NETZWERK DATENSCHUTZEXPERTISE

Wenn aus Spiel Wirklichkeit wird – Potentiale kollaborativer Augmented Reality

Stand: 1.12.2016

Inhalt

Ute Bernhardt
Elchdamm 56A, 13503 Berlin
030-2804 6695
bernhardt@netzwerk-datenschutzexpertise.de
www.netzwerk-datenschutzexpertise.de

Die zunehmende Verbreitung von Datenbrillen in der Kombination mit Anwendungen der „erweiterten Realität", Augmented Reality, macht es notwendig, sich mit den Potentialen ihres kollaborativen Einsatzes näher zu beschäftigen. Der Fokus der Betrachtung liegt auf den Konsequenzen für die zivile Sicherheit durch den Einsatz von Datenbrillen durch kriminelle Gruppen oder Terroristen und den daraus folgenden Implikationen für die Technikgestaltung[1].

1 Augmented Reality auf dem Weg zum Massenmarkt

Die um digitale Informationen „erweiterte Realität" – Augmented Reality, kurz: AR – ist mittlerweile zu einem Massenmarkt mit Millionen Endkunden geworden. Zu den beliebtesten Computerspielen des Jahres 2016 gehörte mit Pokemon Go erstmals ein Spiel, das Smartphones für ein AR-Spiel nutzte, um Spielfiguren in einer realen Umgebung zu finden. Der besondere Effekt des Spieles war die Möglichkeit des Spiels gegen andere Spieler.

Für derartige AR-Spiele, perspektivisch aber vor allem für betriebliche Anwendungen gibt es bereits diverse Datenbrillen, die eine möglichst realistische Kombination von Umgebungsbild und virtuellen Daten liefern und die Hände frei lassen. Für diese Systeme gibt es nicht nur Einzel- sondern auch AR-Gruppenspiele wie etwa „Life is Crime", die daraus bestehen, in der eigenen realen Umgebung bei einer virtuellen kriminellen Gang aktiv mitzuwirken als – so die Werbung – Weg, um das „Leben eines Kriminellen zu führen, ohne dafür ins Gefängnis zu müssen"[2]. Insgesamt haben sich für Datenbrillen schon viele Anwendungsideen, teilweise auch erste Anwendungen entwickelt, die deutlich über Computerspiele und Unterhaltung hinausgehen. So erprobt Volkswagen den Einsatz von Datenbrillen in der Logistik[3].

Durch die Eigenschaften des ersten breit publizierten Produkts Google Glass, einer vernetzten Brille mit Videokamera, Mikrofon und der Möglichkeit sofortiger akustischer oder optischer Rückmeldungen, die in das Sehfeld projiziert werden, wurde bereits eine Datenschutzdebatte angestoßen. Die Debatte war konzentriert auf die durch unbemerkte und ubiquitäre Aufzeichnung und Übermittlung von Live-Videos der Umgebung des Brillenträgers geschaffenen Möglichkeiten zur individualisierten Videoüberwachung der von einem Datenbrillenträger beobachteten Personen, dem Verlust von Kontrolle und Vertraulichkeit und durch die Speicherung und Analyse der Daten auf zentralen Servern zur weitergehenden Analyse der Daten den damit drohenden Verlust von Autonomie und Reputation[4].

---

[1] Ausgangspunkt dieser Betrachtung ist der Beitrag von Ute Bernhardt: Google Glass: On the implications of an advanced military command and control system for civil society. In: International Review of Information Ethics (IRIE): Cyber warfare, Issue No 19, Vol. 20, December 2013, p. 16-27 http://www.i-r-i-e.net/inhalt/020/IRIE-Bernhardt.pdf

[2] Werbung für "Life is Crime" auf: http://www.androidauthority.com/best-ar-apps-and-games-for-android-augmented-reality-584616/; das Spiel ist in Deutschland nicht verfügbar

[3] Wilfried Eckl-Dorna: Datenbrille als Logistik-Helfer Neue Chance für Google Glass - in den Lagerhallen von VW, Manager-Magazin, 09.03.2015, http://www.manager-magazin.de/unternehmen/autoindustrie/datenbrille-google-glass-soll-produktivitaet-von-vw-erhoehen-a-1022591.html

[4] Mark Hurst: The Google Glass feature no one is talking about; Feb. 28th 2013, http://creativegood.com/blog/the-google-glass-feature-no-one-is-talking-about/

Diese Diskussion kreiste bisher darum, Datenbrillen als vernetztes Einzelsystem [5] und das Verhältnis einzelner Nutzer zu ihren Gegenübern zu betrachten. Es fehlt jedoch bisher eine ähnlich umfassende Betrachtung von Datenbrillen als Kollaborations- und Gruppenunterstützungssysteme, die daraus folgenden Potentiale und deren Folgen. In diesem Beitrag sollen daher spezifische Möglichkeiten und Konsequenzen eines Einsatzes vernetzter Datenbrillen durch Gruppen von kollaborierenden Nutzern betrachtet werden.

2 Datenbrillen und ihre Eigenschaften

Die zahlreichen Typen von angekündigten[6] oder erhältlichen[7] Datenbrillen machen es wenig sinnvoll, ein einzelnes spezifisches System als Basis einer Analyse auszuwählen. Ausgangspunkt der Betrachtung hier soll daher zuerst eine Beschreibung der typischen Eigenschaften sein, die diese Systeme heute aufweisen. Zusätzlich werden die dabei bereits dokumentierten Manipulationen der Systeme und die von den Herstellern nicht intendierten oder gar in Abrede gestellten Eigenschaften kurz dargestellt. Dies wird in Bezug gesetzt zu den Zielen bei der ursprünglichen Entwicklung von Datenbrillen, woraus schlussendlich die möglichen Folgen dieser dokumentierten Eigenschaften betrachtet werden.

