Global Institute for
Structure relevance,
Anonymity and
Decentralization i.G.

GISAD Stellungnahme zu Civil, defence and space industries (action plan on synergies)

Vorbemerkung:

GISAD (Global Institute for Structure relevance, Anonymity and Decentralisation i.G.) ist ein Institut in Gründung. GISAD will aus Sicht der Bürger Europas ein Digital-System (EU-D-S) entwickeln, welches sich im Systemwettbewerb mit Torwächtern und einem Social Credit System behaupten kann.

Ziel von GISAD ist die Begleitung bei der Erstellung eines ganzheitlichen Marshallplans, wie dieser von der Präsidentin der Europäischen Kommission, Ursula von der Leyen gefordert wurde. Kern des Marshallplans muss ein auf Bürgerrechte und Vielfalt angepasstes Digitalkonzept sein. Bei Einzelmaßnahmen ohne eigenes Gesamtsystem besteht die Gefahr für Europa, den Systemwettbewerb gegen andere Wirtschaftsräume wie ein zentral gesteuertes China zu verlieren.

- Die Stellungnahme von GISAD steht unter dem Vorbehalt, dass sie als Teil eines Digital-Gesamtkonzepts zu verstehen ist (Mehrfachnutzen der gleichen Infrastruktur ohne Mehrkosten).

Herausforderungen:

Wenn wir Synergien zwischen Raumfahrt-/ Verteidigungsindustrie und Zivilgesellschaft erreichen wollen, dann ist die Basis dafür ein digital eindeutiger Rechtsraum. In Zeiten von Home Office und in einer Zukunft der Besiedelung des Weltraums ist nicht mehr davon auszugehen, dass Bürger ihr Leben lang an einem Standort bleiben. Bürger wollen und müssen im digitalen Raum eindeutig erreichbar sein. Digital-Systeme treten hierfür zunehmend in Konkurrenz. Oft entziehen sich diese zentral verwalteten Digital-Systeme dem europäischen Rechtsraum. Der physikalische Wohnort wird weniger wichtig, als das Digital-System, welches ein Bürger als sein digitales Zuhause wählt. Das Sammeln von persönlichen Profilen findet heute zu Lasten der Privatsphäre und der Bürgerrechte durch Digital-Systeme aus den USA und China statt. Für die Sichtweise der Verteidigung Europas wird Cybersicherheit immer wichtiger. Heute stehen fast alle Informationen, die der EU über ihre eigenen Bürger zur Verfügung stehen, auch ausländischen Diensten zur Verfügung. Grund ist der fehlende Schutz digitaler Kommunikation. Die größte Gefahr geht immer von dem schwächsten Glied einer Kommunikationskette aus. Das ist derzeit der Bürger. Jeder Politiker, jeder Soldat und jeder Mitarbeiter ist auch Bürger. Der nordkoreanische Machthaber Kim Jong-un hat einmal sinngemäß gesagt: „Wir sind im Cyberwar stärker als ihr. Wir haben gute Hacker und unser Volk ist nicht im Internet, deshalb sind wir nicht angreifbar."

Lösungsvorschlag vor dem Hintergrund einer Digitalisierungs-Gesamtstrategie:

Jeder EU Bürger benötigt eine europäische Repräsentanz in einem aufzubauenden EU-D-S, unabhängig von seinem permanenten Wohnort. Er unterliegt den Gesetzen und dem Zugriff der europäischen Repräsentanz, die er gewählt hat. Die europäische Repräsentanz ist idealerweise ein europäischer Notar oder Rechtsanwalt (Trust-Station), der im Einzelfall und nach richterlicher Verfügung die nicht im Internet gespeicherten persönlichen Daten zur Verfügung stellt.

Gemeinsame Nutzung für die Raumfahrt, Verteidigungs- und Sicherheitsindustrie und die Zivilgesellschaft

Mit der Zurverfügungstellung von genauen Satellitennavigationsdaten entstehen viele neue Anwendungen. Wenn wir die Bürgerrechte erhalten wollen, dürfen die Navigationsdaten nur, wenn unbedingt notwendig, mit persönlichen Daten verknüpft werden. Auch die Sicherheit wird erheblich gefährdet, wenn eine Personalisierung von Bewegungsprofilen möglich ist, wie eine Fitness-App von US-Solddaten im Irak und Syrien gezeigt hat.

Im Folgenden zeige ich einige Anwendungsbeispiele, die nach Einführung eines EU-D-S möglich wären.

