Standort ist aus Sicherheitsgründen geheim. Für das Scannen von Iris und Fingerabdrücken wird unter anderem Software von den Firmen Accenture, Greenbit und IriTech genutzt. Nach Angaben des Auswärtigen Amtes[11] liegen derzeit 8,2 Millionen Erwachsene und Kinder in der Datei. In einem ähnlichen des Welternährungsprogramms der Vereinten Nationen sind demnach biometrische Informationen zu 11,4 Millionen Begünstigten aus 32 Ländern gespeichert.

Über Umwege können die In… auch in den polizeilichen oder … landen. Unter „angemessenen U… Personen ermittelt wird[12] oder di… ZeugInnen aussagen sollen, über… bezogene Daten an Strafverfolgungsbehörden oder Gerichte. Dies geschieht auf Anfrage der Behörden oder auch auf eigene Initiative des UNHCR. Die Weitergabe kann auch zur Gefahrenabwehr erfolgen, etwa um Straftaten oder eine Gefährdung der öffentlichen Sicherheit zu verhindern. Die Behörden sollen aber versichern, dass die Daten nicht anderweitig verwendet werden.

Quelle: https://netzpolitik.org/2019/nato-errichtet-biometrie-datenbank-nach-vorbild-der-usa/

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Anmerkungen

1 *https://onezero.medium.com/exclusive-this-is-how-the-u-s-militarys-massive-facial-recognition-system-works-bb764291b96d*
2 *https://www.nato.int/cps/en/natohq/official_texts_156624.htm*
3 *http://dipbt.bundestag.de/doc/btd/19/136/1913673.pdf*
4 *https://www.nato.int/cps/en/natohq/news_117917.htm?selectedLocale=en*
5 *https://www.marines.mil/Portals/1/MCRP%203-33.1J%20*
/stories/threeswords/
s/homepage.aspx
…21/btd/18/014/1801411.pdf
9 *https://netzpolitik.org/2017/europol-startet-datentauschring-mit-geheimdiensten-und-us-militaer/*
10 *https://www.wn.de/Welt/Politik/3157871-Operation-Gallant-Phoenix-Bericht-BND-beteiligt-sich-an-US-Geheimaktion-gegen-IS*
11 *https://www.andrej-hunko.de/start/download/dokumente/1411-sammlung-und-verarbeitung-biometrischer-daten-in-hilfsprogrammen-der-vereinten-nationen/file*
12 *https://www.refworld.org/docid/55643c1d4.html*
13 *https://netzpolitik.org/author/matthias/*
14 *http://www.cilip.de/*

Lesen & Sehen

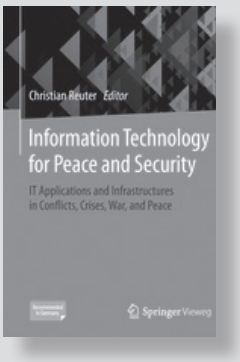
Neues für Bücherwürmer & Cineasten

Stefan Hügel

Christian Reuter (Editor): Information Technology for Peace and Security – IT Applications and Infrastructures in Conflicts, Crises, War and Peace

Der *Cyberspace* gilt längst als fünfte militärische Domäne, gleichrangig oder inzwischen sogar bedeutender als die klassischen militärischen Aktionsfelder Land, See, Luft und naher Weltraum. Der Cyberspace überschreitet physische, geografische und politische Grenzen. Er erfasst mittlerweile (fast) jeden Winkel dieser Erde und wird dadurch zum Ausspähraum gigantischen Ausmaßes. Und dennoch ist er paradoxerweise die letzte Domäne für verdeckte militärische Aktivitäten. Grund: Die Entwicklung und die Produktion von Waffen für Cyberoperationen benötigen keine auffälligen Anlagen; ihr Transport und ihre Stationierung erfordern keinen physischen Raum; ihre Erprobung und ihr Einsatz hinterlassen keine Spuren – zumindest keine physischen, und digitale Spuren können verdeckt, manipuliert oder sogar ausgelöscht werden.