Die für diese Betrachtung relevanten Datenbrillen sind konzipiert als Augmented Reality Systeme, die Daten aus dem situativen Kontext des Betrachters passend in dessen Sichtfeld projizieren. Das Grundprinzip ist dabei, beispielsweise einem Kunden oder einem Werker per Datenbrille Hinweise zur Bearbeitung eines Produktes oder Werkstücks in dessen Sichtfeld einzuspielen oder bei einem komplexen Problem einem Servicetechniker vor Ort per Datenbrille die Hilfestellung durch einen irgendwo auf der Welt befindlichen Experten zu geben. Je nach Bautyp werden für die Projektion unterschiedliche, unter dem Begriff „head-mounted displays“ (HMD) zusammengefasste Techniken eingesetzt. Üblich ist ein semi-transparentes Brillenglas, patentiert ist bereits eine Kontaktlinse[8].

---

[5] “Even share what you see. Live”; http://www.google.com/glass/start/what-it-does/ ; zur Throughglass App: http://glass-apps.org/throughglass-google-glass-app

[6] So: Google Glass-Like Products Can Launch For As Low As $400, Forbes, 21.07.2013; http://www.forbes.com/sites/haydnshaughnessy/2013/07/21/google-glass-like-products-can-launch-as-low-as-400/. Zu dieser Zeit wurde bereits über vergleichbare Microsoft-Entwicklungen berichtet: Microsoft Tests Eyewear Similar to Rival Google Glass, Wall Street Journal Online, 22nd Oct. 2013, http://online.wsj.com/news/articles/SB10001424052702304402104579150952302814782 . Samsung hatte derweil dazu seinerseits Patente angemeldet: Samsung files patent for Google Glass-like device, San Jose Mercury News, 25.10.2013, http://www.mercurynews.com/business/ci_24386791/samsung-files-patent-google-glass-like-device

[7] Beispiele dafür sind Produkte wie Recon Jet HMD (http://reconinstruments.com/products/jet/) , Epiphany Eyewear (http://www.epiphanyeyewear.com/), GlassUp aus Italien (http://www.glassup.net/) und das Vuzix Smart Glasses Accessoire für Smartphones (http://www.vuzix.com/consumer/products_m100.html). Sogar Nissan präsentierte ein AR-Gerät auf der Tokyo Motor Show 2013 unter dem Produktname “3E”: The 3E View of the Tokyo Motor Show, Nov. 19, 2013, http://blog.nissan-global.com/EN/?p=11271;

[8] Doug Bolton: Samsung patents design for 'smart' augmented reality contact lenses; The Independent, 6.04.2016, http://www.independent.co.uk/life-style/gadgets-and-tech/news/samsung-smart-contact-lenses-patent-a6971766.html unter Bezug auf Samsung is working on smart contact lenses, patent filing reveals, http://www.sammobile.com/2016/04/05/samsung-is-working-on-smart-contact-lenses-patent-filing-reveals/ .

Da es darum geht, Hinweise zu einem spezifischen Werkzeugeinsatz an genau definierten Stellen einzuspielen oder Ansatzpunkte und Vorgehensweise für die Fehlersuche in das Sichtfeld einzuspielen, müssen die Umgebung des Anwenders mit einer Videokamera erfasst und die Videodaten detailliert analysiert werden. Die eingesetzte Bildanalyse-Technik ist darauf ausgerichtet, aus den Bilddaten anhand technischer Einzelheiten des Werkstücks optische Marker zu extrahieren, die eine exakte Positionsbestimmung für das Einspielen von optischen Hilfen erlauben. Es gibt aber auch Bilderkennungs-Werkzeuge für Datenbrillen, die eine Gesichtserkennung leisten oder Personen anhand von spezifischen Zusatzmerkmalen erkennen[9].

In der Regel ist außerdem eine Audio-Interaktion vorgesehen, da bei Datenbrillen auf eine manuelle Interaktion mit dem System oft verzichtet werden soll und stattdessen Sprachkommandos zur Steuerung vorgesehen sind. Die Audioübertragung wird auch als Kommunikationsmittel für die Beratung und den Austausch des Nutzers mit einer weiteren Person über die Problemlösung genutzt, die auf die Videodaten des Nutzers zugreifen kann.

Für all dies verfügen Datenbrillen über eine ausreichende Rechenkapazität und Netzwerkanbindung[10]. Verschiedene Systeme sind darauf ausgelegt, zusätzliche Sensoren einzubinden und zu vernetzen, wofür Programmschnittstellen offengelegt werden, die es Entwicklern erlauben, die Datenbrille auf ihre eigene Weise zu nutzen.

Ein Träger einer Datenbrille erstellt also in aller Regel Audio- und Videoaufnahmen der Umgebung, die der Kommunikation und Interaktion mit Back-end-Systemen oder Support-Fachleuten dienen und dazu in Echtzeit an eine Gegenstelle übermittelt werden, die die Bilder analysiert und zur Unterstützung oder auch zur Aufzeichnung nutzt. Wer die Bild- und Tonaufnahmen der Lebensumwelt des Trägers einer Datenbrille sieht, ist dessen Umgebung ebenso unklar wie die Dauer einer Aufzeichnung und die Art der darauf durchgeführten Datenanalyse.

Die Datenschutzprobleme dieser intensiven Umgebungsüberwachung sind unmittelbar einsichtig und bereits intensiv diskutiert. Aus Datenschutzsicht lassen sich dabei vor allem die auf Handhabungsaufgaben bezogenen Systeme in betrieblichen Anwendungen noch relativ gut fassen, wenn personenbezogene Daten zwar über die Handlungen der beteiligten Personen erhoben werden, selten aber über unbeteiligte Dritte[11].

Die Konzepte dazu sind älter: Babak A. Parviz: Augmented Reality in a Contact Lens. IEEE Spectrum, 1st Sept. 2009, http://spectrum.ieee.org/biomedical/bionics/augmented-reality-in-a-contact-lens

[9] The MedRec app offered in 2013 can lookup patient records by taking a picture of their face; http://glass-apps.org/medref-google-glass-app . Auf dem CCC-Kongress Dezember 2013 kündigte Lambda Labs eine Gesichtserkennungs-App an, die nicht von Google unterstützt wurde: Google Glass Face Recognition App Coming This Month, Whether Google Likes It Or Not; Forbes Onlie, 18th Dec. 2013, http://www.forbes.com/sites/andygreenberg/2013/12/18/google-glass-face-recognition-app-coming-this-month-whether-google-likes-it-or-not/

[10] Siehe Beschreibung und Berichte bei: http://www.google.com/glass/start/

[11] Die datenschutzrechtliche Betrachtung kann zurückgreifen auf Überlegungen zu Wearables bei Beschäftigten, siehe dazu auch Thilo Weichert: Wearables – Schnittstelle Mensch und Computer, CuA 10/2016, S. 8 ff.

