Frau Präsidentin, liebe Kolleginnen, liebe Kollegen,

am 21. Februar 2022 hat der russische Präsident Wladimir Putin die beiden zum Staatsgebiet der Ukraine gehörenden Gebiete Luhansk und Donezk als unabhängige Staaten anerkannt und angekündigt russische Soldaten in die ostukrainischen Separatistengebiete zu entsenden. Kurz darauf begann der flächendeckende Angriff auf die Ukraine und die Bilder die wir seitdem bis heute aus der Ukraine sehen sind kaum zu ertragen. Eltern mit kleinen Kindern verbringen in U-Bahn-Schächten ihre Nächte, um Schutz vor Raketen und Bomben zu suchen. Tausende Menschen fliehen. Und hier sind wir bereit als GRÜNE FRAKTION in Baden-Württemberg bestmöglich zu helfen und Flüchtenden den Schutz zu bieten, der ihnen verfassungsgemäß zusteht.

Kommentiert [JW1]: Sowas unterbringen?

Neben den von Bildern bekannte Krieg von Militärfahrzeugen wie Panzern und brennenden Gebäuden in diversen Städten in der Ukraine findet dieser Krieg auch auf einer anderen, weniger intuitiven Ebene statt. Im Cyberraum.
Von DDoS-Attacken, die Webseiten mit Hilfe einer Überlastung der IT-Infrastruktur von staatlichen Institutionen, Banken oder Unternehmen lahmlegen bis zu Wiper-Angriffen, die infizierte Festplatten dauerhaft unbrauchbar machen.
Das Ziel dabei: Die dahinterstehende Organisation soll ein möglichst großer Schaden zugesetzt werden.
Das alles können wir vermehrt sowohl auf russischer als auch ukrainischer Seite beobachten. Oftmals sind die Täter generell Wettbewerber, unzufriedene Nutzer, politische Aktivisten oder einzelne Kriminelle oder Gruppierungen. Wer genau für Cyberattacken verantwortlich ist bleibt häufig unbeantwortet – in diesem Konflikt jedoch haben sich bereits Hackergruppen sowohl mit Russland als auch der Ukraine solidarisiert bis hin zum Verdacht, dass einige Kollektive für einen Staat wie Russland aktiv sind.

Kommentiert [JW2]: Ransomware Conti mit Russland solidarisiert
Sandworm könnte sogar vom russischen Staat sein

Anonymous mit Ukraine

Und ich stimme meiner Parteikollegin und Außenministerin Annalena Baerbock zu, wenn sie sagt, dass „unsere Welt nach diesem völkerrechtswidrigen Angriffskrieg von Putin jetzt eine andere [ist].“

Das trifft jedoch nicht nur auf die physische Welt zu, sondern auch auf die digitale Welt.
So warnt das Bundesamt für Sicherheit in der Informationstechnik (BSI) über eine abstrakt erhöhte Bedrohungslage insbesondere für Bundesverwaltung, kritische Infrastrukturen sowie Unternehmen in Deutschland.

Und somit müssen wir uns als Land Baden-Württemberg auch in der digitalen Welt auf Cyberattacken vorbereiten, um unsere Institutionen und die Demokratie zu schützen.

Hierfür hat das Innenministerium ihre Cybersicherheitsstrategie Baden-Württemberg – Perspektive 2026 – veröffentlicht mit einem Plan wie die Cybersicherheitsagentur Baden-Württemberg (CSBW) in den kommenden 5 Jahren ausgebaut werden soll. Sie wird dabei in die bestehende Cybersicherheitsarchitektur aus EU-, Bundes-, Landes- und kommunaler Ebene eingegliedert, wobei sie auf der Ebene des Landes ein zentraler Baustein der Cybersicherheit unseres Landes wird.
Sie wird die Aufgabe der Prävention übernehmen und so beispielsweise mit Schwachstellenscans für öffentliche Stellen die Resilienz unserer öffentlichen Verwaltung auf kommunaler Ebene stärken. Sie wird zum starken Partner für unsere kommunale Familie und KMUs als lokaler Multiplikator des BSI.
Sie schließt die KRITIS-Lücke zwischen Betreibern die aus Sicht des Landes zu den KRITIS zählen, jedoch nicht von der BSI-Kritisverordnung des Bundes erfasst sind. (– so liegt bei dieser in vielen Sektoren der Regelschwellenwert für kritische Infrastruktur bei 500.000 versorgten Personen). Und sie erstellt Lageberichte, die aufgrund der gegenwärtigen Lage engmaschiger stattfinden, im

Austausch mit dem BSI, den CERTs des Bundes und der Länder, der Polizei, dem Verfassungsschutz, den Rechenzentren der Landesverwaltung, mit Komm.ONE sowie mit vernetzten Unternehmen. Ich möchte mich hiermit für ihren Einsatz und der erhöhten Rufbereitschaft in diesen Zeiten bedanken.

