



SCHRIFTENREIHE
INNERE
SICHERHEIT

1

Sebastian Hartmann

Sicherheit für alle ist die Voraussetzung einer freien und gleichen Gesellschaft

Moderne Sicherheitspolitik beinhaltet
Prävention, fördert Investitionen und
schafft sozialen Zusammenhalt

■ forum
■ INNERE
■ SICHERHEIT

**FRIEDRICH
EBERT** 
STIFTUNG
Forum Berlin



Die Schriftenreihe »Innere Sicherheit« wird in loser Folge vom Forum Berlin der Friedrich-Ebert-Stiftung herausgegeben. Expertinnen und Experten aus Politik, Zivilgesellschaft, Wissenschaft und Verwaltung beleuchten darin aktuelle Entwicklungen und Herausforderungen der inneren Sicherheit und stellen Lösungsansätze vor.

Über den Autor

Sebastian Hartmann ist seit 2013 Mitglied des Bundestages für den rechtsrheinischen Rhein-Sieg-Kreis. Von 2013 bis zum Juni 2018 war er Mitglied im Ausschuss für Verkehr und digitale Infrastruktur. Seit 2015 ist er Mitglied des Innenausschusses. Dort war er bis 2017 für das Thema Migration und Integration zuständig. Seit 2018 ist Hartmann Berichterstatter für IT-Sicherheit und Zivil- und Katastrophenschutz. Außerdem ist er stellvertretender Berichterstatter für Datenschutz und digitale Verwaltung im Innenausschuss. Seit Juni 2018 ist er Vorsitzender der SPD in Nordrhein-Westfalen.

Kernpunkte auf einen Blick

Nur ein handlungsfähiger, starker Sozialstaat kann ein freies Leben in Sicherheit garantieren. Öffentliche und soziale Sicherheit sind untrennbar verbunden. Sicherheitspolitik ist daher mehr als Kriminalitätsbekämpfung, sie muss auch Aspekte sozialer Räume mitdenken. Wohnungsbauförderung, Entwicklung des Wohnumfeldes und quartierbezogene Sozialarbeit sind wichtig und müssen ausgebaut werden, damit alle gut und in Sicherheit leben können.

Es ist ein sicherheitspolitischer Irrtum, dass durch immer mehr Überwachung mehr Sicherheit erreicht werden kann. Tatsächlich geht es darum, die relevanten Informationen aus einer Flut an Daten zu identifizieren. Dafür müssen die Sicherheitsbehörden technisch und personell besser ausgestattet werden.

Digitale und analoge Sicherheit sind zunehmend verwoben. Um bestmöglichen Schutz für Bürger_innen und Unternehmen zu gewährleisten, muss in IT-Sicherheit investiert und die digitale Sicherheitspolitik defensiv ausgerichtet werden. Dazu gehören auch der massive Ausbau der Verschlüsselungsforschung und schnelle sowie transnationale Kooperationen der Sicherheitsbehörden.

Einleitung

Öffentliche Sicherheit zu gewährleisten ist eine zentrale Aufgabe des Staates. Es ist Usus im sozialdemokratischen Selbstverständnis, dass nur ein handlungsfähiger, starker Sozialstaat ein freies Leben in Sicherheit garantieren kann. Denn echte individuelle Freiheit existiert nur dort, wo Menschen sicher sind. Freiheit und Solidarität sind eng miteinander verknüpft. Aus sozialdemokratischer Sicht ist klar: Dafür braucht es den solidarischen Staat, der Regeln setzt, Ordnung schafft und Sicherheit stiftet – in allen Bereichen des Lebens. Trotzdem gilt gerade die Sicherheitspolitik in der öffentlichen Debatte nicht als Steckenpferd der Sozialdemokratie.

