Dr.-Ing. Michael Mertin
Am Röthang 16 · 07739 Jena

Dr.-Ing. Michael Mertin

Wirtschaftstag

1. Elemente von „Sicherheit“ im Zeitalter der 4. Industriellen Revolution:

1.1. Klassische Aspekte von Sicherheit für Bevölkerung und Wirtschaft
- 1.1.1. Territoriale Sicherheit
- 1.1.2. Innere Sicherheit, Gewaltmonopol des Staates
- 1.1.3. Rechtssicherheit, insbesondere Vertragssicherheit
- 1.1.4. Garantie des Eigentums

... usw...

1.2. Globalisierung als zusätzlicher Aspekt Ende des 20. und im 21 Jahrhundert:
- 1.2.1. Global Village („Die Sicherheit Deutschlands wird in Afghanistan verteidigt.“) und asymmetrische Bedrohungen (Terrorismus einer neuen und globalen Generation)
- 1.2.2. Globalisierung, Welthandel und globale Supply Chains als Grundlage moderner westlicher Staaten und Demokratien

1.3. Cyber Security
- 1.3.1. Sicherheit der öffentlichen Infrastruktur; insbesondere bzgl. Strukturen der Daseinsfürsorge (Energie, Wasser, Verkehr, Ernährung, Militär, Polizei, ...)

Dr.-Ing. Michael Mertin
Am Röthang 16 · 07739 Jen
Telefon: +49 173 6378463
mike.mertin.home@gmail.com
BIC:
IBAN:

1.3.2. Sicherheit Digitaler Geschäftsmodelle (Banken/ Transaktionen, Plattform Economy, …)
1.3.3. Sicherheit Digital/Analoger Geschäftsmodelle und Wertschöpfungsstrukturen, insbesondere in der Industrie 4.0
1.3.4. Sicherheit allgemeiner staatlicher Datenstrukturen (Behörden z.B. Finanzämter, kommunale Verwaltungen, …)
1.3.5. Sicherung der Freiheit und (Daten-) Selbstbestimmung des Individuums unter Ermöglichung ökonomischer und staatlicher notwendiger Daten- und Infrastrukturnutzung **(!)**
1.3.6. Sicherung des Zugangs zu einem (Level?) Playing Field für regionale und globale Geschäftsmodelle

2. Bedrohungen

2.1. Globales Machtoligopol versucht nationale Regeln (Handel, Rechtssysteme, Daten, Netze, …) zum eigenen Nutzen global durchzusetzen:
2.1.1. USA, China, Russland, EU (? Allerdings recht schwach)
- Embargos, Compliance, Steuern, diverse Regulierungen aus den USA mit globaler Wirkung
- Einfluss aus nationale Unternehmen um international Datenzugänge zu erhalten (USA/NSA, China ?!)

2.1.2. … sowie einigen Mittelmächten mit wirtschaftlicher und/oder militärischer Bedeutung (Iran, Türkei, Japan, Deutschland, Frankreich, England, Indien, Pakistan, …)
2.1.3. … und einiger internationaler militärischer Bedrohungen (z.B. von Nordkorea, Iran, …)
2.2. Zugang zu Plattform Ökonomien in USA und China; bis heute wenig Angebote aus EU
2.3. Industriespionage, Absicherung von Know-How
2.4. Staatliche oder terroristische Cyber Attacken auf Infrastruktur von Staaten, Unternehmen oder Personengruppen; in der Spitze mit wesentlichen Bedrohungen für die Bevölkerung

3. Thesen zur Cyber Security

3.1. Cyber Security braucht im Zeitalter von Globalisierung, Digitalisierung und Industrie 4.0 den gleichen Stellenwert wie innere und äußere staatliche Sicherheit.
3.2. Die Sicherheit von Netzen und Daten sollte, auch bei privatwirtschaftlichem Betrieb und Nutzung, analog zu Eigentum und Rechtssicherheit, zu innerer und äußerer Sicherheit garantiert werden können.
3.3. Cyber Security ist bei weitem nicht nur Verbraucherschutz ggü vermeintlich bösartigen Unternehmen, sondern der Schutz unserer ökonomischen, freiheitlichen und demokratischen Grundwerte.
3.4. Wir werden über Maßnahmen im Bereich Cyber Security nicht kurzfristig den Anschluss an Systeme der Plattform Ökonomie aus USA oder China finden, können aber die Chance der Industrie 4.0 als führende Industrienation nutzen und Datenanwendungen in klassischen Wirtschaftsbereichen (und damit diese selber) schützen.

