

Auszug aus dem Protokoll des Regierungsrates des Kantons Zürich

Sitzung vom 19. August 2026

834. Stärkung und Vernetzung der Innovations- und Forschungskraft im sicherheitspolitischen Bereich (Stossrichtungen und Massnahmen, neue Ausgabe, Amt für Wirtschaft, Stellenplan)

A. Ausgangslage

Der Wirtschaftsstandort Zürich zählt zu den erfolgreichsten Regionen weltweit. Dieser Erfolg beruht insbesondere auf seiner Anpassungsfähigkeit im Strukturwandel und der Fähigkeit, gestärkt aus Krisen – wie der Finanzkrise – hervorzugehen. Diese historisch gewachsene Krisenfestigkeit gerät nun jedoch zunehmend unter Druck.

Die globale Sicherheitslage ist wegen des strukturellen Grossmachtwettbewerbs, der Schwächung internationaler Institutionen und des zunehmenden Protektionismus instabil. Die weltpolitische Stimmung ist stark fragmentiert, was sich in der internationalen Wirtschaft deutlich in Form von Handelskonflikten und Lieferkettenunsicherheiten niederschlägt. Zudem wachsen die technologischen Abhängigkeiten. Die Schweiz und Europa sind mit neuartigen und komplexen sicherheitspolitischen und wirtschaftlichen Herausforderungen konfrontiert. Drohnen legen europäische Flughäfen temporär lahm, Cyberattacken schwächen die hiesigen KMU und Desinformation verändert die Art, wie sich die breite Bevölkerung im digitalen Raum bewegt und ihre Meinung bildet. Die Bedrohungen lassen sich dabei immer weniger klassischen Abwehrdomänen zuordnen. Sie finden vermehrt übergreifend im Cyber-, Informations- und Wirtschaftsraum statt, richten sich gegen kritische Infrastrukturen und die Gesellschaft insgesamt. Diese hybride Bedrohungslage betrifft Staat, Wirtschaft und Bevölkerung gleichermassen. Sicherheit muss daher integral angegangen werden.

Der Bund verfolgt mit der «Sicherheitspolitischen Strategie 2026», die 2026 verabschiedet werden soll, einen umfassenden Ansatz. Die Sicherheitspolitik soll ganzheitlich gestaltet werden. Sie umfasst zivile und militärische Mittel und Akteure. Die Strategie bezieht sämtliche für die Sicherheitspolitik relevanten Aspekte der Aussen-, Innen- und Wirtschaftspolitik in ihre Planung und Vorkehrungen mit ein. Das nahtlose Zusammenwirken dieser Mittel und Akteure stärkt die Resilienz und die Abwehrfähigkeiten. Die innere Sicherheit ist zu wahren und Verwundbarkeiten im Bereich Handel und Technologie sind zu reduzieren.

Der Kanton Zürich kann auf relevante und gut arbeitende Institutionen wie die Kantonale Führungsorganisation, das Amt für Militär und Zivilschutz, die Kantonspolizei, das kantonale Zentrum für Informationssicherheit im Amt für Informatik oder die Fachstelle für wirtschaftliche Landesversorgung im Amt für Wirtschaft zurückgreifen. Die Kantone unterstützen den Bund in der Kommunikation, geben ergänzende Informationen weiter und sind zuständig für die Krisenbewältigung im Rahmen kantonalen Aufgaben.

Die vorgenannten Institutionen und Organisationen sind in ihrer Aufgabenerfüllung auf technologische Unterstützung angewiesen. In einer hybriden Bedrohungslage haben künstliche Intelligenz, Robotik, autonome Systeme, Biometrie und Cybersicherheit einen besonderen Stellenwert. Verschiedene Technologien und Innovationen entwickeln sich zunehmend zu Dual-Use-Technologien mit sicherheitspolitischer Relevanz. Drohnentechnologien verändern z. B. die zivile und militärische Bedrohung grundlegend, indem sie präzise und kostengünstige Einsätze ermöglichen und gleichzeitig neue Anforderungen an Schutz und Abwehr stellen. Hybride Bedrohungen müssen frühzeitig erkannt, deren Auswirkungen begrenzt sowie die Handlungs- und Funktionsfähigkeit von Staat und Verwaltung sowie Wirtschaft und Gesellschaft aufrechterhalten werden.

