PROTECTED CORE NETWORKING

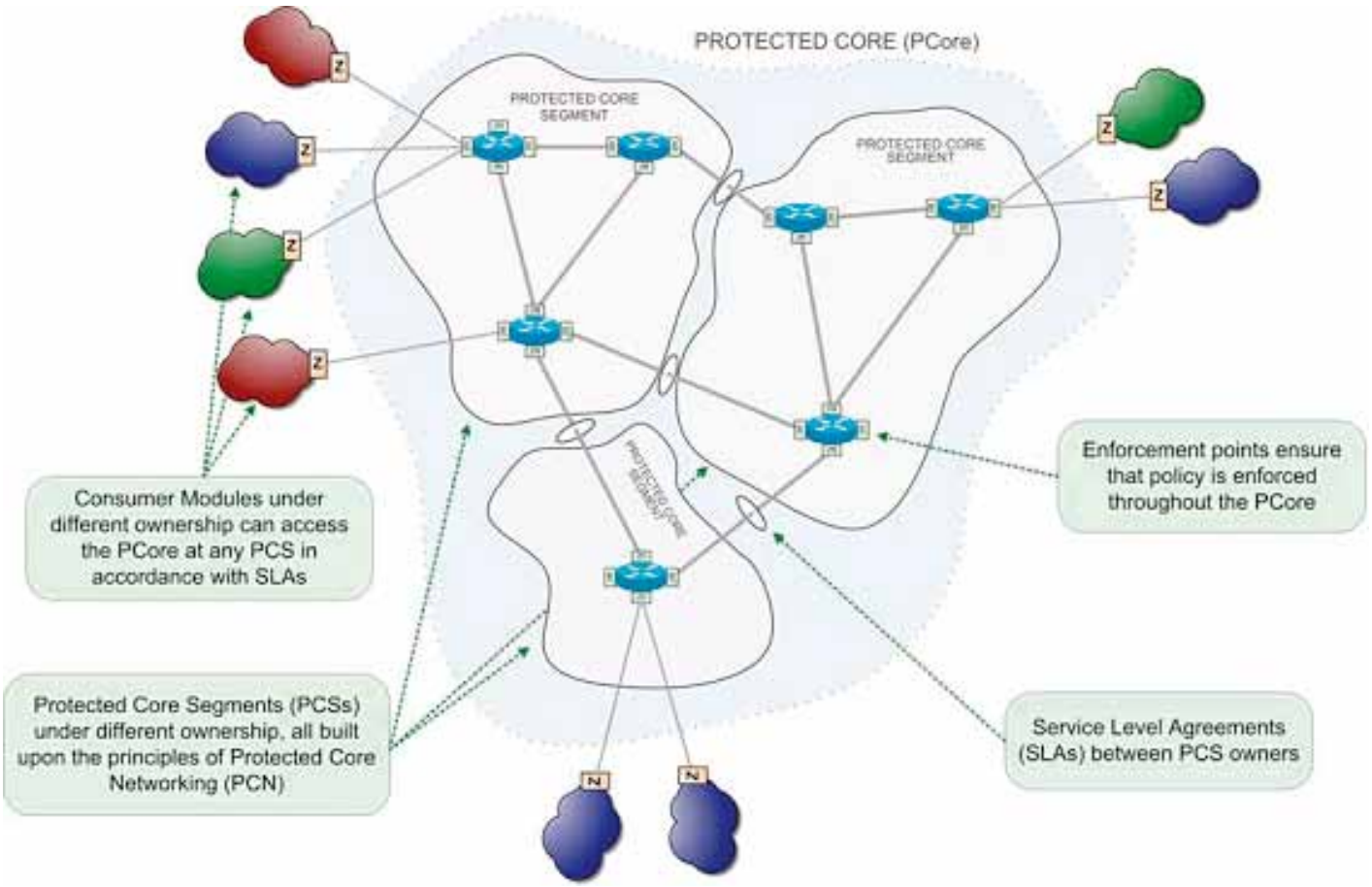
Luitenant-kolonel Ron Bertelink, informatiebeveiligingsarchitect bij DMO/C2SC

Lkol Ron Bertelink is werkzaam bij het Command & Control Support Centre van de Defensie Materieel Organisatie als informatiebeveiligingsarchitect. In deze functie is hij onder meer verantwoordelijk voor de informatiebeveiliging binnen TITAAN en BMS. Naast een groot aantal operationele functies waaronder bataljonscommandant en een tweetal uitzendingen heeft hij meer dan 14 jaar ervaring in verschillende functies als specialist in de militair operationele informatiebeveiliging. In dit artikel beschrijft hij een voor Defensie Netwerk Informatie Infrastructuur geheel nieuwe concept: *Protected Core Networking*.

