Ute Bernhardt:

Google Glass: On the implications of an advanced military command and control system for civil society.

Abstract:

In the early 1990ies, the U.S. Army presented the first experimental units of a future soldier's equipment, featuring a soldier with a networked video camera, various sensors, and connecting the system to the world wide military command and control network. In June, 2012, Google unveiled its prototype Google Glass, a device capable of video and audio capturing with additional augmented reality functions.

In this article, a comparison between those military and civilian augmented reality systems and typical application settings will be used to ask for the implications of this kind of technology for the civil society. It will especially be focused on the consequences for civil safety, when the full range of cooperation capabilities available with Google Glass-like devices will be employed by organized groups of criminals or terrorists. In conclusion, it will be argued to assess the implications of this technology and prepare for a new degree of coordination in the activities of groups in the civilian space.

Agenda:

Author:

Ute Bernhardt

- c/o FIfF e.V., Goetheplatz 4, 28203 Bremen
- eMail: ute@kriton.bn.shuttle.de, http://fiff.de/themen/ruin/ruestung-und-informatik/materialien-und-dokumente/
- Relevant Publications:
  - Ute Bernhardt: Video: die unkontrollierte Überwachungstechnologie; in: Datenschutz-Nachrichten, 11. Jhg., Heft 1, 1988, S. 4-10
  - Ute Bernhardt; Ingo Ruhmann (Hrsg.): Ein sauberer Tod. Informatik und Krieg. Marburg, 1991
  - Ute Bernhardt: Maschinen-Soldaten. Der Mensch auf dem modernen Schlachtfeld; in: dieselben: Ein sauberer Tod. Informatik und Krieg, Marburg, 1991, S. 154-162

- Ute Bernhardt, Helga Genrich, Ingo Ruhmann: Der Prozeß Verantwortung; in: Hans-Jörg Kreowski (Hrsg.): Informatik zwischen Wissenschaft und Gesellschaft. In Erinnerung an Reinhold Franck, Informatik-Fachberichte, Band 309, Berlin, 1992, S. 242-254
- Ingo Ruhmann; Ute Bernhardt; Dagmar Boedicker; Franz Werner Hülsmann; Thilo Weichert: An Appraisal of Technological Instruments for Political Control and to Improve Participation in the Information Society. Study for the Scientific and Technological Options Assessment Programme of the European Parliament. Directorate General for Research, Luxembourg, January 1996, PE: 165.715.
- Ute Bernhardt; Ingo Ruhmann: Von der Verantwortung der Informatiker; in: Werden 97/98. Jahrbuch für die deutschen Gewerkschaften. Frankfurt, 1997, S. 185-193
- Ute Bernhardt: Das Imperium schlägt zurück. in: Gerfried Stocker; Christine Schöpf (Hrsg.): Information.Macht.Krieg. Tagungsband der Ars Electronica 1998. Wien, 1998, S. 154-162
- Ute Bernhardt, Ingo Ruhmann: On Facts and Fiction of „Information Warfare“. in: Bernhelm Booß-Bavnbek; Jens Høyrup (Eds.): Mathematics and War; Basel, 2003, S. 257-281
- Jürgen Altmann, Ute Bernhardt; Kathryn Nixdorf, Ingo Ruhmann, Dieter Wöhrle: Naturwissenschaft – Rüstung - Frieden. Basiswissen für die Friedensforschung. Lehrbuch. Wiesbaden, 2007
- Ingo Ruhmann, Ute Bernhardt: Information Warfare und Informationsgesellschaft. Zivile und sicherheitspolitische Kosten des Informationskriegs. In: Wissenschaft und Frieden, Heft 1/2014, Dossier Nr. 74 http://wissenschaft-und-frieden.de/seite.php?dossierID=078

A Google Glass system, looking quite like a small pair of stylish glasses, is an Augmented Reality (AR) system with a head-mounted display (HMD). Data related to the situational context are automatically displayed into the wearer's field of view. Pictures, audio or video feeds taken by the built-in microphone and camera are transmitted to other users or onto a cloud server where they can be stored or used to recognize people potentially by face recognition – which is until now not offered by Google, but available as a third-party app[1] - or by other personal attributes. Google Glass aims for ease of use through hands-off-controls with voice commands. It thus is a powerful AR gadget with autonomous computing power and connectivity[2]. The system has the perspective to add other sensors the user might find useful. Google Glass is only the most prominent of various systems with common properties on the market[3], and even more are under development[4]. The conclusions in this article are not restricted to a certain product, but are valid for any HMD AR device with comparable properties.