Fragen des Friedens und der Sicherheit werden dadurch zum Anwendungsfeld der Informationstechnik. Damit sollten sie auch Inhalt der (akademischen) Lehre sein. Ihr Einfluss und ihre Nutzung in (kriegerischen) Konflikten ist Thema des hier besprochenen Bandes, der als Lehrbuch konzipiert und, so der Herausgeber, als Grundlage einer Vorlesung geeignet ist.



Christian Reuter *Editor* (2019)
Information Technology for Peace and Security – IT Applications and Infrastructures in Conflicts, Crises, War and Peace.
Wiesbaden: Springer Vieweg,
424 Seiten
Preis: 34,01 €uro
ISBN 978-3-658-25652-4,

Der Herausgeber, Professor am neu eingerichteten Lehrstuhl *Wissenschaft und Technik für Frieden und Sicherheit* (PEASEC) an der Technischen Universität Darmstadt, hat eine Reihe von Autorinnen und Autoren seines eigenen und weiterer Institute versammelt, deren Beiträge die Bedeutung, die Potenziale und die Herausforderungen der Informationstechnik für Frieden und Sicherheit behandeln, wie es im Vorwort heißt. Zu Beginn jedes Kapitels werden dessen Ziele formuliert; am Ende stehen eine

Zusammenfassung und Übungsaufgaben. Die Beiträge sind in Englisch abgefasst. Der Band umfasst 19 Kapitel in sieben Abschnitten von fast 30 Autorinnen und Autoren.

Der Abschnitt *Introduction and Fundamentals* gibt zunächst einen Überblick über die einzelnen Beiträge des Bandes. Danach wird die Rolle der Informationstechnologie (IT) in Friedens-, Konflikt und Sicherheitsforschung vertieft. Der Weg von der konventionellen Friedens- und Konfliktforschung zur technikbezogenen Friedensforschung wird gezeichnet und dabei die IT-Friedensforschung in der Schnittmenge zwischen technischer Friedensforschung und Cybersicherheit verortet. Zuletzt wird ein Überblick über die Forschungslandschaft in Deutschland (Forschungsinstitute und Nicht-Regierungsorganisationen) gegeben. Der letzte Beitrag des Abschnitts erörtert naturwissenschaftliche und technische Friedensforschung. Er geht auf das Sicherheitsdilemma ein, demzufolge verstärkte Sicherheitsbestrebungen letztlich zu mehr Unsicherheit führen. Er erläutert außerdem Maßnahmen zur Verminderung der militärischen Bedrohung (Rüstungskontrolle und verifizierte Abrüstung) und zur Erhöhung der Sicherheit (Nichtverbreitung und Exportkontrollen). Der Beitrag schließt mit Überlegungen, wie Informations- und Kommunikationstechnik sowie Forschung in diesem Feld den Frieden fördern können – wobei sie gleichzeitig eine zunehmende Rolle bei der Vorbereitung militärischer Konflikte spielen.

Der folgende Abschnitt befasst sich mit *Cyber Conflicts and War*. Der erste Beitrag dieses Buchteils zeichnet den Weg der Informationskriegführung von einer militärischen Doktrin zum alltäglichen Element eines permanenten Konflikts nach. Die Entwicklung zur primären Militärdoktrin begann in den 1990er Jahren, als zunächst die USA Konzepte für *Information Warfare* entwickelten: *command and control* gegen militärische Kommandostrukturen, *civil affairs operations* mit psychologischen Mitteln gegen die Zivilbevölkerung und *public affairs operations* als Public-Relations-Aktivitäten. Im weiteren Verlauf wurde Information Warfare weiter intensiviert und automatisiert und mündet heute in eine hybride Kriegführung, mit der man hybriden Bedrohungen durch reguläre Kräfte, irreguläre Kräfte, terroristische Angriffe und kriminelle Anteile begegnen will. Alle großen Mächte verfolgen heute solche Strategien und entwickel(te)n integrierte Waffensysteme auf der Basis von IT. Damit wurden Informationskriegführung und Cyberoperationen zum Mittel eines permanenten Konflikts zwischen staatlichen und nichtstaatlichen Akteuren.

