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

Matthias Monroy

NATO errichtet Biometriedatenbank nach Vorbild der USA

Das US-Verteidigungsministerium speichert Millionen Menschen mit Gesicht, Iris, Fingerabdrücken und DNA, eine dazugehörige Warndatei ist mit Polizeibehörden vernetzt. Die NATO will ein ähnliches System aufbauen. In weitaus größerem Umfang sammeln allerdings Flüchtlingsorganisationen biometrische Daten von Schutzsuchenden.

Das Militär der Vereinigten Staaten verfügt über eine Datenbank mit Millionen Gesichtsbildern, Iris-Fotos, Fingerabdrücken und DNA-Daten. In diesem *Automated Biometric Information System* (ABIS) sind derzeit 7,4 Millionen Identitäten gespeichert, berichtet das Nachrichtenmagazin *OneZero*[1]. Die Angaben stammen aus einer Anfrage nach dem Informationsfreiheitsgesetz und basieren auf der Präsentation eines Mitarbeiters im Verteidigungsministerium.

Die militärische Biometrieagentur verwaltet die Datei. Gesammelt werden Daten in Ländern, in denen das US-Militär aktiv ist. Das System soll Terrorverdächtige und deren Kontaktpersonen identifizieren und aufspüren, biometrische Spuren werden unter anderem von gefangenen oder getöteten GegnerInnen abgenommen. Daten stammen laut OneZero aber auch aus Wählerregistrierungen, Arbeitsverhältnissen oder sonstigen Informationen, an die das Militär gelangt. Auch verbündete SoldatInnen werden erfasst.

Weltweit vernetzte Warndatei

Das ABIS ermöglicht außerdem, einzelne Personen in eine sogenannte *Biometrically Enabled Watch List* (BEWL) einzutragen. Die Warndatei kann mit Systemen von Polizeien oder Geheimdiensten verbunden werden und gibt einen Alarm aus, wenn die Betroffenen eine Grenze passieren oder in eine Polizeikontrolle geraten. Dieses System ist auch über mobile Geräte zum Abgleich von Fingerabdrücken, Iriden oder Gesichtern nutzbar.

Derzeit sollen mehr als 213.000 Personen in der BEWL gespeichert sein. Im ersten Halbjahr 2019 wurden laut der Präsentation des US-Verteidigungsministeriums 4.467 Treffer mithilfe der Warndatei erzielt, davon waren etwa zwei Drittel gegnerische Kräfte in Kriegsgebieten.

Dem Bericht zufolge ist das ABIS unter anderem mit der biometrischen Datenbank des FBI verbunden, die an weitere lokale Polizeidatenbanken angeschlossen ist. US-Behörden arbeiten demnach auch an einer Vernetzung mit der Biometriedatenbank des Heimatschutzministeriums. Auf diese Weise könnte das ABIS zu einem weltweiten zivil-militärischen Informationssystem ausgebaut werden. Auch europäische Polizei- und Geheimdienstbehörden fragen biometrische Daten beim den zuständigen Polizeibehörden und dem US-Militär ab.

NATO-System ohne DNA-Daten?

Vor einem Jahr haben auch die NATO-Mitgliedstaaten den Aufbau einer Biometriedatenbank beschlossen[2]. Unter dem Namen *NATO Automated Biometric Identification System* (NABIS) sollen dort Daten zu Gesicht, Iris und Finger gespeichert werden. Das deutsche Verteidigungsministerium bestätigt die Angaben[3], erwähnt aber keine DNA-Daten.

Zwar ist das System nach offiziellen Angaben noch in der Entwicklung, ein Prototyp wurde der NATO zufolge[4] jedoch schon im Jahr 2014 im gemeinsamen Manöver *Unified Vision* getestet. In einem Papier[5] hat das US-Militär die damaligen technischen Spezifikationen des ABIS erklärt.

In einer späteren Version könnten auch Hände und Venen, Handschriften, Sprechproben, Tastendruck oder der Gang von Personen als biometrische Informationen erhoben und verarbeitet werden. Für die NATO und die mit dem Bündnis verbundenen Truppen sind diese Daten von grundlegendem Interesse[6].

Anbindung internationaler Polizeiorganisationen

Derzeit ist nicht bekannt, welche Hersteller mit der Entwicklung des NABIS beauftragt sind. Zuständig für das Projekt ist die Kommunikations- und Informationsagentur der NATO[7] mit Sitz in Den Haag. Es ist denkbar, dass das NABIS auf dem ABIS des US-Militärs aufbaut oder dessen technische Infrastruktur nutzt. Laut OneZero wird das US-System von dem amerikanischen Konzern Leidos errichtet, der hierfür 150 Millionen Dollar erhielt und weitere US-Firmen als Auftragnehmer verpflichtet.

