Koordinierungsstab Cyber-Außenpolitik
Gz.: KS-CA 310.00
RL: [redacted]
Verf.: [redacted]

Berlin, 9. Oktober 2013

HR: [redacted]
HR: [redacted]

über CA-B

Frau Staatssekretärin und Herrn Staatssekretär

nachrichtlich:
Herrn Staatsminister Link
Frau Staatsministerin Pieper

Betr.: **Cyber-Außenpolitik**
hier: Stand und nächste Schritte nach Dienstantritt CA-B Dirk Brengelmann

Bezug.: BM-Vorlage 02-310.00/4 vom 11.6.13, einschl. „Eckpunkte für eine außenpolitische Cyberstrategie"

Zweck der Vorlage: Zur Unterrichtung

I. Vorbemerkung („Was wollen wir?")

„Cyber-Außenpolitik" wurde in der „Nationalen Cyber-Sicherheitsstrategie für DEU" im Feb. 2011 als Politikfeld definiert; gleichzeitig wurde der ressortübergreifende nationale Cyber-Sicherheitsrat auf StS-Ebene (Cyber-SR) gegründet, sowie im AA der Koordinierungsstab (KS-CA) eingerichtet. Vor diesem Hintergrund lag der primäre Fokus auf Cyber-Sicherheit, bis hin zu einer vom BMI betriebenen Verkürzung auf „Cybersicherheits-Außenpolitik".

---

[1] Verteiler:
(mit Anlagen)

MB	D2, D3, D4, D5, D6
BStS	1-B-2, 2-B-1, 2A-B, E-
BStM L	B-1, VN-B-1, 4-B-1, 5-
BStMin P	B-1, 6-B-3
011	Ref. 200, 300, 403, 405,
013	VN04, VN06
02	StäV Brüssel EU, Genf IO, New York VN; Bo Wash., Neu Delhi, Brasilia, Seoul

Demgegenüber haben wir in unserem Anfang 2012 in den Cyber-SR eingebrachten Strategiepapier klargestellt: *„Cyber-Sicherheit (...) ist daher nur ein Element einer umfassenden Cyber-Außenpolitik, welche die Bundesregierung unter Federführung des Auswärtigen Amts und unter Einbeziehung der sicherheitspolitischen, der menschenrechtlichen und der wirtschaftlich-entwicklungspolitischen Dimensionen erarbeitet.“*

In der Tat hat in den vergangenen zwei Jahren der Cyberraum als Gegenstand von Außenpolitik nicht nur in der Sicherheitspolitik, sondern auch in der Menschenrechtspolitik („Menschenrechte gelten online wie offline“) und Wirtschaftspolitik („Daten als Rohöl des 21. Jahrhunderts“) an Bedeutung gewonnen. Unter dem Eindruck der „Snowden-Affäre“ wurde dies einer breiten internationalen Öffentlichkeit vor Augen geführt. Durch die Digitalisierung erfährt die Globalisierung eine weitere Beschleunigung, gleichzeitig zeigt sich ein zunehmendes Spannungsverhältnis zwischen dem globalen Charakter des Internets auf der einen Seite und dem Ansinnen einiger Staaten nach mehr nationalstaatlicher Kontrolle - und zugleich dem individuellen Bedürfnis nach Sicherheit persönlicher Daten.

Erste Eckpunkte einer ganzheitlichen „Strategie für Cyber-Außenpolitik“ wurden, koordiniert von 02, bereits erarbeitet (s. Bezugsvorlage). Diese basieren auf den o.g. drei Säulen: Freiheit, Sicherheit und wirtschaftliche Aspekte; als vierte, querschnittsartige Herausforderung hat sich „Internet Governance“ herausgeschält. Ziel ist es nun, die o.g. Ziele/Säulen zu konkretisieren und, sofern möglich, in Umsetzungsstrategien zu operationalisieren, d.h. mit konkreten Maßnahmen zu hinterlegen. Hierzu nachfolgend erste Überlegungen.

II. Umsetzungsschwerpunkte („Was steht an?“)

Nach den Dienstantrittsreisen von CA-B Brengelmann (nach FRA, GBR, Brüssel EU, USA, Genf/MRR), nach ersten Kontakten mit den maßgeblichen Ressorts und Verbänden bzw. Unternehmensvertretern sowie mit Blick auf die Teilnahme von CA-B an der ‚Seoul Cyberspace Conference‘ in Südkorea (17.-18.10.), dem ‚Internet Governance Forum‘ in Indonesien (21.-23.10.) und anstehenden Konsultationen mit IND und AUS, später CHN, RUS und BRA, kristallieren sich vier Schwerpunkte heraus:

1. Cyber-Sicherheit: Einen sicheren Zugang, die Integrität von Netzen sowie der darin enthaltenen Daten zu gewährleisten steht bereits im Mittelpunkt von DEU und EU Cyber-Sicherheitsstrategien. Die Berichterstattungen der vergangenen Monate inkl. vermeintlicher NSA-/GCHQ-Hintertüren in Hardware bzw. Verschlüsselungssoftware hat diesen Aspekt verstärkt.
   Zudem hat GBR VM Hammond am 29.9. ein Programm i.H.v. 600 Mio € zum Aufbau einer GBR „Joint Cyber Reserve“ angekündigt, die ähnlich des U.S.