- **Anonyme Freund-Feind-Erkennung**

In den rein militärischen Lösungen ist die Freund-Feind-Erkennung (IFF) in Flugzeugen, Fahrzeugen, und Schiffen, sowie Waffen eingebaut. Solche Systeme funktionieren nur für Soldaten. Zivilisten werden hierdurch nicht geschützt. Im Zusammenhang mit Satellitennavigation ist es möglich, die Standorte von Zivilisten anzuzeigen. Smartphone-Besitzer mit Applikationen, die Navigationsdaten über Funk weitergeben, können militärischen Zielgebieten zugeordnet werden. Eine sichere Freund-Feind-Erkennung ist hierdurch jedoch nicht möglich, kann nur indirekt durch die verwendete Sprache und andere Merkmale vermutet werden. Eine Auswertung größerer Personengruppen dauert für eine aktuelle Gefechtssituation zu lange. Im EU-D-S werden 1000 IP-Adressen je Person von einer Institution mit speziellem rechtlichen Status (Rechtsanwalt oder Notar) in einer Trust-Station ausgegeben. Diese 1000 IP-Adressen werden bei allen Onlinetransaktionen im Wechsel verwendet, um die Profilerstellung zu verhindern. Es ist jedoch für jedermann möglich, über den öffentlichen Teil der IP-Adresse die Trust-Station zu identifizieren, welche die IP-Adresse herausgegeben hat und hier über eine automatische Antwort eine einzelne IP-Adresse zu validieren. Selbst wenn der Feind eine einzelne IP-Adresse fälschen würde, ist es unwahrscheinlich, dass er mehrere gültige IP-Adressen fälschen kann. Zusätzlich kann eine Plausibilitätsprüfung eingebaut werden. Wenn zum Beispiel die gleiche IP-Adresse von kurzes Zeit an einem weit entfernten Ort verwendet wurde, ist sie mit großer Sicherheit gefälscht. Wenn mehrere EU-Bürger über das EU-D-S an einem Zielort angezeigt werden, besteht die große Wahrscheinlichkeit, dass die Information richtig ist. Es bietet sich an, auch befreundete Nicht-EU-Bürger in das EU-D-S aufzunehmen, um diese zu schützen. Ein Ausschluss von Bürgern eines Landes kann einfach dadurch erfolgen, dass die IP-Adressen der entsprechenden Trust-Stationen vom EU-D-S nicht mehr akzeptiert werden.

- **Branchenspezifische anonyme Notfallhilfe**

Wenn man jeder Trust-Station GPS-Koordinaten hinterlegt, dann kann zum Beispiel ein Italiener in Amsterdam hinter der Kategorie „Autoreparaturen“ mit seinen GPS-Daten einen Notruf starten. Das EU-D-S identifiziert die Trust-Stationen mit Sitz in Amsterdam. Diese senden an die in der Kategorie gelisteten Klienten automatisch die Anfrage weiter. Angebote niederländischer Autoreparaturwerkstätten aus der Nähe werden bei dem Italiener angezeigt. Er nimmt Kontakt auf und es liegt an ihm, seine Anonymität aufzuheben.

- **Automatische Erfassung von Carsharing-Daten**

Grundsätzlich müsste gemäß DSGVO bei jeder Datennutzung von Bewegungsprofilen der Fahrzeuge eine wirksame Einwilligung des Nutzers eingeholt werden. Derzeit erfolgt das meist nicht, weil man dadurch potenzielle Kunden abschrecken könnte. Mit dem EU-D-S ist es möglich, nur dann die Anonymität aufzuheben, wenn es auf Grund eines Rechtsverstoßes von einem Richter für notwendig erachtet wurde. Beim Mieten und Bezahlen verwendet der Nutzer eine beliebige der ihm zugeordneten 1000 IP-Adressen. Die Zuordnung ist nur der Trust-Station bekannt. Der Kunde bleibt anonym. Das Nutzungsprofil kann ihm so nicht persönlich zugeordnet werden. Die Akzeptanzprobleme bei Sharing fallen weg. Das gilt auch für Sharing-Möglichkeiten in anderen Branchen.

- **Echte Verfügungsgewalt über die eigenen Daten**

Zunehmend legen wir unsere Daten bei Dienstleistern in der Cloud ab. Clouddienste sind gut darin, die Integrität und Verfügbarkeit von Daten zur Verfügung zu stellen. Bezüglich der Vertraulichkeit bieten sie keinen ausreichenden Schutz, wenn Passwörter und Schlüssel offen über das Internet ausgetauscht werden. Weiterhin ist die Verfügungsgewalt eines Besitzers über seine Daten nicht sichergestellt. Viele Anbieter arbeiten außerhalb des europäischen Rechtsraums. Wir vertrauen darauf, dass diese Rechtsräume stabil bleiben. Tatsächlich jedoch gibt es viele Möglichkeiten, dem Besitzer die Verfügungsgewalt über seine Daten zu entziehen. Dienstleister können abgewickelt oder an ausländische Firmen verkauft und die Daten gelöscht werden. Auch müssen wir selbst dann, wenn der Besitzer eines Unternehmens gewechselt hat, darauf vertrauen, dass kein Mitarbeiter eines Dienstleisters die zentralen Sicherheitsmechanismen aufhebt.

