piratenpartei
www.piratenpartei.ch

Piratenpartei Schweiz, 3000 Bern

Stellungnahme der Piratenpartei Schweiz zur Sicherheitspolitischen Strategie der Schweiz 2026

Sehr geehrter Herr Bundesrat Pfister
Sehr geehrte Damen und Herren

Bezugnehmend auf Ihre Vernehmlassungseröffnung vom 12.12.2025 nehmen wir gerne Stellung und würden es zukünftig sehr begrüssen, wenn wir als politische Partei in ihre Adressatenliste aufgenommen werden.

Im Weiteren finden wir Piraten es sehr bedenklich, dass Sie für die Stellungnahme auf eine proprietäre Software verweisen (Word der Firma Microsoft), wo es doch heute zahlreiche offene und freie Dateiformate gibt. Wir entsprechen ihrem Wunsch mit einer docx-Datei, welche auch in neueren Word Versionen geöffnet werden kann.

Die Piratenpartei Schweiz setzt sich seit Jahren für eine humanistische, liberale und progressive Gesellschaft ein. Dazu gehören die Privatsphäre der Bürger, die Transparenz des Staatswesens, inklusive dem Abbau der Bürokratie, Open Government Data, den Diskurs zwischen Bürgern und Behörden, aber auch die Abwicklung alltäglicher Geschäfte im Rahmen eines E-Governments. Jede neue digitale Schnittstelle und Applikation bedingt aber eine umfassende Risikoanalyse und Folgeabschätzung.

Gerne nehmen wir wie folgt Stellung:

Allgemein

Die vorliegende Strategie greift wichtige Punkte auf, die zum Schutz der Bevölkerung und des Landes beitragen können. Es mag denn auch etwas in der Natur der Sache liegen, dass der vorliegende Text des Öfteren die Sicherheit über alles stellt. Aber bei allen Gefahren sollte nicht vergessen gehen, dass die zu beschützenden Güter auch erhalten bleiben müssen, um sie beschützen zu können. Mitunter ist abzusehen, dass gewisse Massnahmen direkt auf unsere Privatsphäre zielen und es ist zu befürchten, dass die Meinungsfreiheit vermeintlich zu ihrem eigenen Schutz eingeschränkt werden soll.

Wie das Papier durchaus richtig festhält sind Polarisierung, Spaltung, Terrorismus und Extremismus ernstzunehmende Bedrohungen für die innere Sicherheit (vgl. S22f.). Aber neben guten Ansätzen wie Information, Sensibilisierung und Bildung wird erneut die Ausweitung der Möglichkeiten des Nachrichtendiensts gefordert. Die weitere Aushebelung unserer Privatsphäre und die Überwachung unserer Meinungen soll zu deren Schutz beitragen - ein Witz.

Wenn man ausserdem Stärken und Schwächen in unserem föderalistischen (dezentralen) System sieht, wie es das Strategiepapier tut (vgl. S24ff.), sollte die Absicherung gegen die Schwächen nicht die Aufhebung der Stärken bedeuten. Genau dies geschieht jedoch, wenn beispielsweise mit POLAP vorgeschlagen wird, Plattformen bzw. deren Abfragen zu bündeln.

Zu den einzelnen Massnahmen:

M2 Bekämpfung von Beeinflussungsaktivitäten und Desinformation
Empfehlung: Keine Zensurinfrastruktur oder staatliche Instanz zur Deklarierung von «Wahrheit».
Begründung:
Die Massnahme zielt auf die Bekämpfung von Desinformation ab. Die Hervorhebung von politischer Bildung ist dabei besonders erfreulich. Die Kompetenzförderung der Bevölkerung, Desinformation selbst erkennen zu können, ist der liberalste Weg, diesem Problem entgegenzutreten. Sensibilisierung, Medienkompetenz und allgemeine Bildung können die Resilienz relevant stärken.

Etwas schwammig wird in der Massnahme aber auch von «präventiven und reaktiven Massnahmen» geschrieben. Solche Formulierungen lassen es erneut offen, Zensurinfrastrukturen oder staatliche Instanzen zur Deklarierung, was wahr ist (bzw. Verbot von «fake news»), zu entwickeln. Diese Wege sind in einer demokratisch-freiheitlichen Gesellschaft nicht zielführend, da sie gerade die Strukturen zerstören, die sie beschützen sollen.

