Handlungsfähiger Rechtsstaat

2030 wird die Digitalisierung auch in Deutschland weitgehend fortgeschritten sein. Das wird ohne heute zu treffende Gegenmaßnahmen verheerende Folgen für Deutschland haben, weil die Exekutive und Justiz weitgehend auf dem digitalen Auge blind sind.

Die rasche weltweite Ausbreitung des Corona-Virus wird die digitale Angriffslage verschlimmern, da immer mehr Staaten das Geschäftsmodell Nordkoreas nachahmen werden. Mit Hilfe von Cyberangriffen und dem Erpressen von Geld werden die Staatskassen gefüllt.

Andererseits gibt es bereits seit vielen Jahren Synergien zwischen einer globalen, digitalen, datengetriebenen IT-Sicherheits-/Überwachungs- und Verwertungsindustrie und per Gesetz zur Unterstützung der eigenen Wirtschaft beauftragten Geheimdienste.

Cyberkriminelle suchen heute mit automatischen Tools nach Schwachstellen, um bei einem zufälligen Ziel in der Regel einen Erpressungsversuch zu unternehmen.

Die Angriffe von Geheimdiensten unterscheiden sich hiervon vollständig. Diese greifen gezielt an. Die Motivationen sind unterschiedlich. So kann es sich genauso um das Ziel handeln, eine bestimmte Technologie im Auftrag eines zum eigenen Staat gehörenden Unternehmens auszuschalten oder die Erpressung einer Börsenplattform, Geld dafür zu zahlen, damit weitere Manipulationen unterbleiben oder auch langfristige Strategien wie die Austrocknung eines konkurrierenden Innovationsstandorts.

Geheimdienstliche Angriffe über das Internet sind in der Regel nicht nachweisbar. Qualifizierte Cyberkriminelle können ihre Spuren ebenfalls gut verwischen.

Demokratie erhaltende Innovationen können in einem solchen Umfeld nicht mehr entwickelt werden, da jeder Innovator ausgeschaltet werden kann. Wer keine forensisch verwertbaren Beweise vorlegen kann, findet noch nicht einmal einen Ansprechpartner bei der Exekutive, geschweige denn einen entsprechenden Schutz.

Vor diesem Hintergrund halte ich die folgende Vorgehensweise für sinnvoll:

- Eine dezentrale, WAN anonyme Bürgerrechts-Infrastruktur mit Integration aller Bürger, die es wünschen, in ein Digitalsystem, in dem Rechtstaatlichkeit aufrecht erhalten werden kann.
- Die Möglichkeit der Rechtsverfolgung innerhalb dieser Infrastruktur, da hierin alle Handlungen im jeweiligen Rechtsraum begangen werden.
- Die Schaffung einer digitalen sozialen Kontrolle zur Verhinderung von Straftaten im Vorfeld durch Bewertung aller Inhalte in einem Bürgerbeteiligungsportal.
- Im Einzelfall und nur nach richterlicher Verfügung die lückenlose forensische Beweissicherung nach Beschlagnahme eines Backups als Teil der Bürgerrechts-Infrastruktur.
- Die Widerherstellung der WAN Anonymität nach Abschluss eines Verfahrens.
- Die kostenlose Bestellung eines Gutachters und besondere Berücksichtigung dieses Gutachtens im Rahmen von Ermittlungen und Gerichtsurteilen, wenn ein Beschuldigter einen möglichen Angriff auf sich als Innovator zum Beispiel als Patentanmelder glaubhaft machen kann.
- Eine klare Kompetenzabgrenzung zwischen Bundeswehr und Polizei. Alle Cyberangriffe sind Angriffe von innen und somit in der Zuständigkeit der Polizei, solange keine anderslautende

Erklärung (Kriegserklärung, Erklärung einer ausländischen extremistischen Gruppe) vorliegt. Dann jedoch sofortige Übernahme durch die Bundeswehr.

Weitere Informationen finden Sie unter:

Video Social Utopia Talk 4 kurz – Grundlage für WAN Anonymität in einer Bürgerrechts-Infrastruktur

Video Social Utopia Talk 5 – Grundlage für die Verfügungsgewalt über die eigenen Daten

Video Social Utopia Talk 3 – Ist das deutsche Rechtssystem fit für das digitale Zeitalter?

Stellungnahme zu - Digital Services Act: deepening the Internal Market and clarifying responsibilities for digital services

Compliance – Wie China die Handlungsfähigkeit unseres Rechtsstaats beeinflusst

Recht auf selbstbestimmte digitale Teilhabe!

Recht auf Wahlfreiheit zwischen Suchalgorithmen