3 Intendierte und nicht-intendierte Nutzung

Für die weiteren Betrachtungen ist von Bedeutung, dass es für viele der nachfolgend beschriebenen Möglichkeiten noch keine App zu kaufen gibt. Nötig sind daher gewisse Fertigkeiten in der Programmierung von derartigen bzw. vergleichbaren Geräten. Auch dabei liefert Google Glass einige gute Vergleichsangaben.

Um offenbar erwartete, und von Google nicht gewollte Anwendungen von Google Glass zu verhindern oder zumindest zu ahnden, sah Google in den Nutzungsbedingungen vor, dass das Unternehmen „sofern ein Google Gerät die Entwickler-Regelungen oder andere Übereinkünfte, Gesetze, Regularien oder Policies verletzt“, dieses “Glass-Gerät fernabschalten oder das Gerät aus seinen Servicesystemen entfernen kann”[12]. Zu Kontrollzwecken und zur Umsetzung dieser Nutzungsbedingung hatte sich Google zudem das Recht vorbehalten, die Ortungsdaten des Nutzers, sowie alle aufgenommen Photos, Videos und in das Display des Nutzers eingespielte Daten aufzuzeichnen und zu speichern[13]. Damit ist Google in der Position, auf Anforderung oder auf eigene Initiative alle Daten auf unzulässige Handlungen zu scannen. In Googles Version war Google Glass damit als die zivile Version eine mächtigen Kommando- und Kontroll-Systems angelegt.

Allerdings arbeitet Google Glass wie viele andere Datenbrillen mit dem Android Betriebssystem und wurde mit Hilfe dafür gängiger Werkzeuge schon wenige Tage nach Ausgabe der ersten Prototypen an Entwickler gehackt, die danach vollen Zugang zu allen Komponenten des Systems hatten[14]. Zwar wollte Google selbst keine Gesichtserkennungs-Software auf den Markt bringen, dafür kamen Apps alternativer Anbieter in Umlauf, deren Installation teilweise das Hacken der Google-Datenbrille voraussetzte[15]. Googles Überwachungs-Werkzeuge konnten damit auch umgangen werden.

Solche Sicherheitsprobleme sind nicht spezifisch für Google Glass, da alle Datenbrillen nur eine begrenzte Rechenkapazität haben. Kein System mit Ressourcen, wie sie Datenbrillen aufweisen, hat bislang gezielten Angriffen dauerhaft widerstehen können. Es ist daher eine gesicherte Vermutung, dass jedes System von Datenbrille – sofern keine kostspieligen und am Markt nicht durchsetzbaren Sicherheitskomponenten eingebaut werden – nach überschaubarer Zeit kompromittiert wird und seine Technik nach Belieben manipuliert werden kann.

[12] Google Glass Terms of Sale and Use (Dezember 2013); http://www.google.com/glass/terms/
[13] ebd.
[14] Entwicklerversion der Google Glass per QR-Code gehackt; http://www.heise.de/security/meldung/Entwicklerversion-der-Google-Glass-per-QR-Code-gehackt-1919373.html; based on: Lookout: Sicherheit für die vernetzte Welt: Ein Google Glass-Fallbeispiel; company blog, 17.07.2013, https://blog.lookout.com/de/2013/07/17/sicherheit-fur-die-vernetzte-welt-ein-google-glass-fallbeispiel/
[15] Google Glass Face Recognition App Coming This Month, Whether Google Likes It Or Not; Forbes Onlie, 18th Dec. 2013, http://www.forbes.com/sites/andygreenberg/2013/12/18/google-glass-face-recognition-app-coming-this-month-whether-google-likes-it-or-not/

4 Kollaborative Datenbrillen und ihre Urspünge

Über die bisher diskutierten Szenarien hinaus gehen Anwendungsfelder, bei denen es um die Interaktion mit Dritten geht, deren Verhalten mit Datenbrillen beobachtet wird[16]. Noch weitgehender sind die Konsequenzen, wenn Datenbrillen als Mittel der Gruppenkoordination gegen unbeteiligte Dritte eingesetzt werden, wie dies Google in seiner Werbung für Google Glass skizziert hat[17]. Ein Extrem dieser Möglichkeiten sind ein Google Glass ego-shooter[18] und andere Ideen etwa von Microsoft. Sie repräsentieren zugleich eine Rückkehr der Datenbrillen zu den historischen Ursprüngen aller mit HMD-Display gekoppelten AR-Systeme, auf die daher im Folgenden kurz eingegangen werden soll.

1993 führte die U.S. Army verschiedene Manöver mit Bodentruppen durch, um neu entwickelte Informations- und Kommunikationstechnik im Einsatz zu erproben. In der so genannten „Soldier Integrated Protective Ensemble (SIPE) Advanced Technology Demonstration (ATD)“ überfiel eine sehr kleine Gruppe von Soldaten erfolgreich eine weit größere Einheit und eroberte und besetzte verschiedene Positionen im offenen Feld ebenso wie im Häuserkampf. Unter herkömmlichen Bedingungen und gleichwertiger Ausstattung wird davon ausgegangen, dass ein erfolgreicher Angriff die dreifache Personalstärke voraussetzt als sie der Verteidiger aufbieten kann. Mit den Vorläufern von Datenbrillen wurde dieses Verhältnis auf den Kopf gestellt: Der unterlegene Verteidiger war dreimal stärker als der Angreifer.