Dabei gewinnt Sicherheit als Wert in der Gesellschaft an Bedeutung und hat im politischen Meinungskampf einen hohen Stellenwert. Diskussionen über Fragen der inneren Sicherheit werden oft emotional geführt. Sicherheitspolitik darf deshalb keine offene Flanke der Sozialdemokratie sein. Meiner Meinung nach muss es diese offene Flanke auch nicht geben. Es gibt gute Konzepte und konkrete Handlungsvorschläge aus sozialdemokratischer Perspektive. Ohne Anspruch auf Vollständigkeit will ich im Folgenden einige davon skizzieren.

Der Unterschied liegt im Menschenbild

Bei der Frage, was sozialdemokratische Sicherheitspolitik von den Ansätzen anderer Parteien unterscheidet, müssen wir mit einem grundlegenden Unterschied im Menschenbild beginnen.

Auf der konservativen Seite haben wir ein Bild, in dem in Anlehnung an Thomas Hobbes »der Mensch dem Menschen ein Wolf ist« und der Staat seine Bürger bändigen muss. Der Gedanke der Prävention oder einer Resozialisierung nach Verbüßung der Strafe ist hier kaum vorhanden. Auf der anderen Seite haben wir ein sozialdemokratisches Menschenbild in Anlehnung an John Locke, in dem sich die Menschen im Prinzip freundlich gegenüberstehen. Je nachdem in welchem Zustand sich die Gesellschaft befindet und wie stark oder schwach der Staat ist, kann es aber auch hier zu handfesten Konflikten kommen.

Sozialdemokratische Sicherheitspolitik ist mehr als Kriminalitätsbekämpfung

Öffentliche und soziale Sicherheit hängen eng zusammen. Je größer die Ungleichheit zwischen den Menschen ist, desto größer ist das Konfliktpotenzial einer Gesellschaft. Verbessern wir die soziale Lage, gehen auch Konflikte und Kriminalität zurück. Nirgendwo zeigt sich dieser Zusammenhang von Sozial- und Sicherheitspolitik deutlicher als im

urbanen Raum. Der Zusammenhang zwischen Kriminalität und Wohnumgebung ist erwiesen. Wenn in einem Quartier städtische Öffentlichkeit weitgehend fehlt und soziale Brennpunkte existieren, begünstigt das Kriminalität. Das hat nichts damit zu tun, dass Menschen in solchen Vierteln stärkere kriminelle Neigungen hätten. Aber Sicherheitspolitik hat auch immer eine sozialpolitische Dimension.

Wir müssen als Gesellschaft bereits vor dem Entstehen von Kriminalität ansetzen und fragen: »Was brauchen Menschen, um in Frieden und Freiheit zu leben und wie kann der Staat das für seine Bürgerinnen und Bürger ermöglichen?« Eine ausgewogene Stadtentwicklung ist die Voraussetzung für die Vermeidung sozialer Brennpunkte. Sozialdemokratische Sicherheitspolitik wird fühlbar, wenn der Staat seinen Bürgerinnen und Bürgern bezahlbaren und guten Wohnraum zur Verfügung stellt und Menschen nicht aus ihrem vertrauten Kiez verdrängt werden. Gibt es gute Schulen und Betreuungsangebote in der Freizeit oder wird auch noch das letzte Jugendzentrum geschlossen? Ein weiteres ganz konkretes Beispiel, was für mich Sicherheitspolitik ist: Die Bereitstellung sauberer und beleuchteter Bushaltestellen, an denen Bürgerinnen und Bürger auf den Bus warten können, der auch noch nach 19 Uhr fährt, führt zu mehr Sicherheit und einem besseren Sicherheitsgefühl.

