Dankesworte

(Sprechzettel)

von

Toomas Hendrik Ilves

Staatspräsident der Republik Estland a.D.

anlässlich des

Reinhard Mohn Preises 2017

Smart Country – Vernetzt.Intelligent.Digital.
Smart Country - Connected.Intelligent.Digital.

29. Juni 2017

Theater Gütersloh

Es gilt das gesprochene Wort.

Frau Mohn,
Vorstand der Bertelsmann Stiftung,
Freunde,

es ist mir eine große Ehre, den Reinhard Mohn Preis 2017 zu erhalten.

Was Estland im vergangenen Vierteljahrhundert erreicht hat, ist das Ergebnis der Arbeit vieler Menschen. Ich habe skizziert, was damals als skurrile und unmögliche Vision galt, aber so viele kluge Menschen haben sich der Idee angenommen und bald darauf preschte Estland allein voran. Ein Funke genügte, um eine Fackel zu entzünden, die von Vielen getragen wurde. Nennen wir es Zeitgeist – eines der wenigen deutschen Wörter, die Englisch sprechenden Menschen geläufig sind.

Manchmal, wenn gute Ideen mit einfältiger, altmodischer oder wenig sachkundiger Politik zu kämpfen hatten, tat ich mein Bestes, um den Weg für diese Ideen und ihre Weiterentwicklung frei zu machen und denjenigen, die gegen sie waren, einen Schubs zu geben, damit sie diesen Ideen eine Chance gaben. Wenn gute Ideen Ermutigung brauchten, erinnerte ich mich immer daran, wie schwierig es 1995 war, mit einer skeptischen – wenn nicht sogar feindlichen – Öffentlichkeit über Digitalisierung zu sprechen und manchmal auch mit nicht überzeugten Regierungen. Das ist heute schwer vorstellbar, da “e-Estonia” die überwältigende Zustimmung der Öffentlichkeit genießt, ganz unabhängig davon, welche Partei an der Regierung sein mag. Deshalb bedanke ich mich bei all den mutigen und kreativen Menschen, die so viel dazu beigetragen haben, Estland zu dem zu machen, was es heute ist.

Seit ungefähr einem Jahr ist die digitale Welt wesentlich beängstigender geworden als zuvor. Wir lesen täglich von Hacks, Datendiebstahl und Eingriffen in die Privatsphäre. Wir sehen, wie unser eigenes demokratisches System in Formen, die vor einem Jahr-

zehnt als unvorstellbar und unmöglich galten, angegriffen wird. Die Server des Bundestags, von Emmanuel Macrons Wahlkampagne und des Democratic National Committees werden gehackt und Privatkorrespondenz wird gestohlen. Diese wird online gepostet, manchmal in veränderter Form, was wiederum „Fake News“ erzeugt. Roboter oder Bots in den sozialen Medien leiten diese fingierten oder verfälschten Geschichten und Falschmeldungen an Millionen Konten weiter, die sie dann weiter verbreiten. Die sozialen Medien wiederum erlauben es Big-Data-Analyseunternehmen, Profile von Einzelpersonen zu erstellen und sie gezielt in nie zuvor dagewesener Weise anzusprechen. Und schließlich (zumindest zu dem Zeitpunkt, an dem diese Rede geschrieben wird) werden Wahlen gehackt und Wählerdaten von einer ausländischen Regierung gestohlen. Mit welchem Ziel? Wir wissen es noch nicht.

Diese von mir gerade aufgezählten Vorfälle besorgen uns. Einige, die Ludditen, wollen stehen bleiben und die Uhren auf das Papierzeitalter zurückstellen. Andere hingegen wollen aus unterschiedlichen Gründen die „Sicherheit“ erhöhen, indem sie unsere Freiheiten und Privatsphäre einschränken. Und dann gibt es jene, die die erforderlichen Schritte nicht unternehmen wollen, um sowohl unsere Wahl-Demokratie als auch unsere Sicherheit im digitalen Zeitalter zu garantieren – alles aufgrund eines Mangels an Verständnis.

Lassen Sie mich das deutlich aussprechen: Die Sicherheit im Cyberspace geht nicht und darf auch nicht auf Kosten von Freiheiten gehen. Und Estland beweist das. Vergangene Woche veröffentlichte die International Telegraph Union der Vereinten Nationen, heute besser bekannt als ITU – die für Internetangelegenheiten zuständige UNO-Organisation –, ihre Studie über die weltweite Cybersicherheit. Estland ist darin die Nummer Eins in Europa, besser als jedes andere Land in Europa, wobei die Nummer Zwei – Norwegen – nicht einmal in der EU ist.