Möglich wurde dieses umgekehrte Kräfteverhältnis nicht durch Techniken wie die einzeln bereits seit langer Zeit genutzten Laser- und Infrarot-Sensoren sowie Audio-Verstärkung und Richtmikrofone, sondern durch die Vernetzung von Soldaten und Sensoren in einem kollaborativen AR-System. Die Angreifer konnten durch den Sensor-Datenaustausch die Gegner mit passiver Datenerhebung triangulieren und auf einer gemeinsamen Gefechtsfeldkarte markieren. Diese Karte wurde mit anderen Daten in die Helmdisplays eingespielt. Wie heute dank Smartphones vielfach genutzt, wurde mit vernetzten Videokameras unbemerkt „um die Ecke“ gesehen für Bilder, die jeder in der Gruppe sehen konnte. Vor dem Überfall lieferten die Daten in den AR-Displays einen vollständigen Überblick über den Gegner und unterstützten einen hoch koordinierten Ablauf. Die gleichzeitige Datenübermittlung an einen zentralen Befehlshaber erlaubte es, die Aktion in Echtzeit zu verfolgen und mit zusätzlichen Informationen zu unterstützten[19].

Die umfassende Vernetzung zwischen Soldaten und Kommandeuren erwies sich als äußerst wirksamer „Force Multiplier“. Aus den bis in die 1980er Jahre zurück reichenden Ursprüngen

[16] Dies ist natürlich ebenso valide für gleichartige Produkte. Microsoft versuchte, sich eine Datenbrille für Multiplayer-Spiele patentieren zu lassen, so: Microsoft tries to patent AR glasses for multiplayer gaming, engadget, 02.08.2013, http://www.engadget.com/2013/08/02/microsoft-ar-glasses-for-multiplayer-gaming-patent/

[17] Simon Parkin: ButtonMasher: First AR games for Google Glass emerge; New Scientist, Nov. 1st, 2013; http://www.newscientist.com/article/dn24505-buttonmasher-first-ar-games-for-google-glass-emerge.html

[18] http://www.youtube.com/watch?v=QxG5xNktqw0

[19] Victor Middleton, Ken Sutton, Bob McIntyre and John O'Keefe IV: Soldier Integrated Protective Ensemble (SIPE) Advanced Technology Demonstration (ATD), Dayton, Oct. 2000, p. 22f. . http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA384680

der Entwicklung[20] wurde ein technologisches Entwicklungs- und Einsatzziel verschiedener Armeen, allen voran der USA[21]. Dort wurde als erster Schritt ein Kommunikationssystem für den Datenverbund etabliert[22], das danach Audio- und Videodaten in Echtzeit zwischen Kampfeinheiten und Kommandozentralen austauscht[23]. Die Bilder von U.S.-Präsident Barack Obama bei der Erstürmung des Verstecks von Osama bin Laden in Pakistan zeigten den Einsatz vernetzter Spezialeinheiten und deren Steuerung.

Der Schritt zur alltäglichen militärischen Nutzung von Datenbrillen steht allerdings noch aus; die Systeme sind noch nicht leistungsfähig, robust und genau genug. Derzeit werden diverse Systeme von verschieden Armeen erprobt[24]. So ist die Bundeswehr von der Konzeptionsphase im Programm „Infanterist der Zukunft“[25] mittlerweile zur Kampferprobung übergegangen. Das „Gladius“-System für AR-Anwendungen mit einem HMD wurde 2013 an das Heer für den Einsatz in Afghanistan ausgeliefert[26]. Die Einsätze sind jedoch auf spezielle Aktionen *von Spezialeinheiten oder Geheimdienstoperationen* beschränkt[27]. Trotz der Einschränkungen wurde der Markt für AR-Systeme für Anwendungen in Kampfeinsätzen auf 8,2 Mrd. Dollar für 2016 geschätzt[28].

[20] So die *Präsentation des britischen Unternehmens Scicon Computer Systems* bei der British Army Equipment *Exhibition 1984. Diese prototypische Ausrüstung für Soldaten sollte volle AR Funktionalität mit zusätzlicher Infrarot-Fähigkeit in einem integrierten HMD Display bieten, so:* Military Technology, No. 10, 1986, p. 166. Steven M Shaker, Robert Finkelstein: The Bionic Soldier; in: National Defense, April 1987, S. 27 – 32. Head-mounted displays (HMDs) für AR Anwendungen wurden zuerst publiziert als akademisches Paper von Tom Caudell, d.W. Mitzell: Augmented reality: an application of heads-up display technology to manual manufacturing processes; in: Proceedings of the Twenty-Fifth Hawaii International Conference on System Sciences, 1992, Vol.2, pp. 659 - 669

[21] U.S. Army: TRADOC Pamphlet 525-5: Force XXI Operations, A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century, TRADOC Pamphlet 525-5, Fort Monroe, Aug. 1994, p. 2-1ff

[22] U.S. Department of Defense, Office of the Assistant Secretary of the Army: Weapons Systems 2012, p. 108f

[23] Im *“Warfighter Information Network-Tactical Increment 3” Program, see:* U.S. Department of Defense, Office of the Assistant Secretary of the Army: Weapons Systems Handbook 2013, p. 322f

[24] Michael M. Bayer, Clarence E. Rash, James H. Brindle: Introduction to Helmet Mounted Displays, p.47-107; in: Clarence E. Rash, Michael B. Russo, Tomasz R. Letowski, Elmar T. Schmeisser: Helmet-Mounted Displays: Sensation, Perception and Cognition Issues, Fort Rucker, Alabama, 2009; http://www.usaarl.army.mil/publications/HMD_Book09/

[25] Infanterist der Zukunft; http://www.deutschesheer.de/portal/a/heer/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9jNTUIr2S1OSMvMxsvYLUouKC1Gy9zLy0xLySVP2CbEdFAPnFG_s!/

[26] Drittes Auge für Deutsche Soldaten; Spiegel Online, 20.02.2013; http://www.spiegel.de/wissenschaft/technik/militaertechnologie-bundeswehr-will-gladius-system-einfuehren-a-884238.html; see also the Rheinmetall press release: http://www.rheinmetall.com/de/rheinmetall_ag/press/news/archive2012/news_details_5_1664.php

[27] So: Samuel Liles: Cyber Warfare: As a Form of Low-Intensity Conflict and Insurgency; Conference on Cyber Conflict, NATO CCD COE Publications, 2010, p. 47-57

[28] Mind Commerce: Augmented Reality in the Battlefield 2012 – 2016, July 2012, ADS Report, Amsterdam 2012; https://www.asdreports.com/shopexd.asp?id=32490

5 Von der militärischen zur zivilen Nutzung

Nach der Einführung von Google Glass interessierten sich 2014 die Polizeibehörden New Yorks[29] und Dubais[30] für deren Nutzungspotentiale. Berichte über Ergebnisse liegen nicht vor. In Deutschland beschäftigte sich die Innenministerkonferenz im Juni 2016 damit, „aus Streifenbeamten vernetzte Polizisten“ zu machen und „Datenbrillen, um Fahndungsfotos oder Einsatzbefehle direkt an jeden einzelnen Polizisten zu verschicken, schon bald zur Standardausrüstung der Beamten“ zu machen[31].

