CDU/CSU-FRAKTION IM DEUTSCHEN BUNDESTAG

Arbeitsgruppe Innen

Die Freiheit des Internet sichern und erhalten

Positionspapier der Arbeitsgruppe Innen der CDU/CSU-Fraktion im Deutschen Bundestag

Beschluss der Arbeitsgruppe Innen vom 20. September 2011

Vorbemerkung

Kaum eine Technologie hat das Leben der Menschen und die Wirtschaft so verändert wie das Internet. Es ist nicht nur die ökonomische Dimension, die das Internet so wertvoll macht. Es ermöglicht den Menschen, sich aus vielen Quellen frei zu informieren und ebenso frei zu kommunizieren. Hieraus erwachsen ungeahnte Chancen für Freiheit und Menschenrechte. Kein Despot ist auf Dauer in der Lage, seine Schreckensherrschaft auf informationelle Abschottung aufzubauen. Das gesellschaftspolitische Potenzial des Internet geht aber hierüber hinaus. Es gibt unserer Demokratie neue Impulse. Nie konnten die Bürger sich so gut informieren und vernetzen wie heute.

Damit wird deutlich: Internet ist nicht eine Angelegenheit von Ökonomen, Spezialisten und selbsternannten Netzaktivisten. Es geht uns alle an, selbst dann, wenn wir das Netz nicht benutzen – oder irrtümlich glauben, es nicht zu nutzen.

Das Internet ist mehr als ein bloßes Medium, es kann ein Raum für bestimmte Bereiche des Zusammenlebens sein. Politik und Gesellschaft stehen vor der gemeinsamen Aufgabe, diesen virtuellen Raum so zu gestalten, dass er zum Nutzen aller wirkt und die Mehrheit der Menschen ein Grundvertrauen im Netz entwickeln. Ohne dieses Vertrauen kann die Menschheit nicht das enorme Potenzial des Internet für Freiheit und Wohlstand nutzen. Daraus folgt:

- Das Internet geht uns alle an – ob wir es nutzen oder nicht. Die Spielregeln des „Cyberspace“ können nur im rechtsstaatlichen Diskurs unserer freiheitlichen Demokratie gefunden werden. Die Gestaltung unserer Zukunft kann nicht einigen wenigen Meinungsmachern oder selbsternannten Netzaktivisten überlassen werden.

Das Internet muss Wohlstand und Freiheit dienen

Das Internet ist ein globaler Sozial- und Wirtschaftsraum. Technik und Regeln im Netz müssen so gestaltet werden, dass sowohl wirtschaftliche Interessen als auch Nutzerinteressen berücksichtigt werden. Viele der heutigen Geschäftsmodelle des Internet basieren auf der Grundannahme, dass Recht und Gesetz auch im Internet gelten und durchgesetzt werden. Ein solches, auch marktwirtschaftlich orientiertes Betriebsmodell des Internet, ist ohne brauchbare Alternative. Daraus folgt:

- Wer Mobbing, Betrug, Einbruch, Kinderpornografie oder Diebstahl als unvermeidliche Nebenwirkung einer unbeschränkten Freiheit im Internet akzeptiert, untergräbt das Vertrauen in das Netz.

- Ohne Vertrauen in das Netz, ohne Vertrauen auf die Durchsetzung von Recht und Gesetz auch im Internet, werden seine gesellschaftliche Akzeptanz und wirtschaftliche Nutzung stagnieren.

Der Staat gewährleistet Recht und Gesetz auch im Internet

Das Internet bietet unvergleichliche Möglichkeiten zur Ausübung der Grundrechte, wie etwa die freie Entfaltung der Persönlichkeit, die Berufs-, Presse-, Versammlungs- und Meinungsfreiheit. Es ist allererste Aufgabe des Rechtsstaates, diese Grundrechte zu achten und zu schützen.

Dazu muss unsere Rechtsordnung in geeigneter Weise auch im Internet durchgesetzt werden. Das Internet ist kein rechtsfreier Raum. Der Staat benötigt effektive Werkzeuge, um Rechtsverstöße im Internet zu unterbinden und zu ahnden und klare Regeln und Verfahren, die den Gebrauch solcher Mittel eingrenzen und kontrollieren. Hierüber ist eine offene und lebendige Debatte zu führen. Notwendig ist zudem, dass sich dann die für die Rechtsdurchsetzung verantwortliche Justiz mit den technischen Entwicklungen vertraut macht. Daraus folgt:

- Freiheit kann sich nur in Sicherheit entfalten. Das gilt auch im Netz! Freiheit muss ihre Grenzen dort finden, wo die Rechtsgüter anderer unrechtmäßig verletzt werden.

