Onder permanent toezicht:

- de Röntgenfoto van je leven -

André Reinink

Echt wel. Ik wil het allemaal weten!

Wat gebeurt er allemaal in cyberspace?

En wat heeft de eerste Twentse minister-president van Nederland, Dick Schoof, met dit boek te maken?

Lees verder en je weet (bijna) alles.

Op een zaterdagmorgen

Maart 2024. Zaterdagochtend is voor mij even een relaxmomentje. Misschien ken je het wel.
Krantje breeduit op de tafel, verse koffie, een knapperig croissantje en een vers broodje kaas.
Eerst even de krantenkoppen doornemen en alvast de voor mij interessante artikelen selecteren om later uitgebreider te lezen.
In onze krant staan ook boekrecensies. De meeste laat ik links liggen. Maar voor het boek dat ik nu ga bespreken maak ik een uitzondering.
Ik raak meer geïnteresseerd en bedenk me dat ik nog een boekenbon op 'voorraad' heb.
Herken je dat? Je kreeg een boekenbon op je verjaardag, bergt deze ergens op en vergeet deze te verzilveren.
's Middags fiets ik naar de stad en gebruik ik de boekenbon om het boek aan te schaffen.

Het klinkt je misschien bekend in de oren

Ik besprak al eerder een boek in de SoftwareBus:
Je hebt wél iets te verbergen – van Maurits Martijn & Dimitri Tokmetzis.
Je kunt het boek kopen of lenen in de bieb.
Maar je kunt ook mijn recensie op de site **Compusers.nl** er nog eens op nalezen[1].
Inmiddels is het boek qua voorbeelden misschien ietsje achterhaald, maar het thema is nog steeds actueel.
Misschien is het zelfs nog actueler geworden.
Het boek van Huib Modderkolk dat ik hier bespreek kun je min of meer zien als een aanvulling en verdieping van het boek van Martijn en Tokmetzis.

Over Huib Modderkolk

Je kunt natuurlijk alles napluizen over Huib Modderkolk in onze gedigitaliseerde wereld. Maar voor de lezers die van een stukje gemak houden hierbij de volgende informatie.
Huib Modderkolk (1982)is een journalist, en nog iets preciezer: een onderzoeksjournalist gespecialiseerd in inlichtingendiensten, privacy en de digitale wereld.
Hij werkte eerst bij het NRC Handelsblad. Tegenwoordig is hij in dienst bij de Volkskrant.

Ook is Huib bekend van het boek 'Het is oorlog maar niemand die het ziet' uit 2019. Voordat dit boek uitgegeven werd, kreeg Huib een telefoontje van Dick Schoof. Schoof was toentertijd de baas van de AIVD, de Algemene Inlichtingen- en Veiligheidsdienst.
Er werd hem 'dringend' gevraagd enige gevoelige passages in het boek aan te passen voor publicatie.
Voor zijn werk kreeg hij meerdere prijzen en onderscheidingen.

Hoe het allemaal begon

Na de proloog begint de schrijver in het eerste hoofdstuk met de mededeling dat hij, na een vreemde mailwisseling met ene Nasir die informatie heeft over een Mossad (deel van de geheime dienst van Israël) medewerker, een pakketje toegestuurd krijgt. Tja, hoe pak je zoiets aan?
Huib laat het pakketje naar de redactie van de krant waar hij werkt (de Volkskrant) opsturen.
De auteur is wantrouwend over wat te doen met het pakketje en zoekt steun bij een securityspecialist van het Korps Commandotroepen. Zijn alias is 'Hactic'. Oorspronkelijk wilde hij Oekraïne helpen met zijn specialistische kennis, in de Oekraïne wel te verstaan, maar dat viel niet in goede aarde bij zijn dochter. Hij meldt zich aan bij de oorlog in de Oekraïne als digitale expert op afstand en promoveert in korte tijd tot beheerder. Door de ontmoeting met Hactic krijg je als lezer een ruime inkijk in de digitale oorlog. En een oorlog bestaat allang niet meer uit '1000 bommen en granaten'.

