Verteidigung : Chancen für die Schweiz im Zeitalter von Cyberwar und Robotern

Autor(en): **Bubb, Lukas / Frick, Thomas**

Objekttyp: **Article**

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

Band (Jahr): **184 (2018)**

Heft 3

PDF erstellt am: **03.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-772508

Verteidigung – Chancen für die Schweiz im Zeitalter von Cyberwar und Robotern

Zentrale Aufgabe der Schweizer Armee bleibt die Abwehr eines militärischen Angriffes. Hohe Bevölkerungsdichte und tiefe Armeebestände erschweren eine autonome Verteidigung. Die neuen Informations- und Robotertechnologien ermöglichen es nun aber gerade der Schweiz, die Abwehr auf eigenem Territorium wieder glaubwürdig zu führen. Voraussetzungen sind entsprechende technische, personelle, infrastrukturelle und rechtliche Vorbereitungen.

Lukas Bubb, Thomas Frick

Der Sicherheitspolitische Bericht (SIPOL B 2016) hält fest, dass Bedrohungen komplexer, verknüpft und unübersichtlicher geworden sind, die Gefahr militärischer Gewalt aber auch in Europa eine Realität geblieben ist.[1] Der Bericht kommt daher nachvollziehbar zum Schluss, dass die Schweiz die für die Verteidigung kritischen Fähigkeiten bewahren und weiterentwickeln muss, um nicht nur Terror- und Cyber-Angriffe, sondern auch terrestrische Angriffe abwehren zu können. Wie kann die Schweiz im Cyber-Zeitalter ihre besonderen Fähigkeiten und Rahmenbedingungen nutzen, um eine glaubwürdige Abwehrfähigkeit sicherzustellen?

Unverändertes und Neues

Unverändert sind die geographische Lage der Schweiz mitten in Europa und ihre im Mittelland dichte Überbauung mit moderner, hochgradig vernetzter Infrastruktur. Unverändert sind auch der Wohlstand, die hohe Ausbildung der Bevölkerung und das Milizprinzip der Armee. Noch immer wird die Verteidigung im eigenen Land geführt, das heisst in bekanntem und gegebenenfalls vorbereitetem Gelände inmitten der eigenen Bevölkerung und Infrastruktur.

Eine glaubwürdige Verteidigung setzt voraus, dass nicht nur das Gefecht geführt werden kann, sondern dass auch die Bevölkerung und die Infrastruktur effektiv geschützt sind. Das schwergewichtige Training des mechanisierten Kampfs im überbauten Gelände durch mobile Kräfte mit mangelhafter Luftsicherung wird dem nicht gerecht. Es drohen im Ernstfall hohe Kollateralschäden an der (eigenen) Zivilbevölkerung, der zivilen Infrastruktur und unserem Kulturgut und hohe Verluste der kämpfenden Truppe. Dieser Ansatz wirft damit die Frage auf, ob ein politischer Wille zu einer derartigen Verteidigung besteht, und damit die Frage nach der Glaubwürdigkeit der Dissuasion.

Analyse mit Aufklärungsroboter.

Die spezifischen Stärken der Schweiz in der Verteidigung: Datennetz

Die Armee 61 nutzte für die Verteidigung das Gelände, härtete es mit Bunkern und Sprengobjekten und setzte auf eine hohe Anzahl Infanteristen und starke mechanisierte Verbände. Kampfverbände stehen auch heute technisch hochgerüstet und vielseitig ausgebildet für ein breiteres Spektrum an Aufträgen bereit, wurden aber zahlenmässig stark reduziert. Neue Technologien können als Multiplikatoren verkleinerte Bestände kompensieren und die Geländeausnutzung optimieren. Der SIPOL B 2016 (S. 7805) fordert dringend ein krisensicheres Kommunikationsnetz. Ein solches kann auch dezentral gespeicherte Informationen (z. B. gefährliche Anlagen, Hauspläne der Feuerwehren, Verlauf von Gasleitungen) den Partnern des Sicherheitsverbundes Schweiz zugänglich machen. Zusätzlich könnte es aber auch den Einsatz teilautonomer Systeme der Armee unterstützen. Hierfür könnte teilweise auf die Schutzinfrastruktur der Armee 61 als geschützte Basis von Führungs- und Leitsystemen und Sensoren (EKF) sowie von gefechtsfelddominanten Sendern zur Steuerung teilautonomer Systeme zurückgegriffen werden.

Teilautonome Systeme als Chance für Armee und Wirtschaft

(Teil)autonome Systeme[2] werden in verschiedenen Funktionen eingesetzt, wobei viele sich noch in der Testphase befinden: Aufklärungsdrohnen, selbstfahrende Transportroboter, Kampfmittelbeseitigungsroboter und endlich auch mobile und stationäre Waffensysteme. Vollautonome Waffensysteme (das heisst Waffen-

systeme, bei welchen der letztliche Entscheid über den Waffeneinsatz vollständig an den Roboter delegiert ist) werfen zahlreiche juristische und ethische Fragen auf. In absehbarer Zeit ist aber nicht damit zu rechnen, dass derartige Systeme in kriegsvölkerrechtlich zulässiger Weise eingesetzt und von der Schweiz beschafft werden können. Hingegen bieten nicht bewaffnete autonome Systeme und nicht autonome Waffensysteme für die Verteidigung der Schweiz grosse Chancen: Die geringeren Mannschaftsbestände können durch solche «Gefechtsfeldroboter» kompensiert werden, die Gefechtsstärke wird gesteigert und menschliche Verluste werden minimiert. Autonome Gefechtsfeldaufklärung in Verbindung mit einem umfassenden Datennetz rückt zudem das gläserne Gefechtsfeld in Griffweite, wie es das Führungs- und Informationssystem Heer (FIS HE) darstellen soll.

