Wie treedt op als onze digitale samenleving wordt bedreigd?

Hoe kan het vertrouwen in de digitale samenleving groeien?

Highlights

- Vertrouwen in het digitale domein is belangrijk voor de verdere ontwikkeling van de vrije en welvarende digitale samenleving wereldwijd.
- Maar digitale aanvallers hebben nog steeds vrij spel.
- Effectieve digitale verdediging kan niet zonder digitale afschrikking.
- Een vrije digitale samenleving is kwetsbaar, daar moet het publiek op voorbereid zijn.
- De huidige cyberwar moet daarom beter zichtbaar worden voor het publiek.

Scan deze pagina
en bekijk de video.

Het vertrouwen van de burger wordt steeds meer beïnvloed door incidenten in het internationale cyberdomein, blijkt uit ons onderzoek. Cybersecurity is daarom ook al vele jaren een terugkerend thema in verschillende beleidsnota's van de regering, recentelijk onder meer opnieuw in de geïntegreerde Buitenland en Veiligheidsstrategie en de laatste Defensienota. De vraag is alleen of dit beleid nu ook al heeft geresulteerd in meer cyberveiligheid voor de samenleving. In het fysieke domein zijn veiligheidsmaatregelen over het algemeen direct zichtbaar. Maar wat merkt de burger nu van de veiligheidsmaatregelen in het digitale domein en wellicht nog belangrijker: ontmoedigen deze maatregelen ook daadwerkelijk de potentiële buitenlandse cyberaanvallers? Wat zou er nodig zijn om deze effecten te versterken.

De veiligheidsperceptie van de burger is een vaak terugkomend onderwerp in de media en de politiek. En meestal gaat het dan over het verschil tussen de werkelijke veiligheid en het subjectieve veiligheidsgevoel in onze directe leefomgeving.

Het gaat echter minder vaak om de internationale component van die veiligheidsperceptie. Na vele jaren van afwezigheid, werd internationale veiligheid bij de laatste parlementsverkiezingen ineens wel een thema. Er speelt dan ook genoeg om ons zorgen over te maken; MH17, de Krim, Trump, Brexit, Erdogan, vluchtelingen etc. Met de forse herintensiveringen in het defensiebudget kan ons defensiematerieel weer verder gemoderniseerd worden en kunnen de gaten in de personele bezetting weer worden gevuld.

Maar leveren deze intensiveringen dan ook meer vertrouwen op bij de burger? Wat heeft de kiezer nodig om meer vertrouwen te krijgen in onze internationale veiligheid? Hij ziet het militair vermogen bij de daadwerkelijke inzet van de krijgsmacht in ernstmissies, maar ook bij grootschalige oefeningen, bij open dagen en bij openbaar militair ceremonieel. En die waarnemingen dragen bij aan het veiligheidsgevoel. Daarom gebeurt het ook. Maar die demonstraties van militair vermogen zijn natuurlijk niet alleen voor binnenlandse doeleinden. Zeker zo belangrijk, of misschien wel belangrijker, is de internationale uitstraling van dit militair vermogen, naar opponenten en naar bondgenoten.

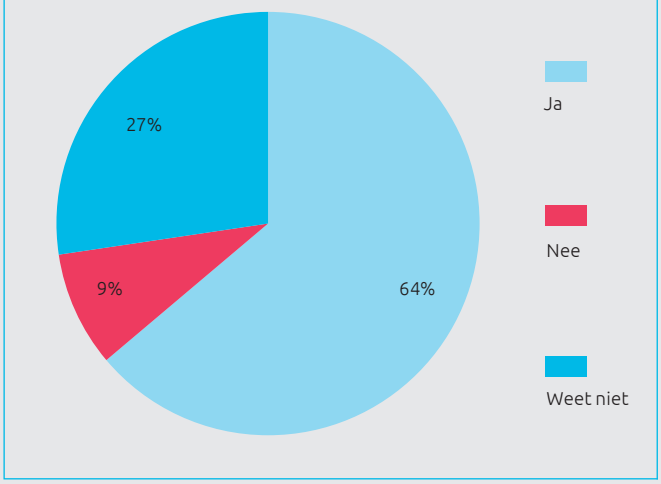
Militair vermogen wordt wel gedefinieerd als het product van 'military capabilities and political intentions'. Intenties kunnen echter snel veranderen, capabilities niet. Opbouw van effectief inzetbare 'military capabilities' kost zeer vele jaren en die moet dus in allerlei vormen voortdurend beschikbaar zijn. Mede door het extra budget wordt daar door defensie nu ook hard aan gewerkt. Ons militair vermogen en dat van onze bondgenoten beïnvloeden het gedrag en de strategie van anderen. Een opponent zal geen aanval uitvoeren als er in geen enkel opzicht voordeel te behalen valt. En dat is wat we willen bereiken: afschrikking.

