NATO Cyber Defence Centre of Excellence

NATO Cyber Defence Centre of Excellence

Wie in der herkömmlichen Verteidigung kann der «Eintrittspreis» auch im Bereich der «Cyber Defence» mehr oder weniger hoch gehalten werden. Das NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Estland leistet einen gewichtigen Beitrag zum Bestreben der NATO-Länder, ihre Systeme besser zu schützen und damit den Ressourcen-Aufwand für potentielle «Cyber»-Attacken massiv zu erhöhen.

Hans Wegmüller, Redaktor ASMZ

Die Baltischen Staaten, allen voran Estland, scheinen seit jeher einen Hang zur Nische der Spitzentechnologie im IT-Bereich gehabt zu haben. So stammt zum Beispiel die Software zu «Skype» ursprünglich aus Estland, und man trug sich dort bereits im Jahre 2003 mit dem Gedanken, ein Kompetenzzentrum für «Cyber Defence» zu schaffen. Als Estland im Jahre 2007 Opfer einer der bisher massivsten «Cyber»-Attacken wurde, wirkte dies im ganzen Baltischen Raum wie ein Fanal und führte zu einer erhöhten Sensibilisierung von Politik und Öffentlichkeit. So wurde der bereits seit Jahren vorliegende Plan zur Gründung eines Kompetenzzentrums für «Cyber Defence» in Estland im Mai 2008 umgesetzt.

Position in der NATO

Die etwas schwerfällige Bezeichnung, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) widerspiegelt die Komplexität seiner Stellung innerhalb der NATO-Gemeinschaft. Als eines der bereits 19 «Centres of Excellence» der NATO steht es ausserhalb der NATO-Kommandostruktur, hat aber am völkerrechtlichen Status der NATO teil. Wie alle andern «Centres of Excellence» wurde es vom «Allied Command Transformation» in Norfolk (Virginia) geprüft und vom NATO-Militärausschuss akkreditiert. Das Zentrum mit Sitz in Tallinn wird aber nicht von der NATO, sondern ausschliesslich von den 14 «sponsoring nations» finanziert. Dazu kommen drei Nicht-NATO-Länder: Österreich als erste «contributing nation» mit Beobachterstatus im Aufsichtsgremium sowie Schweden und Finnland, die als zurzeit «participing nations» denselben Status wie Österreich anstreben. Periodisch nehmen auch die Türkei und Griechenland an Übungen des CCDCOE teil.

Die internationale Trägerschaft des Instituts beteiligt sich mit Personal und Finanzen; jede Nation entsendet mindestens einen Vertreter, ungefähr zu gleichen Teilen militärische und zivile Repräsentanten, je nach Arbeitsbereich (Recht, Strategie, Technologie oder Ausbildung und Übungen), in dem die entsprechende Nation eine Mitarbeit wünscht. Einige Posten sind mehr für Militärs, andere mehr für zivile Wissenschaftler geeignet. Die Position des Direktors und des Chefs des Stabes sind militärische Positionen, wobei die Funktion des Direktors stets von einem estnischen Offizier wahrgenommen wird. Auch in der Abteilung Ausbildung und Übungen, die nicht nur für die eigens am Zentrum durchgeführten Übungen, sondern auch für alle Beiträge zu Übungen der NATO und der «sponsoring nations» verantwortlich zeichnet, sind Militärs gefragt.