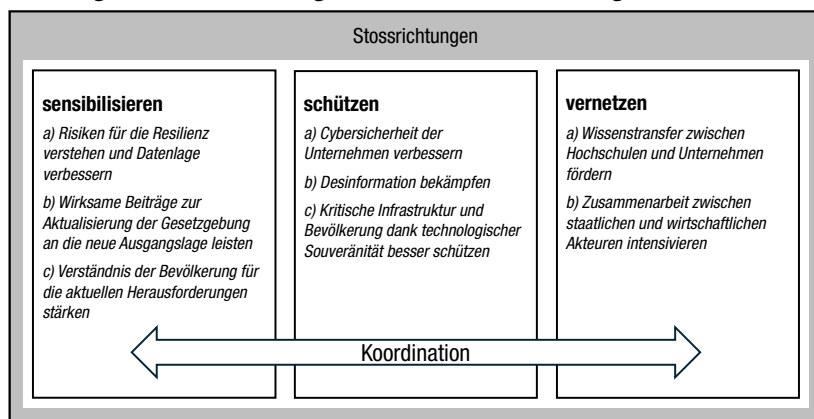
Der Regierungsrat hat sich für die laufende Legislatur zum Ziel gesetzt, dass die Bevölkerung in ausserordentlichen Lagen umfassend geschützt ist und die wesentlichen Lebensgrundlagen sowie die Handlungs- und Führungsfähigkeit auf allen Stufen erhalten bleiben (vgl. Richtlinien der Regierungspolitik 2023–2026, RRB Nr. 871/2023, RRZ 1). Er will zudem den Dialog und die Vernetzung von Wirtschaft, Wissenschaft und Verwaltung fördern (RRZ 8e). Durch eine gezielte Stärkung des wirtschaftlichen Potenzials kann ein wirksamer Beitrag zur Resilienz der Schweiz und des Kantons Zürich geleistet werden.

B. Stossrichtungen und Massnahmen

Der Kanton Zürich verfügt über eine hohe Innovationskraft, eine starke Forschungslandschaft sowie über eine Vielzahl von Unternehmen, die sich mit modernen Schlüsseltechnologien befassen. Damit kann der Kanton einen aktiven Beitrag zur Stärkung der technologischen, wirtschaftlichen und gesellschaftlichen Resilienz des Standorts im Kontext zunehmender hybrider Bedrohungen leisten. Dies soll gestützt auf § 1 des Standortförderungs- und Unternehmensentlastungsgesetzes (LS 930.1) durch die Bestimmung der relevanten Kompetenzen, deren Vernetzung und die Schaffung von geeigneten Rahmenbedingungen gestärkt werden («Zürcher Weg»). Die wirtschaftliche Leistungsfähigkeit soll dabei nicht nur in Zeiten ungestörter Lieferketten funktionieren, sondern auch dann, wenn diese Ketten gestört sind. Hinzu kommt, dass

sich die Technologien sehr rasch entwickeln und damit innert kürzester Zeit neue Bedrohungsbilder entstehen können. Die Sicherheitsbehörden sind daher auf agile Unternehmen und etablierte Partnerschaften angewiesen. Die relevanten Unternehmen und Institutionen sollen als strategische Partner der kantonalen Stellen auch in Krisenzeiten zur Verfügung stehen. Deshalb soll die Zusammenarbeit mit diesen Partnern im Sinne eines strategischen Grundsatzentscheids gezielt angestrebt und gefördert werden. Nur so ist eine Zusammenarbeit auch in Krisenzeiten möglich. Da nicht ausgeschlossen werden kann, dass sich die Bedrohungslage in den kommenden Monaten und Jahren akzentuieren wird, besteht Handlungsbedarf.

Die Fähigkeiten zur Unterstützung der Resilienz sollen mit einem gezielten Einsatz der Standortförderungsinstrumente in den drei Stossrichtungen «sensibilisieren», «schützen» und «vernetzen» gestärkt werden. Für jede Stossrichtung werden Umsetzungsmassnahmen bestimmt. Um Synergieeffekte zu erzielen, müssen die Massnahmen koordiniert und mit den Sicherheitsorganisationen abgestimmt werden. Insgesamt sind folgende Stossrichtungen und Massnahmen vorgesehen:



Stossrichtung «sensibilisieren»

a) Risiken für die Resilienz verstehen und Datenlage verbessern

Eine analytische und faktenbasierte Datenlage ermöglicht es, Verwundbarkeiten und kritische Abhängigkeiten so weit zu reduzieren, dass der Kanton Zürich und die Schweiz weniger Angriffsflächen bieten und das Schadenpotenzial minimiert werden kann. Gemeinsam mit Bundes- und Fachstellen sowie Expertinnen und Experten aus Wissenschaft und Wirtschaft sollen die Auswirkungen der sicherheitspolitischen Lage auf Bevölkerung, Unternehmen und den Standort Zürich eingeschätzt werden. Dabei sind die bereits bestehenden Mittel, Methoden und Prozesse im Kanton Zürich, namentlich die Elemente der Kantonspolizei Zürich, zu berücksichtigen.

