Signatur:	2025.SR.0368
Geschäftstyp:	Interpellation
Erstunterzeichnende:	Michelle Steinemann (Mitte), Georg Häsler (FDP), Lukas Schnyder (SP), Dominic Nellen (SP)
Mitunterzeichnende:	Lukas Wegmüller, Mehmet Özdemir, Bernadette Häfliger, Béatrice Wertli, Andreas Egli, Laura Curau, Nicolas Lutz, Nik Eugster, Chantal Perriard, Simone Richner, Ursula Stöckli, Janosch Weyermann, Thomas Glauser, Alexander Feuz, Ueli Jaisli, Mirjam Roder, Michael Ruefer, Christoph Leuppi, Oliver Berger
Einreichedatum:	6. November 2025

Interpellation: Schutz der Stadt Bern vor Spionageaktivitäten; Antwort

Fragen

Der Gemeinderat wird um Beantwortung folgender Fragen in Zusammenarbeit mit dem Nachrichtendienst des Bundes und den Nachrichtendienst-Elementen der KAPO Bern gebeten:

1. Wie schätzt der Gemeinderat die Bedrohung durch Spionage und Desinformationsaktivitäten in der Stadt Bern und im Umfeld der Stadtverwaltung ein?
2. Welche organisatorischen und technischen Schutzmassnahmen bestehen gegen Spionage oder Cyberangriffe auf städtische Infrastrukturen?
3. Wie erfolgt die Zusammenarbeit zwischen der städtischen Verwaltung und kantonalen bzw. nationalen Stellen beim Verdacht auf Spionage?
4. Welche Massnahmen erachtet der Gemeinderat als angemessen, um dieser Gefahr entgegenzutreten?
5. Welche·Zusammenarbeit besteht mit kantonalen und nationalen Sicherheitsbehörden, um solchen Bedrohungen vorzubeugen?
6. Inwiefern beobachtet die Stadt Bern Versuche der Einflussnahme auf die öffentliche Meinungsbildung oder politische Prozesse durch ausländische Akteure?
7. Gibt es Anzeichen·dafür, dass politische Konflikte/Polarisierung in Bern gezielt durch fremde Nachrichtendienste befeuert werden?

Begründung

Laut dem Bericht «Sicherheit Schweiz 2025» verstärkt die globale Konfrontation den Druck auf die Schweiz. Mit führenden Technologieunternehmen und internationalen Organisationen wird sie für ausländische Nachrichtendienste immer interessanter. Die grösste Spionagebedrohung geht von Russland und China aus, die bekanntermassen beide hierzulande eine starke nachrichtendienstliche Präsenz unterhalten. Sie interessieren sich für Bundesbehörden, Firmen, internationale Organisationen und Forschungseinrichtungen. Gerade Bern ist als Bundesstadt im besonderen Fokus, weil genau diese Institutionen hier ansässig sind. Als konkretes Beispiel für Spionage gab es im Sommer 2025 Berichte über verdächtige Drohnenflüge im Umfeld militärischer Anlagen in der Schweiz, insbesondere in Meiringen BE, und eine explizite Warnung der Armee vor potenzieller Spionage durch ausländische Nachrichtendienste. Damit bestehen erhöhte Anforderungen an den Schutz sensibler Informationen und Infrastrukturen auch auf städtischer Ebene resp. bei der städtischen Verwaltung. Die Stadt Bern hat sich aktiv mit den kantonalen und nationalen Sicherheitsbehörden zu vernetzen und den Informationsaustausch aktiv zu fördern. Angesichts zunehmender Cyberaktivitäten und hybrider Einflussversuche interessiert, wie der Gemeinderat die Risiken für die Stadt Bern einschätzt und welchen Beitrag die Stadt zum Schutz leisten kann und muss.

Antwort des Gemeinderats

Die Stadt Bern ist im Bereich der Spionageaktivitäten und Cyberkriminalität weitestgehend auf die funktionierenden Strukturen auf Ebene des Bundes und des Kantons Bern angewiesen. Sie selbst verfügt weder über die Instrumente der Lageanalyse noch über besondere Zuständigkeiten bzw. Kompetenzen zur Abwehr krimineller Aktivitäten. Die Stadt Bern ist jedoch aktiv im Monitoring auffälliger Aktivitäten in ihren Informationstechnologien oder beispielsweise auch im Bereich der kritischen Energieinfrastruktur. Ebenso betreibt sie eine Sensibilisierung bei den Datennutzenden.