Na de ontmoeting met Hactic opent Huib het pakketje (een bubbeltjesenvelop) op de Haagse redactie van de Volkskrant.
De envelop bevat een A4-tje en een roze Samsung telefoon.
Gek, maar op de een of andere manier prikkelt mij de tekst 'roze Samsung telefoon'.
Het A4-tje bevat instructies wat te doen en vooral wat niet te doen. De telefoon is teruggezet naar de fabrieksinstellingen en bevat de App 'Signal'.
In die App staat slechts 1 contact met de naam 'Nasir'.
Langzaam begint de auteur uit de doeken te doen wat de

banden zijn tussen Nederland en Iran. De naam 'Stuxnet[2]' heeft hier alles mee te maken. Stuxnet loopt alles een rode draad door het boek. En de Iraniër blijft maar aandringen en het onderwerp Stuxnet aankaarten.

'What the Hack'!

Behalve het onderwerp Stuxnet -verderop in dit artikel meer info- probeert Huib inzicht te geven in de wereld van de hackers.
Een hacker[3] verwijst vaak naar een persoon die binnendringt in een computernetwerk door de beveiliging te omzeilen (soms ook wel kraker of cracker genoemd), maar in de originele betekenis kan het ook verwijzen naar iemand die bestaande middelen gebruikt om oplossingen te vinden voor problemen waarvoor dat middel niet oorspronkelijk bedoeld was, zoals deelnemers van een hackathon of door gebruik van life hacks. Hacken gebeurt niet altijd met de bedoeling om zich illegaal informatie toe te eigenen, maar bijvoorbeeld ook om aan te tonen dat het netwerk onvoldoende beveiligd is.
Bron: Wikipedia.

In principe zijn de kenners er het wel over eens: een hack bestaat meestal uit vijf fases[4].
1. Verkenning
2. Scanning
3. Toegang verkrijgen
4. Zorgen voor permanente toegang
5. Bewijsmateriaal verwijderen

Vaak lees je vaak berichten over een hack als er sprake is van zogenaamde 'Ransomware'. De hacker versleutelt het netwerk en versleutelt ook de back-up als dat mogelijk is. Als het slachtoffer geen actuele back-up terug kan zetten blijft er maar één ding over: betalen.
Nu zou je kunnen denken dat een back-up terugzetten eenvoudig te doen is. Voor een deel klopt dat.
Maar stel dat je een magazijn hebt met heel veel artikelen. En dat er tientallen bestellingen per seconde via internet verlopen. Welke back-up zet je dan terug nadat een expert urenlang bezig is geweest met de analyse van de hack? Alle data zijn dan inmiddels verouderd en onbetrouwbaar…

'Ik denk dat het potentieel van wat het internet gaat doen met de samenleving, zowel goed als slecht, onvoorstelbaar is. Ik denk dat we aan de vooravond staan van iets opwindends en verschrikkelijks'.

David Bowie, 1999

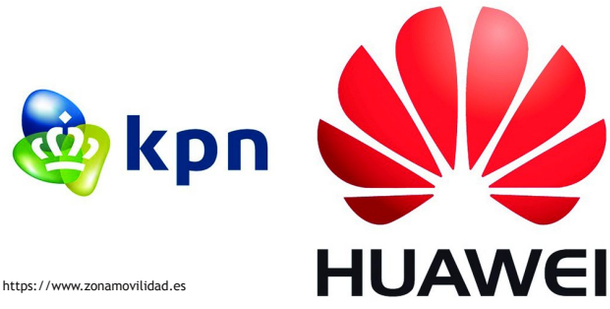
Het boek in het kort[5]

De auteur heeft uitgebreid gesproken met diverse personen die goed op de hoogte zijn van, ofwel hoe je moet hacken, dan wel goed zijn in het zoeken in netwerken naar sporen van hackers. Sommigen worden met hun werkelijke naam genoemd, sommigen worden minder duidelijk omschreven en voorzien van een alias. Ook schetst Huib een beeld van de digitale wereld aan de hand van de diverse gesprekken.
Hij heeft het boek o.a. voorzien van een aantal hoofdstukken die hij analoog aan het hacken genoemd heeft: de eerste, tweede, derde, vierde en vijfde fase.