Was ist nun zu erwarten, wenn Datenbrillen außerhalb von militärischen Kampfzonen im Zivilleben eingesetzt werden? Und – was bisher kaum beachtet wurde – was geschieht, wenn Datenbrillen bei kriminellen oder terroristischen Aktivitäten Verwendung finden? Drei einfache Beispiele mit anwachsendem Gefahrenpotential sollen dazu dienen, diese Möglichkeiten auszuloten.

Alle beschriebenen Eigenschaften von kollaborierenden Datenbrillen-Systemen sind zum Teil bereits im Rahmen heutiger Systeme verfügbar oder so in Reichweite, dass es nicht mehr als ein Jahr bedürfte, sie zu entwickeln. Noch sind solche Anwendungen aber nicht bekannt. Damit stellt sich im Anschluss die Frage, welche Bedingungen, Szenarien und Interessen dafür ausschlaggebend sein könnten, dass eine solche Nutzung von Datenbrillen auch real werden könnte.

5.1 Überwachung und Verfolgung

Eine einfache kollaborative Anwendung für Datenbrillen ist die Navigation. Wenn eine Navigation per Karte nicht zum Ziel führt, wird ein Datenbrillen-Nutzer von einer anderen, ortskundigen Person anhand der Videoaufnahmen der Datenbrille zum Ziel gelenkt – entweder durch gesprochene Richtungsangaben oder durch eingespiegelte Richtungspfeile. Ersetzt man dabei ein geografisches Ziel mit einer Person, die im Sichtfeld der Datenbrille – möglicherweise automatisch – erkannt, getaggt und hervorgehoben wird, so ist unmittelbar ersichtlich, dass vernetzte Datenbrillen ein erhebliches Potential zur Erleichterung bei der Verfolgung von Personen auch in sehr belebten Umgebungen haben.

Ergänzt man im nächsten Schritt einen solchen einfachen Datenaustausch mit den bereits in den 1990er Jahren erprobten Mitteln zur Distanzmessung und der passiven Triangulation durch zwei und mehr kollaborierende Nutzer von AR-Systemen und ergänzt dies durch die mit heutiger Technik mögliche automatische Erkennung und Markierung charakteristischer Features eines Verfolgten aus Videodaten, so sind erhebliche Erleichterungen bei der

[29] Matthew Sparks: New York Police Testing Google Glass; The Telegraph, 07.02.2014; http://www.telegraph.co.uk/technology/google/10623753/New-York-police-testing-Google-Glass.html
[30] Polizei in Dubai geht mit Google-Datenbrille auf Verbrecherjagd; in: Reuters, 2.10.2014, http://de.reuters.com/article/dubai-google-datenbrille-polizei-idDEKCN0HR19T20141002
[31] Peter Welchering: Was die Polizei von morgen über uns weiß, www.heute.de, 15.06.2016, http://www.heute.de/polizeiausruestung-thema-bei-innenministerkonferenz-was-die-polizei-von-morgen-ueber-uns-weiss-43944016.html

Verfolgung zu erzielen. Dass die Kommunikationsunterstützung bei Datenbrillen so unauffällig wie möglich gestaltet ist, vereinfacht die Koordination der Verfolger und verringert die Gefahr, dass Gruppen klandestiner Beobachter erkannt werden.

Für den nächsten Schritt der Überlegungen soll die Möglichkeit zur Sensorintegration betrachtet werden, um die Leistung eines AR-Systems weiter zu steigern. Dabei wurde sowohl in den anfänglichen Militärmanövern als auch in späteren Beispielen gezeigt, dass sich beliebige Sensoren mit AR-Systemen koppeln lassen. Die Videokameras ließen sich daher ersetzen oder ergänzen durch Infrarot- und Nachtsicht-Systeme, um die Wärmeabstrahlung von Personen zu erkennen. Auch dies ist eine attraktive Eigenschaft für diverse Outdoor-Spiele, aber zugleich auch ein nützliches Werkzeug für Sicherheitsbehörden ebenso wie bei kriminellen und terroristischen Aktivitäten.

Mit solchen minimalen Ergänzungen verfügbarer Datenbrillen-Apps lassen sich spannende AR-unterstützte Adventurespiele spielen – oder die von den Sicherheitsbehörden genannte Zahl von bis zu 35 Beamten für eine Observation [32] dank AR-Hilfe mit weit weniger Personal durchführen. Auf gleiche Weise könnten aber ebenso kriminelle oder terroristische Gruppen ein Opfer verfolgen.

Nach Terroranschlägen mit polizeilich bekannten Tätern wurde in Deutschland ebenso wie in Frankreich darüber debattiert, dass eine Observation durch Sicherheitsbehörden so viele Ressourcen bindet, dass sie nur in ausgesuchten und dringenden Fällen infrage kommt. Der ausufernde Einsatz „stiller SMS“ zur Ermittlung des Standortes von Verdächtigen [33] dokumentiert ein hohes Interesse am Einsatz technischer Hilfsmittel. Datenbrillen können – wie beschrieben – den Aufwand für eine Observation eindeutig reduzieren. Noch stärker vereinfacht wird dies, wenn – wie in den Manövern aus den 1990er Jahren beschrieben – Umgebungsintelligenz in Form von installierten Videokameras für die Personenerkennung oder mobile IMSI-Catcher für die Ermittlung von Telekommunikationskennungen von Mobilgeräten Daten mit Observationsteams austauschen, die über Datenbrillen verfügen. Diverse Analysen von Personenflüssen bei Großveranstaltungen[34] auch anhand von Handy-Kennungen zeigen die enormen Potentiale der Vereinfachung gezielter Observation auch in großen Menschenmengen. Es ist zu erwarten, dass entsprechende AR-Technologie in die Anforderungen an Entwicklung und Beschaffung von Technik für die Sicherheitsbehörden in den nächsten Jahren einfließen wird.

