Forum

Schattengefecht um Schweizer Digitaldepartement

Entscheidend ist nicht die Form, sondern die Umsetzungskapazität

DOMINIQUE URSPRUNG, ZHAW School of Management and Law
NICOLAS ZAHN, Digitalisierungsexperte

Abstract The experience of various European countries shows that it is not the name of a new governmental unit or its place in the organisational chart that matter. The decisive factor is its ability to implement digital transformation in the country's public administration. Yet, in Switzerland, the current debate is about whether a state secretariat or a federal office for cybersecurity is needed and to which ministry the new entity should belong. We argue that this debate distracts from more important questions, such as what resources, competencies, and leverage the new authority will need to work with cantons, municipalities, and the private sector to bring about the country's digital transformation.

This article is based, among other things, on interviews we conducted with Estonian government officials. The aim was to identify the lessons learned by Estonia and what exactly Switzerland can learn from them. Estonia is one of the world's leading nations in digital government and has achieved a level that Switzerland will reach in about 10 years at best.

Schlüsselbegriffe Bundesamt für Cybersicherheit; Digitalisierung; Estland; Umsetzungskapazitäten
Keywords Federal Office for Cybersecurity; digital transformation; Estonia; implementation capacity

DOMINIQUE URSPRUNG, M.A International Relations (IHEID), MSc International Management (SOAS), hat in Genf, Tokio und London Internationale Beziehungen und Internationales Management studiert. Ursprung hat an der ZHAW den Bereich Foreign Affairs and Applied Diplomacy mitgegründet und unterrichtet dort seit 2012. Während sechs Jahren hat Ursprung die Geschäftsstelle der Handelskammer Schweiz-Japan (SJCC) geführt, aktuell ist er bei der SJCC Vorstandsmitglied und Sekretär für die parlamentarische Gruppe Schweiz-Japan.

E-Mail: dominique.ursprung@zhaw.ch

NICOLAS ZAHN, M.A International Affairs, befasst sich seit über 10 Jahren mit technologischen Entwicklungen und deren politischen und gesellschaftlichen Auswirkungen. Nach seiner Masterarbeit zu Internet Governance arbeitete er als Berater in der Finanzbranche, um sich anschliessend im Rahmen des Mercator Kolleg für internationale Aufgaben mit der digitalen Transformation des öffentlichen Sektors zu befassen und bei ELCA Informatik als Digitalisierungsberater zu arbeiten. Zahn ist aktuell als Senior Project Manager bei der Swiss Digital Initiative tätig und beschäftigt sich in seiner Milizfunktion als Nachrichtenoffizier u. a. mit den sicherheitspolitischen Auswirkungen der künstlichen Intelligenz.

E-Mail: nicolas@nicolaszahn.ch

Reorganisation als Holzweg?

Es ist oft verlockend, die Schaffung einer neuen Organisationseinheit mit der tatsächlichen Umsetzung komplexer Aufgaben zu verwechseln. Ein Büro mit einer neuen, glänzenden Plakette «Digitalministerium» ist jedoch keineswegs ein Garant für eine erfolgreiche digitale Transformation. Obwohl diese Erkenntnis offensichtlich scheint, wird in Europa viel Zeit damit verbracht, Organigramme bezüglich Digitalministerien oder Digitalisierungsagenturen zu vergleichen (Hammerschmid und Hildebrandt 2021). Es schwingt jeweils die Hoffnung mit, im Organisationsaufbau einen Hinweis auf die Ernsthaftigkeit und den Erfolg von Staaten bezüglich digitaler Transformation zu finden. Dass man mit einem starren Fokus auf die Organisationsstrukturen auf dem Holzweg ist, sagt jedoch Estlands ehemaliger Chief Information Officer (CIO) in einem Interview über seine wichtigsten Erkenntnisse als Verantwortlicher für die Koordination und Beschleunigung dieses digitalen Transformationsprozesses (Ross 2022): «There's nothing magical about Estonia's organisational setup. It doesn't matter where the central team is situated, for example: What matters most is the leverage mechanisms you have, and how much resources you have to charm [agencies] or build stuff yourself.»

In diesem Beitrag werden wir beide in diesem Zitat aufgebrachten Punkte behandeln, zuerst jener zur organisatorischen Struktur, danach die Erfolgsfaktoren für eine solche Einheit. Dieser Text beruht u. a. auf Interviews, welche die Autoren in den vergangenen zwei Jahren mit Verantwortlichen der estnischen Regierung durchgeführt haben, um die Relevanz der in Tallinn gesammelten Erfahrungen für die Schweiz möglichst genau identifizieren zu können. Estland gehört weltweit zu den führenden Nationen bei der digitalen Transformation und ist heute auf einem Niveau, das die Schweiz bestenfalls in etwa zehn Jahren erreichen könnte.