Een paar opvallende passages uit het boek

Het boek staat vol met interessante verhalen, ik wil er hier een aantal noemen. Zaken die daadwerkelijk gebeurd zijn, maar waar je als burger nauwelijks weet van hebt.
In de meeste gevallen wil men de vuile was niet buiten hangen.

De Hack van de KPN[6]



Bron: https://www.zonamovilidad.es

KPN maakt(e) gebruik van Huawei-apparatuur in haar IT-omgeving. Op een gegeven moment wordt ontdekt dat er indringers actief zijn binnen het netwerk. De vingers wijzen richting China. China heeft het grootste beroepsmatige hackersnetwerk ter wereld. Staatshackers wel te verstaan, honderdduizenden.
KPN vond het in eerste instantie niet nodig om melding te doen van de hack omdat er 'geen tot nauwelijks' reden toe was.
Waarom werken de meldingen op de eerste maandag niet altijd en bij iedereen, vraag ik me wel eens af...

Oppikken van wifi-signalen
Tijdens een OPCW-congres (2018) in Nederland proberen Russen via wifi binnen te komen. OPCW staat voor Organisation for the Prohibition of Chemical Weapons. De Russische hackers werden ontdekt.
Omdat de hackers een diplomatieke status hadden kunnen ze niet vervolgd, maar alleen uitgezet worden.
Een paar maanden geleden las ik dat er vissersboten voor de Nederlandse kust in de gaten gehouden worden. Zo varen ze langzamer dan gebruikelijk.
Als men de boten nader onderzoekt ontdekt men banden met het Kremlin.
Die boten varen vast niet langzaam omdat ze wachten tot de haring vet genoeg is...

Energievoorziening
De energievoorziening van een land, dus ook Nederland, is essentieel. Er zijn veel en regelmatig storingen (meer dan 500 in een jaar) die duiden op een hack of 'buitenlandse invloeden'. Maar lang niet altijd krijg je als burger informatie hierover.
Nordstream 1 en 2 zijn we bijna alweer vergeten...

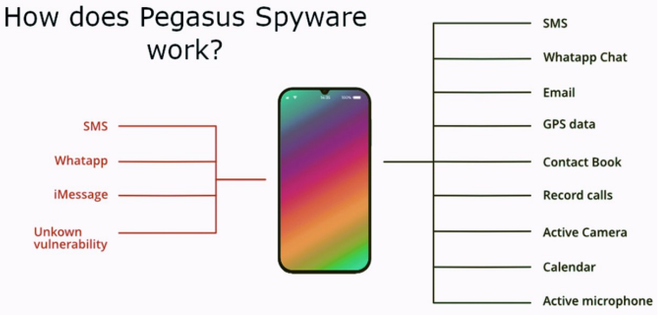
Gestripte laptops en andere apparatuur
Bij diensten als TNO, de AIVD en MIVD worden in apparatuur als een laptop sommige chips vervangen om kans op 'lekkage' te verminderen.

Waterhuishouding
In Nederland, met name in Amsterdam, werd een flink aantal brugwachtershuisjes vervangen door een besturing op afstand. Totdat er spontaan verkeerde bruggen opengingen. Zo ging eens een fietser spontaan de lucht in.

De Iraanse programmeur
Huib beschrijft een boeiend relaas over de Iraniër Amir, die handig is met programmeren en in Iran werd opgeleid tot ethisch hacker. Tenminste dat dacht hij.
Toen hij zich met zijn vrouw in Nederland vestigde liep het allemaal anders dan gepland.