Seriöse Sicherheitspolitik denkt sozialräumliche Aspekte mit

Wohnungsbauförderung, Maßnahmen zur Verbesserung des Wohnumfelds und quartiersbezogener Sozialarbeit müssen daher massiv ausgebaut werden. Wir brauchen einen »New Deal« für soziale Investition und soziale Innovation. Konkret: Es muss endlich massiv in unsere Schulen, Universitäten, unsere Infrastruktur investiert werden. Wir brauchen Zehntausende neuer Bürgerhäuser und Jugendzentren, um mehr Orte der Begegnung zu schaffen. Lokale Demokratie braucht reale Orte. Diese sozialräumlichen Aspekte mitzudenken ist seriöse Sicherheitspolitik. Niemand darf von öffentlichen Gütern abgeschnitten sein.

Um zu einer Ordnung zu kommen, die für die gleichen Rechte und Möglichkeiten der Menschen sorgt, müssen wir viel Geld in die Hand nehmen. Nur Reiche können sich einen schwachen Staat leisten. Doch auch sie werden in einer ungleichen und ungerechten Gesellschaft mit ihren vielen Konflikten nicht glücklich werden. Von konservativer Seite wird in Fragen der öffentlichen Sicherheit zuallererst etwas vom Bürger gefordert. Aber es gibt auch eine Bringschuld der öffentlichen Seite, diese Sicherheit tatsächlich zu liefern. Denn erst wenn der öffentliche Raum sicher ist, kann jeder Einzelne seine Freiheit wirklich ausleben: »Freiheit ist unmöglich, wenn sie nicht durch den Staat gesichert wird« (Karl Popper).

Sicherheit ist auch ein Gefühl von Gerechtigkeit

Zur Sicherheit gehört auch das Gefühl von Gerechtigkeit. Menschen haben ein feines Gespür für die Frage: Was wird mit aller Härte des Gesetzes verfolgt und an welcher Stelle wird Nachsicht geübt? Wenn etwa durch einen Cum-Ex-Raub 33 Milliarden Euro an Steuergeldern gestohlen wurden, diese Praktiken den entsprechenden Stellen spätestens 2010 bekannt waren, aber erst im September 2019 ein einzelnes Strafverfahren gegen zwei Börsenhändler eröffnet wird, dann fühlen sich die Menschen verschaukelt. Wenn gleichzeitig Menschen Haftersatzstrafen antreten müssen, weil sie etwa die Busfahrkarte nicht zahlen konnten, erzeugt das ein Gefühl von Ohnmacht und Wut.

Das Unsicherheitsgefühl wächst

Als Mitglied des Innenausschusses begegne ich einer widersprüchlichen Situation. Objektiv betrachtet wird die Sicherheitslage in Deutschland zunehmend besser. Mit Blick auf Gespräche im Wahlkreis und anhand von Umfrageergebnissen muss ich jedoch feststellen, dass es ein gesteigertes Unsicherheitsgefühl gibt.

Diese Differenz ist allerdings nur scheinbar widersprüchlich. Das Sicherheitsempfinden hängt auch damit zusammen, wie ich den öffentlichen Raum wahrnehme. Es verschlechtert sich, wenn zum Beispiel die Polizei zusammengespart wird, in der Fläche kaum präsent sein kann und nur ein einziger Streifenwagen nachts für mehrere ländliche Gemeinden zuständig ist. Deswegen hat die SPD gefordert, die Polizei in Deutschland um mindestens 15.000 Stellen zu stärken und konnte dieses Ziel im Koalitionsvertrag festschreiben. Bei der Umsetzung sehen wir aktuell aber auch, wie schwer und langwierig es ist, eine einmal zusammengesparte Polizei wieder aufzubauen. Deshalb sind solche Investitionen zukünftig dauerhaft und unabhängig von der wirtschaftlichen Lage zu tätigen.

Ein zweiter relevanter Faktor für das Wahrnehmungsparadoxon in der Sicherheitspolitik ist sicherlich ein verändertes Nachrichtenverhalten. Wir erhalten durch die Digitalisierung immer mehr und schneller Informationen. Gleichzeitig wird es schwieriger, diese zu validieren und in die richtigen Relationen zu setzen. Algorithmen analysieren die Lesegewohnheiten und richten die zur Verfügung gestellten Informationen entsprechend aus. Wer in den sozialen Medien einen Bericht über einen Messerangriff liest, dem werden im Anschluss weitere ähnliche Berichte angezeigt. Social-Media-Kanäle verstärken durch diese Logik ihrer Algorithmen die Fokussierung auf bestimmte Ausschnitte der Realität. Auch so entstehen Parallelwelten in der Wahrnehmung von Wirklichkeit.