Realitätsfremde Zentralisierung?

Die Schweizer Debatte darüber, wie die Umsetzung der digitalen Transformation organisiert werden sollte, hat im November 2021 neuen Schwung aufgenommen, als der Verein CH++ ein Staatssekretariat für Cybersicherheit forderte. Der während der Corona-Pandemie gegründete Verein anerkennt, dass das Nationale Zentrum für Cybersicherheit (NCSC) mit seinen 32 Mitarbeitenden eine beeindruckende Dynamik an den Tag gelegt hat, dennoch sei es in Anbetracht der «enormen Bedrohungslage» notwendig dieses zu einem Staatssekretariat weiterzuentwickeln. Es wird gefordert, dass die Cybersicherheit-Expertise, die heute auf verschiedene Ämter und Departemente verteilt ist, in diesem neuen Staatssekretariat für Cybersicherheit gebündelt werden soll. Digitale Sicherheit sei eine Querschnittsaufgabe und daher sei ein eigenes Staatssekretariat «die dafür angebrachte Form» (Gassert 2021).

Dieser Vorschlag wurde kurz danach von der NZZ kritisiert: Die von CH++ gemachte Analyse und der identifizierte Handlungsbedarf wird zwar geteilt, den Vorschlag, dies mit mehr Zentralisierung zu lösen bezeichnet Digitalisierungsredaktor Lukas Mäder (2021) jedoch als «realitätsfremd»: IT-Sicherheit könne nicht von oben herab verordnet werden, sie müsse von Firmen und Gemeinden im Alltag gelebt werden, «sonst ist sie zum Scheitern verdammt». Er kommt zum Schluss, dass ein Staatssekretariat für Cybersicherheit kaum einen Vorteil hätte gegenüber dem heutigen NCSC. Dennoch wurde die Frage «Staatssekretariat oder Bundesamt für Cybersicherheit?» auch im Nationalrat aufgenommen und im Dezember 2021 dem Bundesrat gestellt.[1]

Diese Episode zeigt gut, wie das Streben nach einheitlichen Standards fundamentaler Teil einer solchen Transformation ist, gleichzeitig stossen solche Zentralisierungstendenzen in der föderalen Schweiz auf viel Widerstand.[2] Ob, respektive wie, das Dilemma des Bedarfs nach einheitlichen Regeln bei gleichzeitig stark gelebtem Föderalismus aufgelöst werden kann, wird u. a. auch die dem Finanzdepartement (EFD) angegliederte, neu geschaffene Organisation «Digitale Verwaltung Schweiz (DVS)» aufzeigen müssen.[3] Hier sind alle relevanten Akteure (Bund, Kantone und Gemeinden) involviert, um die digitale Transformation koordiniert anzugehen. Der Harmonisierungsauftrag respektive die längst überfällige Umsetzung des «Once-only»-Prinzips wird wohl die erste grosse Herkulesaufgabe für die DVS sein (siehe Box *Fehlende Grundlagen für Interoperabilität).*[4]

Cybermacht Finanzdepartement?

Im April 2022 entwickelte sich die Schweizer Debatte weiter mit der Ankündigung von EFD-Vorsteher Ueli Maurer,