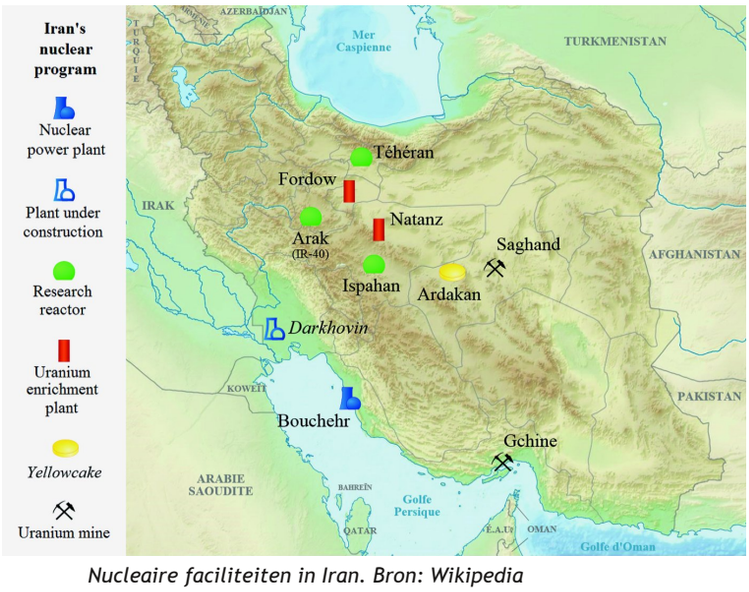
Geen vingerafdrukken
Nooit geweten: er zijn spionnen en agenten die het lijnenpatroon van hun vingerafdrukken wegschuren. Als hen naar de reden van de gladde handjes gevraagd wordt, schrijven ze dat vaak toe aan een huidziekte.

Beperkte (?) mogelijkheden Nederlandse overheid [7]
De overheid in Nederland heeft beperkte mogelijkheden door de strenge privacyregels.
Daar ga ik voor het gemak maar vanuit.



Volgens Huib is het aannemelijk dat Nederland de Israëlische software van Pegasus inzet. Dat wordt natuurlijk niet aan de grote klok gehangen.
Huib krijgt bij de Nederlandse politie geen antwoord op de door hem gestelde vragen over dit onderwerp.

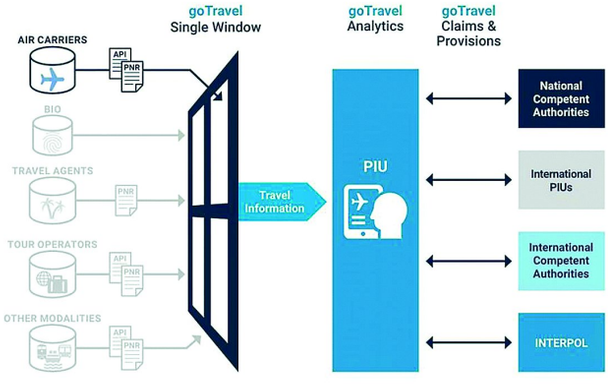
Nederland, Iran en Stuxnet
O.a. In Natanz[8] staat een complex met ultracentrifuges. De Verenigde Staten en Israël zijn zeer gemotiveerd om kernenergie-projecten in Iran te saboteren. Dat konden de landen zonder hulp zelf niet voor elkaar krijgen.



Nucleaire faciliteiten in Iran. Bron: Wikipedia

De Nederlander Erik van Sabben, werkzaam in Iran, speelde een cruciale rol doordat hij in 2007 apparatuur (waterpompen) leverde met daarin verstopt het zeer geavanceerde Stuxnet-virus.
Het is een zeer complex virus dat als een van de eerste de overstap maakt van IT naar machinebesturing. In dit geval heel specifiek naar Siemens PLC's, programmeerbare besturingen.
Erik verongelukte in Iran onder verdachte omstandigheden.

