Divisionär Kurt Nydegger : Projektleiter Cyber Defense

Autor(en): **Wegmüller, Hans**

Objekttyp: **Article**

Zeitschrift: **ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift**

Band (Jahr): **177 (2011)**

Heft 4

PDF erstellt am: **12.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-154237

Divisionär Kurt Nydegger: Projektleiter Cyber Defense

Schon die Risikoanalysen zur Armee XXI erkannten «Information warfare» als Gefahrenpotential mit relativ hoher Eintretenswahrscheinlichkeit und erheblichen existenziellen Auswirkungen. Die Ernennung von Divisionär Kurt Nydegger zum Projektleiter Cyber Defense durch den Bundesrat verleiht der Problematik nunmehr mit Recht strategische Bedeutung.

Hans Wegmüller, Redaktor ASMZ

Herr Divisionär, Sie wurden vom Bundesrat auf Anfang Jahr zum Projektleiter für Cyber Defense gewählt; was hat man darunter zu verstehen, was umfasst Ihr neues Arbeitsgebiet?

Die Schweiz ist wie jeder andere moderne Staat immer abhängiger von Informations- und Kommunikationsinfrastrukturen. Ein Ausfall eines oder mehrerer kritischer Elemente kann katastrophale Kettenreaktionen auslösen – dies kann heute mittels einer Cyber-Attacke verursacht werden. Zugleich ist der Wert von Informationen für eine Dienstleistungsnation wie die Schweiz sehr hoch. Deren Erarbeitung und Speicherung erfolgt zunehmend im «Cyberspace», und damit werden Informationen der Gefahr von Cyber-Spionage ausgesetzt. Es geht also darum, die sicherheitspolitischen Dimensionen dieser Bedrohung zu erfassen und eine gesamtheitliche nationale Strategie des Bundes zu erarbeiten.

Bisher waren Sie Chef der Führungsunterstützungsbasis (FUB). War Cyber Defense nicht auch bisher Teil Ihrer Aufgaben, warum wurde dafür ein neuer Generalsposten geschaffen?

Der Bundesrat hat mit der Ernennung eines Projektleiters für Cyber Defense grundsätzlich eine Aufgabe mit zivilem Charakter geschaffen und keinen zusätzlichen Generalsposten. Die Wahl meiner Person hat sicher mit meiner Ausbildung, der langjährigen Erfahrung als Chef der Elektronischen Kriegführung (EKF) und als Chef der Führungsunterstützungsbasis (FUB) sowie meinem Netzwerk zu tun. All das Wissen über Analyse und Schutz gegen Cyber-Bedrohungen aus meinem beruflichen Werdegang wird mir bei der Bewältigung der neuen Herausforderung nützen.

Führungszentrum der Armee. Bild: FUB

Die Armee hat sich meines Wissens mit dem Phänomen Cyberwar schon seit längerer Zeit befasst; welche Vorarbeiten wurden hier geleistet und wie können sie in die neue Strategie mit einbezogen werden?

Tatsächlich hat die Armee seit längerer Zeit ein umfangreiches Know-how sowie ein mehrstufiges Schutzdispositiv gegen Cyber-Bedrohungen aufgebaut. Aber nicht nur die Armee, sondern auch andere Verwaltungsbereiche haben nach der strategischen Führungsübung 97 (SFU 97) diese spezielle Bedrohungsform erkannt, erste Massnahmen definiert und durch Bundesratsentscheide eingeleitet und umgesetzt. So erfolgte zum Beispiel 2003/2004 der Aufbau der Melde- und Analysestelle Informationssicherung MELANI und des Sonderstabes Information Assurance SONIA.

Weil sich jedoch die Bedrohungsformen nicht in allen Bereichen so schnell entwickelten wie erwartet, wurden Umsetzungsmassnahmen teilweise gebremst oder sogar «auf Eis» gelegt. Ausserdem sind viele der benötigten Fähigkeiten für Cyber Defense nicht zwischen ziviler oder militärischer Eigenschaft unterscheidbar. In diesen Bereichen werden die Synergien geprüft und wenn möglich optimal ausgenutzt.

Bis Ende des Jahres soll eine Strategie für Cyber Defense vorliegen, die Sie nun mit Ihrer Projektgruppe zu entwickeln haben. Angriffe aus dem Cyberspace sind aber – wie angetönt – kein neues Phänomen; gab es denn bisher keine derartige Strategie?

Trotz der Bemühungen des Bundes, das Schutzdispositiv der Verwaltung zu verbessern, ist es bis heute nicht gelungen,

eine strategische Lösung zu finden. Der dezentral strukturierte Ansatz und die relativ geringen Mittel verhindern Lösungen auf Bundesstufe unter Einbezug aller Schlüsselbereiche für ein nationales Krisenmanagement.

Erarbeitete Studien und Konzepte, das aufgebaute Wissen, die Expertise sowie die operativen Erfahrungen der letzten Jahre von zirka zwölf organisatorischen Bereichen in der Verwaltung werden sicher in die Analyse einbezogen und als Teilaspekte Einfluss auf die Nationale Strategie für Cyber Defense haben.

Der gesetzliche Handlungsspielraum für die Abwehr von Angriffen im Cyberspace soll laut einem Gutachten des Bundesamtes für Justiz sehr eng sein; wie beurteilen Sie die Tauglichkeit der geltenden gesetzlichen Grundlagen für die Cyber Defense der Zukunft?