Manipulationen und gezielte Falschinformationen sind auf Social-Media-Kanälen gerade bei Berichten über Kriminalität wirksam. Die Bestätigung des eigenen Gefühls wird wichtiger als rationale Argumente. Verschwörungstheorien haben nicht umsonst Konjunktur. Vorschlagsfunktion und Autoplay begünstigen vor allem auf YouTube eine Parallelwelt von Verschwörungstheorien und Extremismus, während Google die Werbeeinnahmen dafür einfährt. Das ist ein drängendes sicherheitspolitisches Problem.

Social-Media-Anbieter müssen endlich ihrer Verantwortung gerecht werden und viel schneller und öfter die Verbreitung von Fake-News und extremistischen Inhalten unterbinden sowie die entsprechenden Nutzerkonten sperren. Zu lange haben sie sich nicht für gefährliche und menschenverachtende Inhalte auf ihren Plattformen interessiert. Es muss klar sein: Plattformen sind für die Inhalte auf ihren Seiten verantwortlich. Strengere Vorgaben an die Plattformen beim Umgang mit Hate Speech sind wichtig. Denn hier treffen Demagogen für ihre radikale Propaganda auf fruchtbaren Boden.

Digitalisierung und Rechtsextremismus

Das Erstarken extremistischer Bewegungen hat viele Ursachen. Eine ist sicherlich die zunehmende Komplexität der Welt. Extremistische Bewegungen bieten eine Reduktion auf scheinbar einfache Antworten. Sie sind aber die denkbar schlechteste Antwort auf alle Fragen. Der Terrorismus von Rechts ist heute eine der größten Gefahren für unsere freiheitliche Gesellschaft und das friedliche Zusammenleben.

Wer angesichts der bundesweiten Vernetzung und Aktionen von »NSU 2.0«, »Nordkreuz« oder »Combat 18« noch die These von rechtsextremen Einzeltätern proklamiert, verschließt die Augen vor der Realität: In Deutschland agieren organisierte und hochgerüstete rechtsextreme Netzwerke. Das Internet begünstigt dabei die Vernetzung von Gleichgesinnten.

Wir sehen zunehmend die Grenze zwischen Rechtskonservativen, Rechtsradikalen bis hin zu rechtsextremen Neonazis schwinden. Für die Sicherheitsbehörden wird es schwieriger, die realen Gefahren aus der Masse an Informationen und Daten rechtzeitig herauszufiltern. Sie benötigen daher dringend geeignete Werkzeuge, um frühzeitig etwa in Foren und sozialen Netzwerken Radikalisierungstendenzen von Gruppen und Einzelpersonen zu erkennen. Durch Big-Data-Ansätze können systematische Auswertungen und Analysen vorgenommen werden. Dabei ist es allerdings ein sicherheitspolitischer Irrtum, dass durch immer mehr Überwachungsmöglichkeiten mehr Sicherheit erreicht werden könne. Es ist selten so, dass die entscheidenden Informationen nicht vorhanden oder nicht zugänglich waren. Die wahre Herausforderung liegt vielmehr darin, aus dem Wust an Informationen die wirklich rele-