[32] Terrorismusbekämpfung: Zu wenig Ermittler? ARD Hauptstadtstudio-Blog, 15.10.2016, http://blog.ard-hauptstadtstudio.de/terrorismusbekaempfung-zu-wenig-ermittler/

[33] In den ersten sechs Monaten 2016 wurden von den deutschen Sicherheitsbehörden über 210.000 „Stille SMS“ zur Ortung von Handys verschickt, vgl. Antwort der Bundesregierung auf die Kleine Anfrage der Abg. Hunko u.a.: Einsätze von sogenannten stillen SMS, WLAN-Catchern, IMSI-Catchern, Funkzellenabfragen sowie Software zur Bildersuche im ersten Halbjahr 2016, vom 09.08.2016, Bt.-Drs. 18/9366, Frage 4

[34] Marco Dettweiler; Tillmann Neuscheler: Computersimulierte Menschenströme: Eine Viertelstunde in die Zukunft schauen, in: FAZ, 17.10.2016, http://www.faz.net/aktuell/gesellschaft/ende-der-loveparade/computersimulierte-menschenstroeme-eine-viertelstunde-in-die-zukunft-schauen-11008870.html . Siehe auch: Crowd Management: Smartphone soll Massenpanik verhindern ; http://www.golem.de/news/crowd-management-smartphone-soll-massenpanik-verhindern-1209-94331.html

Da eine Observation von Einzelpersonen nicht länger einen derart hohen Personaleinsatz erforderlich macht und die Technologie heute bereits verfügbar ist, um eine begrenzte Zahl von Personen für unterschiedliche Bedarfe parallel in einer Umgebung zu verfolgen, können Oberservationstechniken von einer Einzelbeobachtung zu einem System der Zonen-Observation gegenüber definierten Personen umgebaut werden. Eine deutlich kleinere Zahl von Sicherheitskräften mit Datenbrillen und Sensoren könnte in einer Zone mehrere markierte Verdächtige zugleich observieren, dies über verschiedene Zonen hinweg durchführen und dabei aufgenommenes Videomaterial als Beweismittel nutzen.

Der polizeiliche Wert einer solchen Observation lässt sich bereits erkennen an der Observation einer Gruppe von Taschendieben. Dieser Wert ergibt sich aber in gleicher Weise auch für die Taschendiebe, wenn sie gemeinsam mit AR-Hilfe auf Beutejagd gehen.

5.2 Diebstahl und Einbruch

Auf dieselbe Weise lassen sich Werkzeuge zum Orten und Anzeigen von WLAN-Emittern, Smartphones oder anderen funkgestützten Systemen einbinden, wofür je nach Emitter-Typ Modifikationen der heute in Smartphones vorhandenen Ortungswerkzeuge gegen Diebstahl ausreichen, bisweilen aber komplexere Zusatzinstallationen[35] erforderlich sind.

Das Taggen von WLAN-Emittern erlaubt prinzipiell mit derselben Kombination von Sensoren beispielsweise auch Einbrechern das Auffinden und Markieren funkbasierter versteckter Sensoren und Einbruchserkennungstechnik. Anfällig sind hier insbesondere WLAN-Überwachungskameras, deren Standort sich peilen lässt. Mit einem kollaborativen AR-System können die ermittelten Daten für eine Internetrecherche oder den Rat von Experten irgendwo auf der Welt genutzt werden, um sich Wege zur Umgehung dieser Systeme vorschlagen zu lassen – wenn die Kameras nicht ohnehin offen im Internet zu finden sind[36]. Mit Datenbrillen und solcher Hilfe aus der Ferne können auch untrainierte Einbrecher aus der Ferne unterstützt auf sicherheitstechnisch gut geschützte Objekte angesetzt werden, was für kriminelle Organisationen ganz neue Optionen eröffnen dürfte.

[35] So verfügen Landes- und Bundespolizeibehörden neben IMSI-Catchern, die eine Funk-Basisstation vorgaukeln, über Beweissicherungs- und Dokumentationskraftwagen, die Handy-Besitzer metergenau lokalisieren können sollen, siehe Detlef Borchers: Bessere Handy-Ortung für die deutsche Polizei; heise online, 09.08.2014, http://www.heise.de/newsticker/meldung/Bessere-Handy-Ortung-fuer-die-deutsche-Polizei-2289542.html , siehe auch die Antwort der Bundesregierung auf die Kleine Anfrage der Abg. Hunko u.a. Neue digitale Überwachungsmethoden, Frage 17 ff

[36] Ronald Eikenberg: IP-Kameras von Aldi als Sicherheits-GAU, heise Security, 15.01.2016; https://www.heise.de/security/meldung/IP-Kameras-von-Aldi-als-Sicherheits-GAU-3069735.html

5.3 Organisiertes Verbrechen und Terrorismus

Nicht nur in Hollywood-Filmen werden die Abläufe bei Raubüberfällen auf hochwertige Ziele geplant und geübt. Auch für terroristische Anschläge ist charakteristisch, dass sie detailliert und über längere Zeit geplant und vorbereitet werden.

Unaufdringliche Datenbrillen bieten die Möglichkeit zur Erleichterung und Verbesserung der Koordination von Überfällen – insbesondere bei komplexeren Abläufen. Mit solchen AR-Werkzeugen lässt sich das Timing perfektionieren, lassen sich Ablenkungsmanöver effektiver einsetzen. Datenbrillen werden als Werkzeuge explizit dazu entwickelt und genutzt, Handlungen an realen Orten virtuell durchzuspielen oder die Realität in einem Übungsgelände nachzubilden. Mit der Übung an „Originalschauplätzen“ mit unauffälligen Datenbrillen kann ein risikoreicher Raubüberfall umsetzbar gemacht werden.