Um Cyberspionage und Cyberabwehr geht es im folgenden Beitrag. Er grenzt Cyberspionage von traditionellen Formen der Spionage ab, führt in die Ziele der Informationssicherheit ein und stellt Designprinzipien für IT-Sicherheit, typische Angriffsszenarien durch die Ausnutzung von Schwachstellen und Abwehrmaßnahmen dar.

Der dritte Beitrag des Abschnitts geht auf die spezielle Bedeutung des Darknet für die Cyberkriegführung ein. Das Darknet ist ein Teil des Internet, in dem unbeobachtete, anonyme Kommunikation und die Vermeidung von Zensur, zumeist auf Basis des TOR-Netzwerks, möglich sein und damit die Attribuierung, d. h. die Zuordnung der Urheber von Transaktionen, weiter erschwert werden soll. Das Darknet wird mit seinen Risiken und Möglichkeiten vorgestellt. Im Rahmen der Cyberkriegführung wird es beispielsweise für den verdeckten Waffenhandel mit Cyberwaffen, für Destabilisierung, aber auch für zivilgesellschaftlichen Widerstand genutzt. Abschließend behandelt der Beitrag die *Versicherheitlichung*, d. h. die Transformation politischer Diskurse in Sicherheitsdiskurse, und verortet Cyberkriegführung und Darknets als deren Basis.

Ein Gegenkonzept zur Cyberkriegführung ist das im dritten Buchabschnitt erläuterte Konzept des *Cyber Peace*. Es geht von einer zunehmenden Militarisierung des Cyberspace aus und fragt nach Möglichkeiten für Sicherheit, Stabilität und Frieden angesichts des zunehmenden Fortschreitens der Militärtechnik. Daraus werden politische Schritte und Maßnahmen für eine friedenserhaltende Weiterentwicklung des Cyberspace abgeleitet. Grundprobleme sind die anonyme Nutzung von Cyberwaffen, deren mangelnde Kontrolle und dass sie uns mehr schaden als nützen. Beispielhaft werden bekannt gewordene Cyberattacken beschrieben, ebenso völkerrechtliche Initiativen, beispielsweise das *Tallinn Manual*, das völkerrechtliche Regeln und Normen für die Cyberkriegführung zusammenstellt. Schwierigkeiten der Rüstungskontrolle ergeben sich aus dem Konzept der *Aktiven Verteidigung* (z. B. durch Maßnahmen des *Hackback*) und Dual-use. Die *Cyberpeace*-Initiative des FIfF (Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung) mit dem dort entwickelten Forderungskatalog ist ein zivilgesellschaftlicher Ansatz, die friedliche Nutzung des Cyberraums zu fördern.

Dual-use und die Dilemmata für Cybersicherheit, Frieden und Technikbewertung stehen im Mittelpunkt des folgenden Beitrags. Viele Techniken, die hohen Nutzen stiften, können gleichzeitig zur Verursachung erheblicher Schäden genutzt werden (Dual-use-Dilemma). Dem versucht man mit einem Spektrum von Maßnahmen – von Transparenz bis zu gesetzlichen Regelungen – zu begegnen. Weitere Maßnahmen sind Technologiebewertung und Zivilklauseln an Hochschulen, die militärische Forschung einschränken oder verbieten.

Der letzte Beitrag dieses Abschnitts befasst sich mit Maßnahmen des Aufbaus von Vertrauen und Sicherheit. Die Vorbereitung offensiver Akte der Cyberkriegführung führt zu militärischer Instabilität und muss daher eingedämmt werden. Dazu können vertrauensbildende Maßnahmen beitragen. Entsprechende Initiativen gibt es im akademischen, im staatlichen und im internationalen Bereich.

