Thesen zur Anhörung des Auswärtigen Ausschusses des Deutschen Bundestages am 07.06.2021

Geopolitische Aspekte von Standardisierung und innovativer Technologien

Thesen und Aspekte in Kurzform

1. Langfrist-Implikationen der NOBUS-Strategie der USA im Kontext von IT- und Datensicherheit

2. Decoupling; Ende der US-Hegemonie, Protektionismus und Abkehr vom (digitalen) Freihandel

3. Digitale Kolonialisierung und Aspekte möglicher Strategien zur Wahrung digitaler Souveränität

Andy Müller-Maguhn, Datenreisebüro, Postfach 640234, DE-10048 Berlin, amm@datenreisen.de

Thesen zur Anhörung des Auswärtigen Ausschusses des Deutschen Bundestages am 07.06.2021

1. Langfrist-Implikationen der NOBUS-Strategie der USA im Kontext von IT- und Datensicherheit

Bereits seit den 90er Jahren definiert die US-Regierung IT-Sicherheit im Kontext der NOBUS-Strategie ("no one, but us"). D.h. IT-Systeme (Komponenten, Hard- wie Software) gelten dann als sicher, wenn Ihre Architektur eine hinreichende Sicherheit gegenüber konventionellen Angreifern erwirkt, aber der Zugriff für US-Nachrichtendiensten (in diesem Kontext vorwiegend der NSA) durch spezielle Zugänge (bzw. Schwachstellen) sichergestellt ist.

Obwohl die NOBUS-Strategie in Europa schon viele Jahrzehnte bekannt ist und es durchaus strategische Ansätze gegeben hat, hier Sicherheitskonzepte zu entwickeln, die keine solchen vorgesehenen "Sollbruchstellen" enthalten, hat der klandestine Charakter der US-Vorgehensweise lange eine Illusion der IT-Sicherheit erzeugt.

Zudem waren bzw. sind die eigentlich auch für die IT- und Datensicherheit zuständigen europäischen Sicherheitsbehörden seit vielen Jahrzehnten in einem starken Interessenskonflikt, da ihre US- bzw. Nato-Partner Ihnen die Beteiligung an dieser Welt der Unsicherheit als "strategischen Vorteil im Bündniss" verargumentierten. Es ist aus meiner Sicht keine unzulässige Überspitzung, wenn man zusammenfassend diagnostiziert, daß viele europäische Sicherheitsbehörden – auch im Kontext der Standardisierung, aber auch in der technischen Ausarbeitung von Lizenspflichten und Ausschreibungstexten – nicht der Sicherheit, sondern den nachrichtendienstlichen Zugriffsoptionen amerikanischer Dienste zugearbeitet haben.

Spätestens durch Whistleblower wie Edward Snowden liegen Nachweise für die systematische Ausnutzung von Schwachstellen durch US-Dienste in großteils automatisierten Prozessen *und* die Kollaboration mit europäischen Partnerdiensten vor, die aber eben – wiederum bedingt durch die NOBUS-Strategie – keinen Zugriff auf Rohdaten erhalten, sondern nur ausgewählte (und aufbereitete) nachrichtendienstliche Erkenntnisse.

In den letzten Jahrzehnten sind zudem viele Beispiele für die Ausnutzung von gravierenden Sicherheitslücken durch kriminelle und nachrichtendienstliche Akteure anderer Länder aufgetaucht. Viele dieser Angriffsformen hätten bei einer obligatorischen wissenschaftlichen Untersuchung und Anforderung von überprüfbarer Sicherheit verhindert werden können. Kurz: der Versuch der US-Dienste, die "Hintertüren" und "Sollbruchstellen" geheim zu halten und exklusiv zu nutzen, ist nachweislich oft mislungen; die so entstehenden Risiken sind erheblich.

Angesichts der stark zugenommenen Abhängigkeit von IT-Systemen auf allen Ebenen sollte dies Grund genug sein, europäische IT-Sicherheit nicht nur anders zu definieren, sondern dies auch in voller Kenntnis des internationalen Geschehens – zumindest im Wirkungsbereich der eigenen Länder im Bezug auf Technologieimport und Zulassungen für den Gebrauch in kritischen Bereichen – durchzusetzen. Dies erfordert allerdings zunächst eine kritische Analyse und wohl auch ein Umbau der zur Verfügung stehenden Institutionen im Bezug auf Interessenskonflikten und Abhängigkeiten.

Andy Müller-Maguhn, Datenreisebüro, Postfach 640234, DE-10048 Berlin, amm@datenreisen.de

Thesen zur Anhörung des Auswärtigen Ausschusses des Deutschen Bundestages am 07.06.2021

2. Decoupling; Ende der US-Hegemonie, Abkehr vom Freihandel und offener Protektionismus

Um die der Anhörung zugrundeliegenden Studien zur strategischen Vorgehensweise etwa der chinesischen Regierung zu verstehen, erscheint mir zunächst hilfreich, die dortige Perspektive nachzuvollziehen, da es entscheidene Unterschiede zur westeuropäischen Wahrnehmung gibt. Durch die in Punkt 1 skizzierten nachrichtendienstlichen Interessenskonflikten einerseits, aber auch durch ein Mangel an digitaler Souveränität ist eine neutrale Wahrnehmung in Europa erschwert.

