Autor	Wegmann, Bodo
Titel	**Rezension zu** **Günther K. WEIßE:** **Informationskrieg + Cyber War.** **Die unbekannte Gefahr.** **Motorbuch-Verlag, Stuttgart 2007**
Ort, Datum/Jahr	Berlin, 21.09.2007
GKND-Dok.nr.	RZ-2007-09-21

Während Günter K. Weiße im Frühling dieses Jahres an seinem Computer im Zollernalbkreis die Arbeiten an seinem Manuskript abschloß, saß irgendwo irgendwer und drang heimlich in EDV-Systeme der Bundesregierung in Berlin ein. Vier Tage bevor „Informationskrieg + Cyber War" veröffentlicht wurde, machte *Der Spiegel* diese Angriffe auf die Rechner des Kanzleramtes, der Bundesministerien für Wirtschaft und Forschung sowie des Auswärtigen Amtes öffentlich. „Die gelben Spione [seien] aus Lanzhou in Nordwest-China, aus Kanton im Süden und aus Peking" gekommen, zitierte das Nachrichtenmagazin aus Sicherheitskreisen.[1] Bundeskanzlerin Merkel brachte das Thema auf die Tagesordnung ihres Staatsbesuchs in Peking. Wer diesen Weiße gelesen hat, weiß, daß nicht nur die Volksrepublik China über die Fähigkeiten und Mittel für solche Operationen verfügt und die tatsächlichen Täter kaum eindeutig ermittelt werden können.

Nur wenige sind sich bewußt, in welchem Ausmaß wir bereits mit einer Parallelwelt leben, der Welt der elektronisch-digitalen Telekommunikation und Datenverarbeitung. Jede Kommunikation zwischen A und B besteht aus der Übermittlung von Signalen. Mittels der signalerfassenden Aufklärung, sie wird in der Regel als Signals Intelligence (Sigint) bezeichnet, klärt C die Signale und Modi ihrer Generierung, Übermittlung, Verarbeitung und Speicherung auf - vorzugsweise unbemerkt von A und B. Will C die Signalsysteme der anderen beeinflussen, setzt er Mittel und Methoden der entsprechenden Kriegsführung ein. Welche Dimension der Cyber Warfare mittlerweile erreicht hat, wird dem Leser äußerst faktenreich erläutert.

Einleitend knüpft Weiße an sein erstes Buch an.[2] Es bietet einen ausgezeichneten geschichtlichen Einstieg in die Thematik, die der Autor hier auf „Signals Intelligence, Informationsoperationen und Informationskrieg im 21. Jahrhundert" erweitert. Schon diese Kapitelüberschrift macht deutlich, daß die themenbezogene Terminologie so differenziert ist, wie es die verschiedenen Akteure sind, die auf dem modernsten Kriegsschauplatz handeln. Weiße hat auch hier durchgängig darauf geachtet, das Wer mit dem Wie korrekt zu verbinden: des einen Communications Intelligence ist des anderen Fernmeldeaufklärung. Alle Begriffe werden so erklärt, daß auch Nichtfachkundige den Ausführungen gut folgen und ESM von ECM unterscheiden können.

Gleiches gilt für die beschriebenen Akteure. Weiße konzentriert sich auf staatliche Einrichtungen und dabei auf Streitkräfte, geheime Nachrichtendienste und Sicherheitsbehörden. Auf mehr als hundert Seiten erfährt der Leser, welcher

---

1 Der Spiegel, 27.08.2007, Titelblatt und S. 19.

2 „Geheime Funkaufklärung in Deutschland 1945-1989" (Stuttgart: Motorbuch-Verlag 2005).