Fehlende Grundlagen für Interoperabilität

Dank «Once-only» sollten Bürgerinnen und Bürger, genauso wie Firmen, ihre Daten nur jeweils einer Behörde melden müssen, womit nicht nur die mehrfache Erfassung von Daten verhindert werden soll, sondern auch die Aktualisierung der Daten stark vereinfacht würde. Es muss hier allerdings kritisch angemerkt werden, dass die weiteren in der Tallinn-Deklaration vereinbarten Ziele, insbesondere Interoperabilität, nur erreicht werden können, wenn «Once-only» zusammen mit einem elektronischen Identifikationsnachweis (eID) umgesetzt sind. Eine der wichtigsten Erkenntnisse Estlands ist, dass Effizienzen in einem digitalen Staat mit aufeinander abgestimmten IT-Systemen – Interoperabilität – nur auf der Grundlage einer eID und strikter Umsetzung von «Once-only» gelingen kann. In der Schweiz sind beide Grundlagen noch nicht Realität, um diese Effizienzen zu erreichen. Die Bemühungen zur Umsetzung dieser Ziele sind unterdessen zwar alle angestossen, Fakt ist jedoch, dass die öffentliche Verwaltung der Schweiz bezüglich digitaler Transformation noch im Startblock verharrt (Keller und Ursprung 2022). Will die Schweiz nicht von Estland, Dänemark, Finnland oder Spanien überrundet werden, braucht es bald konkrete Erfolge bei der Umsetzung, wie beispielsweise elektronische Arztrezepte, die via Vorweisen der eID in allen Apotheken des Landes elektronisch abgerufen werden könnten. Estland gibt an, dass medizinische Rezepte von Ärzten innerhalb von 15 Sekunden online erneuert werden können – dies geht jedoch nur, wenn Interoperabilität, dank einer eID und «Once-only»-Prinzip, umgesetzt ist.

das NCSC in ein Bundesamt für Cybersicherheit umwandeln zu wollen. Damit unterstrich das Finanzdepartement seinen Führungsanspruch beim Thema Digitalisierung, gleichzeitig kam damit jedoch auch die Frage wieder auf, welche Rolle die anderen zwei Akteure, die im interdepartementalen Cyberausschuss bereits eng zusammenarbeiten, d. h. das Verteidigungsdepartement (VBS) und das Eidgenössisches Justiz- und Polizeidepartement (EJPD), zukünftig spielen sollen.

Die Autoren haben die damit einhergehende Frage, ob Digitales und Cybersicherheit einzeln oder zusammen behandelt werden sollen in einem Gespräch mit dem ehemaligen CIO Estlands gestellt.[5] Er meinte, jeder Staat müsse für sich abwägen, wie man sich am besten organisieren wolle. Estland hat für sich entschieden, dass die zwei Themen zusammengehören, da es sich um zwei Seiten der gleichen Medaille handle. Im Krisenfall seien zudem kurze Wege und persönliche Kontakte wichtige Elemente für effiziente Teams, daher sei dies für Estland der richtige Weg.

«Obwohl somit eindeutig belegt ist, dass politische Durchsetzungskraft viel wichtiger ist als der organisatorische Aufbau, findet dieses Schattengefecht auch zwischen den vielen, verschiedenen Akteuren der Schweizer ‹Digital Government›-Landschaft statt.»

Länder mit Digitalministerium gehören in Europa nicht zur Spitzengruppe

Der Frage, welcher organisatorische Aufbau am erfolgversprechendsten ist, respektive, ob ein Digitalministerium wirklich erforderlich sei, ist die Hertie School Berlin nachgegangen (Hammerschmid und Hildebrandt 2021). Die Autoren dieser vergleichenden Studie sind zum Schluss gekommen, dass nur sehr selten eigene Ministerien zur Umsetzung der digitalen Transformation geschaffen worden sind. Digitalministerien «finden sich lediglich in Polen, Luxemburg und Griechenland sowie in Singapur. In diesem Zusammenhang wird deutlich, dass alle drei europäischen Länder mit eigenen Digitalministerien lediglich hintere Plätze in den internationalen Digitalisierungsrankings einnehmen» (Hammerschmid und Hildebrandt 2021, 17). Eine Analyse des Think-Tanks Stiftung Neue Verantwortung hält ebenfalls fest, dass die Forderung nach einem Digitalministeriums zwar wahlkampftauglich ist, aber an den grundlegenden Problemen – fehlende Expertise in der Verwaltung, wenig Austausch und Kollaboration (Silos) und Governance-Strukturen – vorbeizielt (Heumann 2021). Obwohl somit eindeutig belegt ist, dass politische Durchsetzungskraft viel wichtiger ist als der organisatorische Aufbau, findet dieses Schattengefecht auch zwischen den vielen, verschiedenen Akteuren der Schweizer «Digital Government»-Landschaft statt.[6]