vanten herauszufischen. Dafür braucht die Polizei die entsprechenden digitalen Analyseprogramme, für diese Arbeit gut geschulte Polizistinnen und Polizisten und eine verbesserte Zusammenarbeit über Ländergrenzen hinweg. Wichtige Projekte wie gemeinsame Datenbanken und ein standardisierter Informationsfluss werden angegangen. Der Weg dorthin hat aber gezeigt, dass die Interoperabilität von Daten und ihre intelligente Verknüpfung von Anfang an mitgedacht werden müssen, um sie nicht erst später mit Verzögerung und viel Aufwand umzusetzen. Beim Informationsaustausch geht es im Übrigen nicht um die Aufhebung des Trennungsverbotes zwischen Polizei und Nachrichtendiensten, welches wir in Deutschland aus sehr guten Gründen haben. Aber die Sicherheitsbehörden müssen durch klare Regeln in die Lage versetzt werden, entlang dieses Trennungsverbotes ihre Aufgaben wahrzunehmen und frühzeitig auf Gefahren reagieren zu können.

Cyberkriminalität und der Schutz davor

Ebenso wie sich Extremisten das Internet zu Nutze machen, agieren Kriminelle auch in anderen Feldern zunehmend digital. Wir sehen, dass digitale und analoge Sicherheit zunehmend miteinander verwoben sind. Menschen werden Opfer von Identitäts- und Datendiebstahl. Industrieanlagen und kritische Infrastrukturen wie Strom- und Wasserversorgung arbeiten vernetzt und sind so über das Internet angreifbar. Es ist eine Frage der öffentlichen Sicherheit, in IT-Sicherheit zu investieren und damit Bürger, Unternehmen und Staat bestmöglich zu schützen.

Angesichts ansteigender Zahlen an IT-Sicherheitsvorfällen sind Antworten dringlich. Dabei kann es in der digitalen Welt ebenso wenig wie in der analogen Welt absolute Sicherheit geben. Der Anspruch muss aber sein, den bestmöglichen Schutz für Bürgerinnen und Bürger und deutsche Unternehmen zu gewährleisten. Dafür sollten wir die digitale Sicherheitspolitik strikt defensiv ausrichten.

Keine Behörde und kein Unternehmen kann gleichzeitig Weltspitze in defensiven und in offensiven Cyberfähigkeiten sein. Um nicht in beidem mittelmäßig zu sein, ist die klare Fokussierung auf einen Bereich notwendig. Wir sollten unsere Anstrengungen auf die Entwicklung sicherer und innovativer Abwehrinstrumente für Bürger, Wirtschaft und Staat richten. Denn die Rechnung von Kriminellen ist recht simpel: Ist der Aufwand für einen Hack teurer, als der zu erwartende Ertrag, wird von dem Angriff in der Regel abgesehen. Eine aktive Cyberstrategie könnte dagegen eine Eskalationsspirale in Gang setzen, deren Folgen nicht abzuschätzen wären und dadurch langfristig nicht zu mehr Sicherheit, sondern zu mehr Unsicherheit führen.

Auf Seite der Strafverfolgungsbehörden besteht aktuell die Sorge, dass ihre Überwachungsmethoden mit zunehmender Verbreitung von Verschlüsselung unbrauchbar wür-

den. Dieses Phänomen wird als »Going Dark« bezeichnet. Um dem entgegenzuwirken, wollen sie noch nicht geschlossene Sicherheitslücken offenhalten. Ich halte das Nichtschließen dieser Lücken, sogenannten »0-Day-Exploits«, hingegen für ein massives Sicherheitsrisiko. Es gibt so gut wie keine Situation der Gefahrenabwehr, die das Risiko einer solchen Offenhaltung rechtfertigt. Stattdessen würde dadurch alles unsicherer. Denn wenn jeder staatliche und nicht-staatliche Akteur auch nur eine Hand voll »0-Days« pro Jahr für offensive Zwecke zurückhalten würde, bedeutete das in der Summe Tausende offene Sicherheitslücken, die genauso von allen anderen Akteuren genutzt werden könnten – und würden.