Die Internet-Sicherheit ist jedoch nicht zu Lasten der Freiheit entstanden. Freedom House listet in seiner Studie Estland als weltweite Nummer Eins in Sachen Internetfreiheit. Die Internetfreiheit in Russland wird andererseits als „unfrei“ eingestuft, weshalb Russland auf Platz 65 von 88 untersuchten Ländern liegt.

Natürlich kann man Cybersicherheit auf unterschiedliche Weise erreichen. Russland zum Beispiel ist die Nummer Eins in der GUS, dem postsowjetischen Raum. Umso mehr Anlass, andere Maßnahmen wie z. B. die Internetfreiheit zu untersuchen, um das Zusammenspiel zwischen Sicherheit und Freiheit zu beurteilen – etwas, das zu oft als Zielkonflikt abgetan wird.

Was diese Studien zusammengefasst deutlich zeigen, ist die Tatsache, dass zwischen Sicherheit und Freiheit nicht zwingend ein Zielkonflikt oder ein Abhängigkeitsverhältnis besteht. Man kann beides haben. Sich dessen bewusst zu sein, ist besonders wichtig inmitten der Flut von Vorschlägen im gesamten demokratischen Westen, dass Kompromisse bezüglich der Freiheit im Internetzeitalter notwendig seien, um die Sicherheit zu garantieren. Die britische Regierung, der amerikanische Justizminister Jeff Sessions und die EU-Justizkommissarin Věra Jourová wollen „Backdoors“ anordnen, Kodierungsschlüssel in den Händen von Regierungen (oder der EU-Kommission). Es wimmelt vor entsprechenden Vorschlägen.

Natürlich ist dieser Rückgriff auf „Backdoors“ das Ergebnis einer Serie von Terroranschlägen in Europa und den USA, bei denen behauptet wird, dass die Terroristen Verschlüsselung nutzten, um das Belauschen ihrer Kommunikation durch die Behörden zu vereiteln. Die Reihe peinlicher Enthüllungen, dass die Behörden über bestimmte, bekannte Terroristen vorgewarnt waren (bei den Anschlägen in Brüssel, Berlin und zuletzt London), wird außer Acht gelassen – die Politiker fordern dennoch „Backdoors“.

Solche Vorschläge sind selten begründet. Erstens hindert niemanden etwas daran, ein anderes Verschlüsselungssystem zu verwenden, selbst wenn auf der einen oder anderen „App“ „Backdoors“ installiert werden. Die einzigen, die von „Backdoors“ betroffen wären, sind diejenigen, die keine terroristischen Absichten hegen, jedoch ihre Privatsphäre wertschätzen – die, wie wir wissen, weder beim Telefonieren noch beim Versenden von SMS gewährleistet ist.

Zweitens: Sobald eine Regierung oder, noch absurder, die Europäische Kommission eine „Backdoor“ verabschiedet, wird diese zum Heiligen Gral aller Hacker. Was könnte für das Prestige oder finanzielle Vorteile wohl verführerischer sein, als die Schlüssel zum Königreich zu stehlen? Würden wir wirklich die Europäische Kommission oder irgendeine nationale Regierung diesbezüglich betrauen, die Schlüssel zu jedweder verschlüsselten Kommunikation in Händen zu halten? Wenn selbst der CIA gehackt wurde und eine Reihe von Zero-Day-Angriffen gestohlen wurden, die es neuerdings Kriminellen ermöglichen, die WannaCry-Ransomware zu verbreiten, die unter anderem das nationale Gesundheitssystem in Großbritannien zum Erliegen brachte?

Sie müssen sich auch nicht vor gut ausgebildeten IT-Hackern fürchten, die in Systeme eindringen könnten. Wie die NSA-Angestellten Edward Snowdon und vor kurzem Reality Winner gezeigt haben, gibt es auch „Insider Threats“, also jemanden im System, der aus persönlicher Verärgerung, ideologischen oder finanziellen Gründen die Schlüssel, den Heiligen Gral, einfach stehlen kann. Eine neuere Sammlung von Matthew Brunn und Scott Sagan belegt, dass Organisationen die Gefahr des Eindringens von innen – nicht von außen – erheblich unterschätzen. Die Wirkung hierbei ist dieselbe wie bei einem Hack: Irgendjemand erhält die Schlüssel zu allen verschlüsselten Kommunikationen, mit Ausnahme derer, die wirklich verschlüsseln wollen und sowieso Alternativen nutzen.

Was können wir daraus ableiten? Zum einen besteht ein erschreckender Mangel an Nachdenken über die Folgen der von Regierungen angeordneten „Backdoors“. Was

mir als ehemaligem politischen Leader auffällt, ist, dass meine Kollegen nicht wirklich verstehen, was sie vorschlagen – die Unmöglichkeit und Undurchführbarkeit solcher Vorschläge.