The intense publicity and the data made available on Google Glass have caused a debate on the system's potential as a tool for surveillance and the imbalance of knowledge between ordinary persons as bystanders on the one side and Google Glass users on the other side. The system's capability of instant video analysis with the power of recognition and identification – based on the rather imperceptible use of mobile connectivity with the computing power of Google's servers - is advertised as giving the Google Glass wearer utmost information about his or her surroundings including data on individuals in the field of view. Regardless whether the system works or will be marketed as advertised, Google Glass promises its users to end anonymous encounters with others in the real world. Google Glass is all the better in urban areas with good connectivity and enough tech-savvy people to look inconspicuous.

The debate on ethical issues to date has mostly concentrated on privacy issues, loss of control, reputation and autonomy[5] of those watched by a Google Glass user, what it means to be subjected to individualized video surveillance in interactions with these users and the possible follow-on analysis of the footage on Google's servers[6].

But these discussions center around Google Glass-like HMD systems only connected to web resources and used by individuals. Although Google promotes Glass with collaboration and data sharing features[7] it has not at all

[1] The MedRec app offered in 2013 can look up patient records by taking a picture of their face; http://glass-apps.org/medref-google-glass-app. At the CCC Congress in December 2013, Lambda Labs announced a face recognition app not supported by Google: Google Glass Face Recognition App Coming This Month, Whether Google Likes It Or Not; Forbes Online, 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/

[2] See the descriptions and reports at: http://www.google.com/glass/start/

[3] Most mentionable of the others are the readily available products Recon Jet HMD (http://reconinstruments.com/products/jet/) , Epiphany Eyewear (http://www.epiphanyeyewear.com/), GlassUp from Italy (http://www.glassup.net/) and the Vuzix Smart Glasses accessory to smartphones (http://www.vuzix.com/consumer/products_m100.html). Even the Nissan car company presented an AR device called "3E" in November 2013: The 3E View of the Tokyo Motor Show, Nov. 19, 2013, http://blog.nissan-global.com/EN/?p=11271

[4] 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/. Microsoft is reported to test an AR prototype, developed since some time: Microsoft Tests Eyewear Similar to Rival Google Glass, Wall Street Journal Online, 22nd Oct. 2013, http://online.wsj.com/news/articles/SB10001424052702304402104579150952302814782. Samsung has filed patents for its developments: 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

[5] See for example European Network and Information Security Agency (ENISA): To log or not to log? - Risks and benefits of emerging life-logging applications, 2011; http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/life-logging-risk-assessment; Katina Michael and M.G. Michael: Computing Ethics: No Limits to Watching? Communications of the ACM, Nov. 2013, p. 26-28

[6] See 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/

[7] See "Even share what you see. Live"; http://www.google.com/glass/start/what-it-does/ and the Throughglass App: http://glass-apps.org/throughglass-google-glass-app

been reflected, to what effect Google Glass might be used by groups of users. What happens in the transformation of Glass functions into a scenario of group support?

This is on the sender side the ability to capture the scene at hand and transmit it to others, and on the receiver end the ability to access data on the same scene and relevant data elements in it, and for all collaborators, to act in a coordinated manner. In an individual mode, both of these functions may seem nice, but lack a convincing functional model. Such a coherent model emerges, when a Google Glass user is seen as a node in a collaborative network producing input for him- or herself as well as others and receiving support out of the data and the activities of others. The automated reality augmentation in applications available today on smart phones – irrespective of their different kind of display style – is often little more than data on the vicinity of a certain location found on Google Maps. It is by far more convincing when a kind of external supervision or other ways to exchange AR items between users comes into play that vastly enhances the potential of Google Glass for its users and has additional consequences for a bystander or the addressee of a Google Glass-empowered group[8].

A glimpse of what is to come in Google Glass groupware can until now only be seen as mockups: Google Glass Games for individuals and groups[9], amongst them a Google Glass ego-shooter[10]. This mock-up ego-shooter and other ideas by Microsoft represent a return to the origins of the development of HMD-based AR systems.