M6 Erhöhung der Informationssicherheit der Bundesbehörden
Empfehlung: Keine ausländische Software- oder Hardwareabhängigkeit inkl. Rechenzentren (z.B. Microsoft 365).
Begründung:
Wir begrüssen das Ziel einer verbesserten Informationssicherheit, sehen jedoch relevante Lücken im Strategiepapier: Technologische Abhängigkeiten von ausländischen Softwareanbietern und Rechenzentren werden kaum adressiert.

So hat der Bund erst Ende 2025 vermeldet, auf rund 54'000 Arbeitsplätzen Microsoft 365 eingeführt zu haben. Zwar wird das Risiko wahrgenommen und zumindest reduziert, indem keine besonders schützenswerten

oder vertraulichen Daten in der Microsoft Cloud gespeichert werden – die Abhängigkeit von einem unzuverlässigen «Partner»-Land bleibt jedoch bestehen.[1] Bei der Beschaffung von Software sollten Open-Source-Lösungen prioritär geprüft werden: Sie ermöglichen unabhängige Sicherheitsaudits, vermeiden Vendor-Lock-in und stärken die digitale Souveränität der Schweiz nachhaltig.

Zuletzt ist es verständlich, dass die Schweiz kaum eine eigene Chipfabrik aufstellen wird; eine gewisse Hardwareabhängigkeit lässt sich nicht verhindern. Aber auch bei Rechenzentren sollte bewusst sichergestellt werden, dass die Hardware unter Kontrolle schweizerischer Unternehmen steht, die nicht von anderen Ländern kontrolliert werden können.

M12 Reduktion von Abhängigkeiten in der Energieversorgung und bei kritischen Technologien
Empfehlung: Stärkere Dezentralisierung der Energieversorgung sowie Förderung digitaler Souveränität bei kritischen Technologien.
Begründung:
Die Stossrichtung dieser Massnahme ist grundsätzlich unterstützenswert. Energieunabhängigkeit und digitale Souveränität sind wichtige sicherheitspolitische Anliegen.

Bei der Energieversorgung sollte jedoch eine Dezentralisierung fokussiert werden. Kleinteilige, dezentrale Lösungen, wie etwa Wasserwirbelkraftwerke, Photovoltaik auf Gebäuden oder lokale Energiegemeinschaften erhöhen die Resilienz des Gesamtsystems deutlich, da sie weniger anfällig für gezielte Angriffe oder grossflächige Ausfälle sind als zentralisierte Infrastruktur. Diese Potenziale sollten explizit gefördert werden.

Bei kritischen Technologien begrüssen wir die angekündigte Analyse von Abhängigkeiten. Auch hier gilt: Wo immer möglich, sollten offene Standards und Open-Source-Lösungen bevorzugt werden, da diese unabhängig überprüfbar sind und versteckte Hintertüren oder Sicherheitslücken zumindest erkannt werden können. Technologische Souveränität ist nicht delegierbar.

M19 Verbesserung der Cyberfähigkeiten
Empfehlung: Offensive Fähigkeiten nicht auf Kosten der Sicherheit der eigenen Bevölkerung.
Begründung:
Die Piratenpartei steht offensiven Cyberfähigkeiten des Staates skeptisch gegenüber. Werden gefundene Sicherheitslücken gehortet statt den Herstellern gemeldet, gefährdet der Staat damit aktiv die Sicherheit der eigenen Bevölkerung.
Die Vergangenheit zeigt zudem, dass staatlich entwickelte Hacking-Tools regelmässig unkontrolliert in falsche Hände geraten.[2] So können die geheimgehaltenen Lücken massiven Schaden anrichten, selbst wenn sie zunächst nicht von zwielichtigen Dritten entdeckt werden.

Gefundene Sicherheitslücken müssen den betroffenen Herstellern gemeldet und geschlossen werden. Offensive Fähigkeiten dürfen nicht auf Kosten der Sicherheit der Bevölkerung aufgebaut werden.