Wir schaffen im Gegenteil mehr Sicherheit, wenn wir Verschlüsselungen noch weiter verstärken. Die Bundesregierung hat nicht umsonst in ihrer digitalen Agenda 2014 das Ziel beschlossen, »Verschlüsselungsstandort Nr. 1 auf der Welt« zu werden. Darauf sollten wir mit dem massiven Ausbau von Verschlüsselungsforschung und dem verpflichtenden Ansatz von »Security by design« und »Security by default« hinarbeiten.

Digitale Prävention

Ebenso wie in der analogen Welt ist in der digitalen Welt Prävention ein wichtiger sicherheitspolitischer Ansatz. Unabhängig von allen technischen Vorkehrungen ist der Mensch weiterhin die größte IT-Sicherheitsschwachstelle. Jedes Jahr wird eine Rangliste der meistgenutzten Passwörter veröffentlicht und jedes Jahr sind Passwörter wie »123456« oder »password« ganz weit oben. Die Menschen für Fragen des IT-Schutzes zu sensibilisieren, kann viel Schaden verhindern. Deswegen wird das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit dem Verbraucherschutz einen ganz entscheidenden zusätzlichen Aufgabenbereich erhalten.

Nicht jede und jeder kann die Sicherheit von IT-Geräten selbst einschätzen. Für Verbraucher war es in der Regel bisher kaum möglich, die Sicherheit von Geräten wie Internetroutern oder Handys einzuschätzen. Sicherheit ist daher bis heute kaum ein Faktor bei der Kaufentscheidung und folglich für Produzenten kein maßgebliches Kriterium. Weil der Markt an dieser Stelle versagt hat, gleichzeitig aber immer mehr vernetzte Geräte Einzug in die Haushalte halten, soll zukünftig ein Kennzeichen Auskunft über die IT-Sicherheit dieser Geräte geben. Angesichts der Dringlichkeit des Themas bin ich über die Abwehrhaltung vieler Unternehmen gegenüber einem solchen Sicherheitszertifikat erstaunt. Denn für mich ist offenkundig: Wer die Sicherheit als wichtiges Feature seines Produktes begreift, müsste sich über solche Standards freuen. Denn so setzt er sich von einer Konkurrenz ab, welche die Schnittstellen für Kriminelle gleich frei Haus liefert.

Digitale Polizeiarbeit

Angesichts der Digitalisierung der Gesellschaft muss sich auch die Polizeiarbeit digitalisieren. Im Feld der Cyberkriminalität steigen die Zahlen gegenüber dem allgemeinen Trend. Gerade hier fehlen Mittel und entsprechend qualifiziertes IT-Personal, um angemessen durchzugreifen. In der Folge bemühen Bürgerinnen und Bürger nicht einmal mehr die Polizei – und die Dunkelziffer steigt. Der Staat hat aber die öffentliche Sicherheit in allen Bereichen zu gewährleisten – sowohl analog als auch digital.

Schnell werden immer neue Gesetze gefordert. Wo es sinnvoll ist, müssen die Gesetze natürlich angepasst werden. Beispiele sind bessere Durchgriffsrechte des BSI zum Schließen eklatanter Sicherheitsmängel oder die Entkriminalisierung von »ethischem Hacking«, bei dem Schwachstellen den betroffenen Unternehmen gemeldet und nicht auf dem Schwarzmarkt verkauft werden.

Aber zu oft ist die Forderung nach neuen Gesetzen nur der Versuch, konsequentes Handeln vorzutäuschen. Zu oft sind nicht aufgeklärte digitale Straftaten weniger ein Problem mangelnder rechtlicher Möglichkeiten für die Sicherheitsbehörden als ein Vollzugsproblem durch fehlende Expertinnen und Experten, veraltete Technik oder fehlenden Austausch der Behörden. Verbrechen im digitalen Raum machen keinen Halt vor nationalen Grenzen, entsprechend müssen auch Sicherheitsbehörden schnell und in enger Kooperation transnational agieren. In der Abstimmung zwischen Ländern und der Bundesebene muss deswegen das Bundeskriminalamt (BKA) in seiner Koordinierungsfunktion für Cyberkriminalität weiter gestärkt werden. Trotz der schwerfälligen Kooperation auf EU-Ebene muss die Sicherheitspolitik auch europäischer werden. Dazu gibt es auch gar keine Alternative. Auf europäischer Ebene sollte aus Europol mittelfristig eine Art »europäisches FBI« entstehen.