Doch nicht nur die IT-Sicherheit am Status Quo ist wichtig. Auch die Cybersicherheitsforschung am Hochtechnologiestandort Baden-Württemberg gilt es weiter voranzutreiben. Das Kompetenzzentrum KASTEL am KIT ist neben der Forschung auch ein Fachkräftegarant welcher in Zukunft meiner Meinung nach von Landesseite noch zusätzlich flankiert werden sollte, um die Schlagkraft einer CSBW zu gewährleisten.

(PAUSE)
Liebe Kolleginnen und Kollegen.
Heute geht es jedoch nicht nur um die IT-Sicherheit, welche laut BSI den Schutz der Vertraulichkeit (Confidentiality), der Integrität (Integrity) und der Verfügbarkeit (Availability) von Daten beinhaltet und diese mit angemessenen Maßnahmen schützt.

(IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.)

Kommentiert [JW3]: Evtl. Zitat des BSI dazu?

Heute geht es um Cybersicherheit und diese ist im Gegensatz dazu breiter angelegt als IT-Sicherheit und umfasst zusätzlich sozio-kulturelle, politische, rechtliche und weitere Dimensionen wie es im §2 Absatz 11 des Cybersicherheitsgesetzes heißt: „alle Aspekte der Sicherheit in der Informationstechnik und den Schutz gesellschaftlich relevanter Prozesse im gesamten Cyberraum.“.

So wurde im letzten Cyber Security Report 2021 erwähnt, dass die größten Cyber-Risiken für die Menschen in Deutschland 2021 die folgenden sind:
Platz 1: Datenbetrug im Internet
Platz 2: Computerviren bzw. Schadsoftware
Platz 3: Fake News

Und bei dem Thema Fake News sehen wir, dass Cybersicherheit nicht nur durch eine Behörde alleine gewährleistet werden kann. Hierbei sind wir alle – in diesem Hohen Hause – wie in der Gesellschaft als Ganzes gefordert. Neben russischen Bot-Farmen/Bot-Netzen (einem Verbund von Rechnern, die von einem fernsteuerbaren Schadprogramm (Bot) befallen sind – teilweise dezentral von Privatpersonen genutzte Geräte, teilweise in Lagerhallen voller Smartphones oder Rechnern), die versuchen die öffentliche Meinung und den öffentlichen Diskurs mit Fake-Accounts auf Social Media oder Troll-Armeen in Kommentarspalten zu verfälschen bis hin zu Telegram-Gruppen, die in ihrer Bubble glauben, dass Echsenmenschen das Weltgeschehen heimlich lenken. Selbst das Hacking von Social Media Accounts und das streuen falscher Informationen über diese authentischen Profile oder DeepFake Videos, die scheinbar eine Person etwas sagen lassen was diese nie gesagt hat.
Das sind Herausforderungen, die durch eine CSBW nicht gelöst werden können und dennoch zur Cybersicherheit gehören und den gesellschaftlichen Zusammenhalt grundlegend gefährden.

Kommentiert [JW4]: Bot-Farm erklären?

Wir müssen alle als Gesellschaft lernen Fehlinformation, Desinformation und Verschwörungserzählungen zu differenzieren.
Wobei die Desinformation als gezielte Verbreitung falscher oder irreführender Informationen abzugrenzen ist von schlechtem Journalismus was in der Regel nicht intendierte Falschinformationen

Kommentiert [JW5]: 1.Dekontextualisierung oder bewusst falsche Interpretation von Informationen
2. Manipulation ursprünglich wahrer Informationen
3. Vollkommen frei erfundene Inhalte

aufgrund journalistischer Fehler sind und schlechter Politik, wobei „Fake News“ als Kampfbegriff gegen etablierte, klassische Medienangebote missbraucht wird.
Denn wir dürfen eines nicht vergessen: Digitale Räume sind gesellschaftliche Räume.
Ich appelliere hiermit an uns alle – achten Sie darauf von wem Sie welche Informationen bekommen. Hinterfragen Sie kritisch und seien Sie bereit Fakten, die unserer Meinung und unserem Gefühl widersprechen anzuerkennen. Denn nur, wenn wir uns auf die Probleme in der heutigen Zeit einigen, können wir über mögliche Lösungswege demokratisch debattieren und somit unsere Demokratie stärken und uns vor Cyberangriffen gesellschaftlich wehren.