Erfolgsfaktor Umsetzungskapazität

Der Befund ist, wie zuvor aufgezeigt, eindeutig: Zentral für den Erfolg der in Europa führenden Länder bei der Digitalisierung, d. h. Estland, Spanien, Dänemark und Finnland, ist, «dass sie neben der Verankerung der Digitalisierung in einem traditionell starken Ministerium umfassende Umsetzungskapazitäten dafür aufgebaut haben» (Hammerschmid und Hildebrandt 2021, 17). In anderen Worten: Weisungsbefugnisse gegenüber anderen Stellen in der Verwaltung, inklusive einem Vetorecht, sind entscheidend für den Erfolg. Die Form die-

ser Einheit kann laut Studie der Hertie School Berlin variieren: in Estland, Dänemark und Finnland sind es Agenturen; in Spanien ist die Umsetzungsbehörde für Digitalisierung direkt im Ministerium integriert. Während in Estland und Spanien das Wirtschaftsministerium zuständig ist, ist es in Dänemark und Finnland das Finanzministerium. Der Blick über Europa hinaus verändert nichts an dieser Feststellung: «Auch bei den aussereuropäischen Spitzenreitern variieren die Governance-Architekturen erheblich» (Hammerschmid und Hildebrandt 2021, 17).

Aufgrund dieser klaren Resultate täte die Schweiz gut daran, sich nicht in einer Diskussion um Namen und Zuordnung zu verrennen, sondern den Fokus auf die Umsetzbarkeit dieser anspruchsvollen und kostspieligen Transformation zu legen. Die NZZ hatte bereits 2017 in einem Beitrag festgehalten, dass ein Mr. Digital oder eine Ms. Digital, der bzw. die diesen digitalen Transformationsprozess voranbringen sollte, nicht nur Durchsetzungsfähigkeit brauche, sondern auch ein Vetorecht gegenüber den Departementen, sowie ein eigenes Budget (Aschwanden 2017).

Erfolgsfaktor Anreize für Gemeinden

Im Gespräch mit dem früheren CIO Estlands hat sich gezeigt, dass auch die dortige Regierung die Zusammenarbeit mit subnationalen Akteuren als eine grosse Herausforderung erlebt: Obwohl die dortigen Gemeinden im Vergleich zur Schweiz viel weniger Kompetenzen haben, können diese dennoch eigene IT-Systeme beschaffen und unterhalten. Angesprochen auf die Risiken, wie sie der Ransomware-Angriff auf die Waadtländer Gemeinde Rolle Ende Mai 2021 gezeigt hat – damals sind sensitive Daten von Einwohnern, Mitarbeitenden und Unternehmen entwendet und im Darknet veröffentlicht wurden[7] –, wurde bestätigt, dass dieses Problem und die damit verbundenen Gefahren auch in Estland bestens bekannt seien. Der Lösungsansatz, den Estland gewählt hat, sind Anreize für Gemeinden, damit diese sich für die von der nationalen Regierung betriebenen IT-Systeme entscheiden: Erstens kann die Zentralregierung die Aus- und Weiterbildung der IT-Verantwortlichen der Gemeinde bei Verwendung der gleichen IT-Systemen übernehmen. Zweitens kann die nationale Ebene Massnahmen im Bereich der Cyberabwehr finanzieren, oder auch bei Bedarf ein Expertenteam zur Verfügung stellen, dass sich der Sache annehmen kann, analog dem Computer Emergency Response Teams des Bundes, GovCERT. Drittens können auch gemeinsam betriebene Server von nationalen Behörden gehostet werden. Kurz: den Gemeinden werden sehr wichtige, kostspielige und risikoreiche Aufgaben, zumindest teilweise, abgenommen. Gerade in der Schweiz, mit vielen Kompetenzen auf subnationaler Ebene, könnten solche Angebote helfen, damit die verschiedenen Digitalisierungsinitiativen auch effektiv auf allen Ebenen umgesetzt und sicher unterhalten werden können.

Während der Pandemie hat Estland diese Anreize weiterentwickelt. Dazu gehören zum Beispiel Cloud-Lösungen oder Software für sichere Online-Sitzungen von Gemeindegremien, welche von nationalen Behörden zur Verfügung gestellt worden sind. Die gleiche Logik kann im Bildungs- und Sozialwesen angewendet werden: Wird von Gemeinden, die von nationaler Ebene empfohlene Software beschafft, übernimmt diese (teilweise) die Kosten dafür. Falls die Gemeinde andere Lösungen bevorzugt, bleibt sie auf den gesamten Kosten sitzen und wird im Falle von Cyberattacken keine Ausreden haben – man hat das Angebot von zusätzlicher Unterstützung wohlwissend ausgeschlagen. Dank diesem Ansatz mit Anreizen, statt Top-down-Verordnungen und Kompetenzgerangel, konnte die in Estland zuvor oft gesehene gegenseitige Beschuldigung nach Cyberangriffen reduziert werden.

