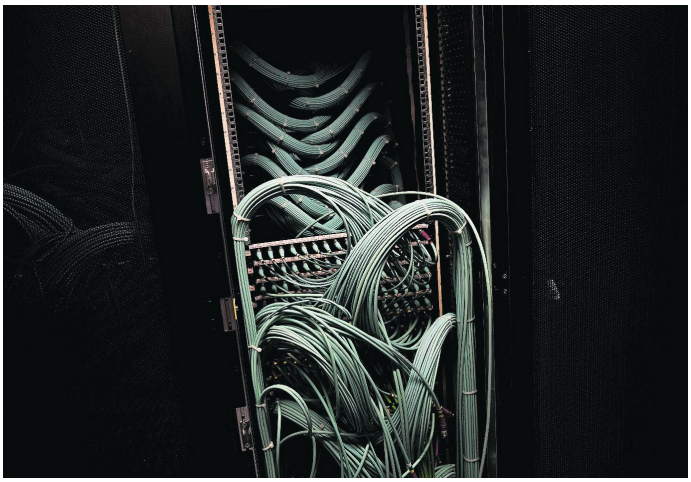

Den Kabelsalat zu ordnen, ist zwar hilfreich, doch nicht die Lösung: Wie lassen sich aggressive Akteure im Cyberspace bändigen? DYLAN MARTINEZ / REUTERS

Den Cyberkrieg nicht eskalieren lassen

Der grossangelegte Cyberangriff auf die USA kommt einem Weckruf gleich. Wie man solch aggressive Akte verhindern kann und wie man ihnen begegnen soll, bleibt unklar. ***Gastkommentar von Paul Meyer und Daniel Stauffacher***

Die USA sind jüngst Opfer eines Cyberangriffs erschütternden Ausmasses geworden: Mittels eines kompromittierten Software-Upgrades hatte sich ein ausländischer Akteur Zugang zu einer Vielzahl sensibler Daten verschafft. Über 18 000 Organisationen innerhalb und ausserhalb der Regierung hatten die Software installiert, und es dauerte sechs Monate, bis die Sicherheitslücke erkannt wurde.

Wie viele Daten entwendet wurden, wird sich nie exakt eruieren lassen. Die amerikanischen Verantwortlichen für Cybersicherheit stehen vor der gewaltigen Aufgabe, die unerwünschten Eindringlinge aus den Computersystemen zu entfernen und zu verhindern, dass die Angriffe im Verborgenen weitergehen. Die Attacke wurde extrem raffiniert durchgeführt, wie in einem Spionage-Thriller. Und genau das war es auch – ein Spionage-Akt, der aller Wahrscheinlichkeit nach vom russischen Auslandsgeheimdienst durchgeführt wurde.

Ex-Präsident Trump spielte die Bedeutung des Cyberangriffs jedoch herunter und unterstellt, dass nicht Russland, sondern China dafür verantwortlich sei. Die Haltung von Jon Biden ist kämpferischer. Er hat versprochen, dass die Verantwortlichen für ihre Taten bezahlen werden, und erklärt, dass eine gute Verteidigung nicht ausreiche: Die USA müssten ihre Gegner davon abhalten, solche Cyberangriffe überhaupt durchführen zu können. Der Aktivismus solcher Ansagen mag beruhigend wirken, birgt aber auch das Risiko einer weiteren Eskalation. Es bleibt unklar, was ein «signifikanter Cyberangriff» ist und wie eine verhältnismässige Reaktion genau aussehen müsste.

Bidens Aussage macht auch deutlich, dass der Begriff «Cyberangriff» oft pauschal eingesetzt wird. Es sollte künftig besser zwischen den Aktivitäten unterschieden werden; korrekter wäre, sie insgesamt als «offensive Cyberoperationen» zu bezeichnen.

Dabei sind drei Haupttypen zu identifizieren: Eine Computer Network Exploitation (CNE) ist eine Aktion, die darauf abzielt, in ein fremdes Computersystem einzudringen und diesem Daten zu entnehmen, ohne dass die Betreiber des Systems dies merken. Eine Computer Network Attack (CNA) hat das Ziel, Daten im System zu stören, zu beschädigen oder sogar zu löschen. Informationsoperationen (IO) wiederum sind Cyberaktivitäten, die darauf abzielen, die Meinung der Bürger in einem Staat im Interesse eines angreifenden (staatlichen) Akteurs zu manipulieren.