Staat über welche Organisationen, Mittel und Interessen in den Bereichen signalerfassende Aufklärung und Cyber Warfare verfügt. Die rund 50 Portraits reichen von Ägypten bis zur VR China; sie umfassen alle Kontinente und behandeln große Länder wie Australien, Großbritannien, Frankreich und Syrien ebenso wie Mazedonien und Luxemburg. Darüber hinaus stellt der Autor die informationser- und verarbeitenden Stellen und Strukturen der Europäischen Union, der NATO und der Vereinten Nationen vor. Der Leser kann dem Buch Grundlagen entnehmen, um die entsprechenden Potentiale von Konfliktparteien wie Indien und Pakistan, der Volksrepublik und National-China oder der beiden koreanischen Staaten gegenüberzustellen.

Die Portraits sind aktuell, gut gegliedert, mit zahlreichen Organigrammen ergänzt und zeugen oftmals von einer beeindruckenden Detailkenntnis. Sie zeigt sich beispielhaft an Großbritannien. Dort behandelt Weiße nicht nur die bekannten Dienste MI 5, MI 6, das GCHQ und die Defence Intelligence, sondern auch so selten betrachtete Einrichtungen wie die SOCA (Serious Organized Crime Agency), das Joint Terrorism Analysis Centre und das Joint Analysis Centre der britischen Armee. Auch die European Network and Information Security Agency der EU dürfte vielen unbekannt sein. Dabei könnte sie sich „künftig zu einer zentralen Schaltstelle für die Kontrolle und Überwachung der Informations- und Kommunikationstechnologie in der Europäischen Union entwickeln“ (S. 90).

Trotz der Vielzahl der untersuchten Länder, ihrer Intelligence Communities und relevanten Bereiche der Streitkräfte wird hier wie an anderen Stellen die Konzentration und Quellenstärke des Buches auf westliche und besonders NATO-Staaten deutlich. Demgegenüber weisen Darstellungen zur östlichen Seiten weniger Fundstellen primärer Provenienz und vereinzelt Fehler auf wie bei den Diensten der Russischen Föderation (S. 164 f.). Israels „Büro für wissenschaftliche Beziehungen“ wurde zwar 1986 geschlossen (Lishka le-Kishrei Mada: S. 172, Fn. 149); im Malmab fand es aber einige Jahre später seine Nachfolge. Die häufig zu findende Feststellung, näheres sei „aus offenen Quellen derzeit nicht verfügbar“, trifft in ihrer Uneingeschränktheit nicht immer zu.

Besonders umfangreich behandelt der Autor Deutschland und die USA. Gerade bei der Darstellung der Nachrichtendienste und Streitkräfte geht er mit großer Gründlichkeit vor und stellt dabei auch behördliche Komponenten vor, die nur wenige Leser von vornherein mit „Informationskrieg und Cyber War“ in Verbindung bringen würden, so z. B. die Bundesnetzagentur. Die Aktualität des Buches zeigt sich hier auch an den Ausführungen zur Umgestaltung des militärischen Nachrichtenwesens. Weiße nimmt den Faden beim Ist-Stand von 1990 auf und führt ihn über Auslandseinsätze der Bundeswehr und die Auflösung ihres Zentrums für Nachrichtenwesen bis in den aktuellen Prozeß mit der Neuordnung der Fernmelde- und elektronischen Aufklärung im KSA und der Streitkräftebasis. Auch die Kompetenzabstimmungen zwischen Bundeswehr und Bundesnachrichtendienst in Form von Leistungsvereinbarungen gehören dazu. Bemerkenswert sind Weißes Angaben zu der Großlegende *Bundesstelle für Fernmeldestatistik*, mit der der BND seit langem Teile seiner technischen Aufklärung tarnt. Gemeinsame Lagezentren wie GTAZ, GMLZ und GIZ fehlen natürlich ebenfalls nicht.

Auch für die Darstellung der USA weisen die verwendeten Quellen die Nähe des Autors zur Materie aus. Sicher führt er den Leser durch das selbst für Kenner nur schwer durchschaubare Gebilde der US Intelligence Community (US IC) mit ihren großen Diensten wie CIA, DIA, Department of Homeland Security und NSA/CSS aber auch so relativ unbekannten Organisationselementen wie dem National Clandestine Service. So läßt sich die enorme Transformation der US IC seit

2001 gut nachvollziehen. Dazu gehört, daß Weiße die zahlreichen Dokumente der höchsten Ebenen (National Strategies, Acts, Directives, Presidential Orders etc.) aufnimmt und ihre Umsetzung in Gesetze, nachrichtendienstliche und militärische Strukturen und Methoden aufzeigt.