In einem EU-D-S werden die Metadaten mit den Schlüsseln für die Datenspeicherung und Kommunikation bei jedem Nutzer einzeln dezentral gespeichert. Die auf Basis der gleichen Metadaten verschlüsselten Daten können bei mehreren Dienstleistern an beliebigen Orten abgelegt werden. Wenn ein Dienstleister ausfällt, ist die Verfügbarkeit weiterhin durch einen zweiten beauftragten Dienstleister sichergestellt. Über ein dezentrales automatisches Backup-System ist auch dezentral die Verfügbarkeit der Metadaten gewährleistet. Für die Raumfahrt-, Verteidigungs- und Sicherheitsindustrie entsteht so ein europäisches Alleinstellungsmerkmal mit hoher Sicherheit für europäische Bürger und Unternehmen.

- **Hardwareproduktion nach dem Dual-Use Prinzip**

Das EU-D-S kosten zirka 30,-€ je Bürger. Mehr als die Hälfte der Kosten entfällt auf die Hardware. Um einen hohen Sicherheitsstandard zu gewährleisten, sind alle Teilkomponenten von Unternehmen in mehrheitlich europäischem Besitz zu entwickeln. 448 Millionen Menschen leben (Quelle Eurostat für 2020) in Europa. Gehen wir von 400 Millionen Teilnehmern im EU-D-S aus (ohne Kinder unter 8 Jahren), so ergibt sich ein Investitionsvolumen von zirka 6 Milliarden Euro. Der Investitionsbedarf entsteht nicht auf einmal, da ein Ausbau in mehreren Stufen durch unterschiedlichste Anbieter sinnvoll ist. Auch können diese Investitionen durch die Vielzahl neuer Anwendungsmöglichkeiten schnell refinanziert werden. Es ist sinnvoll, für ein solch großes Volumen konsequent Vorgaben zu entwickeln, wie die hierfür verwendeten Komponenten möglichst breit eingesetzt werden können.

Voraussetzungen für das EU-D-S

In der eine IP-Adresse eindeutig dem Verantwortlichen für eine Information, ein Produkt, eine Dienstleistung oder eine Maschine zugeordnet werden kann.

- Bestehend aus regionalen Trust-Stationen im Wohnsitz eines EU Bürgers, mit einer einem Notar entsprechenden staatlichen Anerkennung.
- Mit der Vergabe eines eindeutigen öffentlichen IP-Subnetzes an jede Truststation.
- Mit der Herausgabe an jeden EU Bürger durch eine Trust-Station von 1.000 zufällig aus dem IP-Subnetz erzeugten IP Adressen.
- Mit der Verpflichtung der Truststation, die dem EU Bürger vergebenen IP Adressen nur so den persönlichen Daten zuzuordnen, dass deren Speicherort vom Internet physikalisch getrennt ist (keine Netzwerkverbindung).
- Mit dem Recht der Trust-Station, ohne direkte Kenntnis durch den betroffenen EU Bürger, bei einer konkreten Untersuchung mit einem Richter auszuhandeln, welche Daten (zugehörig zu einer Kategorie, Zeitraum, angefallen in einem bestimmten geografischen Raum) herausgegeben werden müssen.
- Mit der Verpflichtung der Trust-Station nach einer angemessenen Frist den betroffenen EU-Bürger über die Herausgabe zu informieren und die WAN Anonymität (WAN bedeutet WIDE AREA NETWORK) durch Herausgabe neuer IP-Adressen wiederherzustellen.
- In der die Speicherung von personenbezogenen Daten über das Internet in Bezug auf die Bürgerrechts-Infrastruktur technisch und rechtlich unterbunden wird.
- In der die physische Verfügungsgewalt über Schlüssel und Identitäten und die darüber erstellen Inhalte beim einzelnen Bürger liegt.
- In der die Sicherheit durch die Bereitstellung einer ausschließlich in Europa erstellten Hardware (USB-Stick als Erweiterung beliebiger Devices) garantiert wird.
- In der alle Metadaten, symmetrischen Schlüssel und Identitäten für die verwendeten Daten so gespeichert werden, dass die Verfügungsgewalt über die Daten beim einzelnen Bürger liegt.
- In der eine automatische Updatemöglichkeit (z.B. beim Laden eines Devices) geschaffen wird, die bei jedem EU-Bürger die Verfügbarkeit seiner Metadaten sicherstellt und im Falle einer Hausdurchsuchung forensische digitale Beweise sicherstellt.
- Durch die Standardisierung von weltweit zirka 1000 Kategorien für aller Branchen.
- Durch einen Sucheinstieg zu den Suchen von verschiedenen Plattformen je Kategorie in bis zu 2500 Sprachen.

Weitere Informationen:

http://gisad.eu/statements/

https://youtu.be/doPXxmX7fec?t=233

https://youtu.be/XZS1YGTULIw?t=57

https://youtu.be/s1occJG5SOw?t=29