Auch die Zivilgesellschaft und der private Sektor äussern zunehmend Besorgnis über unverantwortliche Handlungen staatlicher Akteure im Cyberspace. Dies unterstreicht die Notwendigkeit internationaler Zusammenarbeit. Um Cyberbedrohungen entgegenzutreten, muss für jeden der drei erwähnten offensiven Cyberangriffe eine geeignete Strategie formuliert werden. Die grösste Bedrohung für den zivilen Bereich stellen die CNA dar. Sie können wichtige öffentliche und zivile Dienste und Infrastrukturen beschädigen. Solche Attacken sind im Übrigen auch für die Angreifer schwer zu kontrollieren. Man denke an die Cyberoperationen «Not Petya» und «Wanna Cry» der letzten Jahre.

Der normative Rahmen, der die internationalen Cyberaktivitäten regeln soll, ist erst in Entwicklung.

Internationale Übereinkünfte bei «Informationsoperationen» haben es schwer, denn die Propaganda des einen ist die Meinungsfreiheit des anderen.

Seit 2015 hat man sich bei der Uno auf elf freiwillige Verhaltensnormen geeinigt. Erwähnenswert ist die Norm, die kritische öffentliche Infrastrukturen davor schützt, Ziel von Angriffen zu werden. Die Biden-Administration sollte sich für ein bilaterales amerikanisch-russisches (oder mit China sogar ein trilaterales) «Waffenstillstands»-Abkommen einsetzen, das für CNA-Operationen gelten würde.

Eine wachsende Bedrohung stellen auch Informationsoperationen dar, insbesondere weil sie eine massive Verbreitung von «Fake-News» ermöglichen. Internationale Übereinkünfte in diesem Bereich haben es schwer, denn die Propaganda des einen ist die Meinungsfreiheit des anderen. Nationale Regulierungen oder Kontrollmechanismen durch die Eigentümer von Social-Media-Plattformen stellen zumindest kurzfristig die praktikabelste Lösung dar. Langfristig wäre ein Verbot von Cyberoperationen anzustreben, die sich gegen Wahlinfrastruktur oder Wahlprozesse richten.

Bezüglich CNE ist wenig zu erwarten. Spionage ist ein bewährtes staatliches Mittel und hat sich bisher der Kontrolle der internationalen Gemeinschaft entzogen. 2015 hatten sich die USA und China auf eine Einschränkung des Cyberdiebstahls von geistigem Eigentum und Firmendaten geeinigt. Es wurde jedoch nach der Erhöhung der Spannungen nicht weitergeführt. Es ist anzunehmen, dass die US-Regierung keine Massnahmen unterstützen wird, die auch ihre eigenen ausländischen Cyberaktivitäten einschränken könnten.

Der Cyberspace ist unerlässlich für das Wohlergehen moderner Gesellschaften. Er ist jedoch anfällig für Missbrauch durch böswillige private Akteure sowie durch sich aggressiv gebärdende Staaten. Auf einen wirksamen Schutz vor Hacking kann nicht verzichtet werden.

Paul Meyer ist ehemaliger Botschafter von Kanada und ausserordentlicher Professor an der Simon-Fraser-Universität. **Daniel Stauffacher** ist ehemaliger Delegierter des Bundesrats, Botschafter der Schweiz und Gründer des Think-Tanks ICT4Peace.

E-ID: Dient der Bund nur noch als Datenlieferant?

Die Identifikation der Bürger ist eine Kernkompetenz des Staates, die Ausstellung der E-ID ein zentrales Element von E-Government. Dies darf nicht an Privatunternehmen delegiert werden. ***Gastkommentar von Jörg Mäder***

Am 7. März stimmen wir über die E-ID, die elektronische Identität für die Einwohnerinnen und Einwohner der Schweiz, ab. Dabei ist die wichtige und grundlegende Frage, welche Funktion die E-ID erfüllen soll. Um dies zu klären, beginnen wir mit einer Erklärung am besten in der realen, analogen Welt: Wer am Kiosk ein Brötchen kaufen will, braucht Bargeld, mehr nicht. Im Fitnessklub ist eine Mitgliederkarte und am Bancomat noch zusätzlich ein PIN-Code nötig. Am anderen Ende des Spektrums wäre der Reisepass, der international anerkannt ist, darauf folgt die Identitätskarte. Die ID kann auch zum Reisen benutzt werden, dient primär aber dazu, sich bei amtlichen Geschäften korrekt auszuweisen. Zudem gibt es einige privatwirtschaftliche Geschäfte, die einen amtlichen Ausweis erfordern, beispielsweise das Eröffnen eines Bankkontos oder das Abschliessen eines Handyabos.

In der digitalen Welt ist es ähnlich. Die meisten Webseiten kann man einfach so besuchen, für Newsletter reicht meist eine E-Mail-Adresse, bei Shops sind es oft Name und Passwort, und bei der Bank kommt eine Zwei-Faktor-Authentifizierung hinzu. Dabei helfen Passwortmanager bei der Aufbewahrung der unterschiedlichen Passwörter für die verschiedenen Dienste. Das alles gibt es bereits.