Terrorüberfälle größerer Gruppen von Angreifern gab es auf Hotels, Shopping Center, Flughäfen und andere Orte wie in Mumbai, Nairobi[37], Paris, Brüssel und natürlich auf viele Ziele im Irak und Afghanistan. Selbst beim Amoklauf eines Einzeltäters in München 2016 spielte dessen Chat-Kommunikation mit sich selbst eine Rolle bei dessen Selbstdarstellung und der Bewertung durch die Sicherheitsbehörden. Insbesondere die IS-Terrorgruppe experimentiert schon über längere Zeit mit ferngesteuerten oder durch IT-Einsatz automatisierten Fahrzeugen, Kanonen und anderen Angriffswerkzeugen[38]. All dies ist Anlass für die Vermutung, dass Gewalttäter und insbesondere Terrorgruppen hinreichende IT-Kenntnisse auch für den Einsatz von AR-Werkzeugen haben.

Wie schon in Militärmanövern der 1990er Jahre demonstriert, könnten koordiniert vorgehende größere Terrorgruppen mit Datenbrillen ebenso eine gemeinsame Lagekenntnis zulasten der angegriffenen Zivilbevölkerung ausspielen. Auch bei terroristischen Angriffen ließe sich die Abstimmung von Angriffsabläufen verbessern durch die gemeinsame Kenntnis über Standorte und das Vorgehen der Gruppenmitglieder anhand des visuellen und akustischen Austauschs in Echtzeit.

Eine Terrorgruppe könnte zu Beginn eines Angriffs die Sicherheitskontrollen an verschiedenen Stellen simultan und koordiniert angreifen, bevor Alarm ausgelöst wird. Als zweiten Schritt könnte eine solche Gruppe mehrere Ziele einnehmen und abriegeln, bevor Sicherheitskräfte mobilisiert werden können. Jeder kritische Zugangspunkt ließe sich unter kollaborativer

[37] Drama in Einkaufszentrum: Präsident meldet Sieg über Geiselnehmer in Nairobi; http://www.spiegel.de/politik/ausland/praesident-meldet-sieg-ueber-geiselnehmer-in-nairobi-a-924322.html , zu Pakistan und Indien: Hasnain Kazim: Angriff in Lahore: Taliban richten Blutbad in Moscheen an; Spiegel Online, 28.05.2010; http://www.spiegel.de/politik/ausland/angriff-in-lahore-taliban-richten-blutbad-in-moscheen-an-a-697393.html

[38] Thomas Gibbons-Neff: Why the Army is worried about insurgents turning to remote-controlled weapons; The Washington Post, 30.08.2016, https://www.washingtonpost.com/news/checkpoint/wp/2016/08/30/insurgent-groups-such-as-isis-are-increasingly-turning-to-remote-controlled-weaponry-army-report-says/; siehe auch: Robert J. Bunker, Alam Keshavarz: Terrorist and Insurgent Teleoperated Sniper Rifles and Machine Guns; Foreign Military Studies Office, Kansas, August 2016; http://fmso.leavenworth.army.mil/documents/20160822_BUNKER%20and%20KESHAVARZ_Teleoperated%20Sniper%20Rifles%20article.pdf

Kontrolle halten – möglicherweise sogar unter Einbeziehung vorhandener Sensoren oder Kameras. Im dritten Schritt könnte eine solche Gruppe Geiseln im Gebäude oder Gelände ohne Kontrollverlust so verteilen, dass eine Geiselbefreiung durch Sicherheitskräfte wesentlich risikoreicher würde. Im Fall einer Befreiungsaktion würde die AR-Vernetzung einer Terrorgruppe den Überraschungseffekt verringern, weil selbst getötete Terroristen den Mitgliedern ihres Datennetzwerks weiterhin die Videoaufnahmen des ablaufenden Angriffsgeschehens übermitteln können. Zu allem Überfluss ließen sich die Videobilder der Datenbrillen vom Tatort auch noch zu Propagandazwecken verwenden.

6 Bewertung

Man mag sich einen solchen Terrorüberfall mit Unterstützung durch Datenbrillen nicht einmal ansatzweise vorstellen. Schutz und Sicherheit setzen aber voraus, neue Szenarien durchzuspielen. Deswegen ist es durchaus erstaunlich, dass die einfache Übertragung der Erfahrungen aus militärischen Manövern in die Gegenwart von leicht verfügbarer, kollaborativer Datenbrillen-Technologie bisher nicht unter dem Blickwinkel der zivilen Sicherheit gesehen wurde. Mittlerweile ist die Beschaffung und Adaption der nötigen AR-Technik deutlich einfacher zu bewerkstelligen als die Beschaffung von Waffen, Sprengstoff und anderer Militärausrüstung. Es ist daher leider davon auszugehen, dass wir in den nächsten Jahren Szenarien erleben werden, in denen bewaffnete Täter zusätzlich mit Datenbrillen ausgestattet sind, durch die sich eine neue Art von „Datenbrillen-Überfällen“ oder gar „Datenbrillen-Terrorismus“ entwickeln kann. Wir sollten diese Möglichkeiten nicht ignorieren, sondern heute darüber nachdenken.

Die kollaborativen Einsatzpotentiale von Datenbrillen bergen große Risiken, für illegale Zwecke genutzt zu werden. Die Experimente verschiedener Strafverfolgungsbehörden haben bereits gezeigt, dass diese ihrerseits neue Einsatzszenarien sehen und die Möglichkeiten dieser Technik in der Praxis erproben wollen. Dabei ist in Erinnerung zu rufen, dass HMDs als nicht-zivile Versionen von Datenbrillen heute schon von Spezialeinheiten operativ genutzt werden. Lediglich der Einsatz ziviler, unauffälliger Modelle zu Überwachungszwecken wäre eine wirkliche Neuerung. Einige der möglichen Konsequenzen sind unschwer abzusehen. Andere erfordern grundsätzlichere Überlegungen.

