Safety first

Onlangs was ik te gast bij collega's van het Commando Landstrijdkrachten (CLAS) te Apeldoorn. Een mooi pand op de Frank van Bijnenkazerne, zeer interessante mensen en alleszins bevredigend voor de leer- en nieuwsgierigheid.

Naar aanleiding van een vorige column, die over lek gestoken banden van militaire voertuigen op een geheel andere kazerne, was ik uitgenodigd om me te laten informeren over integrale veiligheidszorg. Inderdaad, onder andere over de beveiliging van militaire complexen.

Beveiliging heeft iets heiligs. Niet iedereen hoeft er het fijne van te weten om te onderkennen welke gevolgen een verkeerde beveiliging kan teweegbrengen. Ik wil zelf niet precies van de hoed en de rand weten welke beveiligingsmaatregelen er allemaal zijn, dus het mag duidelijk zijn dat ik van het 'fijne', gehoord en gezien bij CLAS, niets wereldkundig maak. Onze Minister heeft dat fijntjes duidelijk gemaakt in zijn brief over veiligheidsbewustzijn die bij alle Defensiemedewerkers op de mat is geploft: "Door onzorgvuldig en onjuist gebruik van digitale (opslag)middelen [...] loopt Defensie risico's."

De snelheid én het gemak van de nieuwe media (gsm, internet) werken veiligheidsonbewust gedrag in de hand. De eenvoud waarmee een leek in no-time een weblog of website kan creëren én op het internet kan uploaden, kan het imago van Defensie danig schaden.

Als Defensiemedewerkers vanuit een inzetgebied zo'n site uploaden, dan kunnen alleen al de (deels) herkenbare gezichten en naamplaatjes een risico betekenen voor het thuisfront van de militairen én de organisatie.

Hetzelfde geldt voor gsm-gebruik. Wanneer gebruik kan worden gemaakt van een handige handy, kunnen bij een eventualiteit het thuisfront en de media eerder op de hoogte zijn dan het Defensie Operatie Centrum (DOC). Een ongeval of aanslag, de mobiele telefonie in verkeerde handen, op het verkeerde tijdstip én op de verkeerde plaats is verdoemd.

Terug naar internet. Een machtig mooi medium. Ervan uitgaande dat onze potentiële vijanden minimaal even slim en enthousiast zijn als wij, kan hun inlichtingenwerk op basis van door ons geuploade informatie op het World Wide Web (cijfercoördinaten, gezichten, achternamen, naamplaatjes e.v.a.) soms opvallend gemakkelijk leiden tot een reactie of, erger nog, pro-actie. Operationele schade kan het gevolg zijn. Veiligheids- en imagoschade zijn funest voor elke organisatie, maar beslist voor eentje die deelneemt aan risicovolle operaties waar te allen tijde mensenlevens mee gemoeid kunnen zijn. Een zo groot mogelijke bescherming van het personeel tegen welke dreiging dan ook heeft de hoogste prioriteit. Uruzgan is een schoolvoorbeeld.

Het (her)publiceren van informatie uit zogenaamde open bronnen is geen probleem, tenzij de defensiemedewerker kan weten of vermoeden dat bepaalde informatie operationele en/of politieke consequenties heeft. Niet tot publicatie overgaan is dan een morele verplichting. Veel door defensiepersoneel gemaakte (privé-)websites zijn eerder een copy/paste-samenraapsel van niet-gerubriceerde en positief gezinde informatie die ook elders in open bronnen heeft gestaan, dan een veiligheidsrisico. Gelukkig maar! Ik zou het niet graag op m'n geweten willen hebben dat door mijn toedoen gevaar voor personen plaatsvindt. Vanaf deze plaats dank aan de kolonel X en de overste Y, voor het extra veiligheidsbewuste inzicht dat zij mij hebben bijgebracht.

> "... welke gevolgen een verkeerde beveiliging kan teweegbrengen"

Marcel van Hemert, onderofficier bij het Regiment Geneeskundige Troepen van het Dienstvak Logistiek, schrijft deze column op persoonlijke titel.