Die beispielsweise im Kontext des Internet-Normierungsgremiums ICANN durchgesetzte Anerkenntnis des US Markenrechts war in Westeuropa ohnehin schon etabliert, so daß die Ausweitung auf die weltweite Registrierung von Internet-Domain-Namen nur logisch erschien. Die in anderen Kontinenten und Ländern etablierten markenrechtlichen Mechanismen hatten wenig gemeinsam und noch weniger Chance, in dem – von den USA maßgeblich definiertem - digitalen Neuland zu überleben.

Allerdings ist es der analytischen Aufmerksamkeit u.a. der chinesischen Regierung und ihren Vertretern nicht entgangen, daß hier (etwa im Kontext der Standardisierung von Domainregeln in lokalen Sprachen IDN) der Versuch unternommen wurde, Regeln einer Fremdjurisdiktion mit weitreichenden kulturellen und wirtschaftlichen Implikationen ohne politische Verhandlungen durch technische Argumentation einzuführen.

China hat nicht nur in diesem Bereich erfolgreiche Strategien entwickelt, die Souveränität auch in den weltweit vernetzten digitalen Infrastrukturen zu erhalten. Die im digitalen Westeuropa kaum noch vorhandene Möglichkeit, wirtschaftliche Wertschöpfungsketten ohne US-Konzerne aufzubauen bzw. zu betreiben (präzise: betreiben zu lassen) ist im Gegensatz zu den in China vorhandenen dort ansässigen Plattformen und Handelsplätzen – mit zunehmender Kontrolle über alle Komponenten der Wertschöpfungsketten - ein meßbarer Gegensatz.

Nicht erst seit dem Ende der US-Hegemonie und der von Mike Pompeo eingeführten und von der Biden-Administration weitergeführte Abkehr vom digitalen Freihandel und der aggressiven Verfolgung eines digitalen Protektionismus-Strategie im Kontext der “Clean Network” Initiative (siehe https://2017-2021.state.gov/the-clean-network/index.html) liegen hinreichende Gründe für eine Revision der westeuropäischen Vorgehensweise vor. Die damit eingeleitete Balkanisierung des Internet ist auch eine Gefahr für das friedliche Zusammenleben der Völker.

Während der ehem. Leiter des US-Nachrichtendienstes CIA, Mike Pompeo, nach der dort üblichen “Haltet den Dieb” - Strategie in seiner Rhetorik von chinesischen Unternehmen als “Tools of the Chinese Communist Party’s surveillance state, like Huawei” sprach, fehlte es entweder an analytischer Aufmerksamkeit oder schlicht an Mut, diese Rhetorik mal den von den USA praktizierten “Werkzeugen der weltweiten Telekommunikationsüberwachung durch die Nachrichtendienste der Vereinigten Staaten, wie etwa den ihren gesetzlichen Anforderungen unterliegenden Unternehmen Google, Facebook und Amazon” entgegenzuhalten.

Es fehlt allerdings in Westeuropa auch zunehmend - auch im politischen Raum - an unabhängigen Infrastrukturen, um diese Diskussion außerhalb von digitalen Systemen (die nicht der Kontrolle der USA unterliegen) überhaupt zu führen.

Andy Müller-Maguhn, Datenreisebüro, Postfach 640234, DE-10048 Berlin, amm@datenreisen.de

Thesen zur Anhörung des Auswärtigen Ausschusses des Deutschen Bundestages am 07.06.2021

3. Digitale Kolonialisierung und Aspekte möglicher Strategien zur Wahrung digitaler Souveränität

Mit der Ausweitung geopolitischer Auseinandersetzung in die digitale Welt stehen nun weitere Bewerber an, die durch die US geschaffenen Kolonialisierungsgebiete stückweise anderweitig zu übernehmen. Die Rhetorik des alten Hegemons gegenüber dem neuen als Maßstab zu nehmen erscheint mir jedoch wenig zielführend um eine unabhängige Position zu entwickeln.

Die Aufrechterhaltung offener Standards, aber auch die strategische Analyse von Abhängigkeiten durch Komponenten von Kommunikations- und Wertschöpfungsketten unter Fremdkontrolle bringt erhebliche Chancen für eigenständige Entwicklungen und die Rückerorberung von Komponenten der Wertschöpfungsketten mit sich.

Dazu gehört allerdings auch, propriätere, d.h. nicht offene und allgemein nutzbare Standards abzuwehren, unabhängig davon, ob Sie von Unternehmen kraft ihrer Marktmacht oder Regierungen versucht werden durchzusetzen.

Ob Unternehmen von ausländischen Akteuren der westlichen oder der östlichen Hemisphäre übernommen werden ist nicht nur eine Frage von politische Loyalität bzw. ökonomischer Opportunität, sondern auch eine Frage der Perspektive des eigenen Wirtschaftsraums.

Andernorts ist man bereits im nächsten Schritt nach der analytische Phase und ist vom “Import Replacement” auf dem Weg zum erklärten Ziel der technologischen Unabhängigkeit.

Für eine Strategie der digitalen Souveränität Europas sind sowohl Selbstverständniss als auch Analyse der Abhängigkeiten und Bedeutung der Komponenten stark ausbaufähig.

Andy Müller-Maguhn, Datenreisebüro, Postfach 640234, DE-10048 Berlin, amm@datenreisen.de