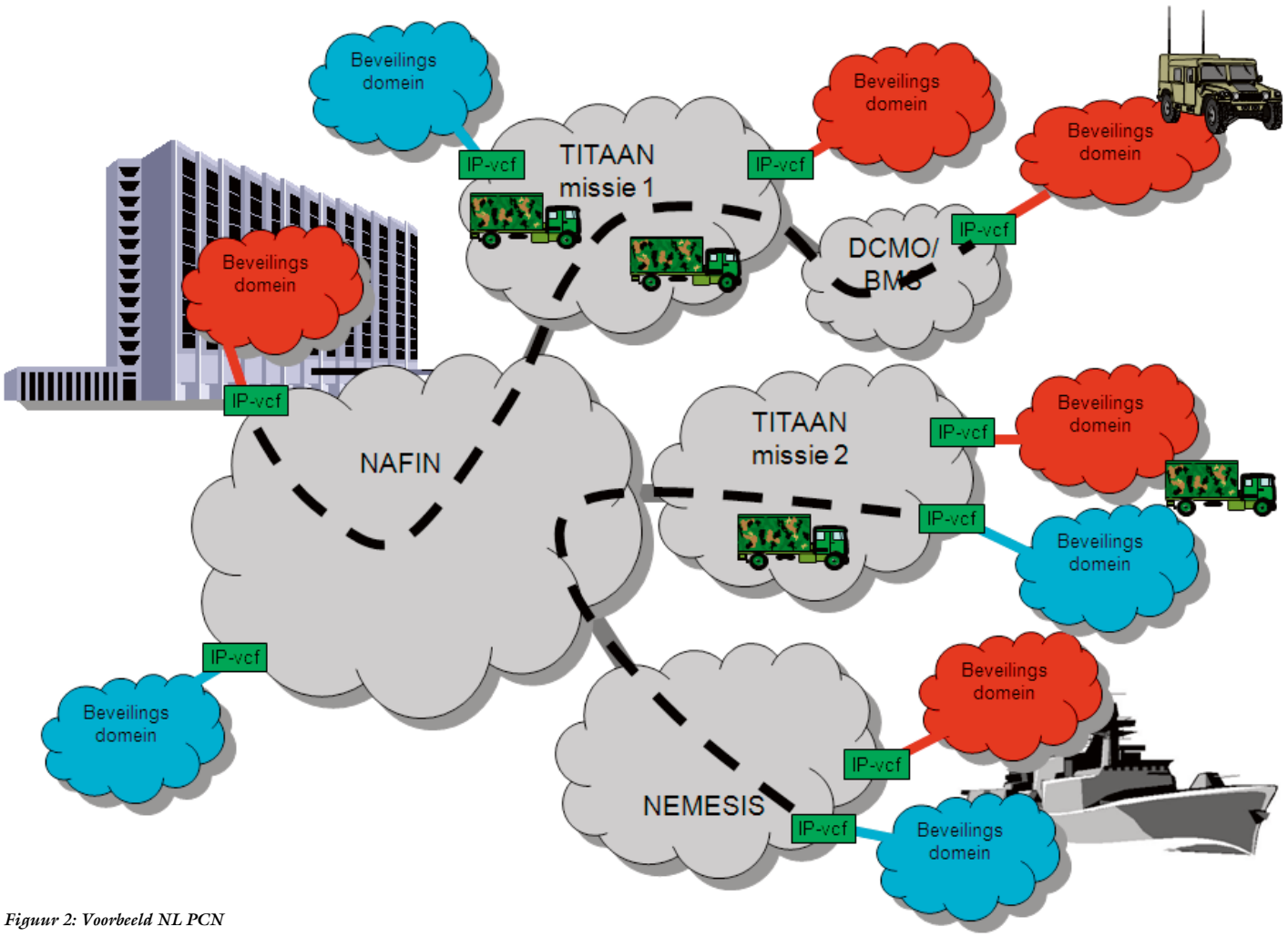
De huidige defensie informatie-infrastructuur laat zich het best omschrijven als een aantal per gebruiksomstandigheid of operationele inzet, verschillende en gescheiden informatie-infrastructuren die zijn gebaseerd op *system-high* mode van beveiligen. Deze infrastructuren hebben een geheel eigen inrichting van transmissie- tot en met applicatielaag en zijn beperkt gekoppeld. Het resultaat is een lappendeken van systemen die veel inspanning kost om in stand te worden gehouden en waarbij informatie niet of nauwelijks vanuit de gescheiden systemen is te verspreiden naar andere systemen.

