

Het is oorlog!

Echt oorlog, en een hele geniepige. Nee, dit keer geen soldaten in loopgraven, tanks op een slagveld, (aatom)bommen of luchtaanvallen. Het zijn cyberoorlog en cyberterreur die ons land, onze samenleving aanvallen. Deze oorlog kost geen levens maar wel ons leven.

Maar niet alleen de cyberaanvallen door naties ondermijnen onze veiligheid, ook wat cybercriminelen, van kleine individuen tot georganiseerde bendes, in de digitale wereld met ons doen. Begrippen als hacken, phishing, DDoS, internetfraude, trollen, computervirussen en nog vele andere, maken duidelijk dat er een nieuwe vorm van criminaliteit is ontstaan. En helaas, we zijn ons nog te weinig van deze bedreigingen bewust (vindt ook defensie minister Ank Bijleveld).

Wie realiseert zich dat ieder apparaat dat met internet verbonden is gezien moet worden als een – potentiële – “spion”? We worden regelmatig gewaarschuwd om onze smartphones niet bij ons te hebben in bepaalde situaties en zeker niet aan te zetten tijdens gesprekken die geheim moeten blijven. Maar wat te denken van een auto met spraak gestuurde functies? Wat denk je dat die spraakfuncties kunnen opvangen en doorgeven? Of wat er via de sociale media aan gegevens van jou ontfutseld worden? De waslijst van mogelijke openingen voor criminele acties is vrijwel onbeperkt.

Het echte probleem daarbij is, dat we ons dat veel te weinig bewust zijn. Wie is er de hele dag mee bezig zijn veiligheid in de gaten te houden als hij iets online doet? Ons eigen gedrag is dan ook het grote lek waar criminelen, en andere landen, gebruik van maken.

Waar we als individuele burger weinig aan kunnen doen, buiten digitale waakzaamheid, is wat landen elkaar aan kunnen doen middels cyberaanvallen, cyberterreur. De taken van Defensie zullen daarom steeds meer (moeten) verschuiven naar de digitale wereld. Het sturen van vliegtuigen, marineschepen of tanks naar andere gebieden, zal grotendeels vervangen worden door de inzet van drones, satellieten, computers en data. Soldaten kruipen niet meer door de modder van een slagveld, maar zitten in eigen land achter de computer te kijken naar wat er op ons afkomt. Er kan van afstand ingegrepen worden door de inzet van drones, al dan niet met bommen of camera's.

Wat wij als individuen ervaren middels bijvoorbeeld hacking, phishing of andere vormen van cybercriminaliteit, gebeurt op grotere schaal tussen bedrijven maar ook tussen landen. We worden de hele dag geconfronteerd met cyberterreur en cyberoorlog. We hebben kwetsbare infrastructuren, zoals de Rotterdamse haven, Schiphol, ons elektriciteitsnet, de waterkeringen, internet en vele andere objecten. Af en toe merken we de gevolgen van een aanval die heeft plaatsgevonden. We moeten ons realiseren dat de cyberdreigingen dagelijks actueel zijn. Zelf kunnen we als individu een bijdrage leveren aan het beperken van die cyberdreigingen door veel bewuster en zorgvuldiger om te gaan met onze digitale middelen.

Het stemt enigszins gerust dat onze eigen Defensie deze richting in lijkt te slaan, mits ze daarvoor de benodigde gelden en mankracht kunnen verwerven. Waar we als land mee bezig moeten zijn, is dat er een voor de burger vrijwel “onzichtbare” oorlog gevoerd wordt, nu al en laten we daar niet naïef over doen. Iedere dag loeren trollen, DDoS-aanvallers, nepnieuws en andere digitale activiteiten op hun kans onze systemen aan te vallen en onze samenleving te ontwrichten. Er is dus heel veel inspanning nodig, zowel kennis als geld, om ervoor te zorgen dat we minder kwetsbaar zijn voor dergelijke aanvallen. Inmiddels is de politiek door schade en schande, die niet altijd publiekelijk bekend wordt gemaakt, wijzer aan het worden.

Voorlichting en ondersteuning van de burgers op dit vlak is daarbij een belangrijke taak voor de overheid. Dat betekent dat zij op een snelle en effectieve manier **alle** burgers moet kunnen bereiken, niet alleen wanneer een dreiging acuut is, maar ook voor het nemen van voorzorgsmaatregelen, voor voorlichting en ondersteuning. Om dat waar te maken, zal van overheidswege geïnvesteerd moeten worden in tenminste een veilig communicatiesysteem met de burgers, en hoe eerder hoe beter. Een kenmerk van de digitale wereld is immers dat alles er erg snel gaat!