Erfolgsfaktor im Kriegsfall: Freiwillige IT-Fachkräfte

Ein weiterer Punkt, den der estnische Experte erwähnte: Zur richtigen Einstellung gehört auch viel Community-Arbeit, das heisst, die lokalen Behörden müssen mit dem nationalen CERT vertraut sein. Diese Fachleute sollten sich gegenseitig von Zusammenarbeit ausserhalb von Notfällen kennen. Wenn das nationale CERT-Team subnationalen Behörden helfen kann Cyberangriffen nachzugehen, was in der Regel sehr aufwändig ist, entsteht nicht nur Vertrauen, sondern auch einen Anreiz, bei Notfällen diese Einheit schneller zu involvieren. Somit ist auch hier nicht eine Veränderung im Organigramm für den Erfolg entscheidend, sondern die richtigen Anreize, so dass subnationale Behörden ihre Stärken und Schwächen kennen und proaktiv den Austausch mit der nationalen Ebene pflegen. In Estland kommt hier noch die *Estonian Defence League* als Eigenheit dazu, um dem Personalmangel entgegenzuwirken: Eine Frei-

«In Estland kommt hier noch die Estonian Defence League als Eigenheit dazu, um dem Personalmangel entgegenzuwirken: Eine Freiwilligenarmee, die auch über eine Cyber Unit verfügt.»

willigenarmee, die auch über eine Cyber Unit verfügt. Laut offiziellen Angaben besteht diese Cyber-Einheit aus Experten für Cybersicherheit in den kritischen Infrastrukturen des Landes, patriotischen Personen mit IT-Kenntnissen, wie auch Jugendlichen, die bereit sind, zur Cybersicherheit beizutragen. Das Center for Security Studies der ETH Zürich ist dem Thema, welche Rolle Reservekräfte für militärische Aufgaben im Bereich der Cybersicherheit spielen, in einer vergleichenden Analyse zur Situation in Estland, Finnland, Frankreich, Israel, der Schweiz und den USA nachgegangen. Autorin Marie Baezner (2020, 34–35) kommt zum Schluss, dass eine offenere Zusammenarbeit zielführend sein kann, doch es brauche ein sorgfältiges Management solcher Reservekräfte und Anreize, zum Beispiel der gute Ruf solch militärischer Einheiten oder die Involvierung bei Übungen, die sonst nicht zugänglich sind, damit private IT-Fachleute – die im Privatsektor zu deutlich besseren Bedingungen ihrer Arbeit nachgehen – ihr Wissen und ihre Zeit zur Verfügung stellen. Mit der Schaffung des Cyber Bataillons 42 geht die Armee den richtigen Schritt vom bewährten Milizprinzip zur Nutzung gewisser Kompetenzen zugunsten der Armee, um auch im digitalen Raum vom zivilen Wissen zu profitieren.[8] Nicht vergessengehen darf allerdings, dass es zwar ausführende Kräfte braucht, für deren Einsatz aber auch eine durchdachte Strategie und eine klare Doktrin vorhanden sein müssen. Lange standen in politischen und öffentlichen Diskussionen die Mittel – sowohl personell als auch technisch, Stichwort «Hack-Backs» – im Fokus, ohne über die strategischen Auswirkungen von Cyber und mögliche Einsatzszenarien zu diskutieren.[9] Doch auch hier scheint die Reise nun in die richtige Richtung zu gehen.[10]

Fazit

Zusammenfassend kann gesagt werden, dass Anreize für subnationale Akteure eine bis jetzt noch unterschätzte Rolle spielen bei der digitalen Transformation der Schweiz. Es gibt keine Hinweise, dass die Form (Staatssekretariat oder Bundesamt für Cybersicherheit) relevante Erfolgsfaktoren sind. Genauso sekundär ist, in welchem Departement dieser Bereich schlussendlich angesiedelt wird – entscheiden ist laut unseren Informationen die Umsetzungskapazität, mit der die treibenden Kräfte ausgestattet werden: Budget, Kompetenzen und Vetorechte. Was das CIO Office in Estland mit lediglich 30 Mitarbeitenden erreicht hat, sollte sowohl als Inspiration dienen, was mit einer kleinen Einheit erreicht werden kann, und gleichzeitig in Erinnerung rufen, dass eben nicht die Form, sondern die Macht, die man dieser Stelle gibt, entscheidend ist, dass die Knochenarbeit, Umsetzung der digitalen Transformation, tatsächlich gelingt. ◆

«Mit der Schaffung des Cyber Bataillons 42 geht die Armee den richtigen Schritt vom bewährten Milizprinzip zur Nutzung gewisser Kompetenzen zugunsten der Armee, um auch im digitalen Raum vom zivilen Wissen zu profitieren.»