Door de Bestuurstaf zijn plannen ontwikkeld om deze situatie te verbeteren en te vervangen door een nieuwe Netwerk Informatie Infrastructuur (NII) geschikt voor de gehele informatievoorziening van Defensie. NII zal worden ingericht conform de nieuw ontwikkelde architectuur voor Hoog Gerubriceerde Informatiedomeinenen (HGI) en daarmee het concept van *Protected Core Networking* gaan gebruiken. In dit artikel wordt uitgelegd wat *Protected Core Networking* is en hoe het kan worden ingericht en gerealiseerd binnen Defensie.

Een veel gehoorde wenskreet is *protect the data, not the network*. Hiermee wordt aangegeven, dat niet gehele netwerken beveiligd moeten worden, maar alleen de te beveiligen informatie (data). Met beveiliging wordt dan feitelijk geheimhouding door middel van datavercijfering bedoeld. Hoewel exclusiviteit en integriteit daarmee gewaarborgd zijn,



Figuur 1: Protected Core Network



Figuur 2: Voorbeeld NL PCN

is vercijfering van data alleen echter niet voldoende om de beschikbaarheid van de informatie te waarborgen. Als er niets aan het transportnetwerk wordt gedaan is het eenvoudig vanaf buiten te verstoren met gerichte aanvallen met bijvoorbeeld *Denial of Service* (DoS) tot gevolg. Om dit te voorkomen zijn er maatregelen op de transmissie en netwerklaag nodig. Het netwerk zelf zal op enigerlei wijze protected moeten zijn om de beschikbaarheid te borgen.

Het NATO Command, Control and Consultating Agency (NC3A) was de eerste die het concept van *Protected Core Networking* (PCN) globaal beschreef. In dit concept wordt gestreefd naar een transportnetwerk (core) dat is voorzien van beveiligingsmaatregelen die puur zijn gericht op het borgen van de beschikbaarheid (protected). Om deze core te realiseren leveren de landen van NATO zogenaamde *Protected Core Segments* aan, die onder regie van NATO worden samengevoegd tot één grote *Protected Core* (Pcore). Zo wordt een federatief netwerk gevormd vergelijkbaar met internet en de diverse Internet Service Providers (ISPs). Deze samengestelde core dient alleen voor NATO-breed betrouwbaar en robuust transport en bevat geen klare gebruikersinformatie. Hij zal aanwezig en bruikbaar moeten zijn in alle gebruiksomstandigheden van statische hoofdkwartieren tot en met de uitgestegen militair.

De gebruikers worden ondergebracht in beveiligingsdomeinen[1] die op de Pcore worden aangesloten d.m.v. IP-vercijferaars. Op deze wijze kunnen over de Pcore virtuele netwerken worden ingericht met verschillende beveiligingsniveaus. Zo kunnen bijvoorbeeld uitlopers van deze netwerken die zich op fysiek andere locaties bevinden via de PCore op een logische wijze met elkaar verbonden worden. De beveiligingsdomeinen worden in NATO termen gevormd door één of meerdere *coloured clouds* of *consumer modules*. Dit deel van het concept verschilt niet wezenlijk van het tunnelconcept zoals toegepast bij TITAAN, NAFIN en NEMESIS. Ook het nieuwe concept bij DataCom Mobiel Optreden (DCMO) sluit goed aan. In figuur 2 is een voorbeeld geschetst van een Nederlands PCN op basis van deze systemen. In de figuur zijn een paar mogelijke informatiepaden getekend die een indruk geven van de mogelijke connectiviteit.

Met alleen het concept van PCN valt nog weinig te beginnen. Het concept moet worden ingericht en realiseerbaar worden. Hoe gaan we beheer inrichten? Welke diensten moeten worden geleverd? De belangrijkste vragen die betreffende beveiliging moeten worden beantwoord zijn:

- Hoe moet de Pcore (en/of *PCore Segments*) worden beveiligd?
- Hoe moet de data die over de Pcore wordt getransporteerd worden vercijferd?