Das amerikanische Potential zur elektronisch-digitalen Kriegsführung erscheint beeindruckend. Ob Weißes umfassenden Ausführungen kann man sich zu der Annahme verleiten lassen, die USA seien auch auf diesem Gebiet nicht nur eine, sondern *die* Supermacht. Doch klugerweise enthält er sich einer solchen Wertung. Er bleibt auch hier bei seinem Anspruch, in erster Linie zu dokumentieren, das darzustellen, was war, was ist und was wahrscheinlich schon bald sein wird.

Dazu gehört die Symbiose der signaltechnischen Aufklärung, Informations-Operationen und -Kriegsführung mit der Open Source Intelligence, kurz OSInt. Gerade hier mißt der Autor dem Internet eine besondere Bedeutung bei - als Chance einerseits, als Risiko andererseits. Mühten sich früher Geheimdienstmitarbeiter, mit Hilfe von Lineal, Nadeln und Fäden Wer-kennt-Wen-Schemata auf geklebten Bögen an ihren Bürowänden auszuarbeiten, geschieht dies heute mit Social-Network-Analysis-Systemen. Sie verbinden allgemein zugängliche Daten mit denen von Finanzdienstleistern, Krankenkassen, Telekom-Providern etc. sowie Behörden aller Art (vom Amtsarzt bis zum Zentralen Melderegister). Das Vernetzungsspektrum, die Ausgabevarianten und die Ergebnistiefe vermag sich nur vorzustellen, wer solche Systeme im Einsatz erlebt hat. [3]

Auch hier unterlegen aktuell bekannt gewordene Ermittlungserfolge die Darlegungen des Autors. Zutreffend ist seine Prognose, daß die kombinierte Nutzung militärischer, behördlicher, ziviler und kommerzieller Datenbestände weiter zunehmen und nationale Grenzen dabei immer geringere Hemmnisse sein werden. Das Total Information Awarness-Programm der USA dient als Beispiel. Weiße macht deutlich, wie weitreichend schon jetzt die Zugriffsmöglichkeiten der US-Nachrichtendienste auf Datenbanken von Sicherheitseinrichtungen der EU und ihrer Mitgliedsstaaten sind.

Die Fähigkeiten des einen sind die Bedrohung des/der anderen. Nach seinen präzisen Schilderungen, wer womit was kann oder könnte, erläutert Günther Weiße die Risiken für Informations- und Telekommunikationssysteme, vom Einzelplatzrechner bis zu supranationalen Großnetzen. Für ihre Ausspähung oder Manipulation (bis zur Zerstörung) können einerseits staatliche Stellen verantwortlich sein. Ihre Palette reicht von begrenzten Maßnahmen, wie sie z. B. im Rahmen der Telekommunikationsüberwachung gerade als sog. Online-Durchsuchungen diskutiert werden, bis zum flächendeckenden Angriff auf die IT- und Kommunikationsinfrastruktur anderer Staaten. Andererseits ergeben sich Bedrohungen durch nichtstaatliche Akteure. Hierbei kann es sich um professionell ausgeführte Konkurrenzspionage handeln oder um Täter mit kriminellen oder terroristischen Motiven und Zielen.

Nur manchmal weicht Günther Weiße von seiner auf Ausgewogenheit bedachten Darstellungsweise ab. Zwar beschreibt er die Bedrohung, die z. B. vom Iran für die westliche Welt ausgehen könnte. Aber den Umkehrschluß, daß die immensen Kapazitäten des Westens mit den USA, Großbritannien u. a. Großmächten des Cyber-Warfare den Iran bedrohen können, unterläßt er.