[1] https://www.news.admin.ch/de/newnsb/frKHCNmrngH8I3vO8ip7o

[2] https://www.derstandard.at/story/3000000314034/akute-gefahr-fuer-millionen-iphone-user-maechtiges-hacking-tool-offen-im-netz-verfuegbar

M20 Revision des Nachrichtendienstgesetzes
Empfehlung: Streichung.
Begründung:
Mehr Überwachungsbefugnisse ohne wirksame Kontrolle stärken nicht die Sicherheit, sondern gefährden die Grundrechte der Bevölkerung.

Die vorliegende Massnahme befeuert erneut in erster Linie den nicht zu bändigen Datenhunger des Nachrichtendiensts, um die Bevölkerung immer umfassender überwachen zu können. Dieses Vorgehen schützt nicht die Bevölkerung, sondern behandelt sie als nicht-vertrauenswürdig. Eine zersetzende ideologische Einstellung, die einer Demokratie unwürdig ist. Die wirksamen und nicht demokratiefeindlichen Ansätze sind bereits in anderen Punkten untergebracht (z.B. Armutsbekämpfung, Bildung, Sensibilisierung etc.), so dass dieser Punkt verlustfrei gestrichen werden kann.

M21 Stärkung der Prävention von Radikalisierung und Extremismus
Empfehlung: Keine Netzsperren.
Begründung:
Radikalisierung und Extremismus sind eine Gefahr für demokratische Gesellschaften und die Ursachenbekämpfung durch Unterstützung von Projekten der Armutsbekämpfung und Bildung sind unterstützenswerte Ansätze. Der Punkt fordert aber z.B. auch die Sperrung von Internetseiten.

DNS-Sperren sind äusserst ineffizient, da sie leicht zu umgehen sind, beispielsweise mit einem VPN - wer beispielsweise den Browser Opera verwendet, kann den dort schon integrierten VPN-Service nutzen. Weiter kann man mit wenigen clicks alternative DNS-Server in Windows, Mac oder Linux/Unix-Betriebssystem eintragen. Auf Android- oder iOS-Geräten geht es noch leichter, indem eine App wie z.B. «1.1.1.1: Faster Internet» oder «Quad9 Connect» installiert wird.

M24 Verstärkung des polizeilichen Datenaustauschs
Empfehlung: Streichung von POLAP.
Begründung:
Die Massnahme will explizit POLAP vorsehen, um den nationalen und internationalen Datenaustausch zu intensivieren. Dies ist aus unserer Sicht abzulehnen. Das POLAP schafft zwar, soweit gesehen, keine eindeutig neuen Zugriffsrechte. Der Bündelungseffekt einer einzigen Abfrage über alle angeschlossenen Systeme senkt die Zugangsschwelle jedoch massiv. Wo vorher eine Sicherheitsschwelle bestand, die den Personendaten einen gewissen sachgerechten Schutz bot, wird dieser mit POLAP aufgelöst.

Der erläuternde Bericht zum POLAP hält selbst fest, dass der EDÖB erhebliche Bedenken hat zur Umsetzung bezüglich unserer Persönlichkeitsrechte (S. 47 Erläuternder Bericht Verbesserung des polizeilichen Informationsaustauschs): «Der EDÖB ist der Auffassung, dass die Erteilung gesetzeskonformer Zugriffsberechtigungen [...] für die Verantwortlichen als anspruchsvoll und entsprechend als mit hohen Risiken verbunden einzustufen sei». Es ist abzusehen, dass das Grundrecht auf Privatsphäre erneut eingeschränkt werden soll. Mit dem Anschluss an internationale Plattformen (SIS, INTERPOL, Europol, ETIAS, EES, Eurodac) wird der Eingriff in das Grundrecht zusätzlich verschärft.

Der ständige nahezu uneingeschränkte Zugriff einer nationalen Plattform mit internationaler Anbindung ist stark unverhältnismässig. Es sollte stattdessen genügen, die bestehenden Amtshilfeverfahren weiter zu digitalisieren.

Schlussbemerkungen

Wir beschränken uns in dieser Stellungnahme auf unsere Kernanliegen. Bei Verzicht unsererseits auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Regelungen, ist damit keine Zustimmung durch die Piraten zu solchen Regelungen verbunden.

Kontaktdetails für Rückfragen finden Sie in der Begleit-E-Mail.

———

Piratenpartei Schweiz, Arbeitsgruppe Vernehmlassungen, 31. März 2026