- Startseite
- Aktuelles
- Untersuchungen
- Publikationen
- Über uns
- Team
- Kontakt
- Gutachter gesucht

Informationen zur Vergabe von Gutachten

Beobachtungstechnologien im Bereich der zivilen Sicherheit - Möglichkeiten und Herausforderungen

Die Einreichungsfrist für Angebote ist abgelaufen.

Thematischer Hintergrund

Die Fortschritte in der Informatik, Sensorik und Biometrie ermöglichen ein weites Einsatzspektrum für diverse Aufklärungs-, Aufzeichnungs- und Auswertungstechnologien (im Folgenden: Beobachtungstechnologien). Im Bereich der zivilen Sicherheit reichen die Anwendungsfelder von der Verkehrsbeobachtung und Unfallhilfe, der Sicherung von Großveranstaltungen über das Monitoring von Waldbränden, Hochwassergefahren und anderen Naturkatastrophen bis zur Kriminalitäts- und Terrorbekämpfung. Dementsprechend haben die Verbreitung und Nutzung von Beobachtungstechnologien durch staatliche Behörden und Einrichtungen in den letzten Jahren stark zugenommen. Aber auch Informationen aus sozialen Netzen und Sensordaten von zunehmend mobilen und vernetzten Telekommunikationsgeräten werden mit stark steigender Tendenz für die Gefahrenprävention und -aufklärung sowie zur Entscheidungsfindung in komplexen Einsatzlagen eingesetzt.

Der Einsatz von Beobachtungstechnologien im Bereich der zivilen Sicherheit wird in gesellschaftlichen wie auch in wissenschaftlichen Debatten kontrovers diskutiert. Einerseits wird Beobachtungstechnologien eine wichtige Funktion in der Gefahrenprävention und -aufklärung sowie bei der Krisenbewältigung zugeschrieben. Für den Staat können sie von Nutzen sein, um eine seiner Kernaufgaben, die Gewährleistung der zivilen Sicherheit, zu erfüllen. Andererseits werden immer wieder Fragen nach der Wirksamkeit, Verhältnismäßigkeit und Zuverlässigkeit solcher Maßnahmen aufgeworfen: Lassen sich durch staatliche Beobachtungsmaßnahmen tatsächlich Gefahrenlagen rechtzeitig vorhersehen, Straftaten wirksam vermeiden oder das Katastrophenmanagement verbessern? Wie viel der Privatsphäre soll für den (vermeintlichen) Gewinn an Sicherheit aufgegeben werden? Wer beobachtet wen und wozu? Was geschieht mit den gesammelten Daten? Im Lichte der immer leistungsfähigeren Beobachtungstechnologien stellen sich für den Staat völlig neue Herausforderungen

Kontakt

Dr. Claudio Caviezel »
caviezel@tab-beim-bundestag.de
Tel.: +49 30 28491-116

Dr. Christoph Revermann »
revermann@tab-beim-bundestag.de
Tel.: +49 30 28491-109

Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB)
Neue Schönhauser Straße 10
10178 Berlin
Tel.: +49 30 28491-0
Fax: +49 30 28491-119

Weitere Informationen

Informationen zur Untersuchung »Beobachtungstechnologien im Bereich der zivilen Sicherheit — Möglichkeiten und Herausforderungen« »

- Hinweise für Gutachter »
- Formblatt PDF [0,04 MB]

bei dem Bemühen, ein Gleichgewicht zwischen den Schutzbedürfnissen der Gesellschaft und den Persönlichkeits- und Freiheitsrechten des Einzelnen zu finden. Dies bedingt eine komplexe Interessenabwägung, bei der zahlreiche Faktoren eine Rolle spielen.

Vor diesem Hintergrund ist das TAB vom Ausschuss für Bildung, Forschung und Technikfolgenabschätzung mit einem TA-Projekt zum Thema »Beobachtungstechnologien im Bereich der zivilen Sicherheit – Möglichkeiten und Herausforderungen« beauftragt worden. Im Rahmen der Untersuchung sollen auf Grundlage heute vorhandener technischer Möglichkeiten, aber auch mit Blick auf erkennbare technische Weiterentwicklungen, die relevanten gesellschaftlichen Fragestellungen und Herausforderungen, die sich mit der zunehmenden Verfügbarkeit von Beobachtungstechnologien im Bereich der zivilen Sicherheit ergeben, identifiziert und analysiert werden. Zentrales Ziel der Untersuchung ist es, die sachlichen Grundlagen für die politische Meinungsbildung bezüglich der erforderlichen Rahmensetzung für deren Einsatz zu schaffen.