Ein wesentlicher Ansatz zur Konfliktvermeidung ist *Cyber Arms Control*. Im ersten Beitrag dieses Abschnitts wird die Rüstungskontrolle aus ihrem historischen Kontext heraus entwickelt, und es werden unterschiedliche Ansätze und schrittweise Fortschritte von Rüstungskontrollabkommen und die unterschiedlichen Vorschläge von staatlichen Organisationen, privaten Unternehmen und nichtstaatlichen Organisationen erläutert.

Eine besondere Herausforderung für die Rüstungskontrolle stellen unbemannte Systeme dar. Gleichzeitig nimmt ihre Bedeutung für militärische Operationen zu. Kritisiert werden autonome Systeme aus technischer, ethischer und rechtlicher Sicht. Sie können die internationale Sicherheit destabilisieren und müssen entsprechend kontrolliert werden. Die Folgen, die sich ohnehin aus der Nutzung von Software, Automation, Autono-

mie und Künstlicher Intelligenz ergeben, sind im militärischen Bereich noch gravierender als im zivilen Bereich – auch wenn die Probleme grundsätzlich die gleichen sind.

Die Verifikation von Maßnahmen der Rüstungskontrolle wird im letzten Beitrag dieses Abschnitts beschrieben. Im Cyberspace gibt es spezielle technische Rahmenbedingungen, die die Verifikation erschweren. Etablierte Maßnahmen werden auf ihre Probleme bei der Anwendung im Cyberspace untersucht. Danach werden Ansätze zur Verifikation im Cyberspace erläutert.

Ein Problem der Cyberkriegführung ist die Attribuierung, also die Zuordnung von Angriffen zu einem Angreifer. Die Möglichkeiten und Schwierigkeiten bei der Attribuierung von Angriff en behandelt der erste Beitrag des Abschnitts *Cyber Attribution and Infrastructures*. Nach der Erläuterung der grundlegenden Prinzipien folgen die speziellen Probleme bei *Malware* und *Advanced Persistent Threats* und bei der Attribuierung im Cyberkrieg. Attribuierung ist weiterhin ein komplexes und ungelöstes Problem.

Resiliente kritische Infrastrukturen sind für die Abwehr von Angriffen von besonderer Bedeutung. Deswegen müssen kritische Infrastrukturen resilient konstruiert werden. Die Bedeutung der Resilienz bei kritischen Infrastrukturen, ihre Definition und Modelle zu ihrer Konstruktion sind Thema des nächsten Beitrags. Dabei wird auch zwischen den englischen Begriffen *safety* und *security* differenziert: Während *safety* sich vor allem auf die Zuverlässigkeit und Fehlertoleranz der Systeme bezieht, die auf der langfristigen Nutzung sicherer Konfigurationen fußen, meint *security* die Fähigkeit, sich laufend ändernde Bedrohungen abzuwehren und dafür stetig angepasst zu werden – ein Zielkonflikt, der aufgelöst werden muss.

Von besonderer Bedeutung ist die Sicherheit (*security*) kritischer Informations-Infrastrukturen. Der letzte Beitrag des Abschnitts untersucht deren Grundsätze, ihre Schlüsselcharakteristika und Funktionalität und die Risiken und Bedrohungen, denen sie ausgesetzt sind. Ein Phasenmodell des Schutzes kritischer Infrastrukturen wird vorgestellt, das von der Analyse über die Umsetzung von Schutzmaßnahmen, Überwachung, Behandlung von Störungen, Wiederherstellung und Verbesserung, Schulung und Wissensverbreitung bis zur Bestätigung und Zertifizierung reicht.

Im Abschnitt *Culture and Interaction* werden zu Beginn erneut die Konzepte von Sicherheit im Sinne von *safety* und *security* vorgestellt, ergänzt um deren zugrundeliegende Theorien und Methodologien. Die Entstehung und Bedeutung von Sicherheitskulturen wird erläutert und das sich ändernde Verhältnis von technologischen zu politischen Problemen reflektiert.