Trip / GoTravel [9]
Misschien wel het meest indrukwekkende verhaal.
Luchthaven Schiphol is een deel van het werkterrein van Jelle Postdam van de AIVD.
'Niet iedere bezoeker van Schiphol komt voor de Floriade' zegt Jelle. Het kost de AIVD moeite om alles in de gaten te houden. Jelle komt in contact met Bosch en TNO. Proefopstellingen met camera's worden geplaatst.
Met software kun je dan heel interessante ontdekkingen doen. Waarom staat iemand al twee uur op dezelfde plek? En waarom komt iemand naar Schiphol en pakt geen aansluitend vervoer en wordt door niemand opgehaald?
Jelle krijgt de opdracht vraag en aanbod bij elkaar te brengen. De hele wereld lijkt geïnteresseerd te zijn in data van telefoonmasten, camera's, kentekens en persoonsgegevens. Door alle data te combineren ontstaat 'Travel Intelligence'. En als je weet dat als een vliegtuig in Nederland landt alle passagierslijsten bekend moeten zijn, dan is 1+1=2. Zo ontstond het 'Travel Information portal', kortweg TRIP.
TRIP wordt ook nog gekoppeld aan de API-gegevens. Dat zijn gegevens die binnengehaald worden als een paspoort gescand wordt. Een gezelschap dat samen een reis boekt maar niet samen verder reist, een passagier die landt op Schiphol en een uur later terugvliegt naar huis. Alles is denkbaar met het koppelen van data. TRIP wordt weggegeven aan diverse landen.
Het intellectueel eigendom van TRIP wordt verkocht aan de Verenigde Naties en wordt omgedoopt tot GoTravel. Helaas kan het ook verkeerd gebruikt worden omdat in de data ook zeer persoonlijke gegevens aanwezig zijn zoals sexuele voorkeur(en). GoTravel gaat de wereld over naar o.a. Saoedi-Arabië, Qatar, Irak, Filipijnen en Soedan.



Netwitness [10]
De Hongaarse instantie NISZ meldt zich bij de Europese directeur van het Amerikaanse RSA.
Zij verkopen het softwarepakket Netwitness dat internetverkeer in de gaten houdt. Netwitness gebruikt deep packet inspection om dataverkeer te ontleden op basis van 'sensoren'. Alles kan worden ontleed. Dus niet alleen mailheaders, website URL's, namen van documenten, maar ook de inhoud ervan.
Hoe meer je betaalt, des te meer sensoren je kunt inzetten.

NETWITNESS®

Bron: https://netwitness.com

Ook het Nederlandse National Cybersecurity Centre gebruikt de software.
De Hongaarse NISZ gaf aan dat ze dreigingen uit Rusland in kaart wilden brengen. Maar na het sluiten van het contract bleek de ware reden: hiermee kon de regering repressie uitvoeren. Het contract en de oplevering van de software

was een half jaar voor de verkiezingswinst van Viktor Orbán van de Fidesz-partij. Een paar jaar later werd het aantal sensoren verdubbeld, tegen bijbetaling natuurlijk.
Iedereen die de krant leest of de media volgt weet wat de gevolgen van de aanschaf van de software zijn in Hongarije.

Tot slot
Ik heb geprobeerd aan de hand van een paar voorbeelden een beeld te schetsen van de inhoud van dat boek. En als ik eerlijk ben is me dat niet volledig gelukt. Het boek bevat gewoonweg te veel informatie om een artikel in de SoftwareBus te vullen. Ook is mijn keuze van de 'highlights' erg selectief. Ik heb gekozen voor onderwerpen die ik interessant vind om door te geven.
Misschien zijn er lezers die inderdaad zeggen: "Dit wil ik inderdaad echt niet weten". En dat kan ik me goed voorstellen. Ook ik als, laten we zeggen, iets meer dan gemiddelde computergebruiker, vind het lastig om een exact beeld te krijgen wat er allemaal mogelijk is.
Maar je kunt ook van menig zijn dat het geen kwaad kan een dergelijk boek te lezen. En na het lezen bepaal je dan zelf wat je met de informatie in het boek doet. De schrijver heeft alle referentie-informatie achter in het boek vermeld.