- Wo der Staat nicht die Grundrechte seiner Bürger auf Menschenwürde, körperliche Unversehrtheit, Meinungsfreiheit und Eigentum schützt, herrscht Anarchie und Terror. Dies gilt auch für das Internet.

- Der Staat muss auch im Internet handlungsfähig sein, Rechtsverstöße effektiv verfolgen und Gefahren abwehren.

- Dabei kann es im Internet ebenso wie in der realen Welt kein grundsätzliches Recht auf Anonymität geben, ebenso wenig wie es eine allgemeine Rechtspflicht für Nutzer gibt, ihre Identität ihrem Gegenüber zu offenbaren. Das tragende Prinzip einer offenen Gesellschaft ist, dass man mit seiner eigenen Identität am öffentlichen Meinungskampf teilnimmt. Wir brauchen eine solche Kultur der Offenheit und keine Foren, die sich in die Feigheit der Anonymität flüchten. Eine anonyme Teilhabe am politischen Meinungs- und Willensbildungsprozess ist abzulehnen.

- Davon zu unterscheiden ist die Frage, unter welchen Voraussetzungen der Staat erfahren können muss, wer sich hinter einem Anschluss im Internet verbirgt. Die Europäische Union hat sich nach langer und intensiver Diskussion für eine solche Möglichkeit durch die Schaffung von Mindestspeicherungsfristen entschieden. Diese Entscheidung gilt es nach wie vor auch bei uns umzusetzen.

Freiheit bedarf der Eigenverantwortung

Die Sicherheitsvorfälle der letzten Monate zeigen, dass das Internet kein gefahrloser Raum ist. Wie in der richtigen Welt gibt es Straftaten wie Betrug, Diebstahl, Spionage und Sabotage. Der Staat kann die Nutzung des Netzes dabei durch Sicherheitsstandards reglementieren und seinen Missbrauch verbieten und ahnden. Dabei gilt aber: Wenn wir das grundsätzliche Prinzip eines freien Internet und seiner Nutzer auch in Zukunft bewahren wollen, sind Eigenverantwortung und gesellschaftliche Normen des Anstands auch im Netz unverzichtbar. Neben der notwendigen Aufklärung der Nutzer, müssen auch die Unternehmen selbst in die Verantwortung genommen werden. Erforderlich sind die Entwicklung und der Ausbau der

Selbstregulierung über Kodizes. Darüber hinaus müssen Firmen und Behörden die Sicherheit ihrer Systeme ständig weiterentwickeln, Bürger und Verbraucher die verfügbaren Sicherheitsprodukte auch nutzen. Daraus folgt:

- Vor staatlicher Regulierung ist Selbstregulierung ein geeigneter Weg zur Wahrnehmung der Eigenverantwortung aller Akteure, insbesondere der Unternehmen. Fehlt es an einer geeigneten Selbstregulierung oder ist diese nicht ausreichend, muss der Staat die Rahmenbedingungen vorgeben.

- Unternehmen und Nutzer müssen zunächst eigenverantwortlich für die Sicherheit und den Schutz ihrer Daten im Rahmen ihrer Möglichkeiten Sorge tragen. Es ist nicht vorrangig Aufgabe des Staates, Bürger und Unternehmen vor den Folgen ihrer eigenen Fahrlässigkeit zu bewahren. Wer unsichere E-Mails schreibt, die Rotlichtbezirke des Internet frequentiert, seine Computer und Netze nicht gegen Viren und andere Schadprogramme schützt oder sein gesamtes Privatleben im Internet verbreitet, darf sich am Ende nicht über den Missbrauch seiner Daten wundern. Unternehmen müssen ihre Systeme sichern, um Datendiebstahl zu verhindern. Zu verhindern ist, dass Opfer durch unzureichende Sicherung, etwa im Rahmen eines Bot-Netzes, selbst zum ahnungslosen Mittäter weiterer Straftaten werden. Staatliche Regeln und Hilfe sind aber dann erforderlich, wenn Gefahren für die Allgemeinheit drohen oder der Einzelne mit dem Schutz seiner Systeme überfordert ist.

- Mit Sicherheitsempfehlungen kann der Staat allen Akteuren unter Beibehaltung ihrer Eigenverantwortung Angebote schaffen, die sowohl bei der Gefahrenabwehr den notwendigen Handlungsbedarf aufzeigen als auch bei der Sicherheitsgestaltung als Hilfe zur Selbsthilfe dienen. Allgemein akzeptierte Empfehlungen fördern das Vertrauen in die Sicherheit des Internets nachhaltig.