Mehr noch als in der analogen Welt wird im Internet um die Frage von Freiheit versus Sicherheit gerungen. Hier ist ein gemeinsames gesellschaftliches Grundverständnis noch nicht erreicht. Während digitale Bürgerrechtlerinnen und Bürgerrechtler zu oft jegliche digitale Polizeiarbeit als Versuch der staatlichen Internetüberwachung brandmarken, gilt auf der anderen Seite viel zu schnell das Mantra »je mehr Kompetenzen und Überwachungsmöglichkeiten, desto besser«. Unionspolitiker lesen den Sicherheitsbehörden jeden Wunsch von den Lippen ab und fragen viel zu selten nach, ob eine Maßnahme tatsächlich die allgemeine Sicherheit erhöht. Während in der analogen Welt etwa niemand auf die Idee käme, Bauunternehmen den Einbau von Sicherheitslücken in Wohnungstüren vorzuschreiben, damit sie im Fall der Fälle bei einem begründeten Verdacht in die entsprechende Wohnung eindringen können, wird aus konservativer Richtung genau diese Forderung bei der Nutzung von sicherer Kommunikation erhoben. In der Fol-

ge würde allerdings das Sicherheitsniveau insgesamt massiv sinken. Was im analogen Bereich gilt, gilt auch im digitalen: Prävention ist die beste Kriminalitätsbekämpfung und verschlüsselte digitale Technik macht es Kriminellen im Internet ungemein schwerer. Dafür braucht es den handlungsfähigen Staat, der investiert.

Fazit: Solidarität und Prävention statt dem Märchen von absoluter Sicherheit

Ist denn Sicherheit heutzutage erreichbar? Die Antwort lautet ja und nein. Es gilt Missstände anzusprechen, ohne sie zu dramatisieren oder zu instrumentalisieren. Wir müssen nicht alles Erreichte schlecht reden. Dass die Kriminalität seit Jahren zurückgeht, ist nicht vom Himmel gefallen, sondern Ergebnis der guten Arbeit deutscher Sicherheitsbehörden und der politischen Voraussetzungen, die von Bund und Ländern geschaffen worden sind.

In der öffentlichen Debatte dominieren zwar immer die lautesten Forderungen und wir befinden uns insofern in einem Zeitalter des Absolutismus und »Sofortismus« – erst hundertprozentige Sicherheit ist ein Erfolg und diese muss sofort gewährleistet sein. Doch wer ehrlich ist, muss einräumen: Es hat immer Kriminalität gegeben und es wird sie auch in Zukunft geben. Der Trend zeigt aber in die richtige Richtung.

Für mich muss Prävention ein sicherheitspolitischer Schwerpunkt der Sozialdemokratie sein – und zwar in allen Kriminalitätsfeldern. Ein zweiter Schwerpunkt ist die Schaffung gesellschaftlicher Solidarität. Sie schafft reale und gefühlte Sicherheit. Sozialdemokratinnen und Sozialdemokraten sind nicht grundsätzlich gegen »Law & Order«, denn wir sorgen für einen starken Staat, der in der Lage ist, Gesetze durchzusetzen. Wir sorgen aber auch dafür, dass Recht und Regeln für alle gelten. Sozialdemokratische Sicherheitspolitik investiert in den sozialen Zusammenhalt. Solidarität hat dabei immer zwei Seiten: Rechte und Pflichten. Ein handlungsfähiger Staat, der alle Menschen wirklich gleich behandelt und ihnen den gleichen Zugang zu öffentlichen Leistungen bietet, ist die beste Grundlage dafür. Der kaputtgesparte und den Märkten ausgelieferte neoliberale Staat hingegen ist schwach, der ausgrenzende national-völkische Staat der politischen Rechten ist unsolidarisch und ungerecht. Ich halte den sozialdemokratischen Ansatz in Verbindung mit einem positiven Menschenbild für den erfolgversprechendsten Weg, Sicherheits- und Freiheitsbedürfnisse in der Gesellschaft zu vereinen und neben objektiv messbaren Sicherheitsdaten auch dem zunehmenden Unsicherheitsgefühl in der Bevölkerung entgegenzuwirken.