Resumerend
Als je je ogen goed de kost geeft zie je dat er veel gebeurt in de wereld om ons heen. Maar er gebeurt nog veel in deze wereld waar je geen weet van hebt, of simpelweg niet te zien krijgt. Met dank aan de auteur krijgen we meer inzicht.
Wat ik erg dreigend vind is het feit dat er een tijd aangebroken is waarin we niet altijd kunnen onderscheiden of we te maken hebben met de werkelijkheid of fictie (Fake News). Helaas zal dat alleen maar erger worden.

Goedbedoelde uitvindingen worden uiteindelijk verkeerd gebruikt.
Ik heb aan de hand van een aantal voorbeelden proberen duidelijk te maken dat sommige onderwerpen ver weg lijken, maar er ook voorbeelden dichtbij huis zijn. Wie gaat er nou niet wel eens op vakantie of werkbezoek door gebruik te maken met een vliegtuig?
En datzelfde geldt zeker voor de digitale wereld.
Op dit moment zien we een groeiende belangstelling voor AI. Uiteraard kan die ontwikkeling kan op een goede manier gebruikt worden, maar de software kan ook gebruikt worden op een verkeerde manier, waarvoor deze niet bedacht is.
Feitelijk is de grote verandering op digitaal gebied begonnen met de introductie van de smartphone en gebruik van mobiele netwerken.
En wie maakt daar tegenwoordig geen gebruik van?

Wat te doen?
Ik kan me voorstellen dat er mensen zijn die geen zin hebben om zich te verdiepen in digitale 'werkelijkheid'. Maar denk na over de apps die je op je telefoon zet, de wachtwoorden die je gebruikt en gebruik van 2FA. Klink vooral niet op elke toegestuurde link: altijd nog de beste 'ingang' voor een hacker.
Met een stukje nuchterheid, gezond wantrouwen en de nodige voorzichtigheid kom je een heel eind.
Een aardig website over dit thema vind je hier[11].

Links:

1: Je hebt wel iets te verbergen: **https://decorrespondent.nl/nietsteverbergen**
https://www.compusers.nl/sites/default/files/swb-jaargangen/2016/2016-6/SwB20166_Een-boek-over-privacy.pdf
https://tinyurl.com/34snvnux

2: Stuxnet: **https://nl.wikipedia.org/wiki/Stuxnet**

3: Hacker: **https://nl.wikipedia.org/wiki/Hacker**

4: De 5 fases van een hack/ransomware aanval
https://infosecuritymagazine.nl/artikelen/de-vijf-fases-van-een-ransomware-aanval-en-wat-er-tegen-te-doen
https://tinyurl.com/2urm34m5

5: Zie ook het interview bij Buitenhof: **https://www.youtube.com/watch?v=BQXmeWCMVZ0**
https://tinyurl.com/5a2kzkca

6: KPN en Huawei: **https://privacy-web.nl/nieuws/huawei-had-toegang-tot-persoonsgegevens-via-serverruimte-bij-kpn/**
https://tinyurl.com/mrhxp9j8

7: Pegasus **https://nl.wikipedia.org/wiki/Pegasus_(spyware)**

8: Iran, nucleaire faciliteiten **https://en.wikipedia.org/wiki/Nuclear_facilities_in_Iran**
https://tinyurl.com/5fy9mc9u

9: GoTravel: **https://www.un.org/cttravel/goTravel**

10: NetWitness: **https://www.netwitness.com/**

11: Laat je niet Hacken **https://www.laatjeniethackmaken.nl/**

Bonus:

Clearview **https://en.wikipedia.org/wiki/Clearview_AI**

Pimeyes: **https://pimeyes.com**

Shodan: **https://www.shodan.io/**