SOG FU Forum 2013 : "Chancen und Risiken in einer digitalen Welt"

Autor(en): **Cantoni, Andreas**

Objekttyp: **Article**

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

Band (Jahr): **179 (2013)**

Heft 12

PDF erstellt am: **21.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-358216

SOG FU Forum 2013: «Chancen und Risiken in einer digitalen Welt»

Am 21.09.2013 fand in Bad Horn das 4. Forum der SOG Führungsunterstützung (FU) statt. Eine Reihe hochkarätiger Referenten beleuchtete die Frage nach den Chancen und Risiken in einer digitalen Welt aus unterschiedlichen Blickwinkeln und teilte mit den Teilnehmenden anschaulich und offen ihre Beurteilungen und Lehren.

Andreas Cantoni, Redaktor ASMZ

Auch wenn das Thema eine Reihe von sehr technischen Aspekten beinhaltet, wurde mehrfach auf die «menschlichen» Elemente hingewiesen. Die Menschen werden bis auf Weiteres das Fundament unserer Armee bilden, denn sie müssen die technischen Sicherheitsmassnahmen im Zusammenhang mit Cyber-Risiken umsetzen. Wir alle erinnern uns dabei an banale Dinge wie den Passwortschutz unserer Computer oder die Sicherheit unserer Daten im öffentlichen und privaten Raum. Ein moderner Musterangriff verläuft dabei unter missbräuchlicher Ausnutzung des menschlichen Vertrauens in etwa so: Die Gegenseite verschickt eine auf den Empfänger massgeschneiderte elektronische Nachricht (dazu werden vorher im Netz Interessen und Kontakte recherchiert). Mit dem Öffnen der Nachricht wird auf dem Rechner oder den Servern des Empfängers ein Programm installiert und aktiviert. Die Daten werden anschliessend kopiert, verschlüsselt und unbemerkt getarnt an die Gegenseite übermittelt. Nach erfolgter Aktion wird das Programm wieder unauffällig «exfiltriert». Ein ehemaliger Hacker führte in einer live Demonstration eindrücklich und unterhaltsam das «Knacken» eines Bankkontos und einer verschlüsselten Festplatte vor.

Die Referenten der Tagung waren: KKdt André Blattmann, CdA; LtGen (Rtd) Jo Godderij, ehemals General der NATO (NL); Dr. U. Gygi, VR-Präsident der SBB; Christian Funk, Senior Virus Analyst, Kaspersky Lab; Gunnar Porada, Hackerspezialist; Oberst i Gst Gérald Vernez, Delegierter des CdA für Cyber-Defence; Daniela Vorburger, Projektleiterin Krisenmanagementausbildung des Bundes; Dr. Andreas Walker, Zukunftsforscher

Cyber-Risiken sind real, heute, hier und jetzt!

Die Instrumente der Cyber-Defence (z.B. Simulation und virtuelle Realität, Bionik, die Datenverarbeitungsfähigkeit, künstliche Intelligenz und Nanotechnologien) werden heute bereits erfolgreich zur Bekämpfung der Kriminalität eingesetzt und müssen auf unsere militärischen Bedürfnisse angepasst werden. Die Grenzen zwischen innerer und äusserer Sicherheit werden dabei weiter verschwimmen. Wer glaubt, hier sei nur die ferne Zukunft gemeint, halte sich kurz die Entwicklung der Zahlen der Cyber-kritischen Events der olympischen Spiele vor Augen: 90 Events in Peking (2008) und 686 Events in London (2012). Auch die SBB ist täglichen Angriffen auf ihre Netze ausgesetzt. Um sich dem Potenzial der Bedrohung bewusst zu werden, mag sich der Leser kurz daran erinnern, wie oft er selber Fahrplanabfragen tätigt oder wie vernetzt die Steuerung der Züge auf dem schweizerischen Eisenbahnnetz aktuell ist.

Interessierte Teilnehmer am Forum 2013 der SOG FU. Bild: Sonja Kaufmann

Konsequenzen ... ausser man tut es!

Als Armee gilt es, in einem vernetzten und unterschiedlich verletzlichen zivil-militärischen Umfeld schon heute Lagen umfassend zu beurteilen, die wirksamsten Handlungsoptionen zu finden und Entscheide zeitgerecht in Aktionen umzusetzen. Die Übergänge sind dabei thematisch fliessend und nur in enger Zusammenarbeit mit den beteiligten, hochgradig vertrauenswürdigen Organen lösbar. Die diesjährige strategische Führungsübung des Bundesrates fand zum Thema Cyber-Attack statt und hat wertvolle Ergebnisse aufgezeigt. Führungsinfrastruktur, Führungssysteme und die entsprechenden Prozesse müssen in diesem Sinne permanent Einsatzbereit sein, wenn wir uns vor unliebsamen Überraschungen im Einsatz schützen wollen. Das Problem mit Cyber-Risiken liegt im permanenten Bedürfnis, diese zeitgerecht zu identifizieren. Vor dem Hintergrund der Initiative zur Abschaffung der Wehrpflicht konnte einmal mehr aufgezeigt werden, wie wichtig dabei auch die Miliz mit ihrer Expertise aus dem wirtschaftlichen Umfeld für die Armee ist (und umgekehrt). Bis Ende Oktober 2013 wird über die zu einsetzenden Mittel in Form eines militärischen Cyber-Defence-Organs entschieden. ■