Digital show of force

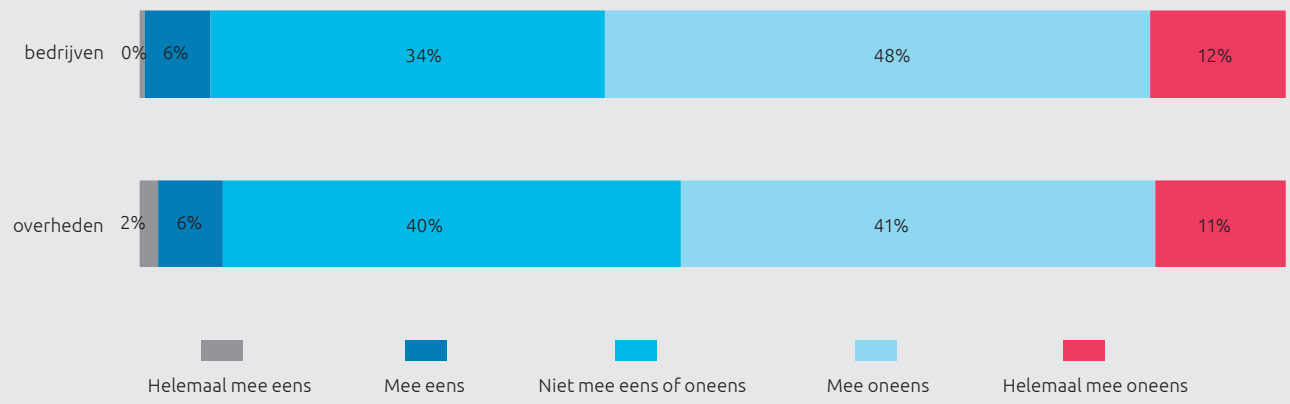
Nu militaire cybercapaciteit onderdeel is van de capabilities van onze krijgsmacht is het de vraag hoe deze capaciteit kan bijdragen aan het versterken van het vertrouwen van de burger in de digitale samenleving. En hoe dit tegelijk onze tegenstanders kan afschrikken: een 'digital show of force' dus. In het GfK-onderzoek in opdracht van Capgemini van 2018 bleek, net als het jaar daarvoor, dat de burger het aanzienlijk aannemelijker vindt dat ons land wordt aangevallen in het cyberdomein dan dat we worden aangevallen in het fysieke domein. Verder blijkt uit het onderzoek dat een grote meerderheid van de burgers er nu geen vertrouwen in heeft dat Nederland voldoende voorbereid is op een cyberoorlog.

Als het veiligheidsgevoel van de burger belangrijk is -en dat is het, zo bleek uit de debatten voorafgaand aan de parlementsverkiezingen in 2017- dan moet de politiek en de krijgsmacht iets doen om te laten zien dat onze military cyber capabilities ook indruk maken en werkelijk inzetbaar zijn. Dat vertrouwen is een randvoorwaarde voor de verdere ontwikkeling van de vrije en welvarende digitale samenleving wereldwijd.

Figuur 1: 64% acht een digitale aanval op Nederland waarschijnlijker dan een fysieke aanval.



Figuur 2: De Nederlands bedrijven/overheden zijn voldoende voorbereid op een mogelijke cyberoorlogvoering.



Hoe kan het vertrouwen in de digitale samenleving groeien?