2. Projektphase

In einer ersten Sondierungsphase des Projekts wurde eine Bestandsaufnahme über den Stand und die Perspektiven der wissenschaftlich-technischen Entwicklungen und möglichen Anwendungsfelder und Einsatzszenarien von Beobachtungstechnologien im Bereich der zivilen Sicherheit erarbeitet. In der nun anschließenden zweiten Projektphase sollen zum einen die internetbasierten Beobachtungstechnologien einer vertieften Behandlung unterzogen und zum anderen mögliche soziale und psychologische Wirkungen technisierter Beobachtung tiefergehend diskutiert werden.

Leistungsbeschreibung zu vergebender Gutachten

Es sollen **Gutachten zu zwei Themenfeldern** vergeben werden. Die nachfolgenden Hinweise umreißen den inhaltlichen Rahmen für die Gutachten. Eigene Ergänzungen, Änderungen oder Konkretisierungen der Untersuchungsaspekte sind möglich (auch durchaus erwünscht) und sollten gegebenenfalls zwischen TAB und potenziellen Auftragnehmern im Rahmen der Angebotserstellung abgestimmt werden. Die grundsätzliche Bereitschaft zur engen Kooperation mit dem TAB wird vorausgesetzt.

Die zur Verfügung stehenden Mittel sowie der vorgesehene Zeitrahmen lassen keine langwierige Erschließung der Themen zu, sondern erfordern, dass die Anbieter bereits über eine ausgewiesene Expertise im Feld verfügen und möglichst auf eigene Vor- und laufende Arbeiten zurückgreifen können.

Themenfeld 1: Internetbasierte Beobachtungstechnologien und Akteurskonstellationen

Bearbeitungsaufwand: bis zu 5 Personenmonate

In der Folge der zunehmenden digitalen Durchdringung aller Lebensbereiche gewinnen datenbasierte Beobachtungstechnologien immer stärkere Bedeutung. Die zentrale Beobachtungsarchitektur bildet das Internet mit seinen unzähligen Anwendungen, Diensten und Funktionen. So bietet die stetig wachsende Menge an öffentlich (und oft sehr freizügig) preisgegebenen nutzergenerierten Informationen in sozialen Netzwerken (Facebook, google+, Twitter, XING etc.) ein weites Feld für

die Beobachtung einzelner Personen und deren Aktivitäten, Anschauungen sowie persönliche und berufliche Lebensgestaltung. Auch nichtöffentliche Nutzerdaten und Inhalte lassen sich mit unterschiedlich hohem Aufwand beobachten. Durch Aufzeichnung und Auswertung von IP-Adressen beispielsweise können die Internetaktivitäten einer Person beobachtet werden, woraus sich deren persönliche Interessen und Netzwerke ableiten und Persönlichkeitsprofile erstellen lassen. Durch die Installation verdeckt arbeitender Software (sog. Trojaner) auf internetfähigen Geräten (Smartphones, Laptops, SmartTV etc.) kann damit geführte Kommunikation mitgehört bzw. mitgelesen werden, auch können eingebaute Kameras, Mikrofone, Ortungssysteme etc. für Beobachtungszwecke verwendet bzw. missbraucht werden. Die Liste an Beispielen ließe sich beliebig erweitern.

