# Positive Bilanz von digital@bw

## Prävention und Kooperation zentrale Bausteine der Cyber-Sicherheit

**(BS) Am 13. April veranstaltet die Landesregierung Baden-Württemberg das diesjährige "CyberSicherheitsForum". Zudem wird die Digitalstrategie "digital@bw" im Sommer fünf Jahre alt. Der Behörden Spiegel nahm dies zum Anlass, um mit Thomas Strobl, stellvertretender Ministerpräsident sowie Minister des Inneren, für Digitalisierung und Kommunen des Landes, über beide Themen zu sprechen. Das Interview führte Guido Gehrt.**

***Behörden Spiegel:*** *Herr Minister Strobl, mit der "Cybersicherheitsagentur" Baden-Württemberg (CSBW) wurde im vergangenen Jahr "das Herzstück der neuen Cyber-Sicherheitsarchitektur des Landes" gegründet. Was zeichnet die CSBW aus?*

**Strobl**: Die Cybersicherheitsagentur ist unsere Antwort auf die wachsenden Gefahren von Cyber-Angriffen im digitalen Raum. Sie verbessert die Cyber-Sicherheit in Baden-Württemberg. Zum ersten Mal hat das Land damit eine zentrale Koordinierungs- und Meldestelle, die im ständigen Austausch mit allen relevanten Sicherheitsbehörden und Akteuren steht. Zum Beispiel, um Informationen über Schwachstellen und aktuell laufende Angriffsversuche in der Landesverwaltung zu dislozieren und so mögliche Lücken schnellstmöglich zu schließen.

Durch die CSBW verhindern wir Doppelstrukturen und sorgen dafür, dass wichtige Informationen alle Beteiligten rasch erreichen, damit die Zusammenarbeit bestmöglich funktioniert. So macht die Cybersicherheitsagentur die Bekämpfung und Abwehr von Sicherheitsbedrohungen im digitalen Raum schlagkräftiger, effektiver und effizienter.

Gerade in der aktuellen Lage im Zusammenhang mit dem Ukraine-Krieg stellt die CSBW unter Beweis, dass sie schnell auf akute Situationen reagiert. Sie hat etwa umgehend das Monitoring der IT-Systeme intensiviert und mögliche kurzfristige IT-technische Maßnahmen zum Schutz der Systeme umgesetzt. Die CSBW entwickelte etwa technische Lösungen zur Identifikation der in der Ukraine entdeckten Lösch-Malware und berät die IT-Bereiche des öffentlichen Sektors, um diese Maßnahmen umzusetzen. Der wichtigste Baustein ist freilich die Prävention. Denn bei der Cyber-Sicherheit spielt der Faktor Mensch eine ganz entscheidende Rolle. Es ist deshalb ganz entscheidend, dass die CSBW Verwaltungsmitarbeiter, Bürgerinnen und Bürger für die Gefahren im Cyber-Raum sensibilisiert. Bei der Sensibilisierung hilft uns auch unser "CyberSicherheitsForum". Es findet in diesem Jahr bereits zum vierten Mal statt. Hierzu lade Sie an dieser Stelle ganz herzlich ein. Im Fokus steht in diesem Jahr der Umgang mit unseren Daten und digitalen Anwendungen: Gemeinsam mit Expertinnen und Experten aus Staat, Wirtschaft, Forschung und Gesellschaft beschäftigen wir uns mit dem Thema "Digitale Souveränität".

*"Die Zusammenarbeit der föderalen Partner – aber auch innerhalb des Landes – ist ein elementarer Baustein für die Sicherheit im digitalen Raum."*

Thomas Strobl ist seit 2016 u. a. Digitalisierungsminister des Landes Baden-Württemberg. Er unterstützt nicht nur das "CyberSicherheitsForum" am 13. April, sondern ist auch in diesem Jahr erneut Schirmherr des Kongresses "Baden-Württemberg 4.0" am 30. Juni in Stuttgart. Foto: BS/Laurence Chaperon

***Behörden Spiegel:*** *Bereits seit Februar 2019 unterhält das Bundesamt für Sicherheit in der Informationstechnik (BSI) ein Verbindungsbüro in Stuttgart. Wie steht es Ihrer Ansicht nach grundsätzlich um die föderale Zusammenarbeit im Bereich der Cyber-Sicherheit?*

**Strobl**: Das Thema Cyber-Sicherheit kann kein Land alleine lösen – Cyber-Angriffe sind grenzenlos. Nur gemeinsam können wir den aktuellen Gefahren im Netz wirksam begegnen. Eine leistungsfähige und nachhaltige Cyber-Sicherheitsarchitektur erfordert eine gemeinsame Anstrengung von Bund und Ländern und in viel stärkerem Maße künftig auch von Europa. Deshalb findet hier ein sehr guter Austausch mit dem Bund statt.