Origins of head-mounted augmented reality systems

In 1993 the U.S. Army conducted several maneuvers to experiment and assess newly developed experimental equipment for ground soldiers in combat. In the so-called Soldier Integrated Protective Ensemble (SIPE) Advanced Technology Demonstration, a group of soldiers only one-third the size of ordinary units ambushed a much larger force, occupied and secured various positions in an open field as well as in a city setting.

The group used sensory augmentation from digitally enhanced video cameras, laser and infrared sensors as well as augmented long-range hearing. Through the exchange of data and through navigation and range-finding equipment the soldiers were able to locate and triangulate their adversaries' positions by passive means without notice and mark them on a common battlefield map displayed in their HMD's AR display together with other data sources. In difficult terrain and in close urban combat, they could use a video camera to look around obstacles, avoiding danger and being noticed. The soldiers exchanged video and audio footage taken of the battlefield independent of weather conditions to achieve a common picture on their adversaries' actions before starting their attack. All data from the battlefield were continually transmitted to a command post, where further intelligence was collected and transmitted back to the soldiers.

Full connectivity between soldiers and between them and a command and control network provide the means to exchange all relevant data as needed. AR in a HMD worked as a hands-off technology and augmentation of perception with complex data on the battle area and the friendly and enemy action developing on it. All combined proved to be a vastly more effective way of combat, so that such systems are rated as "force multipliers". A significantly smaller number of soldiers - by better coordination and access to external sensor data – could achieve a higher lethality at greater distances with fewer losses in a highly intensified battle:

> *The soldiers were able to "accurately direct a lethal volume of fire onto objectives beyond current night vision device ranges and provide the ability to use more smoke and still place effective fire on the objective.*

[8] This of course is also valid for other products of this kind: Microsoft is reported to patent AR glasses for multiplayer games, see: Microsoft tries to patent AR glasses for multiplayer gaming, engadget, 2.08.2013, http://www.engadget.com/2013/08/02/microsoft-ar-glasses-for-multiplayer-gaming-patent/

[9] 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

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

> *With improved communications, response time for fire control is reduced. […] It will also aid in the detection of the enemy's presence before the soldiers themselves are detected." [11]*

These results with experimental technology - that can be traced back to demonstrators from the mid 1980s[12] - have since been translated into the requirements for the ground force of the 21st century. The so-called Force XXI concept was developed in the U.S. to allow for a military engagement of small groups and making full use of information technology to intensify and improve fighting capabilities:[13]

> *"The concept for Force XXI Operations is centered around quality soldiers and leaders whose full potential is more closely realized through information age technologies and by rigorous and relevant training. […] It describes an operational environment where the acquisition, processing, and rapid sharing of information revolutionizes the conduct and tempo of operations." [14]*

The integration of the individual ground soldier into the command and control network and its equipment with real-time data gathering and sharing technology, as well as augmented reality-capable displays is progressing at full speed: Currently, the U.S. Army integrates the "Force XXI Battle Command Brigade and Below" as the digital command and control system for "automatically disseminating throughout the network timely friendly force locations, reported enemy locations, and graphics to visualize the commander's intent and scheme of maneuver" [15]. The next stage will be deployed as a mobile battlefield network for sharing of data and "information via voice, data, and real-time video"[16]. The pictures of U.S. President Obama following live the raid on Osama bin Laden's hideout in Pakistan in a command room showed the world the use of fully connected ground forces in combat.

Although most of these HMD-based military AR applications still do not seem to be perfect in their performance, robustness and accuracy needed in combat, the tactical advantages of the systems developed are obvious enough to see quite a number of different HMD models for AR applications in substantial quantities in various armies' combat missions[17]. Amongst other armies, the German Bundeswehr has proceeded from the concept stage in the program „Infanterist der Zukunft"[18] to battlefield use of the "Gladius" system with production line

[11] Victor Middleton, Ken Sutton, Bob Mclntyre 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

[12] See the description of the presentation by the British Company Scicon Computer Systems at the British Army Equipment Exhibition in 1984. This prototype of a soldiers's equipment was supposed to have full AR functionality with additional infrared vision in the integrated HMD display, see: Military Technology, No. 10, 1986, p. 166. Steven M Shaker, Robert Finkelstein: The Bionic Soldier; in: National Defense, April 1987, p. 27 – 32. Head-mounted displays for AR applications were first published as a scientific paper by T.P. Caudell, D.W. Mizell: 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

[13] 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. 2-1fff

[14] 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, preface

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

[16] In the "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

[17] 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/

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

head-mounted displays (HMDs) for AR applications delivered to German troops in Afghanistan in 2013[19]. The revenues for AR systems on the battlefield are estimated to reach $8.2 billion by 2016[20]. Advanced systems are under development that no longer need any glasses at all, but project data onto contact lenses[21].

