Hightech im Reich der Mitte

Autor(en): **Zhang, Junhua**

Objekttyp: **Article**

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

Band (Jahr): **167 (2001)**

Heft 10

PDF erstellt am: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-67383

Hightech im Reich der Mitte

Wird China einen digitalen Krieg führen?

In unserer Zeit, in der sich die Leistungsfähigkeit der digitalen Technologie alle 18 Monate verdoppelt, hat der Begriff «Information Warfare» (IW) besondere Aufmerksamkeit auf sich gezogen. Dies gilt nicht nur für die USA und andere westliche Länder, sondern auch für China, das in den letzten Jahren seine Anstrengungen zum Aufbau von IW-Truppen stark forciert hat.

Junhua Zhang

Schon im Jahr 1997 wurde auf einem Symposium des Generalstabs ein Plan zur Gründung einer IW-Führungsgruppe vorgelegt. Inzwischen ist ein spezielles Informationsnetzwerk für führende Offiziere zwecks der digitalen Kriegführung errichtet worden. Immer mehr «Netzwerk-Kämpfer» werden in die Armee rekrutiert. Sie kennen zumindest eine Fremdsprache und wissen, wie die Feinde «digital» zu vernichten sind. Seit 1999 werden in zahlreichen Städten «digitale Milizen» gegründet, die im Kriegsfall unmittelbar dem Kommando des Militärs unterstehen. In Shanghai wurde letztes Jahr das «Zentrum der Armeereserven der Informationskontrolle» gegründet, und zugleich wurden Einsatzgruppen gebildet, die sich mit Satellitenkommunikation, Mikrowellen-, Internet- und Elektro-Warfare sowie Information Warfare befassen.

In Praxis erprobt

Neben dem institutionellen Aufbau wurden in jüngster Zeit bereits mehrere Manöver durchgeführt. Im Mai 2000 verlief ein vom Raketen-Regiment der Beijinger Luftwaffe durchgeführtes Manöver mit vernetzten Computern erfolgreich. Im Juni 2000 sollen in eine 96-stündige Operation im Chendu-Militärbezirk mehrere Dutzend Netzwerke (Intranet) und mehrere hundert mit dem Intranet verbundene Endgeräte integriert und über 70 Prozent der führenden Offiziere beteiligt gewesen sein. Eines der wichtigsten Ziele der Operation bestand darin, die Sicherheitsmassnahmen der digitalen Netzwerke zu checken. Im August 2000 wurden in eine Combi-Aktion im Beijing-Militärbezirk IW-Strategien in die konventionelle Kriegführung eingebettet. Und noch ein jüngstes Beispiel, das den raschen Aufbau der elektronischen Kriegführung aufzeigt: Vom 28. Mai bis 2. Juni dieses Jahres haben die Luftwaffe, Artillerietruppen und Fallschirmjägertruppen von drei Militärbezirken erfolgreich ein auf Hightech basierendes Manöver in der Taiwanstrasse durchgeführt.

Grosser Nachholbedarf

Trotz grosser Anstrengungen und beachtlicher Erfolge sollen Chinas Möglichkeiten im internationalen Vergleich realistisch eingeschätzt werden. Laut Urteil westlicher Fachleute ist China generell (noch) nicht in der Lage, einen erfolgreichen digitalen Krieg zu führen und wird es auch mindestens in den nächsten fünf Jahren nicht sein. Zu gross ist der Nachholbedarf an Informationssicherheit. Dazu muss man wissen, dass das chinesische Verständnis von Informationssicherheit zwei Aspekte beinhaltet. Der erste Aspekt bezieht sich auf die Zensurmechanismen bezüglich Software und Institutionen, die den dafür verantwortlichen Behörden die Kontrolle über die Verbreitung beziehungsweise Beschaffung von politischen Informationen von Seiten der Internetnutzer ermöglichen. Beim zweiten Aspekt handelt es sich um die üblichen Sicherheitsmassnahmen, die sowohl in der Hardware des Computers als auch in einem Netzwerk zu treffen sind. Durch mehrere «Hackerkriege» hat China selbst einsehen müssen, dass die chinesischen PCs und Netzwerke jeder Art für Angriffe sehr anfällig sind.

Wachsam und misstrauisch

China betreibt eine sehr aktive Politik im Hinblick auf die Gewährleistung der Informationssicherheit. Der Aufbau eines modernen Sicherheitssystems wird als eine dringende Aufgabe erachtet, sowohl für die militärische Verteidigung als auch zur Aufrechterhaltung der sozialen Stabilität. Schon seit langer Zeit ist China besonders wachsam gegenüber aus dem Ausland importierten Computern. Es wird befürchtet, dass solche Produkte mit «Trojanischen Pferden» präpariert sind. China bemüht sich darum, möglichst wenig IW-Angriffsflächen zu bieten, indem beispielsweise die zu militärischen Zwecken gebrauchten Netzwerke physisch vom Internet getrennt sind und indem eigene Firewall-Software und Chips entwickelt werden. ■

Junhua Zhang, Dr., Wissenschaftlicher Mitarbeiter an der Freien Universität Berlin, stammt aus Shanghai, China.

Information Warfare
International Symposium
An event of AVIA – The Swiss Officers Association of the Air Force
November 21-23 2001, AAL Lucerne

21. bis 23. November 2001 im Armee-Ausbildungszentrum Luzern

Informationskrieg: Bedrohungen und Abwehr

Die modernen Kommunikationsmittel im Verbund mit der Informatik bieten heute – ob Einzelperson, Unternehmen, Staat oder Armee – riesige Chancen. Gleichzeitig nehmen die mit den Informationstechnologien verbundenen Risiken stark zu. Gefahren durch Hacker, Viren sowie das Abfassen und Abhören von Nachrichten sind alltäglich und richten enormen Schaden an.

Vom 21. bis 23. November findet erstmals in der Schweiz ein öffentliches Symposium zu diesem Thema statt. Organisiert wird es durch die Gesellschaft der Offiziere der Luftwaffe (AVIA) im Armee-Ausbildungszentrum Luzern. Referenten aus den USA, Europa und der Schweiz erläutern die Bedrohungen sowie die tauglichen Abwehrmassnahmen.

Anmeldung, Auskünfte und Kosten: Referenten, Themen und Preise sind im Internet unter www.sympinfowarfare.ch ersichtlich oder können beim Sekretariat (Telefon 041 630 19 52) erfragt werden.

Inbegriffene Leistungen: Ausführliche Referatsunterlagen, Getränke und Verpflegung, Parkplatz, persönliche Kontaktmöglichkeiten zu den Referenten sowie hohen Vertretern aus Wirtschaft, Politik und Militär. **Projektleiter:** Oberst Daniel A. Furrer.

Korrigendum: Der Preis für das Kombi A (alle 3 Tage) beträgt Fr. 890.– und nicht Fr. 800.– wie in der letzten Ausgabe irrtümlich erwähnt.