Was fehlt, ist die Möglichkeit, sich gegenüber einer Behörde oder einer Firma online auszuweisen: eine Identitätskarte für die digitale Welt. Eine E-ID dient entsprechend dem Nachweis der eigenen Identität in der virtuellen Welt, wie es auch der Bundesrat als Ziel definiert hat. So enthält die E-ID auch die üblichen amtlichen Personenidentifizierungsdaten wie den amtlichen Namen, das Geburtsdatum, den Geburtsort oder das Bild des Gesichts. Nicht aber die Postadresse.

Die E-ID ist gegenwärtig noch kein international anerkanntes Reisedokument. Bereits gibt es jedoch Bestrebungen wie ID2020 oder die Known Traveller Digital Identity (KTDI), welche Reisedokumente digitalisieren möchten. Es ist eine Frage der Zeit, bis mit einer elektronischen Identität auch gereist – oder zumindest am Postschalter der eingeschriebene Brief abgeholt – werden kann.

Hingegen ist für das Abschliessen von Verträgen und das Nutzen von Dienstleistungen in den meisten Fällen kein Ausweis nötig. Dies muss auch online so bleiben. Eine staatliche E-ID soll für private Online-Portale dann nutzbar sein, wenn solche Anforderungen zur Identifikation oder Vertragserfüllung bestehen. Es ist aber kein Gesetz nötig, das ein universelles Log-in schafft, welches auf möglichst vielen Websites funktioniert – wie die bereits bestehende SwissID von SwissSign als bestes Beispiel zeigt. Zudem könnte ein Grossteil der Log-ins nicht durch eine Schweizer E-ID abgelöst werden, da es keine internationale Lösung ist.

Stellen Sie sich vor, Sie möchten einen Betreibungsregisterauszug auf der Gemeinde abholen. Hierzu müssen Sie sich ausweisen und holen entsprechend Ihre ID hervor. In dem Moment, da Sie diese überreichen wollen, drängt sich ein Mitarbeiter einer privaten Firma dazwischen, nimmt Ihnen den Ausweis ab, ruft kurz in seiner Firma an, prüft die Angaben, notiert sich den Vorgang in sein Notizbuch und bestätigt anschliessend dem Verwaltungsangestellten Ihre Identität. – Das würden wir nie akzeptieren. Genau dies ist jedoch das Konzept des beschlossenen E-ID-Gesetzes. Private sollen die E-ID entwickeln, herstellen und betreiben. Der Bund verkommt zum Datenlieferanten bei der Ausstellung einer neuen E-ID und nimmt lediglich eine Kontrollfunktion wahr. Die Identifikation der Bürgerinnen und Bürger ist jedoch eine grundlegende Kernkompetenz des Staates und die Ausstellung der E-ID ein zentrales Element von E-Government. Diese Aufgabe muss daher weiterhin vom Bund wahrgenommen werden. Er muss für das nötige Vertrauen und schliesslich die Akzeptanz in der Bevölkerung sorgen. Diese hoheitliche Aufgabe soll und kann nicht an Privatunternehmen delegiert werden.

Der Kanton Schaffhausen hat 2018 eine E-ID eingeführt. Die Infrastruktur wird vom Informatikunternehmen von Kanton und Stadt Schaffhausen (KDS) betrieben. Die persönlichen Daten werden dezentral bei den Nutzerinnen und Nutzern gespeichert. Die Lösung wurde von einer privaten Firma eingekauft. Liechtenstein hat 2020 – nur gerade ein Jahr nach der Ausschreibung – eine staatliche E-ID eingeführt. Erst der Einbezug der Privatunternehmen macht ein ausführliches Gesetz, Verordnungen und weitere Regulierungen nötig. Eine E-ID vom Staat wäre schlanker sowie einfacher und rascher umzusetzen.

Lassen Sie es mich wie folgt zusammenfassen: Ein Sportler, der auf dem Fussballfeld bestehen will, muss nicht wissen, wie man einen Fussballschuh herstellt, aber wohl, wie man ihn anzieht und bindet. Ein Staat, der auf dem digitalen Feld bestehen will, muss nicht wissen, wie man eine E-ID programmiert und herstellt, aber sehr wohl, wie man sie betreibt. Am 7. März gilt es, genau das von Bundesbern einzufordern und deshalb das E-ID-Gesetz abzulehnen.

Jörg Mäder ist freischaffender Programmierer und Nationalrat (glp., Zürich).