4. Thesen zur Sicherheit bzw. Absicherung von Digitalen Geschäftsmodellen und Industrie 4.0

4.1. Nationale Alleingänge sind bei global vernetzten Systemen nicht erfolgreich
4.2. Auch ein Vorgehen auf regionaler Ebene (EU, USA, …) wird vermutlich mittelfristig scheitern, da letztendlich in fremden Hoheitsgebieten Geschäfte gemacht werden sollen
4.3. Lediglich Abkommen der wesentlichen Wirtschaftsmächte bzw. Regionen untereinander mit entsprechender Überwachungsmöglichkeit bieten einen Ansatz zur Lösung
4.4. Gleichermaßen gemeine Bekämpfung von (Staats-) Terrorismus und mögliche Verbrechens- und Schadensbekämpfung
4.5. …. da dies voraussichtlich absehbar nicht umsetzbar ist,
  4.5.1. sollten zumindest entsprechende System regional (z.B. innerhalb der EU) etabliert werden; dazu gehören aber auch klare Firewall Strukturen und Datenhandling in andere Wirtschaftsbereiche
  4.5.2. Dazu benötig Europa eine gemeinsame Netz- und Dateninfrastruktur sowie eine Förderung (nicht unbedingt

monetär, aber durch Regulierung/Deregulierung) zum Aufbau entsprechender Industrien und Technologien analog zu USA, China und z.T. Russland

4.5.3. Bilaterale Abkommen über Zugang und (Daten-) Sicherheit von Unternehmen und Investitionen

5. Fazit sowie konkrete Konsequenzen für Europa und Deutschland

5.1. Politik, Unternehmen und Bevölkerung muss begreifen und geschult werden, dass Netze und Daten heute zu existentieller Infrastruktur moderner Industriestaaten gehören. Diese müssen geschützt werden wie alle anderen existentiellen und freiheitlichen Grundlagen eines Staates oder einer Region (Europa), ebenso wie Grenzen, Leib- und Leben der Bevölkerung, öffentliche Infrastruktur und privatwirtschaftliche Infrastruktur.

5.2. Dazu reicht eine Politik des Datenschutzes der eigenen Bevölkerung ggü der eigenen Wirtschaft (Verbraucherschutz) bei weitem nicht aus. US Unternehmen z.B. lassen dann einfach keine europäischen Nutzer mehr zu … wie im Bsp der DSGVO deutlich wird.

5.3. Auch bei den Wirtschaftsskandalen der jüngeren Geschichte müssen wir unsere nationale und europäische Wirtschaft als Freund und wesentliche Säule einer freiheitlichen und demokratischen Ordnung begreifen, gegen die man sich bzw. die Bevölkerung nicht nur schützen muss, sondern welche auch freiheitliche und marktwirtschaftliche Rahmenbedingungen braucht. Innovation, Spitzenkräfte und damit auch Kapital sucht sich den optimalen Nährboden – dieser ist insbesondere im Bereich IT und bei wesentlichen anderen Innovationsthemen im High Tech Bereich nicht (mehr) in Europa.

5.4. Entbürokratisierung, teilweise Deregulierung sowie investitionsfreundliche Steuersysteme sind in Deutschland sowie den Industrienationen Europas Mangelware. Der Ansatz weitere Steuern z.B. auf daten zu erheben ist eine völlige Fehlsteuerung und bewirk Kostensteigerungen in nahezu allen Bereichen des Lebens.

5.5. Datenschutz muss entgegen einer DSGVO vielmehr als Schutz nationalen und europäischen Eigentums gesehen werden. Das

bedeutet eine massive Förderung von Encryption Technologien (Verschlüsselungen), Entwicklung sicherer Datenspeicher und Firewall Systemen, Investitions- und Ausbildungsförderung in diesen Bereichen.

5.6. Wir müssen in Europa intensiv analysieren, warum nicht wir, sondern die USA und vermehrt auch China die Zentren der IT Technologie sowie entsprechender Geschäftsmodelle ist, um

5.6.1. Zumindest im Bereich Industrie 4.0 eine weltweit führende Stellung zu erreichen,

5.6.2. Zumindest ein einigen Bereichen eigene und/oder zusätzliche globale Plattform Ökonomie bezogene Unternehmen/Geschäftsmodelle betreiben zu kommen und

5.6.3. Die Funktionsfähigkeit auch klassischer Wirtschaftsteile, welche ebenfalls mit Daten essentiell arbeiten, weiterhin sicher zu stellen.

5.7. Entweder müssen wir Unternehmen - oder sogar neu zu etablierende staatliche Strukturen -, in enger Abstimmung mit staatlichen Stellen für nationale Sicherheit, befähigen, unsere Daten sowie die entsprechende Infrastruktur ggü Angriffen von innen wie außen zu schützen. Hierzu ist neben einer Überwachung wesentlichen sensitiver Infrastruktur auch die Entwicklung entsprechender Abwehrmechanismen erforderlich. Das wird eine große Anstrengung werden und möglicherweise auf eine Größenordnung wie der Erhalt und Ausbau unserer Mobilitäts-, Energie- oder Sicherheitsstruktur bedeuten.

5.8. Deutschland wird sich überlegen müssen, ob wir endlich mehr Geld für Sicherheit und unsere Zukunft in vielen Bereichen ausgeben oder wie bisher lediglich in den ausufernden Sozialstaat investieren. Diesem wir jedenfalls ohne Bewusstseinsänderung zum Thema Sicherheit mittelfristig auch auf dieser und nicht nur auf der bisherigen klassischen ökonomischen Basis, die Grundlage entzogen. Dies gilt gleichermaßen für die „digitale Verteidigungsbereitschaft" der Bundeswehr. Hier werden wir uns sicherlich nicht alleine auf den Schutz der NATO verlassen können!

5.9. Wir brauchen eine Definition einer besonders „schützenswerten Schlüsselindustrie“ sowie einer solchen „ schützenswerten Schlüssel Infrastruktur“.