Internet of Warriors

Equipping soldiers with AR-capable HMDs and networking them does not only aim to maximize the single warrior's effect, but tries to extend the reach of command to the last independent actor on the battlefield. Officers get immediate control over actions by any individual soldier who automatically communicates his or her position, very often also live video feeds of their action and telemetric data. The Force XXI doctrine stated from the start that it would result in hierarchical organization forms existing in parallel to new network-centered forms in combat missions. These two seemingly conflicting structures come to a combined result, when AR technology on the battlefield is used by "quality soldiers": special forces. For the soldiers, it results in an improved "situational awareness", for their commanders in the data exchange loop, in a better "top sight" of the unfolding battle situation and taken together lead to markedly improved efficiency in small forces combat.

This result of improved command, control and communication capabilities through information sharing is nothing new in military development: The main battle tank appeared on the front lines in World War I, when it was used to breach fortifications and to shield infantrymen from enemy fire in an assault. In most armies, this was still the dominant tactic at the beginning of World War II. In contrast, the German army had equipped their tanks with VHF radio communications, and through command and communications formed a unified force of heretofore unknown speed and fighting power that changed the way ground wars are fought until the present day.

An analogous process is taking place on the battlefield. Soldiers are being equipped with sensors, cameras, computing power and communications equipment. The soldier becomes a node in the network of military command and control to interconnect the world of information warfare with actual fighting on the ground. The result will be the "Internet of Warriors": Just as the Internet of Things, where data are stored in production items and used to control the production line, soldiers in the "Internet of Warriors" are supposed to act autonomously and collaboratively against their adversaries and feeding data back to their commanders.

Information Dominance

"Top sight" and "situational awareness" for ground forces are synonyms of a warfighting doctrine of modern armies that centers around a better knowledge of the situation on the battlefield. The improved knowledge of a tactical situation is used to assess the plans of an adversary, and to act preemptively with the aim not only to outmaneuver opposite forces, but to influence their assessment of the situation, thus ultimately modifying an enemy's perception of battle. This can obviously be achieved through conventional camouflage. In the age of distance sensors, however, this camouflage and work on situational perception has moved to the digital realm and means the disruption and alteration of any sensor data, of data communication and of data processing in any kind of IT equipment – regardless if in military or civilian systems. The term used for this IT-

[19] 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

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

[21] 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

related disruption of perception, in the terminology of the most advanced army in this discipline, is "Information Dominance".

After years of conceptual development and actual application in warfighting, the U.S. Army has refined its operational repertoire from a rather broad approach of Information Warfare to a quite detailed definition of so-called „Inform and Influence Activities"[22]. In short, Inform and Influence Activities start with public relations, cover electromagnetic and cyber activities, encompass all data sharing in the Theater of War and end with physical attack on the battlefield. This broad view is by no means new, but has been used since the end of the 1990s[23] and especially encompasses the capabilities of soldiers equipped to Force XXI standards.

Contrary to common perception, the term "Cyber Warfare" is not in the official vocabulary of the U.S. Forces. "Cyber Warfare" can only be found as a tool in Electronic Warfare[24]. In the literature, cyber warfare is used as a synonym for a disruptive use of manipulation tools in computer networks and described as a tool in low-intensity, often asymmetrical conflicts[25]. The equivalent official DoD term is "Information Operations" encompassing all "information and information systems and to influence decision making"[26].

It is obvious that the development of ground combat to a stage that rests on fully IT-equipped soldiers and the interconnection to a command and control network, necessarily implies undisrupted IT and communications systems: "Information Assurance is the cornerstone of the strategy for ensuring information dominance in a net-centric warfare environment" [27].