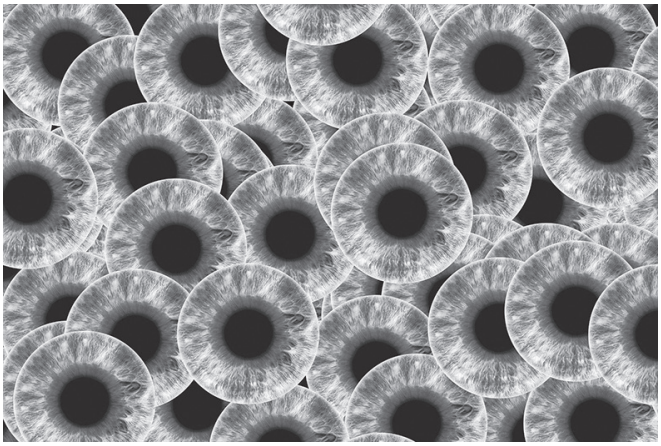

Bild: Hebi B. auf Pixabay

Für eine Datenbank in Afghanistan ist demnach die Firma Ideal Innovations Incorporated verantwortlich. Dabei handelt es sich vermutlich um das System HAMAH, eine ähnliche Datensammlung zu „Daten von Kriegsschauplätzen" (*battlefield data* oder *battlefield information*) betreibt das US-Militär unter dem Namen VENLIG im Irak. Auch die Polizeiagentur Europol sowie Interpol werden vom US-Militär in die beiden Systeme eingebunden und liefern bei Bedarf Daten zu gespeicherten Personen. Werden „Bezüge zu Deutschland festgestellt", erfolgt laut der Bundesregierung[8] auch eine Anfrage an das Bundeskriminalamt (BKA) über dort vorhandene Informationen.

HAMAH und VENLIG dürften die Vorläufer der neuen US-Biometrie-Datei gewesen sein, jedenfalls schreibt OneZero, dass die meisten der sieben Millionen Identitäten aus Afghanistan und dem Irak stammen. Auch in der Operation *Gallant Phoenix*[9] sammelt das US-Militär biometrische Daten in Syrien und dem Irak. Aus EU-Dokumenten ergibt sich, dass daran auch Europol beteiligt ist, aus Deutschland außerdem der Bundesnachrichtendienst[10].

UN-Flüchtlingskommissar betreibt eigenes System

Neben Militär, Geheimdiensten und Polizei sammeln auch Hilfsorganisationen in großem Umfang biometrische Daten. Der Hohe Flüchtlingskommissar der Vereinten Nationen (UNHCR) betreibt in 66 Ländern ein System zur Identifikation, Registrierung und Verwaltung von Schutzsuchenden. In diesem *Biometric Identity Management System* werden auch Kinder ab fünf Jahren mit Gesichtsfoto, Fingerabdrücken beider Hände und Bildern beider Irides erfasst.

Das Biometriesystem des UNHCR wird zentral geführt und in Gebieten ohne Internet auf lokalen Servern gespiegelt. Ihr

Matthias Monroy

Matthias Monroy[13], Wissensarbeiter, Aktivist und Mitglied der Redaktion der Zeitschrift Bürgerrechte & Polizei/CILIP[14]. In Teilzeit Mitarbeiter des MdB Andrej Hunko. Publiziert in linken Zeitungen, Zeitschriften und Online-Medien, bei Telepolis, Netzpolitik und in Freien Radios. Alle Texte und Interviews unter digit.so36.net, auf englisch digit.site36.net, auf Twitter @matthimon. *Viel zu selten auf der Straße (dafür im Internet) gegen Faschismus, Rassismus, Sexismus, Antisemitismus. Kein Anhänger von Verschwörungstheorien jeglicher Couleur. Freut sich nicht über Kommentare von AnhängerInnen der genannten Phänomene. Benutzt das (altmodische) Binnen-I trotz Gepolter nervtötender Maskulisten.*

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 Informationen zu Geflüchteten auch in den polizeilichen oder militärischen Biometriedateien landen. Unter „angemessenen Umständen", etwa wenn gegen Personen ermittelt wird[12] oder diese (mit ihrer Zustimmung) als ZeugInnen aussagen sollen, übermittelt das UNHCR personenbezogene 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/

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%20BIOMETRICS%201.pdf*
6 *http://www.jwc.nato.int/images/stories/threeswords/Biometrics_2018.pdf*
7 *https://www.ncia.nato.int/Pages/homepage.aspx*
8 *https://dipbt.bundestag.de/dip21/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/*

CC BY NC SA

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