Datenbasierte Beobachtungstechnologien im Allgemeinen und die Internetbeobachtung im Besonderen haben auch für den Bereich der zivilen Sicherheit zahlreiche (potenzielle) Anwendungsfelder. Im polizeilichen Bereich gehören manuelle Recherchen in sozialen Netzwerken bereits heute zum Instrumentarium polizeilicher Arbeit, um beispielsweise Lagebeurteilungen im Vorfeld von Demonstrationen oder Risikospielen im Fußball zu unterstützen. Über das Für und Wider der Vorratsdatenspeicherung zwecks Verhütung und Verfolgung schwerer Straftaten wird seit Jahren sehr kontrovers diskutiert. Und laut aktuellen Medienberichten plant das Bundeskriminalamt den Einsatz von Trojanern neben PCs nun auch auf Smartphones auszuweiten. Im nichtpolizeilichen Bereich umfassen mögliche Anwendungsfelder etwa die Infektionsepidemiologie, die eine Früherkennung und Nachverfolgung von Infektionsausbrüchen anhand von nutzergenerierten Daten im Internet ermöglichen soll. Die Feuerwehren könnten mithilfe von intelligenten, mit optischen und thermischen Sensoren ausgestatteten Rauchmeldern künftig schnellere und präzisere Lagebilder von Schadensereignissen erstellen, um Rettungseinsätze zu unterstützen.

Der Sinn und die Verhältnismäßigkeit eines Einsatzes von daten- bzw. internetbasierten Beobachtungstechnologien im Bereich der zivilen Sicherheit wird allerdings in gesellschaftlichen Debatten noch weit kontroverser diskutiert, als dies schon generell für Beobachtungstechnologien der Fall ist.

Vor diesem Hintergrund sollen im Rahmen des Gutachtens die vier nachfolgend dargestellten Aspekte vertieft bearbeitet bzw. erörtert werden:

1. Identifikation, Systematisierung und exemplarische Beschreibung von internetbasierten Beobachtungstechnologien und deren Anwendungen

Folgendes methodische Vorgehen wird vorgeschlagen:

- *Beschreibung der technischen Infrastrukturen*: Zwecks Systematisierung sollen zunächst die generellen technischen Infrastrukturen des Internets modellhaft beschrieben werden.
- *Identifizierung von internetbasierten Beobachtungstechnologien und Anwendungen*: Entlang der modellhaften Beschreibung der technischen Infrastrukturen sollen bestehende und künftige internetbasierte Beobachtungstechnologien und deren Anwendungen im Bereich der zivilen Sicherheit identifiziert sowie der jeweilige Stand der wissenschaftlich-technischen Entwicklung abgeschätzt werden.
- *Exemplarische Beschreibung*: Für eine Teilmenge der identifizierten Technologien und deren Anwendungen sollen die technisch-funktionalen Zusammenhänge detaillierter beschrieben werden. Die Auswahl erfolgt in Abstimmung mit dem TAB. Für die Auswahl sollen darüber hinaus folgende Fragen erörtert werden:

- Was ist der (potenzielle) Nutzen dieser Technologien bzw. Anwendungen für den Bereich der zivilen Sicherheit?
- Welche Kompetenzen, Mittel und Ressourcen sind für den (sinnvollen) Einsatz dieser Technologien vonnöten?
- Welche Akteure verfügen über die entsprechenden Kompetenzen, Mittel und Ressourcen?

2. Risiken und Folgen von internetbasierten Beobachtungstechnologien

Da digitale Informations- und Kommunikationstechnologien mittlerweile in sämtlichen Lebensbereichen beinahe omnipräsent sind, verweisen Kritiker von datenbasierten Beobachtungstechnologien vor allem auf die Gefahr einer allgegenwärtigen und kontinuierlichen Überwachung, die die Persönlichkeits- und Freiheitsrechte des Einzelnen massiv einschränken würde. Am Beispiel der internetbasierten Beobachtungstechnologien erhoffen wir uns Antworten auf mindestens folgende Fragen:

- Welche gesellschaftlichen und politischen Risiken und Herausforderungen sind mit dem Einsatz von internetbasierten Beobachtungstechnologien im Bereich der zivilen Sicherheit verknüpft? Durch welche technischen und organisatorischen Maßnahmen ließen sich mögliche negative Auswirkungen vermeiden oder abmildern?
- Welche Definitionsmacht wird den Beobachtungstechnologien zugestanden? Inwieweit werden Entscheidungen von (vermeintlich neutralen und vorurteilsfreien) intelligenten Algorithmen getroffen, welche Rolle spielt der menschliche Beobachter (noch)?
- Welche regulativen Problemstellungen ergeben sich?