In Baden-Württemberg legen wir großen Wert darauf, unseren verfassungsgemäßen Auftrag im Bereich der Abwehr von Cyber-Angriffen in eigener Verantwortung wahrzunehmen. Darum haben wir die CSBW als zentrale Ansprechpartnerin in Baden-Württemberg für Organisationen der Cyber-Sicherheit geschaffen, sowohl auf Bundes- wie auch Länderebene. Die Zusammenarbeit der föderalen Partner – aber auch innerhalb des Landes – ist ein elementarer Baustein für die Sicherheit im digitalen Raum. So hat sich beispielsweise ein guter und regelmäßiger Austausch zwischen der CSBW und dem CyberCompetenceCenter Hessen3C sowie dem bayerischen LSI etabliert.

*"Gerade bei der Digitalisierung ist eine agile, ja auch mal mutige Pionierarbeit gefragt: Neues wagen, Risiken eingehen, pfiffige Lösungen erarbeiten."*

***Behörden Spiegel:*** *Inwieweit verändert sich die Cyber-Bedrohungslage hierzulande durch den Krieg in der Ukraine?*

**Strobl**: Die Bedrohungslage im Zusammenhang mit dem Ukraine-Krieg hat sich noch einmal verschärft. Es besteht zwar gegenwärtig keine akute Gefährdung. Diese Situation kann sich freilich jederzeit ändern. Uns liegen Informationen vor, dass es in Bälde zu einer konkreten Lageverschärfung mittels Cyber-Angriffen auf Hochwertziele kommen könnte. Dies ist übrigens auch die Einschätzung des BSI.

Bislang kam es in Deutschland nur zu einigen wenigen Vorfällen, die in Zusammenhang mit dem Krieg in der Ukraine stehen. Allerdings sind beispielsweise auch erste Phishing-Mails mit Bezug zum Ukraine-Krieg auf Deutsch im Umlauf. Hier ist jeder einzelne zur Vorsicht und Wachsamkeit aufgerufen.

***Behörden Spiegel:*** *Im Sommer 2017 wurde die Digitalstrategie "digital@bw" verabschiedet. Nach fast fünf Jahren Umsetzung: Wie fällt ihre Zwischenbilanz aus? Steht ggf. ein größeres "Update" an?*

**Strobl**: Unsere Bilanz ist sehr positiv. So können wir auf große Fortschritte im Bereich der Cyber-Sicherheit, der Künstlichen Intelligenz, der Green-IT und beim Gigabit-Ausbau zurückblicken. Dies bestätigt uns auch eine im letzten Jahr erstellte Studie des Zentrums für Europäische Wirtschaftsforschung ZEW zu Chancen und Herausforderungen der Digitalisierung in Baden-Württemberg. Derzeit gehen wir die uns dort aufgezeigten weiteren Optimierungspotenziale und Herausforderungen an. So haben wir bereits Ziele und Schwerpunkte für eine weiterentwickelte Digitalisierungsstrategie festgelegt, die wir dieses Jahr verabschieden wollen.

***Behörden Spiegel:*** *Die Digitalisierung der Verwaltung hat in den vergangenen Jahren spürbar an Dynamik zugenommen. Dennoch, das sagen auch die Beteiligten, dauert die Implementierung neuer Technologien im Behördenbereich oftmals noch zu lange, insbesondere vor dem Hintergrund immer kürzerer Innovationsintervalle. Was kann man tun, um hier Prozesse zu beschleunigen?*