Die beiden weiteren Beiträge des Abschnitts lenken den Blick auf die sozialen Medien. Zunächst stehen kulturelle Aspekte im Fokus: das Verhältnis sozialer Medien und der ihnen zugrundeliegenden Informations- und Kommunikationstechnologien zu Gewalt und Frieden. Kulturelle Eingriffe durch Nutzer sozialer Medien wie auch durch Social Bots können Konflikte anheizen, aber auch gesellschaftlichen Frieden fördern. Die interessengeleitete Nutzung von sozialen Medien und von Informations- und Kommunikationstechnologien durch unterschiedliche Akteure in Konflikten wird im letzten Beitrag dieses Abschnitts angesprochen und kritisch betrachtet.

Den Abschluss des Bandes bildet ein *Outlook*, der von den AutorInnen des Lehrbuchs gemeinsam zusammengestellt wurde. Hier werden aktuelle Trends und abzusehende künftige Entwicklungen vorgestellt und bewertet. Die AutorInnen gehen davon aus, dass die Unsicherheit durch informationstechnische Angriffe und damit der Bedarf an technischen Lösungen und internationalen Abkommen zur Reduzierung des Risikos weiter zunehmen werden.

Von einem Lehrbuch erwartet man, dass es die wesentlichen Aspekte seines Themengebiets umfassend und auf Basis aktueller wissenschaftlicher Erkenntnisse behandelt. Diesem Anspruch wird der Band gerecht. Zahlreiche Beispiele realer Cybervorfälle illustrieren den Inhalt. Die Bedeutung der Informationstechnologie für Frieden, Sicherheit und Konflikte wird weiter zunehmen, wie regelmäßig Berichte in den Medien zeigen. Dies zeigt der Band auf, indem er aktuelle Trends und Entwicklungen im Ausblick zusammenstellt. Er bietet damit entsprechend seiner Zielsetzung eine gute und umfassende Einführung in die Thematik.

Der Zusammensetzung des Bandes aus Beiträgen einzelner Autorinnen und Autoren ist wohl geschuldet, dass die Themen nicht immer klar abgegrenzt sind. So erläutert das Kapitel zur Spionage beispielsweise viele Grundlagen der IT-Sicherheit, die auch für andere Bereiche relevant sind und deswegen in einen eigenen Grundlagenabschnitt ausgelagert werden sollten. Im Beitrag über das Darknet werden ausführlich die Grundlagen von Konflikten referiert und die mit dem *Framing* verbundenen Probleme erläutert. Die eigentliche Thematik, das Darknet, kommt im Vergleich dazu zu kurz. Mit vielen Querverweisen wird versucht, inhaltliche Verknüpfungen herzustellen. Dennoch würde eine stringentere, übergreifende Strukturierung den Wert des Bandes noch erhöhen.

Für eine zweite Auflage würde ich mir eine intensivere Behandlung von Verfahren der Spieltheorie, der Künstlichen Intelligenz und des Maschinellen Lernens im militärischen Bereich wünschen – die Nutzung sowie Möglichkeiten und Grenzen sowohl für Cyberoperationen und IT-Sicherheit als auch für Verifikation und Forensik. Auch die Konsequenzen daraus – die Frage der Realisierbarkeit, Möglichkeiten und Probleme einer Maschinenethik – könnten ausführlicher behandelt werden. Ein Abschnitt zu Ansätzen des Transhumanismus imMilitär wäre ebenfalls wünschenswert. Dazu könnten die Verflechtungen von Wissenschaft und Forschung – insbesondere an Hochschulen – Inhalt eines weiteren Abschnitts sein.

In Summe tun diese Kritikpunkte dem Wert des Bandes aber keinen Abbruch. Wer sich einen fundierten Überblick über die aktuellen Entwicklungen der Informationstechnologie für Frieden und Sicherheit verschaffen will, dem ist dieses Buch zu empfehlen.

Die Rezension erschien zunächst in Wissenschaft & Frieden 4/2019. Wir danken der Redaktion für die freundliche Genehmigung zum Nachdruck.