It has become impossible to decouple physical and digital operations. Applying cyber and electronic warfare operations in counterinsurgency means - amongst other tasks - to prevent the detonation of explosive devices and facilitate the disruption of many other command and weapons systems of insurgents. In an age when improvised explosive devices are remotely controlled by mobile phones, applying a smart phone computer trojan in a battlefield setting obviously has a physical and possibly lethal effect. The interdependency of digital and physical world has also been demonstrated by the Stuxnet computer trojan: It was physically mounted at the uranium enrichment site by USB stick and physically damaged machinery at this and other locations.

The Internet of Warriors blurs the distinction between digital and physical battle. Cyber Warfare Operations thus must strictly be seen as the small section of Information Operations that have a very broad range and employ very different means.

Enter Google Glass

Comparing the technical features, Google Glass and comparable products – that are used synonymously here - are a somewhat reduced version of typical HMD systems found in military use today. The Android operating system version for Google Glass makes app development easy. Irrespective of further modifications in the software of the system, it can safely be assumed, that a civilian HMD device equipped like Google Glass will be available in the near future that either is useful for special demands or can and will be modified to any dedicated

[22] U.S. Department of Defense: Field Manual 3-13, Inform and Influence Activities, Jan. 2013, p. 1-1

[23] See: Ute Bernhardt, Ingo Ruhmann: Informatik; in: Jürgen Altmann et al.: Naturwissenschaft – Rüstung – Frieden; Wiesbaden, 2007, p. 392ff

[24] U.S. Department of Defense: Field Manual 3-36, Electronic Warfare, Nov. 2012, p. E-1

[25] See for example: 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

[26] U.S. Department of Defense: Field Manual 1-02, Operational Terms and Graphics, 2004, p. 1-99

[27] Association of the United States Army: Information Assurance - Defending and Securing Army Networks and Systems. August 2006. p. 11, http://www.ausa.org/publications/torchbearercampaign/tnsr/Documents/TBSecRepAug06.pdf

users' special demands – be it only for gaming purposes, incentives for efficient modifications are clear enough to see.

Because Google Glass captures and displays data strictly in relation to the location or the people in the vicinity of its user, a group collaboration with Google Glass can be safely assumed to mostly use the same categories of data relating to the current location or the social interaction of Google Glass users. A foreseeable and simple civilian application, that only slightly extends today's smart phone apps, will be the interactive Google Glass wayfinding, where a Google Glass user is steered by another person – looking at the video image taken by the Glass device - through a location by augmenting direction cues into the HMD and highlighting points of interest.

Now let us replace "points of interest" with "persons" being highlighted and tagged in the HMD by some remote party. This not only makes identification easier but – through four or more eyes looking at the same detail of reality captured on live video – clearly eases the pursuit of target subjects even in the most crowded locations. Couple this with the range finding and passive position triangulation of third parties by two or more Google Glass users seen already in the SIPE maneuvers in the 1990s. Today's technology is additionally able to automatically track the features of the target subject and share the data amongst all Google Glass participants once the tagging has been done. So, with only these minimal additional properties easily realized by software, one can have an exciting time together in an AR-enhanced reality adventure game - or do the duties of police or secret service officers, or groups of criminals or terrorists following their victim. That the Google Glass communication gear, made for imperceptible use, eases the coordination and reduces the danger of one's cover being blown, is an additional support for clandestine observation groups.

Now let us go one step further adding more sophisticated elements. Since HMDs have been shown to – in principle - integrate all sensors made available for data exchange on the scene, one can replace the video images with infrared and night vision equipment for operations in darkness or of hunting warm body signatures in hiding places in rugged or urban terrain. This, too, is an attractive gimmick for today's outdoor gaming scene. It is also very useful for policing and many illicit activities directed against third parties.

One can just as well add civilized versions of electronic warfare equipment for direction finding and identifying cell phones, or WLAN emitters – just a slight modification of the equipment on your smart phone - and other frequencies, and tagging the emitter locations together with their identifiers in the HMD's field of view. You thus can pinpoint mobile phone users in the field of view of your Google Glasses, helpful for hot pursuit in a criminal investigation.

Or one can just as well find and mark hidden sensors and intrusion alarm equipment relaying data by radio like a perimeter surveillance camera. More sophisticated tools might even identify such sensors by their relay patterns, instantly looked up on the web, and automatically or by remote advice suggest ways to circumvent them. Remotely controlling non-experts with the proper instrument and advice on burglar alarms can prove to be a vastly more intelligent way to have crimes committed than showing up on a crime scene oneself.