Dieses Gutachten geht hauptsächlich auf die Frage des Handlungsspielraums der Armee ein. Es ist allerdings so, dass es auch für die zivilen Aspekte von Cyber Defense Grauzonen gibt, welche geklärt und auf eine solide Rechtsgrundlage abgestützt werden müssen. Insbesondere die Frage, wie aktiv Cyber Defense in einem schwerwiegenden Fall gegen die Angreifer-Infrastruktur vorgehen soll oder darf, ist umstritten. Auch diesbezüglich verlangt die Politik von uns eine Abklärung und eine entsprechende Antwort.

Was kann gegen einen Angriffe wie denjenigen auf das Computersystem des EDA im Jahr 2009 in Zukunft vorgekehrt und wie können solche Attacken abgewehrt werden?

Die Bundesverwaltung ist einer wachsenden Bedrohung durch Cyber-Spionage ausgesetzt. Dort treffen sich die strategischen Interessen verschiedener Länder. Obschon Schutzmassnahmen getroffen worden sind, befinden wir uns auf einem ungleichen «Schlachtfeld»: Die Angreifer müssen nur eine Schwachstelle finden und ausnutzen, wir müssen alles unter Kontrolle haben. Die Konsequenz ist, dass wir unsere sensitiven Daten nicht in den öffentlichen Netzen exponieren dürfen und einen zunehmend aktiven Ansatz zum Schutz unserer Infrastrukturen anwenden müssen.

Heute sollen Fragen zur Internetkriminalität und zum Cyberwar von verschiedenen Amtsstellen des Bundes bearbeitet werden, sah man bisher keine Notwendigkeit, diese Anstrengungen zu bündeln und wo sehen Sie die Möglichkeiten der besseren Koordination in Zukunft?

Internetkriminalität, Cyber-Crime und Cyberwar sind unterschiedliche Bedrohungsformen, welche auch unterschiedlich angegangen werden müssen. Bei Cyber Defense geht es darum, dafür zu sorgen, dass die Schweiz ihre «Achillesferse» im Bereich der kritischen Informationsinfrastrukturen nicht ungeschützt präsentiert. Die Internetkriminalität andererseits ist ein Phänomen, das seit Jahren am Wachsen ist und durch Bund (Federführung hat das Bundesamt für Justiz) und Kantone polizeilich verfolgt und geahndet wird. Es gibt in diesen beiden Tätigkeiten selbstverständlich Gemeinsamkeiten. Mir ist es ein grosses Anliegen, dass die Fachspezialisten aus diesen Bereichen den bereits vorhandenen regen Austausch untereinander noch optimieren und intensivieren. Inwieweit alle Anstrengungen gegen Cyber-Bedrohungen gebündelt oder zentral gesteuert werden können, soll die bis Ende 2011 zu erarbeitende Strategie aufzeigen.

Laut Medienberichten haben die USA kürzlich ein neues «Cyber Command» gegründet, Deutschland plant offenbar ebenfalls die Schaffung eines «Cyber-Abwehrzentrums» und die chinesische Armee investiert bekanntlich massiv in die Vorbereitung für «das virtuelle Schlachtfeld des 21. Jahrhunderts»; der Bundesrat dagegen hält das heutige Schutzdispositiv des Bundes für «gut und effizient». Wie beurteilen Sie die heutige Situation?

Das heutige Dispositiv ist insofern gut, als die wichtigsten Aufgaben und Rollen abgedeckt sind. Unsere Leute haben gezeigt, dass sie die Bedrohung im Alltag bewältigen können. Und dies mit im internationalen Vergleich sehr wenig Personal. Wir sind allerdings im Falle einer Krise noch zu wenig gerüstet. Ich sehe es als meine Aufgabe an, im Rahmen der nationalen Strategie aufzuzeigen, wo unsere Stärken und Schwächen sind. Darauf aufbauend soll mit Vorschlägen bezüglich Standards für Analyse, Schutz, Alarmierung, Abwehr sowie organisatorischen Vorkehrungen (Pikett, Steuerung etc.) sichergestellt werden können, dass wir auch für eine grössere Krise mit strategischen Konsequenzen gut gerüstet sind und nicht improvisieren müssen.

Herr Divisionär, ich danke Ihnen für das Gespräch. ■

Kurt Nydegger

Divisionär
Projektleiter für Cyber Defense
Geboren am 18. Dezember 1950
Verheiratet, zwei Kinder
Bürger von Rüschegg BE

Beruf / Tätigkeiten

Lehre als FEAM bei HASLER AG
Abendtechnikum in Bern

- **1972–1977** Laborassistent, Testzentrum Telefonie Hasler AG
- **1978–1979** Entwicklungsingenieur, Forschungsabteilung Hasler AG
- **1980–1987** Chef Elektronische Aufklärung, Bundesamt für Übermittlungstruppen
- **1988–1995** Chef Sektion EKF/Betrieb, Bundesamt für Übermittlungstruppen
- **1996–2003** Chef Abteilung EKF, Untergruppe Führungsunterstützung

Militärische Laufbahn

1982–1985 Hptm, Kdt Ristl Kp
1986–1988 Hptm i Gst, Gst Of Armeestab
1989–1991 Maj i Gst, Kdt Ristl Abt
1992–1995 Oberstlt i Gst, USC Op Uem Br 41
1996–2002 Oberst i Gst, Chef Astt
2003 Brigadier, Chef J 6 im FST A, Verteidigung, VBS
2004–2010 Divisionär, Chef Führungsunterstützungsbasis, Verteidigung, VBS
2011 Projektleiter für Cyber Defense, GS VBS