In der NATO gibt es mehrere Stellen, die sich mit dem Thema «Cyber Defence» befassen, allen voran das «Communication and Information Command», die «Emerging Security Challenges Division» sowie die «NATO Cyber Reaction Force», die aber alle der NATO-Kommando-Struktur angehören. Nach Aussage des aktuellen Direktors des CCDCOE, Oberst Artur Suzik, verleiht der Status als nicht von der NATO finanzierte und nicht in die NATO Kommando-Strukturen eingebettete Institution dem Zentrum einen grossen akademischen Freiraum und prädestiniert es als Think Tank in seinem Kompetenzbereich. Bedacht darauf, nicht das Gleiche zu tun wie andere NATO-Institutionen, wird versucht, einen Mehrwert für die Weiterentwicklung der NATO im Bereich «Cyber Defence» zu erbringen. Somit würden auch Themen in das Forschungsprogramm aufgenommen, die andere NATO-Institutionen nicht bearbeiten wollten oder könnten. Dennoch erhält das Zentrum seine Aufträge – neben den Wünschen der «sponsoring nations» – zu einem schönen Teil vom «Transformation Command» in Norfolk, das die Anträge und Anfragen aller interessierten NATO-Stellen entgegennimmt, sie auf ihre Relevanz für die NATO überprüft und priorisiert, um sie dann an die «Centres of Excellence» weiterzuleiten. Entscheidend für den Geschäftsgang des Zentrums ist aber das Aufsichtsgremium («steering committee»), das aus je einem Vertreter der «sponsoring nations» besteht und mit Einstimmigkeit entscheidet.

Der Direktor des CCDCOE, Oberst Artur Suzik. Bild: Autor

Flaggen der «sponsoring nations».

Kooperation

Das Tallinner Zentrum pflegt mannigfaltige Zusammenarbeit mit nationalen Einrichtungen und Instituten der «sponsoring nations». Mit der Bundeswehr-Universität in München besteht zum Beispiel eine Vereinbarung, die es dem Zentrum ermöglicht, Themata für Master-Arbeiten vorzugeben, die dann von Münchner Studenten aufgenommen und zum Teil am Zentrum in Tallinn bearbeitet werden können. Ein anderes Beispiel ist die Zusammenarbeit mit der estnischen «Defence League», einer Art freiwilligen Nationalgarde, die auch über eine «Cyber Defence Unit» verfügt. Diese rekrutiert sich aus Cyber-Spezialisten aus allen Bereichen des gesellschaftlichen Lebens in Estland, die einen Beitrag zur Landesverteidigung leisten möchten und ihr ziviles Know-how der Armee zur Verfügung stellen. Während das CCDCOE der «Cyber Defence Unit» die nötige technisch-elektronische Infrastruktur für Übungen zur Verfügung stellt, leistet diese einen bemerkenswerten Beitrag zu den vom Zentrum durchgeführten Übungen. Neben militärischen wird auch mit zivilen Institutionen zusammengearbeitet, so wurde das «Tallinn Manual» (Originaltitel: «Tallinn Manual on the International Law Applicable to Cyber Warfare») auf Einladung des CCDCOE von ungefähr zwanzig, meist zivilen Experten bearbeitet, die an verschiedensten Instituten und Universitäten tätig sind, darunter am Genfer Institut für Sicherheitspolitik. Das «Manual» war das erste Handbuch, das die Problematik der völkerrechtlichen Grundlagen im Bereich «Cyber Defence» und «Cyber Warfare» zum Thema hatte.

Nationale Verantwortung

Die Standards im Bereich «Cyber Defence», die im CCDCOE erarbeitet, überprüft und weiterentwickelt werden, entbinden die beteiligten und interessierten Nationen nicht, auf Grund ihrer spezifischen Gegebenheiten, ihren nationalen Ansprüchen, Kapazitäten und Traditionen das eigene Anspruchsniveau in einer nationalen «Cyber Defence»-Strategie zu definieren und die nationalen Eckwerte abzuleiten. Eine der Aufgaben, mit der sich das Zentrum zu beschäftigen hat, besteht gerade darin, die «sponsoring nations» bei der Erarbeitung und – aktuell – Weiterentwicklung und Verbesserung ihrer nationalen Strategien zu unterstützen. Dabei werden laufend neue Erkenntnisse und Erfahrungen («lessons learned»), die in den zahlreichen Übungen gesammelt und ausgewertet wurden, mit einbezogen und den NATO und «sponsoring nations» zum Beispiel in Form von «after action reports» und «manuals» zur Verfügung gestellt.

Ausbildung am CCDCOE.

