

Blick in die Glaskugel:

Bundeswehr will politische Ereignisse vorhersehen

von Matthias Monroy

[3]

Schon seit einigen Jahren forscht das Verteidigungsministerium an der Auswertung offener Quellen im Internet, um im Mandatsgebiet der Bundeswehr die „Meinungs- und Stimmungslagen der Bevölkerung“ zu ermitteln. Medienberichten zufolge will das Militär nun auch „potenzielle Krisen“ vorhersehen. Zum Einsatz kommt demnach die Software „IBM Watson“.

Die Bundeswehr optimiert ihre Bedarfsplanung mit neuen Anwendungen zur Verarbeitung großer Datenmengen. Das Verteidigungsministerium beschafft dazu die Datenbank-Anwendung „SAP Analytics“, mit der „vorausschauende Analysen“ über Lieferprozesse möglich sein sollen. Der Einsatz ist Teil einer „Digitaloffensive“ der Bundeswehr und erfolgt [laut der Berliner Zeitung Tagesspiegel](#) [4] im Rahmen eines Pilotprojekts, an dessen Ende über eine endgültige Beschaffung entschieden werden könnte.

► Schon länger „Bedarf“ für In-Memory-Technologie

„Analytics“ basiert auf der In-Memory-Technologie, die der deutsche IT-Konzern SAP als „Hochleistungsanalyseanwendung“ (HANA) vermarktet. Die zu verarbeitenden Datenbestände werden im Arbeitsspeicher der Rechner gehalten und sind damit um ein Vielfaches schneller durchsuchbar. Das System verknüpft sogenannte Vergangenheitsdaten mit Informationen, die in Echtzeit anfallen. Auf Basis dieser Prognosen empfiehlt „HANA“ Entscheidungen. SAP benutzt dafür den Begriff „[vorausschauende Wartung](#) [5]“ („predictive maintenance“).

Den „Bedarf für den Einsatz einer In-Memory-Technologie“ hatte das Verteidigungsministerium bereits [vor drei Jahren mitgeteilt](#) [6]. Damals wurde außer „HANA“ auch die Software „Blu“ des US-amerikanischen Konzerns IBM für eine mögliche Beschaffung untersucht. Vorher hatte das Ministerium [eine Marktsichtung](#) [7] zu Anwendungen zur Prognose von großen Datenmengen durchgeführt und mit einigen Firmen anschließend „[ein Gespräch](#)“ geführt.

► Entscheidung gegen Palantir

Mit „SAP Analytics“ will die Bundeswehr „mögliche Ausstattungs- und Versorgungsprobleme“ identifizieren. In dem derzeit laufenden Pilotprojekt testet das Verteidigungsministerium außerdem die [Plattform „IBM Watson“](#) [8], die unter anderem [vom US-Militär eingesetzt](#) [9] wird und dort ebenfalls die „[vorausschauende Wartung](#)“ erledigt. „Watson“ nutzt dafür einen Pool aus mehreren Milliarden Daten, die von Sensoren an militärischer Ausrüstung geliefert werden. Laut IBM gehören hierzu neben Fahrzeugen und anderem Gerät auch Drohnen.

Dem Tagesspiegel zufolge will die Bundeswehr mit „Watson“ jedoch auch „potenzielle Krisen“ bis zu 18 Monate im Voraus erkennen. Vor der Entscheidung für die IBM-Software hatte das Verteidigungsministerium auch die von der hessischen Polizei genutzte Vorhersagesoftware „Gotham“ der US-Firma Palantir Technologies geprüft.

► Welche Datenquellen werden genutzt?

Es ist unklar, mit welcher Datenbasis früherer „Krisen“ oder sonstiger politischer Ereignisse „Watson“ gefüttert werden soll. Eine solche Datenbank „Global Data on Events, Location and Tone“ (GDELT) wird beispielsweise von dem Informatiker Kalev Leetaru betrieben (www.gdeltproject.org [10]) und wertet täglich tausende Berichte aus öffentlich zugänglichen Medien aus. Ziel von GDELT ist das Aufspüren zukünftiger Unruhen, Revolten oder Anschläge.

Auch das von Google und dem US-Geheimdienst CIA gegründete Unternehmen [Recorded Future](#) [11] bietet entsprechende Dienste an. Unter anderem hatte das US-Militär derartige Verfahren 2011 im Rahmen seiner Intervention [in Libyen eingesetzt](#) [12]. Hierfür werden öffentlich zugängliche Quellen im Internet ausgewertet (sogenannte OSINT-Verfahren).