---

[3] Robert O'Harrow hat sie in „No place to hide" (New York/London u. a.: Penguin Books 2005/2006) eindrucksvoll beschrieben.

Fast zwingend ergibt sich nicht nur für den Autor, daß Regierungen verpflichtet sind, Schutz- und Abwehrmaßnahmen gegen diese Bedrohungen zu schaffen. Wohl nicht jeder ist sich ihrer aber bewußt, was sie wiederum vergrößert. Auch unter diesem Aspekt kann der Untertitel des Buches verstanden werden. Weiße führt historische Beispiele an, die zeigen, zu welchen verhängnisvollen Entwicklungen derartiges Fehl- und Nichthandeln auf politischer oder militärischer Führungsebene geführt hat.

Besonders kenntnisreich ist der Autor in bezug auf die technischen Mittel und Methoden. Akribisch listet er entsprechende Geräte und Systeme auf. Das mag manchem Leser an mancher Stelle als ein Zuviel des Guten erscheinen, zumal Beispiele aus der Anwendungspraxis leider nur selten beschrieben werden. Das betrifft auch Einrichtungen, deren besondere Aufgaben sich nicht jedem Leser erschließen werden. Zwar erfährt er z. B. viel über die technische Ausstattung des Bundesamtes für Post und Telekommunikation (S. 218 f.). Doch was und warum das Amt damit konkret überwacht hat, kann er dem Buch nicht entnehmen.

Günther Weiße hat ein interessantes und vielseitiges Buch geschrieben, in dem er für den Leser ein sehr umfangreiches Spektrum der Risiken aus der und für diese uns umgebende Parallelwelt ausbreitet

- von Ausspähungs- und Angriffsszenarien gegen einzelne Computer bis zu nationalen kritischen Infrastrukturen,
- von Streitkräften bis zu Gruppierungen der internationalen Organisierten Kriminalität, des Terrorismus und der Business Intelligence,
- von ‚Desert Storm' und ‚Iraqi Freedom' über den Balkan bis nach Afghanistan.

Der Vorgang um die Angriffe der „gelben Spione", die Debatte um Online-Durchsuchungen und Lawful Interception zeigen, wie aktuell dieses Buch ist. Gleiches gilt für die Auslandseinsätze der Bundeswehr, strategische Interessen der USA sowie Risiken für Unternehmen und die Forschung durch Economical Intelligence-Maßnahmen geheimer Dienste und Cyber-Kriminelle.

Weiße belegt die große Faktenmenge durch eine Fülle von Quellen. Viele von ihnen liegen jenseits der Standardliteratur, über die der Autor zweifelsohne auch verfügt hat. Er legt Wert darauf, ausschließlich offen zugängliche Quellen verwendet zu haben. Eindrucksvoll zeigt er damit die Möglichkeiten, die sich aus der OSInt und dem Internet ergeben. Der Verlag hätte dem Leser einen Dienst erweisen können, hätte er das Buch mit einem Stichwortregister und einem Verzeichnis der zahlreichen Abkürzungen ausgestattet.

Die „Nutzung der elektronischen Kommunikationsmittel [wird] immer mit einem gewissen persönlichen Risiko verbunden sein [...], da der Nutzer damit rechnen muß, seine Kommunikationsbeziehungen und deren Inhalte [...] rechtfertigen zu müssen", bilanziert Günther K. Weiße (S. 367). In der elektronisch-digitalen Parallelwelt geht nichts verloren. Wer weiß, in welche Lagebilder und Stimmungsprognosen unsere E-Mails eingehen, wer uns wann unsere Google-Recherchen vorhalten, welche Einreise uns unter Vorhaltung vermeintlich suspekter Telefonverbindungen verweigert wird? Krisen, Konflikte und Kriege werden mit zunehmender Tendenz nicht mehr nur mit konventionellen Mitteln geführt, sondern zugleich auf dem Cyber War Theatre.