DE PCORE

In de NATO-visie is het voor het beveiligen van de Pcore vooral van belang om ongeautoriseerd verkeer te weren. Om het gebruikmaken van de Pcore, en het koppelen van netwerken zo eenvoudig mogelijk te laten zijn, is het voorkomen van ongewenst verkeer reactief ingericht. Ongewenst verkeer zou het netwerk binnen kunnen komen, maar eenmaal binnen wordt het aangepakt. Voor dit doel worden binnen het netwerk zogenaamde *Policy Enforcement Points* (PEP) ingericht die ongewenst verkeer tegenhouden en van het netwerk verwijderen. Aan deze oplossing kleven een paar nadelen. PEP-functionaliteit is weliswaar al beperkt aanwezig in sommige routers maar de PEP zoals gewenst bestaat nog niet en zal moeten worden ontwikkeld. Over het hoe, wat en wanneer is echter nog weinig duidelijkheid. Een ander nadeel is dat de PEP's moeten worden voorzien van *policies* die het verkeer op de *core* gaan regelen. Deze *policies* zullen moeten worden gewijzigd als de *core* wordt uitgebreid en als er nieuwe beveiligingsdo-

meinen worden toegevoegd. De verwachting is dat het vaststellen en onderhouden van de policies een beheers- en beheerprobleem gaat opleveren.

Een andere manier om de Pcore te beveiligen is het afschermen van de core voor potentieel ongewenst gebruik. Dit afschermen kan relatief eenvoudig door maatregelen te treffen die normaal worden toegepast om restricted of departementaal vertrouwelijke info te beveiligen. Door daarnaast een vorm van Network Acces Control (NAC) toe te passen, zodat alleen verbindingen van geautoriseerde apparatuur wordt toegestaan naar de PCore, worden indringers en ongewenst verkeer voorkomen. NAC kan technisch worden ingericht maar het is goed denkbaar dat het fysiek en procedureel wordt geregeld.

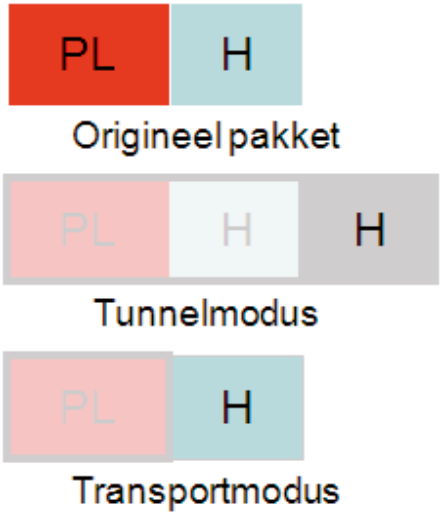
Omdat de laatste oplossing waarbij de core met bestaande maatregelen wordt afgeschermd voldoende bescherming biedt en realiseerbaar is maakt hij een grote kans om te worden toegepast voor de Defensie Pcore. Om de Nederlandse Pcore eenvoudig te koppelen met Pcores van andere landen is het van belang dat het beveiligingsniveau van de diverse Pcores zo veel mogelijk gelijk is. Als de beveiliging aan weerszijde van de koppeling verschilt, zal dit extra maatregelen op het koppelvlak gaan vereisen.

Uiteindelijk zal het resultaat zijn dat heel Defensie, van statisch tot uitgestegen en van schip tot compound, verbonden is door één grote Pcore. Deze Pcore zal bestaan uit diverse transmissiesystemen en netwerken. Sommige delen zullen zeer breedbandig zijn, andere delen juist zeer smalbandig omdat de transmissie over bijvoorbeeld radio's gaat. Om de Pcore maximaal te benutten zal bij de inrichting van het concept worden uitgegaan van een smalbandige PCore.

De Pcore vormt feitelijk de hoogbeschikbare backbone van de Defensie Informatie Infrastructuur (ik zou zeggen NII). Deze backbone kan worden aangevuld met het internet als transportnetwerk. De beschikbaarheid van het internet blijkt in de praktijk erg groot maar het internet is ook een omgeving die erg kwetsbaar is en wel degelijk grote risico's kent op het gebied van beschikbaarheid, denk hierbij aan DoS aanvallen. Het internet moet daarom voor wat betreft de beschikbaarheid worden beschouwd als een onbetrouwbaar medium. De PCore zal moeten worden gekoppeld met het internet met aanvullende maatregelen om dreigingen zoveel mogelijk buiten te houden en de kracht van de Pcore te borgen.