b) Wirksame Beiträge zur Aktualisierung der nationalen Gesetzgebung an die neue Ausgangslage leisten

Eine nachhaltige Resilienz setzt voraus, dass die Regulierung mit dem Wandel Schritt hält. Dazu braucht es eine enge Abstimmung mit dem Bund, den zuständigen Fachstellen und relevanten Verbänden. So kann der Kanton Zürich die Bedürfnisse des Standorts gezielt in die Weiterentwicklung von Gesetzgebung und Verordnungen auf nationaler Ebene einbringen.

c) Verständnis der Bevölkerung für die aktuellen Herausforderungen stärken

Eine gut informierte und eingebundene Bevölkerung ist entscheidend dafür, dass Massnahmen im Krisenfall greifen und von der Gesellschaft mitgetragen werden. Vor diesem Hintergrund soll das Verständnis für Krisen-, Vorsorge- und Sicherheitsthemen gestärkt und den gesellschaftlichen Dialog gezielt gefördert werden. Dafür sollen bestehende Formate des Kantons Zürich genutzt und mit dezentralen Dialogplattformen in den Gemeinden ergänzt werden.

Stossrichtung «schützen»

a) Cybersicherheit der Unternehmen verbessern

Cyberangriffe stellen für Unternehmen und insbesondere für KMU eine wachsende Bedrohung dar. Sie können einzelne Betriebe direkt schädigen, Produktionsprozesse unterbrechen oder sensible Daten gefährden. Ein besonderer Bedarf besteht beim Schutz von Lieferketten. Cyberangriffe über Zulieferer, Software oder externe Dienstleister nehmen zu und können ganze Wertschöpfungsketten destabilisieren und damit auch die Stabilität des Wirtschaftsstandorts schwächen.

Aktuelle Erhebungen zeigen, dass sich nur rund die Hälfte der Schweizer KMU im Bereich der Cybersicherheit ausreichend geschützt fühlt und Investitionen in Schutzmassnahmen teilweise unter Druck geraten.

Abgestützt auf die Angebote des Bundesamtes für Cybersicherheit soll deshalb der Aufbau einer zentralen Anlaufstelle für KMU geprüft werden. Im Vordergrund stehen der erleichterte Zugang zu Wissen, bestehenden Bundesangeboten und vertrauenswürdigen Fachstellen sowie die gezielte Stärkung der Cyberresilienz der KMU. Angeboten werden soll ein strukturierter Zugang zu bestehenden Angeboten und Hilfsmitteln, etwa in den Bereichen Wachsamkeit und Schulungen oder mit einem KMU-spezifischen Bedrohungsradar. Die Massnahmen sollen bestehende Angebote berücksichtigen (z. B. des Bundesamtes für Cybersicherheit, der Cyberklinik der Universität Zürich, ITSec4KMU des Kantons Zug). Parallelstrukturen sind zu vermeiden.

b) Desinformation bekämpfen

Desinformation kann nicht nur Einzelpersonen oder Unternehmen schädigen und in Verruf bringen, sondern auch das Vertrauen in Institutionen und Medien untergraben sowie den politischen Meinungsbildungsprozess und insbesondere die direkte Demokratie vor Abstimmungen gezielt beeinflussen. Mit entsprechenden Programmen, unter Einbindung der Schweizer Hochschulen, in Abstimmung mit den Wirtschaftsverbänden, wie auch in Kooperation mit dem International Panel on the Information Environment mit Sitz in Zürich, soll der Gefahr der Desinformation entschieden entgegengetreten werden. Die bereits laufenden Bemühungen des Kantons Zürich, beispielsweise die Massnahmen im Bereich des integralen Risikomanagements werden dabei berücksichtigt.

c) Kritische Infrastruktur und Bevölkerung dank technologischer Souveränität besser schützen

Drohnen sind heute eine akute Gefährdung für die Infrastruktur. Es wird zwischen Drohneneinsatz, Drohnerdetektion und Drohnenabwehr unterschieden. Die Drohnerdetektion und die Drohnenabwehr gehören zu den sich am schnellsten entwickelnden Themen im Bereich des Schutzes kritischer Infrastrukturen. Die Abhängigkeit von ausländischen Drohnenanbietern und Anbietern wirksamer Abwehrtechnologien ist derzeit hoch und führt dazu, dass Anpassungen auf heutige Bedürfnisse oftmals nicht oder nur beschwerlich möglich sind.

