



De enige plek in het Center of Excellence Cooperative Cyber Defense in Tallinn waar we binnen mochten fotograferen.

Digital War Room

In Estland werken IT-experts uit tien verschillende landen samen onder toezicht van de NAVO om de toekomst van oorlogsvoering het hoofd te bieden. Want of het nu vijandige militaire organisaties, geïnfecteerde botnets of enthousiaste pubers met een internetverbinding zijn, iedereen kan communicatienetwerken, websites en uiteindelijk zelfs een heel land platleggen.

Grenscontroles ontregelen, de luchtverdediging lamleggen, e-voting beïnvloeden, het kan allemaal in cyberspace

Op een legerbasis vlakbij het historische centrum van de Estse hoofdstad Tallinn ligt een van 's werelds meest geavanceerde militaire onderzoeksinstituten. Ooit legerde Tsaar Nicolaas II hier zijn verbindingstroepen. Nu heeft de NAVO er een Center of Excellence, een onderzoekscentrum met dertig medewerkers dat de juridische en vooral technische aspecten van digitale oorlogsvoering onderzoekt. 'Typisch iets wat je op internationaal niveau moet aanpakken', zegt Kenneth Geers, een Amerikaanse onderzoeker en een van de weinige burgers in het centrum waar verder vooral breedgeschouderde mannen in groene uniformen rondlopen. 'Beeld je maar eens in hoe dat werkt. Als men ergens ter wereld te maken krijgt met een serieuze cyberaanval, dan zie je niet veel meer van je dader dan een lijst met IP-adressen uit alle hoeken van de wereld. Bij de lokale politiedienst gaat dat zo weer de prullenbak in. Daarom is de NAVO de ideale organisatie om de eerste stappen te zetten. Grenscontroles ontregelen, de luchtverdediging lamleggen, e-voting negatief beïnvloeden of uiteindelijk zelfs je vijand met zijn eigen wapens aanvallen, het kan allemaal in cyberspace', legt hij uit. 'Maar nog niet iedereen heeft in de gaten dat het allemaal samenhangt.'

Als er één land ter wereld is waar dat besef wel is doorgedrongen, dan is het Estland. Toen de overheid in 2007 een oorlogsmonument uit de Sovjettijd naar een bui-

tenwijk wilde verplaatsen, brak er heibel uit. De Russische minderheid voelde zich gekrenkt en ging de straat op. In Moskou moest de Estse ambassadeur zijn spullen pakken en terwijl in Tallinn demonstranten vochten met de oproerpolitie gingen de websites van verschillende overheidsdiensten, banken en dagbladen offline. Een 'ouderwetse' DDoS-aanval waarbij computernetwerken worden ingezet om zo vaak webpagina's op te vragen dat de servers onder de druk bezwijken. Het elektronisch bankiersstelsel werkte niet meer, de nieuwsvoorziening lag plat en wat in Estland al jaren gemeengoed was - de digitale overheid - bestond plots niet meer. In de ministeries, banken, bedrijven en scholen moesten de directeurs en ministers plots op zoek naar faxpapier.

Pionierswerk

'Betere promotie konden wij ons natuurlijk niet voorstellen', lacht Geers. De plannen voor het Cooperative Cyber Defense centrum lagen al sinds 2003 op tafel, maar dankzij de cyberaanval kwam het project op stoom. 'Als we er nu op terugkijken viel het wel mee, zo'n DDoS-aanval is vrij amateuristisch. Maar er zijn in die tijd ook routers overgenomen en de interface van een aantal belangrijke sites is gehackt', legt Kaur Kasak uit, een jonge Estse onderzoeker. 'We konden het na een tijdje rerouten naar zwarte gaten, maar het heeft wat moeite gekost.'

ADV



Ziekenwagen op de binnenplaats: een virus alert?

Het is oorlog, alleen zie je 'm niet

Tussen de twee onderzoekers zit een jonge vrouw die fanatiek aantekeningen maakt en uitlegt wat ik wel en niet mag fotograferen. Beeldschermen, hardware, nooduitgangen, videocamera's en zelfs stopcontacten mogen niet op de foto. 'En liever geen foto's van de bibliotheek', zegt ze. 'We hebben een magere collectie. Alles is digitaal tegenwoordig. Maar dat ziet er zo treurig uit, een lege bibliotheek.'

Hoewel het voor de hand ligt dat de daders in Rusland gezocht moeten worden, wijst het centrum niemand aan. 'De golf aan internetverkeer kwam uit de hele wereld, van Peru tot Egypte. En het probleem is dat bewijs niet alleen moeilijk te verkrijgen is, het is ook nog makkelijker te fabriceren', legt Geers uit. 'Daarom hebben we hier een juridische afdeling. Want wat is een aanval precies? En als het dan een aanval is, hoe zit het met het principe waar de NAVO uit ontstaan is, namelijk dat een aanval op een lidstaat een aanval op alle lidstaten is? We doen hier pionierswerk.' In de kelder van het gebouw staat de technische hardware, een 'NAVO Zone II' gebied. Niet voor potentiekijkers dus. De rest van het gebouw doet aan een middelbare school denken.

'Het is oorlog, alleen zie je 'm niet', zegt Ain Rasva, hoofd IT bij SEB, de op één na grootste financiële dienstverlener in Estland. 'Wij kunnen ons steeds beter beveiligen, maar hackers worden steeds innovatie-

ver. Wat er toen gebeurde is kinderspel vergeleken bij wat we nu zien, zij het op een veel kleinere schaal.' In 2007 lag het elektronisch bankiersysteem van SEB er twee dagen uit. 'En je moet je realiseren dat 95 tot 97 procent van onze transacties digitaal verlopen. We hebben het dataverkeer moeten afsluiten voor het buitenland, maar daar dupeer je nog altijd een groot deel van je klanten mee.' Volgens Rasva is het een geluk dat Estland maar een klein land is. 'Iedereen kent elkaar. Met één telefoontje kon ik bij de hoster aanpassingen doen en een paar minuten later heb je de minister van Defensie aan de lijn.' In Estland zijn ondertussen op parlementair niveau afspraken gemaakt en bestaan er draaiboeken voor het geval Russische hackers weer toeslaan. Net als veel andere instellingen tekende ook SEB-bank een samenwerkingsverdrag met het NAVO-centrum.

'Wat hier gebeurde was niet zomaar een incident', legt Kenneth Geers uit. Het gebeurt veel vaker. 'Toen het Centraal-Aziatische land Kirgizië onlangs overwoog wel of geen bases te herbergen voor de Amerikanen in het kader van de oorlog in Afghanistan heeft ook dat land lang onder digitaal vuur gelegen. Ze hebben het weken met amper 20 procent van de bandbreedte moeten doen. Dit zijn relatief kleine, geïsoleerde landen. In de westerse wereld zou de schade enorm zijn.'