Zu Frage 1:
Gemäss Lagebericht 2025 des Nachrichtendienstes des Bundes (NDB) wird die Spionagebedrohung in der Schweiz als hoch eingeschätzt. Dies umfasst u.a. auch Beeinflussungsaktivitäten ausländischer Akteure. Die Lageeinschätzung bezüglich verbotener Nachrichtendienste obliegt dem NDB. Aufgrund der allgemeinen Beurteilung des NDB ist naheliegend, dass solche Aktivitäten (auch) in Bern stattfinden (können).

Zu Frage 2:
Der Schutz bzw. die Resilienz von kritischen Infrastrukturen ist von zentraler Wichtigkeit. Unter kritischen Infrastrukturen werden Dienstleistungs- und Versorgungssysteme verstanden, die essenziell für die Wirtschaft bzw. die Lebensgrundlagen der Schweizer Bevölkerung sind (Stromversorgung, medizinische Versorgung, Informations- und Telekommunikationstechnologien usw.).

Zum Schutz der städtischen Energieinfrastruktur: Der Schutz der städtischen Energieinfrastruktur vor Spionage und Cyberangriffen basiert auf einem ganzheitlichen Sicherheitskonzept. Dieses umfasst klare organisatorische Zuständigkeiten, ein etabliertes Informationssicherheits-Management, geschulte Mitarbeitende, Notfall- und Krisenpläne sowie verbindliche Sicherheitsanforderungen für externe Partner. Ergänzend werden technische Massnahmen wie Netzwerksegmentierung, mehrstufige Schutzsysteme, starke Zugriffskontrollen, Verschlüsselung, kontinuierliches Monitoring, regelmässige Updates und physische Sicherheitsvorkehrungen eingesetzt. Dabei orientiert sich Energie Wasser Bern (ewb) an anerkannten Standards, insbesondere an der nach ISO/IEC 27001 zertifizierten Informationssicherheit, sowie am IKT-Minimalstandard des Bundes. Die Schutzmassnahmen werden laufend überprüft und in Zusammenarbeit mit zuständigen Behörden und Fachstellen weiterentwickelt.

Zum Schutz der städtischen IT-Infrastruktur: Die Stadt Bern betreibt mehrere Schutzsysteme, welche Zugriffsversuche, den Datenverkehr sowie potenzielle Schwachstellen kontinuierlich und automatisiert überwachen. Zudem arbeitet die Stadt Bern eng mit externen Partnern wie dem Bundesamt für Cybersicherheit (BASC) zusammen und erhält regelmässig relevante Informationen zur aktuellen Bedrohungslage und zu identifizierten Sicherheitslücken. Die Security Spezialistinnen und Spezialisten von Informatik Stadt Bern (IBE) beobachten die Bedrohungssituation fortlaufend und leiten bei Bedarf proaktiv geeignete Massnahmen ein. Die Stadt Bern beabsichtigt, das Themenfeld Cybersecurity künftig weiter zu stärken und erarbeitet zurzeit eine Strategie zur digitalen Sicherheit. Zum Schutz vor Spionage werden auf IT-Ebene der Stadt gegenwärtig keine technischen oder organisatorischen Massnahmen umgesetzt.

Zu Frage 3:
Wie einleitend erwähnt wird der Staatsschutz auf Ebene der Stadt Bern durch die Behörden von Bund und Kanton betrieben. Auffälligkeiten werden der Kantonspolizei Bern und/oder den zuständigen Bundesstellen gemeldet. Die Stadt Bern und auch ewb erhalten vom BACS Informationen zur aktuellen Bedrohungslage sowie Meldungen, falls sie von sicherheitsrelevanten Vorfällen betroffen wären.

Zur Organisation und Zusammenarbeit im Allgemeinen kann der Gemeinderat Folgendes festhalten:

Der Bund koordiniert die Cybersicherheit auf nationaler Ebene und legt mit der Nationalen Cyberstrategie (NCS) den strategischen Rahmen fest. Er unterstützt Kantone, Gemeinden und die Wirtschaft bei der Umsetzung und steuert die Cybersicherheit der Bundesverwaltung. Das BACS dient dabei als zentrale Fach- und Koordinationsstelle und stellt Lageinformationen, Warnungen und Unterstützung zur Verfügung. Der Nachrichtendienst des Bundes beobachtet die Bedrohungslage, insbesondere im Bereich Spionage, und informiert kantonale und nationale Behörden über relevante Erkenntnisse. Zudem ist der Bund für die internationale Zusammenarbeit im Cyberbereich zuständig.