And if necessary, one can drive the practice of mobile phones modified into exploding devices one step further. One just has to convince someone to carry around some kind of sealed container, and transmit back Google Glass live video footage with the result, that the explosive device in the container can be triggered at the most effective moment.

All of these Google Glass scenarios are just very slightly beyond the actual technology available, which mostly means less than one year of development time. But even here, technology is of no use without experienced users and a reason for the application of novel technological means. Let me therefore describe just three scenarios to shown the advantages and likelihood of the use of Google Glass-like systems.

1. Legal observation by police or intelligence often is a difficult and resource-consuming business. The use of radio trackers or silent SMS's on mobile phones for location determination shows the effort to use more sophisticated technology to be less dependent of purely optical means. Google Glass as a group collaboration tool can be used to alleviate observation. As a prerequisite, any group of Google Glass users can bring a variable and mobile set of sensors anywhere these are needed, and have them – by GPS – pinpointed on the map allowing for passive position triangulation. Through common sensor

fusion algorithms or by manual assistance in a coordination center, all sensorial input about the target person can be fused to accurately and reliably follow and keep track of a target independent of any weather condition.

Since observation no longer would have to rest on a limited number of persons shadowing a target person, observation techniques might be changed altogether from a system of man-marking into a system of zone defense: A number of Google Glass users might follow one or more target persons, marked by tags in their AR visions, and hand over targets when they leave the observation zone. The live video footage taken will produce evidence, if for example, an illicit transfer of goods shall be observed. The usefulness of this scenario starts with just an observation of pickpockets doing their work – or tech-savvy pickpockets looking for prey.

2. Meticulously planned heists are not confined to Hollywood films. Groups can plan, exercise and execute crimes, not just a bank robbery or an assault on an armored car. Of course, many terrorist attacks have also been exercised before execution. Any improvement to alleviate coordination by unobtrusive HMD devices while staging a succession of activities by a group of persons will undoubtedly be used to exercise and realize crimes that can consist of more steps and actors than today. Timing can be perfected, diversionary tactics tested. AR tools are being explicitly developed to open up the opportunity for even a complete dress rehearsal played through at the real location. Exercising with inconspicuous AR tools can give a well planned heist a new level of perfection.

3. Attacks by large terrorist groups on hotels and shopping malls have been staged in Mumbai, Nairobi[28] and of course many targets in Iraq and Afghanistan. With Google Glass-like HMDs such a group can operate on common knowledge about their exact positions, location data augmented into view, and visual and auditory information on the activities by all group members just like in military maneuvers. At the beginning of the attack, the group can move decisively and simultaneously at different points against security guards, before anyone can activate the alarm. As a second step, the group members can access specific targets in the location and cordon off an area as desired before any external help can arrive on the scene. Any critical access point can be kept under control cooperatively even from a distance; external sensors can be integrated into the network. As a third measure, the group can spread hostages to several different locations in the compound or building without losing control thus raising the stakes for evacuation raids by security forces. Finally and in case of a raid, fully networked group members nullify the moment of surprise, since even a dead terrorist may still transmit the video and audio stream of the surroundings, alerting every other one in the loop.

Google Glass-like HMDs in civilian contexts provide the equipment and force augmentation for attacks that until now strictly required highly trained professionals. One may not forget, that conventionally equipped professionals - if possible - train a raid on a model of the situation at hand to reach a high level of cooperation. What they need as an exercise to gain the upper hand, a cooperation based on a Google Glass-like system would provide terrorists without that much effort.

Being watched by a Google Glass user might be an uncomfortable feeling, since one does not know, what data the Google Glass user might have accessed on the web and have in his or her display.

In a cooperative Google Glass scenario, a Google Glass user watching you might be in the same observation loop as someone totally unrelated some moments ago. One might even have entered a scene where a group of pickpockets scan for victims and coordinate their robberies by Google Glass. In a holdup or in a robbery, one might not know as a victim, whether an attacker is alone or supported by a Google Glass user nearby scanning the crime scene to cover the attacker. In an armed attack, the person with the gun and the Google Glass equipment is not the only pair of eyes and ears that might thwart an attempt to escape, but will rather be

[28] As for example recently seen in a shopping center in Nairobi. Kenia (Drama in Einkaufszentrum: Präsident meldet Sieg über Geiselnehmer in Nairobi; see: http://www.spiegel.de/politik/ausland/praesident-meldet-sieg-ueber-geiselnehmer-in-nairobi-a-924322.html) Or see attacks in Pakistan and India: 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.htm***

connected to someone overlooking the scene and ordering to forcefully stop any escape or uncontrolled situation.