Um dieses Thema verstehen zu können, muss ich auf Estland und eine Lektion zurückkommen, die ich wiederholt gelernt und im World Bank Development Report des vergangenen Jahres – Digital Dividends, für dessen Produktion ich die Ehre hatte, als Mitvorsitzender mitzuwirken – empirisch dargestellt habe.

Die Lektion ist folgende: Wie wir diese „Schöne neue digitale Welt“ angehen, ist eine analoge Aufgabe. Es geht um Politik, Gesetze und Vorschriften.

Hier kommt eine dritte Studie ins Spiel. Ja, Estland hat die größte Internetfreiheit der Welt und es hat die beste Cybersicherheit in Europa – aber eine dritte Studie, der Digital Economy and Society Index 2017 der Europäischen Union, bewertet Estland als Nummer Eins bei der Online-Bereitstellung öffentlicher Dienste.

Mit anderen Worten: in dieser Hobbesschen Welt des Internets sind die Esten sowohl sicherer als auch freier, da wir dafür gesorgt haben, unseren Bürgern Sicherheit zu bieten, wo es darauf ankommt, und sie frei sein lassen, wo kein Anlass besteht, eine falsche Sicherheit aufzuzwingen.
Lassen Sie mich kurz ausführen, was ich für notwendig halte:

1. Man braucht einen starken digitalen Identitätsnachweis, der von der Regierung ausgegeben wird – im Fall Deutschlands von den Ländern oder Berlin. Heute können kriminelle Akteure nicht physisch, sondern online in Ihr Leben treten. In der physischen Welt fordern und stellen Regierungen Ausweise aus, um zu wissen, wer wer ist.
In der digitalen Welt ist es dasselbe. Man braucht einen starken digitalen Identitätsnachweis.

2. Um die Vorteile der Digitalisierung genießen zu können, muss man dieser digitalen Identität einen legalen Status geben, d. h. die digitale Signatur der physischen Signatur gleichstellen. Alle Transaktionen, die eine physische Signatur erfordern, müssen mit einer digitalen Signatur möglich sein. In Estland gibt es nur zwei Transaktionen, die physisch und in Anwesenheit von Zeugen geleistet werden müssen: die Heirat und die Scheidung. Um das jedoch zu tun, muss man den digitalen Identitätsnachweis mit einem nationalen Register verknüpfen, so wie es bei Ausweisen gemacht wird. Diese Verknüpfung gibt es in Deutschland nicht, es gibt keine Bürgerkarte wie z. B. in Österreich, und deshalb können Sie keine digitalen Verträge abschließen.

3. Dieser Identitätsnachweis muss obligatorisch und allgemein-gültig sein. Warum? Wenn er optional ist, werden optimalerweise 15-20 Prozent der Bevölkerung ihn wollen. Betrachten Sie es aus Sicht des privaten Sektors oder sogar einer Regierung: Nur 15% der Bevölkerung könnten dann möglicherweise eine Dienstleistung wie z. B. digitale Rezepte nutzen. Weshalb also Geld und Zeit verschwenden, um die Dienstleistung zu entwickeln, wenn 85% der Bürger sie nicht einmal nutzen können? Aus der Sicht von Unternehmen oder der Regierungspolitik werden sie das aber tun, wenn er entwickelt wird. In Estland ist die Zahl der Nutzer digitaler Rezepte in vier Monaten von vereinzelten Nutzern auf über 98% gestiegen. Niemand benutzt mehr Papierrezepte ... außer den Touristen.

4. Nutzen Sie die Macht des Ausweises, um die Bürokratie zu transformieren. Die Bürokratie ist ungefähr 5000 Jahre alt – aber eines hat sich nie geändert: sie war immer ein serieller Prozess. Ein Dokument – ob in Hieroglyphen auf Papyrus oder heute auf Papier, oder sogar als Email-Anhang – geht zuerst zu einem Amt, auf dem es genehmigt wird, dann zum nächsten und übernächsten Amt, und so weiter. Eins nach dem anderen. Seriell. Mit einem digitalen Ausweis finden alle erforderlichen Recherchen parallel statt. Deshalb gibt es in Estland eine „Once-Only“-Vorschrift; die Regierung darf Sie nie um eine Information bitten, die ihr bereits vorliegt. Und deshalb können

Sie in Estland in 15 Minuten eine Firma eintragen – wohlgemerkt mit allen Überprüfungen und Kontrollen, die andere EU-Staaten identisch durchführen; dort dauert dieser serielle, manuelle Prozess jedoch oft Monate.