3. Akteurswandel und Kompetenzaufbau

Während die Nutzung von Beobachtungstechnologien und Kontrolle damit erhobener Daten und Informationen lange Zeit vorrangig staatlichen Behörden und Einrichtungen vorbehalten war, treten seit einigen Jahren zunehmend auch private Akteure in diesem Feld in Erscheinung (z.B. im Kontext von privat betriebenen Fernerkundungssatelliten). Dieser Wandel in den Akteurskonstellationen wird am Beispiel der datenbasierten Beobachtungstechnologien besonders deutlich, da die relevanten Daten und Inhalte, die beobachtet werden (sollen), in aller Regel von privaten Unternehmen erhoben, verarbeitet, übertragen, gespeichert und kontrolliert werden. Staatliche Organisationen sind daher regelmäßig auf eine freiwillige oder gesetzlich reglementierte Kooperation der privaten Akteure angewiesen, wenn es darum geht, nichtöffentliche Daten und Inhalte einer Beobachtung zum Beispiel für Strafverfolgungszwecke zugänglich zu machen. Die Privatwirtschaft und im Besonderen die hier dominierenden Unternehmen wie Apple, Google, Microsoft etc. erhalten damit eine ungeahnte Machtfülle, während staatliche Behörden teilweise in die Position von Bittstellern gedrängt werden, wie etwa der jüngste Disput zwischen dem US-amerikanischen FBI und Apple um die Entsperrung eines von Terroristen benutzten Smartphones deutlich vor Augen führte. Auf diese Entwicklung kann die Politik entweder mit regulatorischen Maßnahmen reagieren (z.B. gesetzlich verankerte Kooperationspflichten) und/oder durch den Aufbau eigener staatlicher Ressourcen und Kompetenzen, zum Beispiel um Verschlüsselungstechniken zu umgehen.

Am Beispiel der internetbasierten Beobachtungstechnologien sollen vor diesem Hintergrund u.a. folgende Aspekte und Fragen erörtert werden:

- Welche Veränderungen in den Akteurskonstellationen zeichnen sich ab?

- Welche politischen und rechtlichen Herausforderungen ergeben sich daraus?
- Welche politischen Handlungsmöglichkeiten gibt es, um diesen Herausforderungen zu begegnen? Welche staatlichen Kompetenzen und Ressourcen müssen dazu aufgebaut bzw. genutzt werden, wie kann dies geschehen?

4. Entwicklungstrends und Handlungsmöglichkeiten

Aus den gewonnenen Erkenntnissen sollen die Entwicklungstrends und politische und rechtliche Handlungsmöglichkeiten bzw. -erfordernisse abgeleitet werden.

Themenfeld 2: Soziale und psychologische Wirkungen technisierter Beobachtung

Bearbeitungsaufwand: bis zu 3 Personenmonate

Der Einsatz von Beobachtungstechnologien im polizeilichen Bereich zielt in erster Linie auf (potenzielle) Straftäter, die entweder durch die (vermeintlich) abschreckende Wirkung der Beobachtungsmaßnahme von der Durchführung der geplanten Tat abgehalten oder anhand des aufgezeichneten Materials ermittelt und strafrechtlich belangt werden sollen.

Beobachtungsmaßnahmen betreffen aber nicht nur potenzielle Straftäter, sondern auch alle anderen im Wirkungsbereich der Beobachtungstechnologie anwesenden Personen. Die Größe des betroffenen Personenkreises variiert dabei stark je nach Technologie und Anwendung. Sensorbasierte Beobachtungstechnologien wirken in der Regel lokal und betreffen etwa bei der Videobeobachtung im öffentlichen Raum die Nutzer der jeweiligen Infrastrukturen sowie Passanten. Personen können sich der Beobachtung entziehen, indem sie die beobachteten Räume meiden – und gegebenenfalls deshalb beispielsweise auf die Teilnahme an einer Demonstration verzichten. Datenbasierte Beobachtungstechnologien dagegen wirken typischerweise räumlich uneingeschränkt, weshalb beispielsweise von der Vorratsdatenspeicherung sämtliche Nutzer der Informations- und Telekommunikationsinfrastrukturen tangiert sind. Hier gibt es – abgesehen von einem vollständigen Verzicht auf moderne Kommunikationsmittel – kaum einfache Möglichkeiten, sich der Beobachtung zu entziehen.