Der Standort Zürich verfügt mit führenden Hochschulen, innovativen Start-ups und einer leistungsfähigen Hightech-Industrie bereits über wesentliche Voraussetzungen, um die technologische Souveränität und Handlungsfähigkeit im Bereich der Drohnentechnologien sicherstellen zu können. Dieses Potenzial ist für den Schutz der kritischen Infrastruktur vor Ort zu nutzen.

Stossrichtung «vernetzen»

a) Wissenstransfer zwischen Hochschulen und Unternehmen fördern

Die Stärkung der Industriebasis ist eine wichtige Voraussetzung für die Resilienz. Der Wissens- und Technologietransfer im Sicherheitsbereich ist mit besonderen Anforderungen verbunden. Insbesondere Aspekte der Vertraulichkeit, regulatorische Vorgaben sowie Rahmenbedingungen der internationalen Zusammenarbeit erschweren etablierte Transfermechanismen und erfordern angepasste Formen der Kooperation. Plattformen und Formate für den regelmässigen Austausch sollen den Zugang zu relevanten Partnern erleichtern. Brückenfunktionen zwischen Wissenschaft und Wirtschaft erleichtern den Wissenstransfer. In diesem Kontext spielen Innovationshubs wie der Innovationspark

Zürich eine wesentliche Rolle. Sie bieten Platz für die Zusammenarbeit der Akteure, Zugang zu Test- und Pilotumgebungen und können mit gezielten «Accelerator»-Programmen und Unterstützungsdienstleistungen auch zur Formierung weiterer Start-ups beitragen. Durch branchenübergreifende Vernetzung und den Austausch mit Fachpersonen aus Wissenschaft, Wirtschaft und Verwaltung können Unternehmen besser befähigt werden, sicherheitsrelevante Technologien zu entwickeln und zu produzieren.

b) Zusammenarbeit zwischen staatlichen und wirtschaftlichen Akteuren intensivieren

Die Entwicklung im Bereich der Sicherheitstechnologien verläuft zunehmend dynamisch und ist stark von der Fähigkeit abhängig, Innovation rasch in die Anwendung zu überführen. Gelingt es der Schweiz, mit neuen Lösungen oder Komponenten auch im europäischen Kontext ein relevantes Gewicht (Pfand) zu entwickeln, stärkt dies ihre Position als verlässliche Partnerin im internationalen Umfeld.

Die Innovationskraft und technologische Lösungen müssen deshalb möglichst direkt auch für die Landesverteidigung nutzbar gemacht werden können. Dafür braucht es eine wirkungsvolle Zusammenarbeit zwischen den Unternehmen und den staatlichen Akteuren, die es ermöglicht, dass neue Lösungen frühzeitig unter realen Bedingungen erprobt und durch die öffentliche Hand rasch als erste Anwenderin aufgenommen werden können.

Gerade für Start-ups ist das Wissen über regulatorische Anforderungen, Beschaffungsprozesse, Sicherheitsstandards und die besonderen Rahmenbedingungen im sicherheitsrelevanten Umfeld oftmals neu und nur schwer zugänglich. Entsprechend wertvoll ist eine gezielte Orientierung und Unterstützung entlang des Entwicklungspfad.

Koordination

Die Stossrichtungen umfassen technologische, wirtschaftliche, gesellschaftliche und sicherheitstechnische Aspekte. Die Massnahmen sind inhaltlich und organisatorisch übergreifend anzugehen und eng aufeinander abzustimmen. Eine koordinierte Vorgehensweise ist dabei zentral, um Synergien zu nutzen, Doppelspurigkeiten zu bestehenden Aufgaben und Tätigkeiten zu vermeiden und die Wirksamkeit der Massnahmen insgesamt zu erhöhen. Wirtschaft und Wissenschaft sind miteinander zu vernetzen. Zudem soll der Austausch mit anderen Kantonen und dem Bund sowie mit weiteren relevanten Institutionen vertieft werden. Dieser Austausch ermöglicht eine zielführende Vorgehensweise und die Abstimmung gemeinsamer Herausforderungen. Bei der Umsetzung soll primär auf bestehende Strukturen, Kooperationen, Netzwerke und Institutionen abgestellt werden.