Über uns

Die **Friedrich-Ebert-Stiftung** (FES) ist die älteste politische Stiftung Deutschlands. Benannt ist sie nach Friedrich Ebert, dem ersten demokratisch gewählten Reichspräsidenten. Als parteinahe Stiftung orientieren wir unsere Arbeit an den Grundwerten der Sozialen Demokratie: Freiheit, Gerechtigkeit und Solidarität. Als gemeinnützige Institution agieren wir unabhängig und möchten den pluralistischen gesellschaftlichen Dialog zu den politischen Herausforderungen der Gegenwart befördern. Mit unserer Arbeit im In- und Ausland tragen wir dazu bei, dass Menschen an der Gestaltung ihrer Gesellschaften teilhaben und für Soziale Demokratie eintreten.
(www.fes.de)

Das **Forum Berlin** ist ein Arbeitsbereich im Haus der Friedrich-Ebert-Stiftung in Berlin-Tiergarten. Unsere Aufgabe besteht in der Organisation politischer Bildung und Kommunikation sowie Politikberatung in den bundespolitischen Arbeitsbereichen. Die Themen unserer Arbeitsbereiche vermitteln wir in Fachtagungen, Kolloquien, Lesungen, Gesprächskreisen, digitalen Debattenforen und Publikationen an die Öffentlichkeit. Unser Bemühen gilt dem demokratischen Diskurs und der Kommunikation zwischen Bürgerinnen und Bürgern, Politik, Wissenschaft und Praxis.
(www.fes.de/forum-berlin)

Im **Forum Innere Sicherheit** beschäftigt sich die Friedrich-Ebert-Stiftung mit den aktuellen Herausforderungen und Entwicklungen im Politikbereich »Innere Sicherheit«. Sicherheit ist für alle da und gehört zur Bringschuld des Staates. Mit unseren Angeboten zur politischen Bildung leisten wir einen Beitrag zur Aufklärung und zum Diskurs in diesem komplexen Politikfeld und entwickeln gemeinsam mit Expertinnen und Experten Vorschläge für eine funktionierende und vertrauenswürdige Sicherheitsarchitektur, die den Werten der Sozialen Demokratie verbunden ist.
(www.fes.de/forum-berlin/innere-sicherheit)

Impressum

© 2020

Friedrich-Ebert-Stiftung, Forum Berlin

VERANTWORTLICH

Jan Niklas Engels, Forum Berlin,
Friedrich-Ebert-Stiftung
Hiroshimastraße 17, 10785 Berlin

LEKTORAT

Gaby Rotthaus, Forum Berlin,
Friedrich-Ebert-Stiftung

LAYOUT/SATZ

Heike Wächter, Punkte + Striche,
Büro für Grafikdesign, Berlin

BILDMATERIAL

© Timon Studler/unsplash.com

DRUCK

Druckerei Brandt GmbH, Bonn

Die in dieser Publikation zum Ausdruck
gebrachten Ansichten sind nicht notwen-
digerweise die der Friedrich-Ebert-Stiftung.

Eine gewerbliche Nutzung der von der FES
herausgegebenen Medien ist ohne schrift-
liche Zustimmung durch die FES nicht
gestattet.

ISBN: 978-3-96250-489-2