DE BEVEILIGINGSDOMEINEN

Defensie verwerkt informatie van verschillende rubriceringen en classificaties. Elk niveau vereist zijn eigen beveiligingsmaatregelen. Hiervoor worden beveiligingsdomeinen ingericht die voldoen aan alle beveiligingseisen om dat niveau te mogen verwerken. Denk hierbij niet alleen aan technische maatregelen maar ook aan personele en fysieke beveiliging. Doorgaans is een beveiligingsdomein verspreid over een groot aantal locaties waarbij per locatie de omvang kan variëren van een enkele gebruiker met werkstation tot een compleet hoofdkwartier met een groot *Local Area Networks*. Al deze locaties van alle beveiligingsdomeinen zullen over de Pcore worden verbonden. NATO spreekt hierbij zoals eerder beschreven over *coloured clouds* of *consumer modules*.
Dit is enigszins vergelijkbaar met een bedrijfsnetwerk waarbij geografisch gescheiden kantoren met een VPN-achtige constructie door service providers (b.v. IP VPN dienst) met elkaar zijn verbonden.



Figuur 3: IP Vercijfering

Op de Pcore zal informatie van verschillende rubriceringen moeten worden getransporteerd. Door op de netwerklaag met een IP-vercijferaar de informatie te vercijferen kunnen de diverse rubriceringen en classificaties worden gescheiden en binnen één en dezelfde Pcore worden verwerkt. Dit levert wel een paar uitdagingen op.

Een cryptoapparaat moet zijn gecertificeerd voor de verwerking van gerubriceerde en geclassificeerde informatie. Nederland, NATO en de EU kennen hiervoor hun eigen regels. Het gaat voor dit stuk te ver om daar diep op in te gaan, maar de praktijk is dat er nog geen IP-vercijferaar bestaat die alles mag verwerken. Een dergelijk apparaat zou zeer gewenst zijn zodat het onderscheid tussen de domeinen puur kan worden gebaseerd op het gebruik van de juiste sleutels. Er zijn op dit moment wel initiatieven die streven naar het realiseren van deze wens zoals HAIPE (*High Assurance IP Encryptor*). HAIPE is een US-standaard en beschrijft een manier van IP-vercijferen waarbij interoperabiliteit de drijfveer is om de gewenste onafhankelijkheid van cryptoapparatuur te verwezenlijken. NATO heeft inmiddels voor HAIPE gekozen als nieuwe standaard.

Een andere uitdaging is dat de hedendaagse generatie gecertificeerde IP-vercijferaars (zoals de TCE-621) werken in tunnelmodus. In deze modus wordt het rode IP-pakket in zijn geheel - *payload* en *header* – vercijferd. Door de vercijferaar wordt er vervolgens een nieuwe header aan het vercijferde pakket toegevoegd zodat het pakket zijn route over de core kan vinden. Deze modus heeft als pluspunt dat de rode header onzichtbaar is op de core en hiermee is *traffic flow analysis* lastig. De minpunten van tunnelmodus lijken echter zwaarder te wegen:

- De pakketgrootte neemt toe en dus het bandbreedtegebruik. Bij IP-verkeer met een kleine pakketgrootte (b.v. real-time informatie zoals spraak, video en sensordata) kan de overhead oplopen tot 800%!.
- De rode header bevat allerlei mogelijkheden voor een slim gebruik van het netwerk. Omdat de rode header niet op de core kan worden gebruikt – hij is daar immers vercijferd - is veel functionaliteit van de hedendaagse IP verdwenen. Denk hierbij aan QoS (Quality of Service) en multicast.

Deze nadelen laten zich vooral voelen bij netwerken die weinig bandbreedte hebben of die last hebben van instabiliteit. Dit geldt voor het expeditionaire deel van de Pcore. Tunnelmodus is daarmee minder geschikt voor PCN in operationele omstandigheden waarbij bandbreedte en stabiliteit niet gegarandeerd kunnen worden.