Die Kantone gestalten ihre Organisation zur Cybersicherheit selbst, orientieren sich dabei jedoch an den Vorgaben und Zielen der NCS. Sie verfügen über eigene Koordinations- und Fachstrukturen und arbeiten untereinander über interkantonale Gremien und Konferenzen zusammen.

Die Gemeinden können von den bestehenden Strukturen des Bundes und der Kantone, etwa durch Lageinformationen, Empfehlungen und Schulungsangebote profitieren. Neben dem oben erwähnten Melde- und Informationsfluss mit den Bundesbehörden nehmen beispielsweise ewb sowie die IT-Security-Spezialist*innen der Stadt Bern an den wöchentlichen Lagebild-Meetings des BACS teil und ergreifen aufgrund der aktuellen Bedrohungslage proaktiv die geeigneten Massnahmen.

Sicherheitsvorfälle müssen nach einheitlichen Prozessen gemeldet werden, damit eine koordinierte Reaktion über alle Verwaltungsebenen hinweg möglich ist. Wichtig sind regelmässige Risikoanalysen betreffend Spionage und Cyberangriffe. Schulungen und Sensibilisierungsmassnahmen können das Sicherheitsbewusstsein der Mitarbeitenden fördern. Die Sensibilisierung der Mitarbeitenden erfolgt im Rahmen der ICT Sicherheitsschulungen, durch Meldungen zu aktuellen Bedrohungen im Intranet und künftig im Rahmen der geplanten Security Awareness Kampagne sowie der entsprechenden Massnahmen.

Wird ein Cyberangriff gemeldet oder identifiziert, analysieren die IT Security-Spezialistinnen und -Spezialisten der Stadt Bern die verfügbaren Informationen und holen bei Bedarf zusätzliche Angaben bei den betroffenen Stellen ein. Anschliessend erfolgt die Meldung des Vorfalls an das BACS mittels des standardisierten BACS-Formulars. Sollten dem BACS weitere Informationen fehlen, sind diese innerhalb der definierten Frist von 14 Tagen nachzureichen. Wird beim Vorfall eine Unterstützung durch das BACS benötigt, kann dies im Rahmen der Meldung entsprechend angegeben werden.

Die Zusammenarbeit zwischen Bund und Kantonen wird durch den Sicherheitsverbund Schweiz gestärkt, der als Plattform für Austausch, Koordination und gemeinsame Empfehlungen dient. Die Nationale Cyberstrategie bindet alle staatlichen Ebenen sowie weitere Akteure ein und fördert die gemeinsame Verantwortung. Ein regelmässiger Informationsaustausch zwischen Bund und Kantonen stellt sicher, dass Bedrohungen frühzeitig erkannt und koordiniert behandelt werden können. Eine funktionierende Zusammenarbeit zwischen den Behörden ist in diesem Bereich essentiell. Grundlage dafür bildet die Nationale Cyberstrategie (NCS), welche Rollen, Zuständigkeiten und Koordinationsmechanismen klar definiert.

Auf kommunaler Ebene der Stadt Bern soll das Thema Cybersicherheit wie erwähnt im Rahmen einer Strategie zur digitalen Sicherheit weiter gestärkt werden.

Zu Frage 4:
Der Gemeinderat erachtet auf Stufe der Stadt Bern ein Bewusstsein für Meldungen und somit die Sensibilisierung als essenziell. Für weitergehende Massnahmen der Abwehr von Spionage- und Cyberaktivitäten ist jedoch der Bund zuständig. Der Gemeinderat verweist an dieser Stelle auf die vom Bundesrat am 18. Februar 2026 in Aussicht gestellten Arbeiten für entsprechende Gesetzesentwürfe, um die Resilienz und die Datensicherheit kritischer Infrastrukturen zu verbessern.

Zu Frage 5:
Siehe Antwort zu Frage 3.

Zu Frage 6:
Wie erwähnt liegt die Lageanalyse und Beobachtung nicht im Zuständigkeitsbereich der städtischen Behörden. Warnungen erhält die Stadt Bern via Bundesamt für Cybersicherheit und/oder Kantonspolizei Bern.

Zu Frage 7:
Dem Gemeinderat liegen aktuell keine konkreten Anzeichen oder Meldungen dafür vor. Im Allgemeinen ist aber die Stadt Bern von solchen Aktivitäten nicht ausgenommen (s. Antwort zu Frage 1).

Bern, 4. März 2026

Der Gemeinderat