**Strobl**: Die Corona-Pandemie ist ein Booster für die Digitalisierung: Auch der Letzte hat gemerkt, wie wichtig das schnelle Internet für uns alle ist – und unsere gigantischen Investitionen und unsere ambitionierte Arbeit der letzten fünf Jahre waren so was von richtig. Nun setzen wir alles daran, dass die Menschen im Land die Digitalisierung in allen Lebensbereichen bestmöglich nutzen können. So ist es unser klares Ziel: Das Amt muss zu den Bürgerinnen und Bürgern kommen und nicht umgekehrt. Ob Baugenehmigungen, Elterngeld, Geburtsurkunden oder Gewerbeanmeldungen: All das soll "24/7" – 24 Stunden am Tag, 7 Tage die Woche – vom heimischen Schreibtisch oder Sofa aus erledigt werden können. Mir ist bewusst, dass die Modernisierung der Verwaltung an der einen oder anderen Stelle oftmals noch zu viel Zeit – und übrigens auch viel Kraft – in Anspruch nimmt. Um hier schneller voranzukommen, ist eines ganz wichtig: Digitalisierung bedeutet auch, Dinge auszuprobieren und mit Projekten an die Öffentlichkeit zu gehen, die noch nicht zu 100 Prozent optimiert sind – auch auf die Gefahr hin, dass beispielsweise eine digitale Verwaltungsleistung nicht auf Anhieb perfekt ist. Dies freilich erfordert eine Art und Weise zu arbeiten, die der öffentlichen Verwaltung sowie der politischen und medialen Szene bisher eher fremd ist. In den Behörden ist oftmals und zu Recht ein ausgeprägtes Bedürfnis für Verfahrenssicherheit und Fehlerfreiheit vorherrschend. Das politische Umfeld und die mediale Öffentlichkeit verzeihen keine Fehler – Häme und Spott sind nicht nur im Netz schnell bei der Hand. Gerade bei der Digitalisierung ist dagegen eine agile, ja auch mal mutige Pionierarbeit gefragt: Neues wagen, Risiken eingehen, pfiffige Lösungen erarbeiten. Mut, Ambition und eine anerkannte Fehlerkultur sind hier der Schlüssel zum Erfolg! Hier haben wir bei uns im Land durchaus Luft nach oben …

Aktuell haben gerade im letzten Jahr viele Kommunen auch Einsatz gezeigt, sie haben gemeinsam mit dem Land intensiv getüftelt und dabei tolle Ergebnisse produziert. Doch erst wenn jede einzelne Kommune sich der Digitalisierung annimmt, erreichen wir unser Ziel einer flächendeckenden digitalen Verwaltung im Flächenland Baden-Württemberg. Hierfür brauchen wir klare technische, organisatorische und kommunikative Standards beim Land und bei den Kommunen. Wir reden noch zu oft aneinander vorbei, obwohl wir dasselbe meinen. Wir benötigen mehr Fachkräfte in den Landkreisen, Städten und Gemeinden. Leider macht der Fachkräftemangel auch vor dem Öffentlichen Dienst nicht Halt. Ich spreche hier ausdrücklich nicht nur von Informatikerinnen und Informatikern, sondern von Projektleiterinnen und Projektleitern, von Menschen, die um die Ecke denken und Gegebenes kritisch hinterfragen – zu Neuem bereit sind. Und zu guter Letzt benötigen wir finanzielle Ressourcen bei den Behörden im Land. Den Aufbau einer digitalisierten, den Nutzerinnen und Nutzern zugewandten Verwaltung, aus meiner Sicht ein Mammutprojekt, gibt es eben nicht zum Nulltarif. Das müssen einfach alle wissen: Wer langfristig sparen möchte, muss hier erst mal kräftig investieren. Es gilt wieder mal die einfache Wahrheit: ohne Moos nix los.

# Hatespeech und Fake News

## Zur Bekämpfung ist Wissen um die Funktionsweise des Internets nötig

**(BS/Prof. Dr. Robert Müller-Török*) Die beiden Schlagworte Hatespeech und Fake News stehen nicht nur wegen des jüngsten Überfalls der Russischen Föderation auf die Ukraine im Mittelpunkt der öffentlichen Debatte, sondern haben in den letzten Jahren an Wahrnehmung gewonnen. Angriffe gegen lokale und regionale Politiker und Verwaltungsspitzen in Sozialen Medien finden täglich statt, auch daraus resultierende physische Gewalt gegen Menschen und Einrichtungen kann vermehrt registriert werden. Neben dieser Hatespeech hat die gegenwärtige Pandemie auch Fake News Konjunktur beschert: Fast täglich erhalten auch Normalbürger über alle möglichen Kanäle "Nachrichten", deren Wahrheitsgehalt für sie nur schwer überprüfbar ist.**

Auch der Kongress der Gemeinden und Regionen des Europarats befasst sich damit, vor allem weil gerade lokale und regionale Politiker leichter zum Ziel von dadurch ausgelöster physischer Gewalt werden als vergleichsweise gut personengeschützte Staatsspitzen und Minister. Die Ermordung des Danziger Bürgermeisters *Pawel Adamowicz* 2019 oder der Mordanschlag auf die Kölner Oberbürgermeisterin *Henriette Rieker* 2015 sind hier wohl nur die Spitze des Eisbergs.