Es ist deshalb naheliegend danach zu fragen, welche sozialen und psychologischen Wirkungen die Beobachtungsmaßnahmen auf diese »unbeteiligten« Personen ausüben. Eine positive Wirkung wäre zum Beispiel, dass die Beobachtung zu einer Steigerung des subjektiven Sicherheitsgefühls beitragen kann. Unbeteiligte Personen könnten aber auch mit Verhaltenseinschränken oder -anpassungen auf die Beobachtungsmaßnahmen reagieren, die je nach Maßnahme und Vorstellungen über die beobachtenden Instanzen individuell sehr unterschiedlich ausfallen könnten und letztlich gegebenenfalls die Personen an der Ausübung ihrer Grundrechte behindern.

Das Gutachten soll sich der Frage widmen, ob, inwieweit und unter welchen Bedingungen Beobachtungsmaßnahmen bei unbeteiligten Personen Verhaltensänderungen und -einschränkungen induzieren (können). Dies soll einerseits für sensorbasierte (z.B. anhand des Beispiels Videobeobachtung im öffentlichen Raum), andererseits und vergleichend dazu für datenbasierte Beobachtungstechnologien (z.B. Speicherung von Internetnutzerdaten) betrachtet werden.

Von besonderem Interesse sind dabei folgende Fragestellungen:

- Stellen sich durch Beobachtung gegebenenfalls induzierte Verhaltensänderungen

in unterschiedlichen sozialen Räumen bzw. Milieus unterschiedlich dar?
- Haben die »Snowden-Veröffentlichungen« diesbezüglich etwas verändert?
- Welche Erklärungsansätze gibt es hierfür aus sozial-psychologischer Sicht?
- Welche gesellschaftlichen, ethischen, politischen und rechtlichen Implikationen ergeben sich daraus im Hinblick auf die Ausübung der Grundrechte (Freie Entfaltung der Persönlichkeit, Gleichberechtigung, Versammlungsfreiheit etc.)
- Sind ähnliche Verhaltensänderungen auch beim Einsatz von Beobachtungstechnologien für Anwendungen im nicht-polizeilichen Bereich zu erwarten (z.B. intelligente Rauchmelder, Luftaufklärung im Kontext von Naturkatastrophen)?

Zur Erörterung der Fragestellungen sollen einerseits die verfügbaren evidenzbasierten Studien ausgewertet (und ggf. eigene Erhebungen durchgeführt) sowie andererseits und vergleichend dazu die entsprechenden sozialwissenschaftlichen und psychologischen Theorien sowie ethischen Ansätze herangezogen werden.

Termine

- Abgabefrist für alle Angebote ist der **14.11.2016**.
- Mit der Bearbeitung soll voraussichtlich am **01.02.2017** begonnen werden.
- Die Vorlage der Gutachten muss bis zum **02.05.2017** erfolgen.

Die Gutachtenerstellung innerhalb der vorgesehenen Zeiträume erfolgt vorbehaltlich der rechtzeitigen Beauftragung durch den Deutschen Bundestag.

Hinweise zur Angebotserstellung

Bei der Erarbeitung der Angebote sind die »Hinweise für Gutachter« zu beachten. Insbesondere muss die Kompetenz der Anbietenden aus den Angeboten hervorgehen, und es müssen die beabsichtigte Vorgehensweise und der erforderliche Bearbeitungsaufwand verdeutlicht werden.

Nach unseren Erfahrungen müssen die eingehenden Angebote oft inhaltlich wie kalkulatorisch noch modifiziert werden. Senden Sie uns deshalb zunächst eine elektronische Version Ihres vollständigen Angebots zusammen mit dem **Formblatt** PDF [0,04 MB](s.a. Hinweise für Gutachter) an unsere E-Mail-Adresse buero@tab-beim-bundestag.de.

Sollten wir Ihr Angebot in die engere Wahl ziehen und dem Deutschen Bundestag zur Vergabe vorschlagen wollen, werden wir Sie um die Zusendung eines unterschriebenen Originalangebots an das TAB bitten (Neue Schönhauser Straße 10, 10178 Berlin).

Zum Seitenanfang

Erstellt: 19.10.2016 Aktualisiert: 29.04.2019

Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag
Neue Schönhauser Straße 10, 10178 Berlin| buero@tab-beim-bundestag.de | Tel.: +49 30 28491-0