► Ermittlung von „Meinungs- und Stimmungslagen“

Zu einer solchen „[IT-gestützten Nachrichtengewinnung aus offenen Quellen](#)“ hatte die Bundeswehr am Standort Mayen in der Eifel bereits die beiden Analysetools „Texttragic“ und „Brandwatch“ getestet. Zuständig ist das [Zentrum Operative Kommunikation der Bundeswehr](#) [13], die beiden Programme sollen dort helfen, bei Auslandseinsätzen die [Lage im Informationsumfeld](#)“ zu ermitteln.

Mit „Texttragic“ und „Brandwatch“ werden dem Verteidigungsministerium zufolge keine Personendaten erhoben, sondern [Meinungs- und Stimmungslagen der Bevölkerung](#) ermittelt. Die Bundeswehr vergleicht die Auswertung sozialer Medien im Internet mit der Analyse von Leserbriefen, bei denen es sich in beiden Fällen um „öffentlich zugängliche Meinungsäußerungen“ handelt.

► Auch BKA beforscht Auswertung offener Quellen

Breiter aufgestellte Forschungen für eine militärische „Wissenserschließung aus offenen Quellen“ (WeroQ) waren zwar für den [Zeitraum von 2014 bis 2016](#) [14] beauftragt, diese wurden aber wegen eines fehlenden Zuwendungsbescheides des Bundesamtes für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) für das Fraunhofer Institut FKIE [nicht durchgeführt](#) [15]. „WeroQ“ sollte das „Informationsumfeld“ erschließen, wozu die Bundeswehr [laut einer Grafik](#) [13] die „Heimat“, das „Einsatzgebiet“ und die „internationale Öffentlichkeit“ zählt.

Unter Koordination des Bundes Deutscher Kriminalbeamter [bdk](#) [16]) hatte auch das Bundeskriminalamt mit dem Fraunhofer-Institut IAIS die Auswertung offener Quellen beforscht. Heraus kam die Software „[FuhSen](#) [17]“ (föderierte und hybride Search-Engine), die über Schnittstellen auch Soziale Medien, das „Deep Web“ (etwa Online-Marktplätze) oder das „Dark Web“ durchsucht.

Matthias Monroy

Matthias Monroy ist Wissenschaftler, Aktivist und Mitglied der Redaktion der Zeitschrift [Bürgerrechte & Polizei/CILIP](#) [18]. In Teilzeit Mitarbeiter des MdB [Andrej Hunko](#) [19]. 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](https://twitter.com/matthimon).

[netzpolitik.org](#) ist eine Plattform für digitale Freiheitsrechte. Die Betreiber und deren Autoren thematisieren die wichtigen Fragestellungen rund um Internet, Gesellschaft und Politik und zeigen Wege auf, wie man sich auch selbst mithilfe des Netzes für digitale Freiheiten und Offenheit engagieren kann. Mit [netzpolitik.org](#) beschreiben sie, wie die Politik das Internet durch Regulation verändert. Und wie das Netz Politik, Öffentlichkeiten und alles andere verändert. Sie verstehen sich als journalistisches Angebot, sind jedoch nicht neutral. Ihr Haltung ist: Engagement für digitale Freiheitsrechte und ihre politische Umsetzung.

[3]

► **Quelle:** Erstveröffentlicht am 07. Juni 2018 auf NETZPOLITIK.org >> [Artikel](#) [20]. **Lizenz:** Die von NETZPOLITIK verfassten Inhalte stehen, soweit nicht anders vermerkt, unter der Lizenz Creative Commons (Namensnennung - Nicht-kommerziell - Weitergabe unter gleichen Bedingungen 4.0 International ([CC BY-NC-SA 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/) [21])). Die Bilder im Artikel sind nicht Bestandteil des Originalartikels und wurden von KN-ADMIN Helmut Schnug eingefügt. Für sie gelten ggf. andere Lizenzen, s.u..

► Bild- und Grafikquellen:

1. **Hochleistungsrechner** sorgen mit hochwertigen Komponenten für effizienten IT-Betrieb und ermöglichen eine Wissenserschließung der durch Massenüberwachung gewonnenen Erkenntnisse im Informationsumfeld des gläsernen Menschen. Die Bundeswehr optimiert ihre Bedarfsplanung mit neuen Anwendungen zur Verarbeitung großer Datenmengen. Das Verteidigungsministerium beschafft dazu die Datenbank-Anwendung „SAP Analytics“, mit der „vorausschauende Analysen“ über Lieferprozesse möglich sein sollen. Der Einsatz ist Teil einer „Digitaloffensive“ der Bundeswehr. **Bildgrafik:** Fotocitizen / Jorge Guillen. **Quelle:** [Pixabay](#) [22]. Alle bereitgestellten Bilder und Videos auf Pixabay sind gemeinfrei (Public Domain) entsprechend der Verzichtserklärung [Creative Commons CC0](#) [23]. Das Bild unterliegt damit keinem Kopierrecht und kann - verändert oder unverändert - kostenlos für kommerzielle und nicht kommerzielle Anwendungen in digitaler oder gedruckter Form ohne Bildnachweis oder Quellenangabe verwendet werden. >> [Foto](#) [24].