### Wissen schaffen und verbreiten

Im Spätsommer 2021 ergab sich die Möglichkeit, im Rahmen eines studentischen Projektes für den Kongress eine wissenschaftlich fundierte Basis in Buchform zu schaffen, die v. a.

- Definitionen von Hatespeech (die in Form von formellen Europaratsdokumenten existieren) und von Fake News (die nicht existieren) analysieren sollte,
- technische und rechtliche Möglichkeiten der Bekämpfung beschreiben sollte,
- mittels einer Umfrage unter den Kongressdelegierten deren Betroffenheit und Einschätzung der Umsetzbarkeit möglicher Abhilfen erfassen sollte,
- gangbare mögliche Bekämpfungsstrategien, v. a. Open Government und Open Data sowie mehr Transparenz der Politik und Verwaltung, beschreiben und somit
- als Grundlage einer politischen Debatte im Kongress bzw. im Europarat dienen sollte.

Daraus wurde ein Buch in englischer Sprache mit ca. 200 Seiten, welches von 13 Studenten der Hochschule Ludwigsburg unter Anleitung von Wissenschaftlern der TU Budapest, der WU Wien, der Pavol Jozef Šafarik Universität Košice sowie der Nationalen Universität für Politische Studien Bukarest verfasst und am 23. März 2022 im Rahmen der 42. Session des Kongresses im Plenum überreicht wurde. Das Buch mit dem Titel "COUNTERFAKE: A scientific basis for a policy fighting fake news and hate speech" ist als Open Access unter *ocgitservice.com/demo/counterfake2022/index.html* gratis downloadbar sowie in gedruckter Form im Buchhandel *(ISBN 978-3-7089-2274-4, facultas Verlag)* erhältlich.

### Wesentliche Erkenntnisse

Wie seitens der Herausgeber und Autoren zu Beginn angenommen, sind die meisten der von den Kongressdelegierten identifizierten technischen und rechtlichen Maßnahmen gegen Hatespeech und Fake News aus einem Grund nicht durchsetzbar: Das Internet ist so international verwoben, dass eine Maßnahme bspw. eines Bonner Amtsgerichts oder einer hessischen Polizeibehörde nur innerhalb der Staats-, bestenfalls Unionsgrenze wirksam ist und gegenüber dem Betreiber eines Webangebots mit Sitz und Server in einem oder mehreren Drittstaaten de facto keine Wirkung entfaltet. Dazu kommt im Heimatstaat der meisten großen Internetplattformen, den USA, eine völlig andere (Rechts-)Auffassung von Meinungsfreiheit, da dort der Erste Verfassungszusatz auch Sachverhalte schützt, die hierzulande unter Verbotsgesetze fallen. Andere beabsichtigte Maßnahmen, bspw. Uploadfilter, sind technisch unausgereift und der Einsatz außerhalb des Nationalstaats bzw. der EU nicht durchsetzbar. Gleiches gilt für eine Klarnamenpflicht, die, wenn in Deutschland angeordnet, einem Betreiber einer Social-Media-Plattform in einem Nicht-EU-Drittstaat gleichgültig sein wird.

Die empirische Umfrage mit ca. 200 von Delegierten retournierten Fragebögen in englischer und französischer Sprache bestätigte, dass die meisten Lokal- und Regionalpolitiker hier Trainings- und Unterstützungsbedarf haben – und diese Trainings- und Unterstützungsangebote auch gewünscht sind.


Übergabe des Buches "COUNTERFAKE: A scientific basis for a policy fighting fake news and hate speech" in Brüssel Foto: BS/privat

### Ausweg: Open Government und Open Data

Über 80 Prozent der befragten Lokal- und Regionalpolitiker sehen "Open Data, transparency of the grounds of political decision making" als sinnvoll zur Bekämpfung von Hatespeech und Fake News an, über 75 Prozent "Better explanation of decisions to the citizenry". Dies zeigt doch, dass der Weg zur Bekämpfung eher in mehr Transparenz, mehr Schulung und Training, aber auch besseren Angeboten der nationalen Polizeibehörden für Betroffene liegt. Verbote und Gebote sind in einem offenen Internet, wie wir es haben, faktisch nicht durchsetzbar, da die Kompetenz des Nationalstaates auf sein Staatsgebiet (bzw. das Unionsgebiet in der EU) beschränkt ist.

**Prof. Dr. Robert Müller-Török ist Professor für Informationsmanagement und E-Government an der Hochschule für öffentliche Verwaltung und Finanzen Ludwigsburg.*