijk anoniem en *stealthy*. Wij kunnen grote delen van hun infrastructuur gijzelen als prachtige bron van inkomsten en zij kunnen daar nauwelijks iets tegen doen, vanwege hun eigen 'cyberkramp'.

Onze soft-cyber-aanvallen gaan niet zo grof in tegen het Internationaal Recht dat zij gewapende reactie rechtvaardigt. Zo kunnen wij hun meer schade toebrengen, dan zij ons. Onze aanvallen zijn zo goedkoop - slechte business-case. Raketten zijn een stuk duurder. Ten derde mag het Westen fysiek militair sterker zijn, op cybergebied hebben zij hun escalatie dominantie echt nog niet bewezen. Zij durven onze acties niet te wreken, omdat hun eigen economische belangen zo verstrengeld zijn, dat zij als de dood zijn voor onze vergelding.

Daar staan ze dan met hun Open Samenleving. In plaats van dat hun internet onze burgers 'vrij' maakt, maakt het ons autoritaire staten juist machtiger. Een gesloten samenleving kent geen vergelijkbare dreiging. Wij hebben nauwelijks nieuwsbronnen; geen open democratisch verkiezingsproces en wij manipuleren onze bevolking al decennia tot gelatenheid. Een foto maken in de openbare ruimte is bij ons al genoeg voor politie aandacht.
Daarom laten wij onze vrouwen de foto maken haha, de zogeheten 'Siberische Scheiding'.

Nederlanders trollen wij via hun eigen sociale media, wij verspreiden nepnieuws en hebben informatiemogelijkheden die hun eigen overheden niet kunnen of mogen controleren. Vals of ontwrichtend nieuws kunnen wij makkelijker en sneller verspreiden dan zij onze verhaaltjes met waarheidsgetrouwe, samenhangende informatie kunnen weerleggen. De Russische burger is lang niet zo online en mobiel en bij ons domineert internetcultuur en sociale media ook niet onze nieuwsgaring. Als iemand hier iets lulligs zegt, reguleren wij het gewoon weg. Als hun overheden op een vergissing te betrappen zijn, staat dat meteen breed in de media. Dit alles maakt het voor ons super simpel om reputaties om zeep te helpen met een *doxing* aanval. Denk maar aan onze *phishing* aanvallen van 2016 op het Amerikaanse Democratisch Nationaal Comité. Het dagelijks vrijgeven van gestolen informatie verzekert een continue, uitgebreide en versterkte dekking via hun eigen reguliere media. Zie die geest maar eens in de fles te houden! Zeker nu iedereen een Chelsea Manning of Edward Snowden kan zijn, omdat het nu makkelijker is om data te kopiëren, te stelen en te verspreiden dan in de tijd van *Deep Throat*.

Een USB stickje wegmoffelen is eenvoudiger dan maandenlang fotokopietjes van de Pentagon Papers maken. Dankzij de GDPR/AVG moeten zij data lekkages zelfs publiceren, met alle imagoschade van dien! Onze *fake news* operaties vormen een politieke splijtzwam, waarmee wij de legitimiteit van hun verkiezingsintegriteit ondergraven en hun samenlevingen fragmenteren. Van Zwarte Piet tot de Gele Hesjes hype wakkeren wij hun emoties aan met honderden *troll sites*.
Terwijl wij onze eigen datalekkers jaren na dato nog een Skripal cocktail komen toedienen! Wij zorgen er wel voor dat het in Rusland een stuk risicovoller is om data te lekken dan andersom.

Gaandeweg kalft zo de macht van het Westerse staatsconcept af. Hun burgers willen beschermd worden en hun overheden willen daders vangen. Het onbehagen groeit. Hun verliezen aan geld en imagoschade worden groter dan een fysieke aanval ooit had kunnen veroorzaken. Hun geloofwaardigheid kalft af en steeds meer datahaaien ruiken bloed.Intussen kopen wij samen met de Chinezen de strategische goederen en locaties op. Havens van Narvik tot Thessaloniki.

"Een USB-stickje wegmoffelen is eenvoudiger dan maandenlang fotokopietjes van de Pentagon Papers maken."

Hun drang tot legitimiteit en verantwoording verhindert hun eigen creativiteit voor verdediging. Wij, hun autoritaire tegenstanders, hebben een stuk minder last van wetten van welke aard ook. Leuk hoor die privacy regelgeving, maar wij eisen domweg toegang tot alle binnenlandse communicatie, wij eisen toegang tot versleutelde communicatie en broncode, wij hanteren formele regels tegen anonimiteit en kunnen ongewenste content makkelijk kalt stellen. Kunnen zij niet!
Wij pakken het Westen bewust op haar zwakke punten, maar andersom mogen zij alleen de andere wang toekeren. Wij maken ons niet druk om de schendingen van de soevereiniteit van 'neutrale' landen, maar hun juristen blokkeren het gebruik van de infrastructuur van derde landen om een digitaal doel aan te mogen grijpen. Helemaal als hierdoor burgers gevaar zouden kunnen lopen.
Waar hun eigen regelgeving hun ontzagwekkende innovatieve vermogen mogelijk maakt, blokkeert diezelfde regelgeving het beschermen van die mooie nieuwe concepten.
Nog thee?