Cyber Command auch „Gegenangriffe im Cyberraum" durchführen wird. Wir als AA werden die sich verstärkende Diskussion zu „Cyber-Defence/-Security" in NATO, VN und OSZE (VSBM) bzw. EU (GSVP) koordinieren und in vernünftigen Bahnen halten. Auch gilt es, Irritationen in Folge der Snowden-Affäre einzufangen.

2. Freiheitsrechte, erweitert um Datenschutz: Das Thema „Internetfreiheit" wurde bis Mitte 2013 primär definiert als die Gewährleistung eines zensurfreien Internetzugangs zum freien Meinungsaustausch. Seit den NSA-Enthüllungen wird auch der internationaler Datenschutz, u.a. verankert in Art. 17 VN-Zivilpakt, als wesentliche „Internetfreiheit" angesehen. Auch angelsächsische IKT-Unternehmen müssen dabei europäischen Datenschutzerfordernissen genügen, Stichwort: Evaluierung Safe-Harbour-Abkommen, verbunden mit einer stärkeren Berücksichtigung des Marktortprinzips (vs. Niederlassungsprinzip). Anzeigeerfordernisse von Unternehmen bzw. Nutzerzustimmung bei Datenweitergabe an Dritte sind weitere Forderungen. Es liegt auch an uns als AA – z.B. im Nachgang des MRR-Side Events in Genf zu „Privacy" – weiter für eine Verbesserung im internationalen Datenschutz zu werben, in der EU, ggü. USA/GBR sowie in internationalen Foren.
3. Digitale Standortpolitik: Cyber-Sicherheit und Datenschutz als Standortfaktor für Unternehmen wie für Bürger/ Nutzer gewinnt entscheidend an Bedeutung. Dies gilt sowohl für Internet-Serviceprovider als auch für -Hostprovider, Stichwort „German bzw. Euro Cloud". Deutsche Telekom und United Internet haben bereits hierzu erste Produktangebote vorgestellt; SAP/ Hasso-Plattner-Institut sind bei Verschlüsselungsverfahren und „Big Date" innovativ. Dabei stehen wir vor der Herausforderung, berechtigte Datenschutzaspekte aufzugreifen bzw. Marktungleichgewichte ordoliberal zu regulieren (auch „Steuerflucht" von Google, Facebook, Apple etc.), ohne dabei unseren transatlantischen Beziehungen fundamental zu schaden (incl. TTIP). Datenschutz als Standortfaktor ist ein grundrechtlich geschützter Wert und zugleich legitimes deutsches Interesse bzw. unterstützendes Argument bei der Digitalisierung der deutschen Exportwirtschaft („Industrie 4.0."). Der EU-Gipfel Ende Oktober zur ‚Digitalen Agenda' wird weitere Ansatzpunkte aufzeigen.
4. Internet Governance: Die WCIT-Verhandlungen im Dezember 2012 in Dubai hatten bereits erste Risse bei der globalen Regelsetzung für Betrieb und Entwicklung des Internets aufgezeigt. Die jüngsten Entwicklungen „Post-Snowden" bergen das Risiko einer Fragmentierung, vulgo: Balkanisierung, des Internets. Für eine sich digitalisierende Exportnation wie Deutschland kann dies nicht in unserem Interesse sein. Der bisherige Narrativ der westlichen Welt

eines „free & open Internet leading to global economic and social benefits" hat jedoch beträchtlichen Schaden genommen, wie nicht zuletzt die Rede der BRA Präsidentin Rousseff vor der VN-GV zeigte. Kosmetische Änderungen bzw. Ergänzungen hieran werden den entstandenen Vertrauens- und Glaubwürdigkeitsverlust nur bedingt auffangen, stattdessen muss Transparenz, Rechtsstaatlichkeit und demokratische Kontrolle stärker betont werden. Am Rande der Cyber-Konferenz in Seoul (16.-17.10.) wird CA-B hierzu u.a. mit „EU-G5" (GBR, FRA, SWE, NLD, DEU) und US-Kollegen konsultieren. Beim anschließenden Internet Governance Forum in Indonesien (21.-23.10.) sollten wir Risse im „westlichen Camp" vermeiden, die u.a. CHN und RUS in der „Post-Snowden"-Zeit erhoffen. USA sind hier auf unsere anhaltende Unterstützung angewiesen; wir erwarten dafür Entgegenkommen beim Datenschutz; dies ist kein Paket, reflektiert aber den inneren Zusammenhang zwischen den Punkten.