«Cyber»-Strategie

Ein Vergleich vorhandener nationaler Strategien zeigt, dass insbesondere folgende Elemente unverzichtbar sind: Die Definition der zu schützenden kritischen Infrastrukturen (Bank- und Gesundheitswesen, Wasser- und Energieversorgung, öffentlicher Verkehr, Verwaltung etc.), die Bekämpfung von «Cyber»-Kriminalität und Massnahmen zur Erhöhung des allgemeinen Bedrohungsbewusstseins im «Cyber»-Bereich. Drei Erfolgsfaktoren sind nach Aussage von Oberst Suzik bei deren praktischer Umsetzung zu beachten: Erstens, die Unverzichtbarkeit eines verbindlichen Umsetzungsplanes, zweitens, die Schaffung einer soliden Vertrauensbasis zwischen den agierenden Institutionen und Dienststellen und drittens, die Festlegung klarer Verantwortlichkeiten und Zuständigkeiten, denn im Ernstfall und unter Zeitdruck sei entscheidend, dass jede Dienststelle ihre Obliegenheiten genau kenne. Dabei werde man um die Schaffung eines obersten zentralen Leitungsorgans kaum herumkommen, und es müsse auch die Schaffung eines «computer emergency response team» ins Auge gefasst werden. Anleitung dazu kann das vom Zentrum herausgegebene «National Cyber Security Framework Manual» geben.

Die entscheidende Frage, wie aktiv und offensiv eine «Cyber Defence»-Stratgie gestaltet werden soll, hat jede Nation auf Grund ihres Rechtsverständnisses selber zu entscheiden. Nach Oberst Suzik schlössen einige nationale Strategien offiziell den Aufbau von offensiven Kapazitäten und die Vorbereitung entsprechender Massnahmen ein und auch in den konzeptio-

nellen Vorgaben der NATO sei ein gewisser Trend zu mehr Kühnheit festzustellen. Eine dieses Jahr vom CCDCOE durchgeführte internationale Konferenz mit etwa 500 Teilnehmern war denn auch dem Thema «active cyber defence» gewidmet, wobei bereits der Palette der Begriffe «offensive, active, reactive defence» zu entnehmen war, wie undeutlich und fliessend die Grenzen zwischen offensiven und defensiven Massnahmen im «cyberspace» sind. Die verwendete Technologie schliesst ohnehin beide Möglichkeiten ein («dual-use»), so dass eine klare Trennung nicht nur konzeptionell und definitorisch, sondern auch technisch praktisch unmöglich ist. Wichtig ist daher, dass die nationale Strategie diesbezüglich klare Leitlinien vorgibt, damit im Ernstfall situativ entschieden werden kann, wie weit zu gehen ist. Im NATO-Verbund sind gegenseitige Hilfestellungen im Fall eines Angriffs auf einen der NATO-Staaten durchaus denkbar, indem die offensive Komponente der Abwehr von einem andern NATO-Staat oder von der NATO selbst erbracht werden könnte.

Sowenig wie in andern Lebensbereichen wird auch im «cyberspace» nie vollständige Sicherheit zu erreichen sein, aber die Abwehr kann mit gezielten, koordinierten und energischen Massnahmen auf ein hohes Niveau gebracht werden, das eine inhärente dissuasive Wirkung zu erzielen vermag. Je besser es gelingt, Systeme zu schützen, desto grösser ist der Ressourcen-Aufwand für einen potentiellen Gegner, diese zu attackieren. Dabei ist nach Aussage der Vertreter des CCDCOE zu bedenken, dass das Prinzip «one shot – one hit» dazu führt, dass alles auf eine Karte gesetzt werden muss und die materiellen Verluste im Falle eines Misserfolgs ausserordentlich hoch sein können, zumal wenn es sich – wie in letzter Zeit immer häufiger – um Schadprogramme («malware») mit nachrichtendienstlicher Zweckbestimmung handelt. ■

CCDCOE in Tallin. Bilder: CCDCOE