Sollte es dazu kommen, dass Datenbrillen mit ihrer Übermittlung von Videodaten in Echtzeit an zentrale Server zu einer breiteren Nutzung kommen, ist absehbar, dass die Sicherheitsbehörden versuchen werden, auf diese Daten Zugriff mit dem Argument zu erlangen, dass Nutzer der Datenbrillen unwissentlich Aufnahmen eines für die Behörden wichtigen Geschehens machen könnten. Die Durchsuchung des zentral gesammelten Videomaterials von Datenbrillen im Hinblick auf Daten zu einem Tatort bzw. Tathergang entweder ex post durch Beschlagnahme oder bei Verdacht in Echtzeit von allen dort vorhandenen Nutzern dürfte sich zu einer vergleichbar eingesetzten Methode entwickeln wie heute die Auswertung von Überwachungskameras bzw. Handyvideos.

Verschiedene der zuvor beschriebenen illegalen Nutzungspotentiale dürften mit einer Manipulation insbesondere auch der gemeinsam genutzten Kommunikationsverbindungen einhergehen, um die bei einigen Modellen vorgesehene zentrale Datensammlung durch eigene Kommunikationskanäle zu umgehen. Für die Sicherheitsbehörden wird daraus die Forderung erwachsen, die lokale Kommunikation von Tätergruppen – etwa per WLAN – am Ort eines Geschehens analysieren, überwachen oder stören zu können. Nach IMSI-Catchern und anderem Gerät wird daher der Wunsch nach weiterer Überwachungstechnik laut werden.

Grundsätzlich anders fällt die Betrachtung aus, wenn es um die Frage geht, ob und wie Datenbrillen gegen eine Nutzung für illegale Aktivitäten gesichert werden können, die mit großen Gefahren für die Allgemeinheit, aber auch für die Sicherheitsbehörden verbunden sind. Hier fällt eine Antwort ziemlich ernüchternd aus. Schon heute ist zu viel Software im Umlauf, die für Einzelnutzer und Nutzergruppen die Grundlagen für eine Weiterentwicklung zur Realisierung der vorab beschriebenen kollaborativen AR-Anwendungen schafft. Diese Entwicklung ist nicht mehr einzudämmen.

Was das Verhindern der Anbindung externer Sensorik an Datenbrillen und das AR-typische Taggen von Elementen im Sichtfeld des Nutzers angeht, so ist auch dies „nur“ eine Frage der softwareseitigen Datenintegration. Da es regelmäßig um nur wenige Daten geht, ist der dafür nötige Aufwand überschaubar.

Datenbrillen, die mit einem gängigen Betriebssystem für den Massenmarkt angeboten werden, sind nicht wirksam gegen Manipulation und Missbrauch zu sichern. Die Hersteller müssten schon an verschiedenen Punkten ihrer Systeme Mechanismen vorsehen, die bei Manipulationen die Datenbrille zur Selbstzerstörung bringen oder eine Deaktivierung von außen erlauben. Doch auch hierbei ließe sich letztlich nur an der konkreten Implementierung ermessen, ob solche Maßnahmen ausreichen.

7 Fazit

Festhalten lässt sich, dass gegen die meisten und vor allem die extremsten der beschriebenen illegalen Nutzungsszenarien von Datenbrillen nur sehr wenige technische Mittel infrage kommen, deren Wirkung erfolgversprechend ist. Ideen zur unbegrenzten Datenerhebung wiederum würden massive Grundrechtseingriffe für die Allgemeinheit ohne erkennbaren Nutzen bedeuten.

Zur Prävention vor erwartbarem Missbrauch notwendig wäre vielmehr ein „code of conduct“ von Selbstbeschränkungsregeln der Anbieter und Softwareentwickler. Hardwareseitig sollte ernsthaft über Manipulationshemmnisse nachgedacht und sollten entsprechende Erschwernisse eingebaut werden. Softwareseitig sollten kollaborative Spiele und andere Anwendungen gar nicht erst auf den Markt gebracht werden, die sich ohne größere Veränderungen für illegale Einsatzszenarien nutzen lassen und so selbst Tätern ohne vorheriges Training die erheblichen Gefährdungsmöglichkeiten einer kollaborativen Datenbrillennutzung eröffnen. Mehr als fraglich ist, ob für eine solche Bewertung die bisherigen Prüfverfahren der Altersfreigabe für Computerspiele ausreichend sind.

Datenbrillen weisen ein erhebliches Potential zur Überwachung des Alltags Unbeteiligter auf. Dieses Potential ist für die Sicherheitsbehörden von großem Interesse. Militärische HMDs werden bereits operativ genutzt und dürften zukünftig auch bei Sondereinheiten der Polizei Verwendung finden. Unauffällige zivile Datenbrillen eröffnen den Sicherheitsbehörden ganz erhebliche neue Perspektiven für die Observation und Überwachung. Dies sind nur bedingt positive Aussichten, die aber prinzipiell regelbar und in bestimmten Konstellationen auch nutzbringend sind.

Nicht regelbar ist der Einsatz von Datenbrillen für kriminelle und terroristische Zwecke. Es ist daher umso erstaunlicher, dass diesen Fragen bisher so gut wie nirgendwo nachgegangen wurde und sie für Entwickler und Anbieter keine Rolle zu spielen scheinen.

Bevor wir die ersten „Datenbrillen-Terroristen“ erleben müssen, wäre es dringend geboten, in der Informatik daran zu arbeiten, wie diese Technik eingegrenzt werden kann, oder die missbräuchlich nutzbare Arbeit an solchen Geräten aus ethischer Verantwortung heraus einzustellen. Sicherheitsbehörden und Gesetzgeber sind aufgefordert, sich unter operativen und regulatorischen Gesichtspunkten mit den Missbrauchspotentialen von Datenbrillen auseinanderzusetzen. Die Hersteller schließlich sollten mit der bisher unhinterfragten Inkaufnahme erheblicher Risiken konfrontiert werden.

Jetzt ist der Zeitpunkt für eine breite Debatte über die Implikationen eines kollaborativen Einsatzes von Datenbrillen und deren Missbrauch für unsere Gesellschaft, unsere Sicherheit und über mögliche Lösungsansätze – bevor uns die Wirklichkeit äußerst schmerzhafte Lektionen lehrt.