Wat gebeurt er nu al in het militaire cyberdomein? Waarneembare activiteiten van het Nederlandse militaire cybercommando zijn nu onder meer strategische beschouwingen in diverse nationale en internationale fora en kleinschalige oefeningen. Verder trekken nu eigenlijk alleen cyberoperaties van de grote machthebbers de aandacht. Mede dankzij Snowden weten we dat de Amerikanen daarin heel ver zijn. Dat bleek onder meer ook uit de Stuxnet-operatie in Iran. Maar natuurlijk ook de voorbeelden van vele andere cyberoperaties van bijvoorbeeld Rusland tegen de Oekraïne, Georgië en de Baltische staten. Ook over de capaciteiten van China, Israël en Iran wordt regelmatig gepubliceerd. Het effect van deze incidenten is dat we weten dat deze landen serieus werk gemaakt hebben van hun 'cyber capability building'. De vraag is wat wij daar als Nederland, op onze schaal, tegenoverstellen?

'Hackers AIVD leverden cruciaal bewijs over Russische inmenging in Amerikaanse verkiezingen'

Publicaties in de Volkskrant over de cybercapaciteit, van onze inlichtingendiensten in de affaire rond de Russische inmenging in de Amerikaanse verkiezingen, hebben nationaal en internationaal indruk gemaakt. Een opzienbarend relaas over de wijze van optreden, waaruit blijkt dat er kennelijk geavanceerde cybercapaciteit aanwezig is en ook het inzicht om de juiste doelen te onderzoeken. Maar er is meer bijzonder aan dit incident. Daar waar een vergelijkbare operatie van Rusland in het fysieke domein direct zou leiden tot tegenreacties, gebeurt er nu ogenschijnlijk weinig. De drempel voor operaties in het cyberdomein is dus veel lager. Ook lijkt het erop dat de cyberwar al lang aan de gang is, maar dat die zich grotendeels afspeelt in en tussen inlichtingendiensten en daarmee buiten het zicht van het publiek. Op korte termijn is dat prettig omdat daarmee de perceptie van onveiligheid bij burgers niet verder wordt vergroot. De keerzijde is dat de urgentie bij burgers en bedrijven om zich beter te beschermen, achterblijft. Daar hebben de krijgsmacht en de inlichtingendiensten niet direct last van, maar de samenleving als geheel natuurlijk wel. Want het blijft voor de burger de vraag of de regelmatig optredende verstoringen in de publieke dienstverlening nu gewone verstoringen zijn, of dat ze het resultaat zijn van cyberhacks van geheime diensten?

> *The defensive form of war is not a simple shield, but a shield made up of well-directed blows.*
>
> **Generaal Von Clausewitz**

Bescherming van de vrije digitale samenleving, wereldwijd

Hoe dik je de muren van de digitale beschermingswal ook maakt, er zijn altijd zwakke plekken te vinden en ook zullen er altijd aanvallers zijn die de risico's zullen trotseren. Ondermijning van onze westerse rechtsorde en bondgenootschappen is nu eenmaal een erkend doel van onze opponenten. Veiligheid heeft daarom ook een morele kant: de bereidheid om te incasseren en offers te brengen omdat we ervan overtuigd zijn dat het doel, de vrije digitale internationale samenleving, een universeel mensenrecht is. En dat een vrije digitale samenleving in alleen één land of regio, 'America first', geen recht doet aan die universaliteit en daardoor feitelijk zal leiden tot vermindering van onze weerbaarheid. Die morele weerbaarheid, het collectieve incasseringsvermogen, staat in de huidige tijd onder druk. Voorbeelden daarvan zijn de reacties van het grote publiek op het Oekraïne referendum, het vluchtelingdebat en de Brexit.

Weerbaarheid

Vaak blijkt uit analyses van cyberincidenten dat de aanvalsmethoden niet bijzonder geavanceerd waren maar dat de cyberslachtoffers hun basisbescherming niet op orde hadden. Onder weerbaarheid wordt de combinatie verstaan van kennis en bewustzijn van burgers, de technische beschermingsmaatregelen en de capaciteit om in geval van crisis weer snel te herstellen. Het versterken van onze digitale weerbaarheid is deels een individuele en deels een collectieve verantwoordelijkheid en het vergroten van onze maturity bij het invullen van die verantwoordelijkheden vereist nog veel meer aandacht en investeringen. De krijgsmacht heeft hier geen bijzondere rol in, anders dan het ondersteunen van de civiele autoriteiten in het geval van (digitale) rampen.