Enter security

Some future apps might prove to be highly useful in the scenarios described above. No one is expected to explicitly develop a "pickpocket support app" for Google Glass or something more elaborated for terrorist assaults. As a precaution against the legal problems already foreseen, a condition in Google's terms is that the company "may remotely disable or remove any such Glass service from user systems in its sole discretion" as Google "discovers a Glass service that violates Google developer terms or other legal agreements, laws, regulations or policies" [29].

How might violations be identified? Google Glass is the civilian version of a powerful command and control system. Google already reserved itself the right to store and use the user's location data, all the "photos and videos taken […] and [to] display information sent to devices that are synced with it"[30]. So Google is in the position to scan the data upon request or by itself to identify proper and improper use.

But there will also be demands by public authorities to exploit the data. Some technically inept petty criminals might get along with ordinary Google Glass features for their purposes. Even some terrorists sent on a suicide mission might be content with ordinary Google Glass features. Publicity for any such case will most certainly lead to the demand that Google Glass pictures and video feeds must be monitored in a manner comparable to today's CCTV systems. It will also be argued, that even innocent Google Glass users may visit areas of higher criminal activity ort security needs where they might accidentally and inadvertently take footage of illegal activities thus making it necessary to use Google Glass and other product's live feeds for general surveillance purposes.

The potential of Google Glass-like products for security purposes is enormous. The technology will give its users a huge boon for illegal activities as well as clandestine countermeasures by security forces.

As a way to prevent interference with illicit Google Glass uses and to circumvent surveillance, some of the scenarios described above will presume the skill and motivation of users to modify Google Glass and similar products to their specific needs. Since all Google Glass-like products have only restricted resources available, the options to tamper-proof them are limited. The Android operating system, Google Glass works on, is attacked by specific viruses, topping the mark of 100.000[31]. Google Glass was hacked only days after the first prototypes were given to developers giving full access to the system's capabilities[32]. One of the first Google Glass face recognition apps requires the hacking of the system to install it[33]. But the problem is not specific with the product: No embedded system with as limited resources as Google Glass-like products has yet withstood any dedicated digital engineering and attack. In consequence, one cannot assume any technological barrier against misuse in any of Google Glass-like systems to withhold modifications of the product beyond tight hardware

[29] Google Glass Terms of Sale and use (as of December 2013); http://www.google.com/glass/terms/

[30] Google Glass Terms of Sale and use (as of December 2013); http://www.google.com/glass/terms/

[31] Kaspersky Security List: IT Threat Evolution: Q2 2013; https://www.securelist.com/en/analysis/204792299/IT_Threat_Evolution_Q2_2013#16

[32] 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/

[33] 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/

restrictions – for example the abdication of a camera or processors that self-destruct on tampering – that are costly or debilitating for the product.

Any of these developments are clearly disadvantageous for a bystander to a Google Glass user. For any innocent bystander, there will only be a slight difference in the level of discomfort between a legitimate Google Glass user confronting him or her, taking a live video feed that actually is or can be used later on for surveillance purposes extending today's stationary CCTV systems into a ubiquitous surveillance with anyone as a potential suspect as one option or an illicit user that has modified the HMD system to remain undisturbed while committing unlawful deeds as the other, making the bystander a potential victim.

Ethical Justification for Google Glass?

It is clear that applications will be developed for Google Glass-like products to be used in gaming or collaborative work whose features will allow the product's users to apply these features acting as a group against others. These features will be highly useful as a force multiplier for a wide range of unlawful activities. As Google Glass comes to the market, it can be expected that within the next five years "Google Glass Terrorists" will test this potential in their attacks.

Google Glass-like devices may have some advantages for crime enforcement and rescue operations by special military or police forces. However, these forces already have rugged HMD systems in their equipment. Military HMDs today are instruments for the Internet of Warriors and central to Information Warfare on the battlefield. Special Forces do not need any civilian version. They are the ones who would have to fight attackers vastly more dangerous through Google Glass-like devices. From a security forces perspective, Google Glass-like devices pose a clear danger.