C. Personelle und finanzielle Mittel

Mit dem vorliegenden Beschluss soll das bestehende Potenzial des Standorts Zürich besser genutzt werden, um die Resilienz des Kantons Zürich zu stärken. Das Know-how ist in bestehenden Institutionen, Organisationen und Unternehmen vorhanden. Durch eine gezielte Vernetzung kann das Potenzial jedoch noch besser genutzt werden. Die Aufgabe besteht nicht darin, Wissen aufzubauen, sondern darin, das vorhandene Wissen zu vernetzen und übergreifend zu nutzen. Dafür ist die Einrichtung einer Gesamtprojektleitungsstelle notwendig. Deren Aufgabe besteht darin, die Stossrichtungen und Massnahmen aus einer Gesamtsicht zu konkretisieren, zu koordinieren und aufeinander abzustimmen. Sodann ist die Stelle zuständig für die Vernetzung der Stakeholder aus Verwaltung, Wissenschaft und Wirtschaft über alle Ebenen und untereinander. Die Arbeiten erfolgen in einem komplexen und sensitiven Umfeld. Das Zusammenbringen von sicherheitspolitischen, technologischen und wissenschaftlichen Stakeholdern erfordert gleichermassen koordinatorisches und fachliches Know-how, was eine gewisse Seniorität und Erfahrung voraussetzt.

Für die Gesamtprojektleitung ist eine Stelle als Adjunkt/in in der Lohnklasse 20 vorgesehen. Die Schaffung neuer Stellen ist vom Regierungsrat zu bewilligen (§§ 4 f. Vollzugsverordnung zum Personalgesetz [VVO, LS 177.111]). Die Stelle hat einen Zusammenhang mit der Standortförderung und wird deshalb beim Amt für Wirtschaft angesiedelt. Der Stellenplan des Amtes für Wirtschaft ist per 1. Oktober 2026 wie folgt zu ergänzen:

Stellen	Funktion	Richtposition	Klasse VVO
1,0	Gesamtprojektleitung	Adjunkt/in	20

Das Personalamt, Fachstelle Lohn, hat die Einreihung des neuen Stellenprofils geprüft und erachtet diese als nachvollziehbar.

In finanzieller Hinsicht sind neben den Lohnkosten (Fr. 175 000 pro Jahr) weitere Mittel für die Umsetzung erforderlich. Für die Planung der Umsetzung und für erste Massnahmen sind 2026 bis 2028 Ausgaben von insgesamt Fr. 1 080 000 vorgesehen (2026: Fr. 180 000, 2027 Fr. 400 000 und 2028 Fr. 500 000). Es handelt sich um eine neue Ausgabe (§ 37 Abs. 1 Gesetz über Controlling und Rechnungslegung [LS 611]). Folgekosten sind keine zu erwarten. Die Mittel 2026 und 2027 sind im Budget 2026 bzw. im Konsolidierten Entwicklungs- und Finanzplan 2026–2029, Planjahr 2027, nicht enthalten und zu kompensieren. Die Mittel 2028 sind ordentlich zu budgetieren. Demzufolge ist für 2026 bis 2028 eine neue Ausgabe von insgesamt Fr. 1 080 000 zulasten der Erfolgsrechnung der Leistungsgruppe Nr. 5301, Amt für Wirtschaft, zu bewilligen.

Die Mittel für die einzelnen Massnahmen können erst bestimmt werden, wenn die Massnahmen durch die Gesamtprojektleitung konkretisiert sind. Die entsprechenden Mittel sind später separat zu beantragen.

Auf Antrag der Volkswirtschaftsdirektion
und der Sicherheitsdirektion

beschliesst der Regierungsrat:

I. Die Stossrichtungen und Massnahmen zur Stärkung und Vernetzung der Innovations- und Forschungskraft im sicherheitspolitischen Bereich werden festgelegt.

II. Die Volkswirtschaftsdirektion wird mit der Umsetzung beauftragt. Die anderen betroffenen Direktionen sind eng einzubeziehen.

III. Im Stellenplan des Amtes für Wirtschaft wird mit Wirkung ab 1. Oktober 2026 folgende Stelle geschaffen:

Stellen	Richtposition	Klasse VVO
1,0	Adjunkt/in	20

IV. Für die Planung der Umsetzung der Massnahmen gemäss Dispositiv I wird eine neue Ausgabe von Fr. 1 080 000 zulasten der Erfolgsrechnung der Leistungsgruppe Nr. 5301, Amt für Wirtschaft, bewilligt.

V. Mitteilung an die Mitglieder des Regierungsrates, die Sicherheitsdirektion und die Volkswirtschaftsdirektion.



Vor dem Regierungsrat
Die Staatsschreiberin:

Kathrin Arioli