Digital combat capabilities en digital human rights

Nog meer dan in de civiele omgeving is het ook voor de krijgsmacht essentieel om de digitale weerbaarheid in al haar eigen structuren en systemen goed in te richten. Onze eigen fysieke en digitale militaire capaciteit mag immers niet aangetast kunnen worden door cyberverstoring. Maar dat is niet zo eenvoudig. Ook een goed beveiligde krijgsmacht zal mede door de vele afhankelijkheden van civiele capaciteiten en services altijd kwetsbaar blijven. Voor die gevallen is offensieve vergeldingscapaciteit nodig. Een cyberaanval mag, volgens sommige internationaalrechtelijke experts, beantwoord worden met een tegenaanval in het fysieke domein. Maar strategisch gezien is dit niet erg realistisch door de onvoorspelbaarheid van het effect en de risico's van verdere escalatie. Bovendien blijft de attributie ingewikkeld: weet je wel voldoende zeker wie er achter een aanval zit? Ten slotte geldt altijd dat een tegenaanval proportioneel moet zijn en subsidiair. Als een fysieke tegenaanval niet realistisch is dan resteert dus alleen een reactie in het cyberdomein zelf. Vergeldingsvermogen in het cyberdomein is dus eigenlijk onmisbaar.

Vergeldingsvermogen moet vervolgens ook publiek bekend zijn en dus niet geheim blijven. Om het beoogde doel te bereiken, zal het publiek én de opponent moeten kunnen waarnemen dat dit digitale vergeldingsvermogen er echt is en dat die ook indrukwekkend is. Natuurlijk zullen sommigen betogen dat deze vorm van afschrikking een magneeteffect kan hebben ('honeypot') en digitale aanvallen zal uitlokken en zo zal bijdragen aan een cybergeweldspiraal. Ook kan het een impuls geven aan de groei van een militaire cyberindustrie en daarmee aan verdere proliferatie van dergelijke cyberwapens naar ondemocratische regimes. Allemaal waar, net zo waar als dat in het analoge domein ook was en nog steeds is. Maar het alternatief, digitaal pacfisme, is ook ook geen oplossing.

Zoals eerder gesteld, is weerbaarheid meer dan alleen het voorzien in digitale beschermingsmaatregelen. Het bevorderen van de internationale rechtsorde, dus ook de digitale, is de tweede hoofdtaak van de krijgsmacht en van groot belang voor de geloofwaardigheid van onze waarden op het gebied van democratie, mensenrechten en de rechtstaat. Onze militaire digitale capaciteiten moeten dus ook geschikt zijn om daar een bijdrage aan te leveren. En het is belangrijk dat dat ook zichtbaar is voor het grote publiek, maar ook voor de dissident ver weg en zeker ook voor zijn onderdrukker.

Conclusie

We moeten onszelf digitaal goed beschermen, dat spreekt voor zich. We hebben alleen wel een capabel en zichtbaar apparaat nodig dat ons daarbij helpt. Een apparaat dat, als het toch fout gaat, hard kan terugslaan. De aanvaller moet vooraf weten dat dit terugslaan ook echt gebeurt en dat dit pijn gaat doen.

Het moet tenslotte mogelijk worden om ons digitale militaire vermogen in te zetten voor het waarborgen van de digitale internationale rechtsorde en de mensenrechten. Dat kan consequenties hebben als een dergelijke interventie tot repercussies leidt. De offers die we dan eventueel moeten brengen, zijn echter de moeite waard. Niet alleen omdat onze interventies bijdragen aan een betere wereld, maar ook omdat dit van belang is voor de geloofwaardigheid van onze waarden en het publieke draagvlak van de digitale krijgsmacht.

Over de auteur:

Peter Kwant (Executive Master Security & Defence) is principal consultant cybersecurity bij Capgemini en voormalig marineofficier.

Voor meer informatie kunt u contact met de auteur opnemen via:

peter.kwant@capgemini.com |
https://www.linkedin.com/in/peter-kwant-06b5b811/