III. Ansätze für AA („Was können wir tun?")

In den Extrempositionen einer US-dominierten Internetarchitektur vs. eines länderfragmentierten und somit seiner globalen Vorteile beraubten Internets besteht Notwendigkeit und Handlungsspielraum für deutsche Cyber-Außenpolitik. Aufgrund DEU Glaubwürdigkeit und Vertrauensvorteil können wir in alle Richtungen wirken und müssen dabei den Spagat wagen, um kontinental-europäische mit US-/GBR-Interessen zu versöhnen.

Wir wollen vermeiden, dass TTIP „in Geiselhaft" genommen wird. Gleichzeitig müssen wir jedoch klar machen, dass die jüngsten Forderungen aus dem 8-Punkte-Programm der BuRegierung zum besseren Schutz der Privatsphäre nicht qua Bundestagswahlen aufgehoben sind: besserer Datenschutz ist eine Forderungen aller deutschen Parteien. Unsere zum Datenschutz in die EU eingebrachten Forderungen haben Augenmaß und wurden von allen Ressorts gebilligt. Fortlaufende Snowden-Enthüllungen, die damit verbundene US-innenpolitische Debatte und der Einfluss der Firmen im Silicon Valley können evtl. einen langsamen Sinneswandel in den USA bewirken.

Gleichzeitig wollen wir einen „digitalen Graben" Nord-Süd vermeiden. Daher ist ein Outreach zu „Swing States" wie BRA und IND prioritär. BRA hatte die Reaktionen der BuReg auf die Snowden-Affäre intensiv verfolgt und stellte ähnliche Forderungen.

Wichtig bei alldem ist eine europäische Einbettung und Abstimmung: Mit allen EU-MS in der informellen Ratsformation „Friends of the Presidency on Cyber", regelmäßig und formlos als „G3" mit GBR und FRA – mit jeweils durchaus unterschiedlichen Interessen – bzw. als „G5"erweitert um NLD und SWE.

Weitere konkrete und zeitnahe Ansatzpunkte für uns sind:

- Aufsetzen einer AA-internen Arbeitsgruppe „Internet Governance" ab Oktober 2013: Teilnehmer Ref. 405 (ITU, ICANN u.a.), 603-9 (UNESCO), VN04 (UN Commission on Science and Technology for Development), 403, 500.
- Runderlass zur Benennung von „Cyber-Referenten" an ausgewählten AVen und Erstellung nationaler „Cyber-Sachständen", jeweils unter enger Einbindung der Länderreferate.
- Aufsetzen eines Transatlantischen Cyber-Forums unter Einbeziehung von Privatsektor und Zivilgesellschaft; hierzu Vorgespräch CA-B mit Cyberkoordinator im White House, Michael Daniel, Mitte November in Berlin.
- Fortführen des „Runden Tisches für Internet und Menschenrechte", gemeinsam mit MRHH-B unter Einbindung „digitaler Zivilgesellschaft"; Unterstützen des Projekts „Freedom Online House" in Berlin.
- Reaktivieren von Blogger-Reisen im Rahmen des Besuchsprogramms, v.a. für EGY und TUN (Rückfall in „vorrevolutionäre Internetzensur" vermeiden).
- Intensivieren des Kontakts mit deutschen Firmen, Verbänden, NGOs etc.
- Vereinbaren dreimonatiger Strategietreffen AA-BMI-BMBF-BMWi und BMVg.
- Ausarbeiten eines „Cyber-Themas" hin zur DEU G8-Präsidentschaft 2015, ggf. in Zusamenarbeit mit OECD.
- Abhalten internationaler Cyber-Events hier im Hause: Nach unseren Konferenzen zu Cybersicherheit 2011 (mit BMI), zu „Internet & Menschenrechte" 2012 (mit BMJ) und der von Abt. 5 geführten Fachtagung zum Völkerrecht im Cyberraum übernimmt AA im Juni 2014 Gastgeberrolle des „European Dialogue on Internet Governance/EuroDIG" (mit BMWi). Ferner gibt es bereits das Projekt eines „Cyber-Gipfels" in Zusammenarbeit mit dem East-West-Institut im IV. Quartal 2014 (hierzu folgt separate Leitungsvorlage nach DA des neuen BM). Für eine weitere Konferenz zur entwicklungspolitischen Dimension gab es bereits Sondierungsgespräche mit BMZ, aber noch keine Konkretisierung. Dabei bedarf dieses Thema (Stichworte: „ICT for development") verstärkter Aufmerksamkeit mit Blick auf das Gewicht der Schwellen- und EL in der oben skizzierten Debatte um Internet Governance.

403-9 hat mitgezeichnet, 2-B-1, E-B-1, 2A-B und 02 waren beteiligt.

gez. [redacted]