- Von besonderer Bedeutung ist die Verantwortung der Provider für die von ihnen an das Internet angeschlossenen Rechner. Kein Provider sollte Rechner am Netz lassen, von denen eine Gefahr ausgeht.

Das Internet ist eine kritische Infrastruktur, die besonderen Schutzes bedarf

Das Funktionieren von Staat und Wirtschaft ist aufgrund der vernetzten Prozesse längst vom Internet abhängig. Das Internet ist damit ebenso eine kritische Infrastruktur wie die Wasser- und Energieversorgung. Angriffe auf diese Infrastruktur bedrohen den Staat und das Gemeinwesen insgesamt.

Der Schutz dieser kritischen Infrastruktur gegen Sabotage und Spionage ist eine Aufgabe, die Staat und Wirtschaft nur gemeinsam lösen können. Zuerst ist zu fordern, dass die Betreiber und Nutzer dieser kritischen Infrastruktur, wie öffentliche Verwaltung und Wirtschaft, alles unternehmen, was möglich und zumutbar ist, um sich gegen Spionage und Sabotage im Netz zu schützen.

Das hohe Schadenspotenzial dieser kritischen Infrastruktur gebietet aber auch, dass der Staat dort wo es erforderlich ist Mindestsicherheitsanforderungen vorgibt und angemessene Fähigkeiten entwickelt, verbleibende Risiken wirksam zu minimieren. Angesichts eines hohen möglichen Schadens sollte keine rechtlich zulässige Gegenwehroption ausgeschlossen werden. Daraus folgt:

- Cyberwar und Cyberterror sind keine Fiktion, sondern können Realität werden. Ein Angriff auf das Internet kann die Kommunikationsstränge von Staat und Wirtschaft zerstören – mit unabsehbaren Folgen für uns alle.

- Auch wenn der Schutz vor Sabotage im Internet eine gesamtstaatliche Aufgabe ist, gilt: Wenn öffentliche Verwaltung und Wirtschaft sich vom Internet abhängig machen, müssen sie sich auch in eigener Verantwortung und auf eigene Kosten schützen, soweit dieses technisch machbar ist.

- Hoheitliches Handeln ist dann erforderlich, wenn die Nutzer und Betreiber des Internets mit dem Schutz überfordert sind. Angesichts der Folgen eines digitalen Angriffs darf dann auf keine Option zur Gefahrenabwehr verzichtet werden.

- Da kritische Infrastrukturen überwiegend von privaten Unternehmen betrieben werden, die innerhalb der Europäischen Union untereinander im Wettbewerb stehen, bedarf es EU-weiter Mindeststandards für die IT-Sicherheit. Rein nationale Vorgaben laufen Gefahr, den Wettbewerb zu verzerren. Dies kann etwa durch harmonisierte Haftungsrege-

lungen und EU-weite Selbstverpflichtungen hinsichtlich bestimmter *Best Practices* verhindert werden.

- Weiterer Handlungsbedarf auf europäischer Ebene besteht in der Schaffung EU-weiter *Computer Emergency Response Teams* (CERTs), die der Frühwarnung über neue IT-Risiken, Schwachstellen und Schadprogramme dienen. Sie sind der geeignete Mechanismus, um Erkenntnisse auszutauschen und Betroffene in geeigneter Weise zu warnen. Daher sollte jeder Mitgliedstaat der Europäischen Union über ein nationales CERT verfügen, die dann untereinander zu vernetzen wären.

Das Internet ist eine der zentralen Herausforderungen für Politik und Gesellschaft

Das Internet und die heute noch unabsehbare technische Entwicklung wird Politik und Gesellschaft immer wieder vor neue Herausforderungen stellen. Die Politik darf den Fragen, die sich daraus ergeben, nicht ausweichen. Sie muss grundlegende Weichenstellungen selbst vornehmen, ohne nur die technische Entwicklung nachzeichnen zu wollen. Der aus dem technischen Wandel resultierende Handlungsbedarf muss sorgfältig aufbereitet werden, die erforderlichen Schlüsse sind zu ziehen und notwendige gesetzgeberische Maßnahmen müssen zügig erfolgen.

Bisher war die Politik Zaungast einer vermeintlich unaufhaltsamen technischen Entwicklung. Es sollte eine wissenschaftliche Einrichtung geschaffen werden, die alle Aspekte des Mediums Internet grundlegend aufarbeitet und durch die Berücksichtigung aller relevanten Wissenschaftsdisziplinen eine laufende Beobachtung und Bewertung neuer technischer Entwicklungen vornehmen kann. Nur so kann verantwortungsvolle Politikberatung geleistet werden.