2. Blick in das Combined Air Operations Center der Al Udeid Air Base der US-Luftwaffe in Katar. Das Air Force Distributed Common Ground System (AF DCGS), auch als AN/GSQ-272 SENTINEL-Waffensystem bezeichnet, ist das primäre Intelligenz-, Überwachungs- und Aufklärungssystem (ISR) der US-Luftwaffe, das die Sammlung, Verarbeitung, Nutzung, Analyse und Verbreitung (CPAD) umfasst. **Foto:** U.S. Air Force. **Quelle:** [Wikimedia Commons](#) [25]. Diese Datei ist ein Werk eines Angestellten der [U.S. Air Force](#) [26], das im Verlauf seiner offiziellen Arbeit erstellt wurde. Als ein Werk der Regierung der Vereinigten Staaten ist diese Datei [gemeinfrei](#) [27].

3. Datenkrake. Bildgrafik: GDJ / Gordon Johnson, USA. **Quelle:** [Pixabay](#) [22]. Alle bereitgestellten Bilder und Videos auf Pixabay sind gemeinfrei (Public Domain) entsprechend der Verzichtserklärung [Creative Commons CC0](#) [23]. Das Bild unterliegt damit keinem Kopierrecht und kann - verändert oder unverändert - kostenlos für kommerzielle und nicht kommerzielle Anwendungen in digitaler oder gedruckter Form ohne Bildnachweis oder Quellenangabe verwendet werden. -> [Foto](#) [28].

Quell-URL: <https://kritisches-netzwerk.de/forum/blick-die-glaskugel-bundeswehr-will-politische-ereignisse-vorhersehen>

