

# Donderdag 25 augustus 2011

## België heeft geen antwoord op cyberaanvallen

Sofie Vanlommel

25-08-2011

Pag. 10

België heeft geen antwoord op cyberaanvallen

BRUSSEL | Een gebrek aan coördinatie en globaal beleid maakt ons land erg kwetsbaar voor cyberaanvallen. Dat stelt het Comité I in een scherp onderzoeksrapport. Het controleorgaan stelt voor dat de Staatsveiligheid achter de stuurknuppel van de cyberbescherming gaat zitten. Maar die heeft te weinig middelen.

Door Sofie Vanlommel

Een van de Belgische drama's, zo noemt Bart Preneel, hoogleraar informatiebeveiliging van de Katholieke Universiteit Leuven, het federale cyberbeleid. Of beter: de afwezigheid ervan. "De noden zijn nationaal, het onderzoek zit regionaal, de kritische massa zit verspreid en er is geen rampenplan." Het Comité I lijst eigenlijk oude noden op, zegt Preneel. "Al jaren roepen we om een coördinatiecentrum. Er is dringend nood aan een geïntegreerd beleid waarin overheid, industrie en onderzoek betrokken zijn. Idealiter wordt dat gevoerd door de premier, die op kritieke momenten knopen doorhakt."

Maar liefst zeven instellingen houden zich bezig met de virtuele beveiliging van ons land: de inlichtingendiensten van Defensie (ADIV) en hun civiele tegenpool (Staatsveiligheid), de Federal Computer Crime Unit van de gerechtelijke politie, de Nationale Veiligheidsoverheid, die verschillende federale overheden verenigt, de Federale Overheidsdienst Informatie- en Communicatietechnologie, die belast is met e-government, de beheerder van het glasvezelnetwerk Belnet en de Belgische Regulator voor de Postdiensten en de Telecommunicatie.

Te veel bomen in het bos en niemand die nog weet nog wat er van hem of haar verwacht wordt, concludeert het rapport. Dat alles maakt ons land "zeer kwetsbaar voor aanvallen tegen zijn vitale informatiesystemen en netwerken". Lees: één welgemikte trap uit cyberspace, en het land gaat plat.

Volgens het Comité I is de dreiging reëel. Op dit moment is er geen plan als de informaticasystemen van de federale overheden online onder vuur worden genomen. Hetzelfde geldt voor levensbelangrijke infrastructures zoals water, licht en energie. "ICT en kritische infrastructuur raken steeds meer met elkaar verbonden", zegt Bart Perneel. "Van het beheer van chemische fabrieken tot de coördinatie van het waterbeheer, alles verloopt via internet. In Australië zijn hackers al ingebroken in het afwateringssysteem."

## Gebrek aan personeel

Bij een virtuele aanval op militaire informatie mag de inlichtingendienst van Defensie counteren. Het Comité I stelt voor om de Staatsveiligheid hetzelfde te laten doen voor de overheid en de burgers. Al kampt diezelfde inlichtingendienst volgens het rapport met een manifest gebrek aan gekwalificeerd ICT-personeel, dat liever naar de beter betaalde privésector trekt.

Er is bij alle betrokken diensten een gebrek aan efficiënte technische middelen: gevoelige informatie wordt niet veilig genoeg uitgewisseld. De technologie die de Nationale Veiligheidsoverheid gebruikt noemt het rapport "absoluut ontoereikend". En de leveranciers van de noodzakelijke software komen uit het buitenland. De banden die deze firma's met andere buitenlandse veiligheidsdiensten hebben, zijn onduidelijk. Volgens het Comité I is er dringend nood aan meer controle op die bedrijven.

"Als men ons bevoegdheden wil toekennen, moeten daar meer middelen en mensen tegenover staan", reageert directeur-generaal Alain Wynants. "Cyberveiligheid neemt zeer grote proporties aan." Al rekent hij niet op grote gebaren. "Het budgettaire klimaat is niet positief."