Die technischen Hochschulen der Schweiz gehören in den Bereichen künstliche Intelligenz, Sensortechnik und Robotersteuerung zu den weltweit Führenden. Aber auch die mechanischen Komponenten der zurzeit noch eher kleinen Geräte[3] können durch die Schweizer Rüstungsindustrie eher abgedeckt werden, als ein Grossprojekt wie z.B. ein eigener Kampfpanzer. Endlich würden zahlreiche neue, hochqualifizierte technische und EDV-lastige Funktionen in der Armee geschaffen, die aus den «Digital Natives» der Generation Y leicht zu rekrutieren sein dürften. Die eingeführte differenzierte Tauglichkeitsprüfung bei der Rekrutierung sowie ein eigenes Dienstleistungsmodell für Cyber-Spezialisten sind der richtige Weg.[4]

Was ist zu tun (oder zu unterlassen)?

Das gesicherte Datennetz muss rasch realisiert werden, mit breiterer Funktionalität als nur Kommunikation. Es sollte geprüft werden, wie weit die noch vorhandene Infrastruktur der Armee 61 genutzt werden kann; bis zum Abschluss der Prüfung sollten die laufenden Liquidationsbestrebungen sistiert werden.

Sodann müsste dem Aspekt von möglichen (teil)autonomen Einsätzen auch bei der anstehenden Beschaffung von Grossgeräten (Artillerie, Kampfpanzer, Schützenpanzer) Beachtung geschenkt werden. Aufgrund der Gefahr technischer Kompromittierung von High-Tech-Waffensystemen durch Dritte («Hacking» und bewusster Einbau von Sicherheitslücken) ist soweit möglich auf Eigenentwicklungen durch Zusammenarbeit von Armee, Ruag und den Schweizer Hochschulen zu setzen. In der Armee sind nicht nur Cyber-Defense-Rekruten auszubilden[5], sondern auch Spezialisten für autonome und teilautonome Systeme und Roboter.

Endlich ist zu prüfen, ob ein besonderer juristischer Rahmen geschaffen werden muss, der militärische Einsätze autonomer Transport- und Aufklärungsmittel in der Schweiz regelt. Das gesellschaftliche Bild autonomer Systeme ist von der Filmindustrie geprägt und weckt starke Emotionen – (voll) autonome Waffen stehen in der Schweiz aber zur Zeit nicht zur Diskussion, was klargestellt werden muss. In den laufenden Beratungen im Kreise der CCW-Staaten (UN-Waffenübereinkommen) zu einem Verbot, respektive zur Beschränkung von autonomen Waffensystemen ist aber darauf zu achten, dass die künftige Handlungsfreiheit der Schweiz nicht eingeschränkt wird.[6] ■

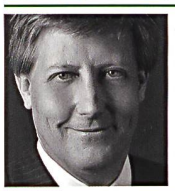
Diverse unterirdische Anlagen liegen derzeit brach. Bilder: VBS

Weitere Literatur

Ford, Martin: The Rise of the Robots, London 2015; Schneider, Henrique: Armee: Die Innovationsfront, in: ASMZ 2017/4, S. 14f.; Jenni, Peter: Gefahr: Killerdrohnen (Vortrag Dr. Frank Sauer), in: Schweizer Soldat Oktober 2017, S. 51; Fray/Savolainen/Schmid: Innovation in Defense, in: ASMZ 12/2017, S. 30f.; United Nations Institute for Disarmament Research (UNIDIR): The Weaponization of Increasingly Autonomous Technologies: Concerns, Characteristics and Definitional Approaches, September 2017.

1 SIPOL B 2016, S. 7794.
2 Zur Definition vergleiche Müller, Peter: Wer gibt den Befehl zu töten?, in: ASMZ 08/2017, S. 24f.; Krummenacher, Martin: Letale autonome Waffensysteme – Fluch oder Segen? in: Military Power Revue 2/08/2017, S. 60ff.; und insbesondere die umfassende Studie von Christen, Markus; Burri, Thomas; Chapa, Joseph; Salvi, Raphael; Santoni de Sio, Filippo; Sullins, John (2017): An Evaluation Schema for the Ethical Use of Autonomous Robotic Systems in Security Applications, November 1 2017, UZH Digital Society Initiative White Paper Series No. 1, University of Zurich.
3 Freedberg, Sydney: Roboter: USA enttäuscht, in: Schweizer Soldat Januar 2018, S. 41.
4 VBS, publiziert am 09.11.2017: Aktionsplan für Cyber-Defence (APCD).
5 Wyler, Ariel: Cybercrime und Cyberwar – vom Aufbau einer schlagkräftigen Cyber-Truppe, in: ASMZ 12/2017, S.16f.: Mäder, Lukas: Cyber-Rekruten im Anmarsch, in: NZZ vom 14. Dezember 2017, S. 13.
6 Siehe auch www.stopkillerrobots.org.

Major
Lukas Bubb
lic. iur.
AIG Europe Ltd
8712 Stäfa



Oberstlt
Thomas Frick
Dr. iur. et lic. phil. I,
Rechtsanwalt, LL.M.
8702 Zollikon