Links

- [1] <https://kritisches-netzwerk.de/user/login?destination=comment/reply/72111%23comment-form>
- [2] <https://kritisches-netzwerk.de/forum/blick-die-glaskugel-bundeswehr-will-politische-ereignisse-vorhersehen>
- [3] <https://netzpolitik.org/>
- [4] <http://www.bundeswehr-journal.de/2018/blick-in-die-zukunft-big-data-software-fuer-die-bundeswehr/>
- [5] <https://www.sap.com/products/predictive-maintenance.html>
- [6] <https://dipbt.bundestag.de/doc/btd/18/051/1805196.pdf>
- [7] <https://dipbt.bundestag.de/doc/btd/19/019/1901979.pdf>
- [8] <https://www.ibm.com/watson/de-de/>
- [9] <https://www.ibm.com/blogs/cloud-computing/2017/09/07/army-logistics-cloud-contract-watson/>
- [10] <https://www.gdeltproject.org/>
- [11] <https://www.recordedfuture.com/>
- [12] <https://www.recordedfuture.com/twitter-analysis-as-a-tool-in-libyan-engagement/>
- [13] http://cir.bundeswehr.de/portal/a/cir/start/dienststellen/ksa/zopkombw/ueber_uns/!ut/p/z/1/04_Sj9CPyKssy0xPLMnMz0vMAfIjo8zizSxNPN2Ngg18LSzcDA0c_RwD3PxDLyZcXQz0wwkpiAJKG-AAjgb6wSmp-pFAM8xmx2GqH6wfpR-ViViWWKFXkF9UkpNaopeYDHKhfmRGYi5KTmpAfriJRKAgN6LcoNxREQCOvBXy/dz/d5/L2dBISEvZ0FBIS9nQSEh/#Z7_694IG2S0M88F10ANAPFOU82GD5
- [14] <https://www.andrej-hunko.de/start/download/dokumente/485-nachfrage-zur-schriftlichen-frage-monat-juni-2014-veroq/file>
- [15] <https://dipbt.bundestag.de/doc/btp/18/18192.pdf>
- [16] <https://www.bdk.de/der-bdk/startseite>
- [17] https://www.iais.fraunhofer.de/content/dam/iais/fb/linked_open_data/FuhSen.pdf
- [18] <https://www.cilip.de/>
- [19] <https://andrej-hunko.de/>
- [20] <https://netzpolitik.org/2018/blick-in-die-glaskugel-bundeswehr-will-politische-ereignisse-vorhersehen/>
- [21] <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.de>
- [22] <https://pixabay.com/>
- [23] <https://creativecommons.org/publicdomain/zero/1.0/deed.de>
- [24] <https://pixabay.com/de/wolke-daten-hex-computer-3333628/>
- [25] https://commons.wikimedia.org/wiki/File:Air_Force_Distributed_Common_Ground_System_AN_GSQ-272_SENTINEL.JPG
- [26] https://de.wikipedia.org/wiki/United_States_Air_Force
- [27] https://de.wikipedia.org/wiki/Public_domain
- [28] <https://pixabay.com/de/krake-tentakel-f%C3%BCnf-auge-dhs-cia-1220817/>
- [29] <https://kritisches-netzwerk.de/tags/analysertools>
- [30] <https://kritisches-netzwerk.de/tags/baainbw>
- [31] <https://kritisches-netzwerk.de/tags/bka>
- [32] <https://kritisches-netzwerk.de/tags/blu>
- [33] <https://kritisches-netzwerk.de/tags/brandwatch>
- [34] <https://kritisches-netzwerk.de/tags/bund-deutscher-kriminalbeamter>
- [35] <https://kritisches-netzwerk.de/tags/bundeskriminalamt>
- [36] <https://kritisches-netzwerk.de/tags/bundeswehr>
- [37] <https://kritisches-netzwerk.de/tags/cia>
- [38] <https://kritisches-netzwerk.de/tags/dark-web>
- [39] <https://kritisches-netzwerk.de/tags/datenbanken>
- [40] <https://kritisches-netzwerk.de/tags/datenmengen>
- [41] <https://kritisches-netzwerk.de/tags/deep-web>
- [42] <https://kritisches-netzwerk.de/tags/digitaloffensive>
- [43] <https://kritisches-netzwerk.de/tags/drohnen>
- [44] <https://kritisches-netzwerk.de/tags/fkie>
- [45] <https://kritisches-netzwerk.de/tags/föderierte-und-hybride-search-engine>
- [46] <https://kritisches-netzwerk.de/tags/fraunhofer-institut>
- [47] <https://kritisches-netzwerk.de/tags/fuhsen>
- [48] <https://kritisches-netzwerk.de/tags/gdelt>
- [49] <https://kritisches-netzwerk.de/tags/gdeltprojectorg>
- [50] <https://kritisches-netzwerk.de/tags/global-data-events>
- [51] <https://kritisches-netzwerk.de/tags/gotham>
- [52] <https://kritisches-netzwerk.de/tags/hana>
- [53] <https://kritisches-netzwerk.de/tags/hochleistungsanalyse>
- [54] <https://kritisches-netzwerk.de/tags/hybride-search-engine>
- [55] <https://kritisches-netzwerk.de/tags/iais>
- [56] <https://kritisches-netzwerk.de/tags/ibm>
- [57] <https://kritisches-netzwerk.de/tags/ibm-software>
- [58] <https://kritisches-netzwerk.de/tags/ibm-watson>
- [59] <https://kritisches-netzwerk.de/tags/informationsumfeld>
- [60] <https://kritisches-netzwerk.de/tags/memory-technologie>
- [61] <https://kritisches-netzwerk.de/tags/kalev-leetaru>
- [62] <https://kritisches-netzwerk.de/tags/meinungs-und-stimmungslagen>
- [63] <https://kritisches-netzwerk.de/tags/location-and-tone>
- [64] <https://kritisches-netzwerk.de/tags/matthias-monroy>
- [65] <https://kritisches-netzwerk.de/tags/nachrichtengewinnung>
- [66] <https://kritisches-netzwerk.de/tags/osint-verfahren>
- [67] <https://kritisches-netzwerk.de/tags/palantir-technologies>
- [68] <https://kritisches-netzwerk.de/tags/pilotprojekt>
- [69] <https://kritisches-netzwerk.de/tags/predictive-maintenance>
- [70] <https://kritisches-netzwerk.de/tags/recorded-future>
- [71] <https://kritisches-netzwerk.de/tags/revolten>
- [72] <https://kritisches-netzwerk.de/tags/sap>
- [73] <https://kritisches-netzwerk.de/tags/sap-analytics>
- [74] <https://kritisches-netzwerk.de/tags/texttragic>
- [75] <https://kritisches-netzwerk.de/tags/unruhen>
- [76] <https://kritisches-netzwerk.de/tags/verteidigungsministerium>
- [77] <https://kritisches-netzwerk.de/tags/vorausschauende-wartung>
- [78] <https://kritisches-netzwerk.de/tags/vorhersagesoftware>
- [79] <https://kritisches-netzwerk.de/tags/veroq>
- [80] <https://kritisches-netzwerk.de/tags/wissenserschliessung>
- [81] <https://kritisches-netzwerk.de/tags/zentrum-operative-kommunikation-der-bundeswehr>
- [82] <https://kritisches-netzwerk.de/tags/zopkombw>