Endnoten

1 Siehe Interpellation 21.4389 «Ein Staatssekretariat oder Bundesamt für Cybersicherheit?»

2 Siehe hierzu auch https://www.staatslabor.ch/de/guest-post-foederalismus-als-vor-und-nachteil-fuer-die-digitale-schweiz-nicolas-zahn sowie https://www.staatslabor.ch/de/wenn-wettbewerb-fortschritt-ausbremst-foederalismus-und-digitalisierung

3 Siehe dazu: https://www.efd.admin.ch/efd/de/home/digitalisierung/e-government-schweiz.html

4 Die fünf zentralen Ziele in der 2017 von der Schweiz unterzeichneten Tallinn-Deklaration zu E-Government sind Digital-by-Default, Once-only, Vertrauenswürdigkeit und Sicherheit, Offenheit und Transparenz sowie Interoperability-by-Default. Zum Stand der Umsetzung siehe Interpellation 19.3686: «Tallinn-Deklaration zu E-Government. Wo steht die Schweiz heute, und was ist zu tun?»

5 Interview mit Siim Sikkut, CIO von Estland 2017–2022, durchgeführt durch die beiden Autoren am 26. November 2021.

6 Siehe «Digital Government»-Landschaft der Schweiz des staatslabors hier: https://www.staatslabor.ch/sites/default/files/2022-01/eGovernment_Landkarte%20und%20Details_Januar%202022_Version%201.5.pdf

7 Siehe dazu: Tausende persönliche Daten im Darknet: Die Cyberattacke auf Rolle ist gravierender als von den Behörden kommuniziert, Neue Zürcher Zeitung (NZZ), 25.08.2021 https://www.nzz.ch/schweiz/cyber-attacke-auf-rolle-ist-deutlich-schlimmer-als-kommuniziert-ld.1642093

8 Siehe https://www.vtg.admin.ch/de/aktuell/themen/cyberdefence/cyber-miliz.html

9 Leider ein weit verbreitetes Problem, da die Sicherheitspolitik häufig mit der digitalen Welt zu «fremdeln» scheint, siehe https://www.digitale-gesellschaft.ch/2021/04/26/cyber-goes-sicherheitspolitik-es-gibt-viel-zu-erklaeren/

10 Siehe z. B. dieses Interview https://www.nzz.ch/technologie/cyberangriffe-ist-die-armee-fuer-den-cyberkrieg-gewappnet-ld.1590150

Litertaurverzeichnis

Aschwanden, Erich. 2017. «Die Schweiz braucht eine ‹Ms. Digital› oder einen ‹Mr. Digital›.» *Neue Zürcher Zeitung*, 21. November.

Baezner, Marie. 2020. «CSS Cyber Defense Report: Study on the use of reserve forces in military cybersecurity.» *Center for Security Studies (CSS), ETH Zürich*, April.

Gassert, Hannes. 2021. «Die Schweiz muss ihre digitale Souveränität verteidigen [Gastbeitrag].» *NZZ am Sonntag*, 7. November.

Hammerschmid, Gerhard , und Tim Hildebrandt. 2021. «Ist ein Digitalministerium erforderlich? Ein Blick auf internationale Erfahrungen.» *PublicGovernance: Zeitschrift für öffentliches Management*, 15–17.

Heumann, Stefan. 2021. *Stiftung Neue Verantwortung.* 17. März. https://www.stiftung-nv.de/de/publikation/scheinloesung-digitalministerium.

Keller, Florian, und Dominique Ursprung. 2022. «Covid-Pandemic as an Accelerator for E-Government? An Analysis of Switzerland's Progress to Implement the Tallinn Declaration on E-Government from 2017.» *EURAM 2022 Conference, Proceedings.*

Mäder, Lukas. 2021. «Forderung nach einem Staatssekretariat für Cybersicherheit: Bürokratie schützt nicht vor Hackern.» *Neue Zürcher Zeitung*, 9. November.

Ross, Matt. 2022. «From mini-state to digital giant: Siim Sikkut on Estonia's remarkable journey.» *Global Government Forum*, 21 February. https://www.globalgovernmentforum.com/from-mini-state-to-digital-giant-siim-sikkut-on-estonias-remarkable-journey/.