PAYLOADVERCIJFERING

In tegenstelling tot de huidige generatie gecertificeerde IP-vercijferaars, kent IPSEC naast de tunnelmodus tevens de transportmodus. In deze modus wordt alleen de *payload* vercijferd en de *header* intact gelaten. Deze modus heeft geen van de minpunten van tunnelmodus. Het nadeel van de transportmodus is dat *traffic flow analysis* op de core door onbevoegden iets eenvoudiger is. Dezelfde header die in de *coloured cloud* wordt gebruikt is nu namelijk ook zichtbaar in de laagbeveiligde *core*. Als een onbevoegde toegang tot de *core* zou krijgen, dan kan hij inzicht krijgen in de verkeersstromen tussen de werkstations in de diverse *coloured clouds*. Naast de beschikbaarheidseis moeten maatregelen worden getroffen om te voorkomen dat onbevoegden toegang krijgen tot de PCore.

Zowel transportmodus als tunnelmodus hebben een paar gemeenschappelijke nadelen.

- *Replay*. Door legitiem verzonden vercijferde pakketten op de core te onderscheppen, op te slaan en later opnieuw te verzenden is het mogelijk verouderde en daarmee corrupte informatie in de *coloured clouds* te krijgen. Dit kan worden opgelost door bij de ontcijfering te zorgen voor betrouwbare tijdsgegevens van de pakketten. Zodra deze bij controle wijzen op *replay* kunnen de pakketten worden gedumpt.
- *Congestie*. Vanuit de PCore kan niet worden gecommuniceerd met de *coloured cloud* achter de vercijferaar. Zelfs indien routering van de PCore naar *coloured clouds* zou worden toegestaan, lopen statusmeldingen in klare tekst stuk op de vercijferaar die vercijferde tekst verwacht. De *coloured cloud* maakt dus gebruik van de core zonder te weten of het netwerk in staat is het aanbod aan verkeer te verwerken. Indien het netwerk overbelast raakt (congestie) dan kan het dit de *coloured cloud* niet melden. Door de vercijferaar een betrouwbaar filter te geven die deze klare meldingen naar de *coloured cloud* doorgeeft is het probleem op te lossen. Beveiligers zullen zich achter de oren krabben bij een dergelijke kortsluiting van de core naar de *coloured cloud*. Het is gelukkig minder risicovol dan andersom, zeker als het doordacht wordt geïmplementeerd, en voor een smalbandig militair netwerk een voorwaarde om betrouwbaar te kunnen presteren.

Om voor de Nederlandse Defensie PCN te laten slagen zal moeten worden beschikt over een IP-vercijferaar zoals hierboven genoemd. Hij zal informatie van – liefst - alle beveiligingsniveaus moeten kunnen verwerken in de modus met uitgebreide *payload*-vercijfering. Om internationaal inter-operabel te zijn is het wenselijk dat hij gaat voldoen aan de door NATO aangenomen HAIPE standaard. Er is hierbij sprake van een grote uitdaging. Een nieuw product moet worden ontwikkeld en de verwerving daarvan moet passen in de geldende wet- en regelgeving. Lichtpunt is dat er bruikbare componenten en halffabricaten bestaan die als basis kunnen dienen voor dit nieuwe defensiebreed in te zetten cryptoapparaat.

PCORE IN MULTINATIONAAL VERBAND

Door de Pcore's van verschillende landen onderling te koppelen kan één grote Pcore worden gerealiseerd met een grote dekking waardoor de deelnemers meer mogelijkheden krijgen om hun beveiligingsdomeinen aan te sluiten op verafgelegen locaties. Bij dit koppelen moeten wel een aantal zaken worden overwogen.

- Bandbreedtegebruik en routering. Door zonder restricties een externe partij het gebruik te gunnen van de defensie-PCore bestaat het gevaar dat zoveel bandbreedte wordt gebruikt dat het eigen verkeer wordt gehinderd. Eigen prioriteitsverkeer mag geen last krijgen van ongewenst extern verkeer dat wordt gerouteerd over smalbandige paden.
- Toegang tot de PCore wordt alleen aan een externe partij verleend voor transport van vercijferde pakketten. Voorkomen moet worden dat externe partijen, waarvan de betrouwbaarheid nooit onomstotelijk vast staat, toegang tot de PCore krijgen die hen in staat stellen inzicht en invloed te krijgen op de Nederlandse informatie-infrastructuur.

Om andere landen te koppelen zijn maatregelen nodig die bovenstaande risico's wegnemen. Het feit dat de koppelingen alleen gemaakt zullen worden met vertrouwde partners en er geen risico's zijn te verwachten v.w.b. lekkage van informatie kunnen de maatregelen op de koppelvlakken betrekkelijk eenvoudig zijn.