5. Die Interaktionen mit diesem Ausweis müssen hochsicher sein. Ich will nicht ins Detail gehen, aber wir haben eine Verschlüsselung mit RSA 2048, von der ich garantieren kann, dass sie zurzeit nicht zu knacken ist. Sie muss auch vor der Regierung sicher sein. Wir wissen, dass unser System funktionieren kann, wenn – und nur wenn – die Bürger wissen, dass die Regierung ihre Daten nicht einsehen kann. Wenn die EU eine „Backdoor" verabschiedet, die die verschlüsselten Daten von Bürgern Estlands beinhaltet, wird unser System zusammenbrechen. Die Bürger müssen darauf vertrauen können, dass ihre Daten privat bleiben.

6. Man braucht die richtige Backend-Architektur. Das Backend ist in der Tat das Rückgrat des Systems. Wir nutzen eine verteilte Datenaustauschschicht, was bedeutet, dass jede Interaktion direkt zwischen Nutzer und Server stattfindet und jedes Mal authentifiziert wird. Das bedeutet auch: Wenn Sie drin sind, sehen Sie das, wofür Sie authentifizert sind, aber Sie können darüber hinausgehend nichts sehen. Sie können die Daten von Anderen nicht sehen – was heißt: Sie können die Daten Anderer nicht stehlen.

Alle dieser Lösungen sind technisch und digital, aber alle diese Lösungen erfordern das Analoge: Politik, Gesetze und Vorschriften. Das ist der schwierige Teil – die Technologie ist einfach. Die Technologie ist überall und sie ist erstaunlich günstig. Jede Regierung oder jeder Staat kann die Technologie bekommen. Zudem ist unsere Technologie in Wahrheit alt, das heißt: wir machen heute wenig, was vor 25 Jahren nicht bereits möglich gewesen wäre. Außer, dass es damals nicht umgesetzt wurde.

Was aber erklärt dann den großen Unterschied zwischen einzelnen Ländern, sogar in Europa? Es ist die Bereitschaft der politischen Entscheidungsträger, Politik zu machen, der Gesetzgeber, Gesetze zu erlassen, und der Regulierungsbehörden, die den Rückhalt der Gesetze haben, Vorschriften zu erlassen.

Die Technologie ist digital, Gesellschaften sind analog. Leider sind sie viel zu lange als unterschiedliche Bereiche betrachtet worden.

Lassen Sie mich zwei Beispiele nennen:

1. Die App vor Snowden – die Rückverfolgung Ihrer Bewegungen über Mobiltelefondaten;
2. Wieviel ist 2 hoch 3?

Diese Kluft zwischen Wissenschaft und Demokratie oder zwischen IT und Politik ist das, was ich im vergangenen Vierteljahrhundert versucht habe, zu überbrücken.

1959 hat ein britischer Physikochemiker in Cambridge, C. P. Snow, der zufälligerweise auch Schriftsteller war und den Begriff der „Korridore der Macht“ prägte, einen Essay über diese zwei Welten mit dem Titel „The Two Cultures“ – „Die zwei Kulturen“ – veröffentlicht.

Seine Metapher: die Esstische in seinem College in Cambridge.

Er war der Einzige, der an beiden Tischen Platz nehmen konnte.

Heute ist das, was Snow als Problem der Universität beschrieb, ein Problem für uns alle. Damals schauten uns Fernsehgeräte nicht an und Telefone hörten nicht zu oder verfolgten unsere Bewegungen.

Heute tun sie das. Oder sie können es. Dies sind politische, nicht technische Themen.

Damals kam die Propaganda ausländischer Gegner nicht wirklich beim Durchschnittsbürger in westlichen Demokratien an.

Heute tut sie dies durch die sozialen Medien. (Tatsächlich veröffentlichte Facebook erst vor Kurzem ein Whitepaper und gab zu, dass es bei der Wahl 2016 manipuliert wurde.)

In der Tat wurden und werden digitale Mittel eingesetzt, um den Wahlverlauf zu beeinflussen – nicht nur im letzten Jahr in den USA, sondern auch in laufenden und kommenden Wahlen in Europa.

Dies ist ganz bestimmt ein politisches Thema. Es ist ein so grundlegendes politisches Thema, wie es das in einer Demokratie nur sein kann.

Ich will also hiermit schließen: mit dem Aufruf an politische Entscheidungsträger zu lernen, worum es bei der Technologie geht, und an die Computerfreaks, die die Programme, Algorithmen und Apps entwerfen, die wir benutzen, zu lernen, was eine liberale Demokratie ist – zu verstehen, dass die drei Pfeiler liberaler Demokratien in diesem neuen digitalen Zeitalter erhalten werden müssen: freie und gerechte Wahlen, Rechtsstaatlichkeit sowie grundlegende Rechte und Freiheiten.