The ethical questions posed by Google Glass and its likes are fundamental. First of all, it must be asked, if it is ethically sound to program apps that can easily be used for criminal activities. What feature combination of these systems could at maximum be tolerable to prevent a potentially highly dangerous technology to fall into the wrong hands? Is it realistic to assume such a reduced product to be competitive? Should there be a special code of conduct in developing these apps or bringing them on the market?

Could the effects of Google Glass and similar systems be alleviated by limiting the capabilities of these systems? If the system's set-up is left unchanged, reducing connectivity and bandwidth could be used as limiting factors making recording and transmission inconvenient. Automatically preventing the recording of sensitive situations or unwilling bystanders by the system through on-board image and sound processing is severely limited by the necessary computing power that will not fit into the design. Controlling Google Glass's use on the network end of the system would mean to employ a forced personal supervision on the transmitted data, since today's systems for automatic scene analysis assess the activities of the person in the field of view that, in the Google Glass case, will be not the Google Glass user, but a harassed bystander. Scene analysis or personal supervision of anyone in the field of view of a Google Glass system – that is, to collect data on a random set of bystanders and analyzing their behavior - to eventually prevent such a systems user's potential misbehavior is an extremely invasive and by no means reliable way to limit Google Glass misuse. Even if this would be legal – which it is not even in a majority of U.S. States – it would not result in the detection of aberrant behavior of the Google Glass user as the culprit and person responsible. So, surveillance of Google Glass use will more often than not lead to no detection of misbehavior whatsoever and thus would only help in the mass surveillance of bystanders.

Google Glass is an ideal instrument from another point of view. Modern warfare rests on the collection of data from all possible sources. The NSA and similar agencies collect communications data to track individuals and to spy on their plans. Surveillance drones are used to provide live coverage of their operation area. Google Glass users provide live coverage and recordings anywhere and on any human interaction imaginable – together with exact location data. Special forces are equipped with HMDs for exactly this reason. Google Glass provides a trove of valuable data for any military or secret service organization they simply cannot resist to use. The broad communications surveillance by intelligence agencies that we can see today is a cornerstone of information warfare. The use of Google Glass and the data acquired will vastly extend this surveillance, opening up new dimensions for the application of information warfare tactics.

Google Glass is a technology that provides a high incentive for monitoring, which can have almost no effect for the user and originator but instead most certainly will have consequences for innocent third parties. Misuse may lead to a call for a better control of Google Glass users. But can there be an ethical justification for a mass surveillance of third parties as a way to potentially limit the misuse of Google Glass? Even if society would see the permanent surveillance by Google Glass users of any private interaction as a way to improved conformity and obedience to rules, this fundamental change in social interaction should be a result of debate - especially, because Google Glass as the instrument for obedience is not used by legitimate public officials against citizens, but between individuals. The second set of ethical questions therefore centers around the technology’s control potential that is quite useless against the genuine perpetrators, but will mostly harm third parties and has disruptive potential for the society as a whole.

Since the basic design of these systems offers only limited security protection against tampering, ethical assessments should not be based on the idea that misuse might be prevented by the technical protection of specific app features or explicit design to leave some features incomplete or incompatible. The history of smart embedded systems with restricted resources shows, that with some effort there will always be a way to combine useful features to achieve unintended system properties useful for criminal acts. It has not yet been answered, that there are convincing legitimate uses for this technology in the civilian sphere. We must therefore finally ask a fundamental question: Can IT professionals ethically approve the work on such systems at all?

Conclusions

None of the producers of Google Glass-like systems has yet made any comment on the potential problems arising of this very special kind of collaboration features. No one in the IT world has yet spoken out to address the potential dangers of these systems to the general public. Google Glass, however, is only a symbol and the starting point for novel collaboration technologies for ubiquitous use. Now is the time to start a broad discussion on the implications for society, safety and security – before reality will teach us painful lessons.

The civil security authorities must assess the risks inherent in this technology and develop tactics to reduce the impact of a “Google Glass Terror Attack”. Research is necessary to safeguard this kind of embedded and networked AR system against misuse. The companies involved must publicly be confronted with the responsibilities their product entails. And it is time to think, if work on these systems can ever be seen as an ethically responsible professional task.