HOE KOM JE TOT EEN PCN

Het mag duidelijk zijn dat het inruilen van onze oude infrastructuren door PCN niet in één snelle actie kan worden gedaan. Geleidelijk zullen systemen moeten worden vervangen door hun PCN opvolger. Belangrijk hierbij is dat de oude systemen worden gesplitst in een core en een IV-laag. De *core* zal deel moeten gaan uitmaken van de grote Pcore en daarvoor worden aangepast en voorzien van de benodigde maatregelen. Op deze manier zal de Pcore steeds verder groeien en steeds meer IV gaan ondersteunen. Nieuwe IV kan gebruik maken van de al aanwezige Pcore, maar kan ook extra Pcore capaciteit vereisen.
De ontwikkeling van PCN zal dus gefaseerd gebeuren in het ritme van de upgrades van de huidige systemen. Door NAFIN en het transportnetwerk van TITAAN om te vormen tot één Pcore zal een grote stap richting PCN worden gezet. Inmiddels zijn netwerkarchitecten van DMO (C2SC, C3I, MABE) en IVENT o.l.v. HDIO en ondersteund door TNO, bezig een NLD PCN uit te werken.

VOORDELEN

Het switchen naar PCN betreft een forse verandering die de nodige inspanning zal kosten. Vraag is dan of deze verandering ook voldoende verbetering oplevert. PCN zal als opvallende voordelen t.o.v. de huidige situatie hebben:

- Verbondenheid. Alle defensielocaties zijn met elkaar IP-technisch verbonden via de Pcore. De Pcore kent zowel opstijgpunten op kazernes, schepen, compounds als voertuigen. Zelfs de uitgestegen soldaat kan via een mobiel apparaat aan de Pcore worden verbonden.
- Herbruikbaarheid. Nieuwe systemen kunnen gebruik maken van de al aanwezige Pcore en zijn niet gedwongen om over een eigen transmissie en netwerk te beschikken.
- Standaardisatie. Zowel de inrichting van de beveiligingsdomeinen als de Pcore zal gedwongen door het PCN concept sterk gaan standaardiseren en aansluiten op NATO.
- Beheer. Het beheer van de standaard Pcore en de dito beveiligingsdomeinen zal effectiever en efficiënter zijn. Met toepassing van het 'gele domein' concept kan dit ook nog eens centraal plaatsvinden. Feitelijk ontstaat een situatie alsof slechts één systeem wordt beheerd. Voor de multinationale PCore zal federatief beheer moeten plaatsvinden.
- Beveiliging. PCN levert een concept dat op een afgewogen manier de beschikbaarheid, integriteit en geheimhouding van de te verwerken informatie regelt. Het toepassen van nieuw ontwikkelde cryptoapparatuur zal meer gebruiksgemak opleveren dan gewoon is bij oudere apparatuur. Vooral zaken als sleutelmanagement, vormfactor en prestaties zullen beter zijn dan gewend.
- Schaalbaarheid en uitbreidbaarheid. De Pcore zal het toelaten om zonder onderbreking van de informatievoorziening snel en dynamisch te worden uitgebreid om nieuwe locaties aan zich te verbinden, of ingekrompen als locaties worden verlaten. De Pcore biedt tevens de mogelijkheid om te worden aangevuld met Internet waardoor uitbreiding wereldwijd mogelijk is. Maar ook de beveiligingsdomeinen zijn door gebruik van cryptoapparatuur met de juiste sleutels eenvoudig te vormen en qua omvang aan te passen. Een beveiligingsdomein kan bestaan uit een paar werkstations maar ook uit een wereldwijd aanwezig netwerk met vele honderden werkstations.

TOEKOMST

De komende jaren zal invulling worden gegeven aan de nieuwe Netwerk Informatie Infrastructuur van Defensie. Huidige infrastructuren zullen bij een upgrade gaan migreren naar PCN. We gaan er over een paar jaar zeker meer van merken in onze dagelijkse praktijk.

[1] Een beveiligingsdomein is dat deel van het systeem waarop een bepaald beveiligingsregime van toepassing is (Aspectarchitectuur Informatiebeveiliging 1.0). Bijvoorbeeld een STG GEHEIM, NATO SECRET of Departementaal Vertrouwelijk domein.