Terrorismuswatch | #terrorism_watch
www.terrorismismuswatch.de
buero@terrorismuswatch.de

TERRORISMUSBEDROHUNG

BELARUS

Belarus weist gegenwärtig ein niedriges Niveau klassischer terroristischer Gewalt auf und zählt im internationalen Vergleich nicht zu den Staaten mit einer ausgeprägten terroristischen Bedrohung. Das sicherheitspolitische Lagebild wird vielmehr durch die Wechselwirkungen zwischen autoritärer Herrschaft, hybriden Bedrohungen und den Auswirkungen des russischen Angriffskrieges gegen die Ukraine bestimmt. Eigenständige transnationale jihadistische Organisationen, separatistische Bewegungen oder andere terroristische Akteure mit dauerhaft etablierter operativer Infrastruktur innerhalb des Landes sind derzeit nicht erkennbar. Die Wahrscheinlichkeit komplexer Anschläge mit hoher Opferzahl bleibt entsprechend gering.

Die sicherheitspolitische Dynamik wird stattdessen von einer weitreichenden Ausdehnung des staatlichen Terrorismus- und Extremismusbegriffs geprägt. Die belarussischen Behörden wenden diese Kategorien nicht ausschließlich auf terroristische Gewalt im international anerkannten Sinne an, sondern beziehen sie in erheblichem Umfang auf oppositionelle Organisationen, Exilstrukturen, zivilgesellschaftliche Akteure und cybergestützte Widerstandsnetzwerke. Diese Praxis erschwert die internationale Vergleichbarkeit offizieller Statistiken erheblich und macht eine differenzierte Bewertung der tatsächlichen Bedrohungslage erforderlich.

Parallel hierzu hat sich seit Beginn des russischen Angriffskrieges gegen die Ukraine ein sicherheitsrelevantes Umfeld entwickelt, das durch dezentrale Sabotageakte gegen militärisch bedeutsame Infrastruktur, Cyberoperationen oppositioneller Netzwerke sowie die enge militärische Kooperation zwischen Belarus und Russland geprägt wird.

Diese Entwicklungen besitzen zwar erhebliche sicherheitspolitische Relevanz, erfüllen jedoch überwiegend nicht die Kriterien klassischer terroristischer Gewalt. Die größten Risiken ergeben sich daher weniger aus einer unmittelbaren terroristischen Anschlagsbedrohung als aus hybriden Bedrohungen, politisch motivierter Sabotage, Cyberoperationen sowie den regionalen Auswirkungen des Krieges in der Ukraine.

1. Strategische Bedrohungslage

1.1 Gesamtlage

Die strategische Terrorismuslage in Belarus wird durch eine vergleichsweise geringe operative Aktivität terroristischer Organisationen bestimmt. Im Gegensatz zu zahlreichen Staaten Europas, des Nahen Ostens oder Afrikas existieren keine belastbaren Hinweise auf dauerhaft etablierte jihadistische Netzwerke, separatistische Terrororganisationen oder ideologisch motivierte Gruppierungen mit einer kontinuierlichen Anschlagsfähigkeit innerhalb des Landes. Auch eine systematische Serie terroristischer Anschläge gegen staatliche Einrichtungen, kritische Infrastruktur oder die Zivilbevölkerung ist gegenwärtig nicht festzustellen. Das allgemeine Gefährdungsniveau klassischer terroristischer Gewalt ist daher als niedrig einzustufen.

Die sicherheitspolitische Bewertung wird allerdings durch die nationale Begriffsverwendung erheblich erschwert. Die belarussischen Sicherheitsbehörden ordnen eine Vielzahl oppositioneller Aktivitäten unter den Tatbestand des Terrorismus oder Extremismus ein, obwohl diese nach

international anerkannten Definitionen überwiegend als politische Opposition, Sabotage, Cyberaktivismus oder staatsfeindliche Aktivitäten bewertet werden. Hieraus ergibt sich eine deutliche Diskrepanz zwischen der offiziellen nationalen Kriminalstatistik und der internationalen Lageeinschätzung. Die hohe Zahl staatlicher Terrorismusverfahren spiegelt daher nicht zwangsläufig eine entsprechende Entwicklung terroristischer Gewalt wider, sondern ist wesentlich durch die sicherheitspolitische Strategie des Staates geprägt.

Für die Bevölkerung sowie für internationale Unternehmen und ausländische Staatsangehörige ergibt sich daraus ein abweichendes Risikoprofil. Während das unmittelbare Risiko, Opfer eines terroristischen Anschlags zu werden, weiterhin gering bleibt, haben politische Repression, weitreichende Sicherheitsbefugnisse sowie die konsequente Strafverfolgung tatsächlicher oder vermeintlicher Regimegegner deutlich an Bedeutung gewonnen. Die sicherheitsrelevanten Herausforderungen entstehen somit primär aus staatlichen Kontrollmaßnahmen, hybriden Bedrohungen und geopolitischen Spannungen und nicht aus einer klassischen terroristischen Gefährdungslage.

1.2 Sicherheitsumfeld und regionale Einflüsse

Das strategische Sicherheitsumfeld Belarus' wird maßgeblich durch die enge politische, wirtschaftliche und militärische Anbindung an die Russische Föderation geprägt. Seit Beginn des russischen Angriffskrieges gegen die Ukraine hat sich das Land zu einem zentralen Bestandteil der russischen Sicherheitsarchitektur im westlichen Operationsraum entwickelt. Die Nutzung belarussischen Staatsgebiets für militärische Operationen, logistische Unterstützung sowie gemeinsame Streitkräfteübungen hat die sicherheitspolitische Bedeutung des Landes erheblich erhöht und gleichzeitig seine Einbindung in die strategische Konfrontation zwischen Russland und den NATO-Staaten vertieft.

Diese Entwicklung verändert die nationale Bedrohungslage grundlegend. Das sicherheitspolitische Risiko ergibt sich heute weniger aus eigenständigen terroristischen Organisationen als aus der zunehmenden Überlagerung militärischer, nachrichtendienstlicher und hybrider Bedrohungen. Cyberoperationen, Desinformationskampagnen, Sabotageakte gegen militärisch relevante Infrastruktur sowie geheimdienstliche Aktivitäten gewinnen kontinuierlich an Bedeutung und prägen das strategische Umfeld in deutlich stärkerem Maße als klassische Formen des Terrorismus. Belarus entwickelt sich damit zunehmend zu einem sicherheitspolitischen Knotenpunkt hybrider Konflikte, ohne selbst ein Schwerpunkt terroristischer Gewalt zu sein.

Die hohe wirtschaftliche und sicherheitspolitische Abhängigkeit von Russland verstärkt diese Entwicklung zusätzlich. Internationale Sanktionen, die fortschreitende militärische Integration sowie die außenpolitische Isolation des Landes begrenzen den strategischen Handlungsspielraum der belarussischen Führung und erhöhen zugleich ihre Abhängigkeit von russischen Sicherheitsstrukturen. Dadurch entstehen zusätzliche Risiken für die regionale Stabilität, die sich jedoch überwiegend im Bereich militärischer Eskalation, hybrider Einflussoperationen und staatlicher Sicherheitsmaßnahmen manifestieren und nicht in einer Zunahme klassischer terroristischer Aktivitäten.

1.3 Staatliche Terrorismusbekämpfung und Begriffspolitik

Die Terrorismusbekämpfung nimmt innerhalb der belarussischen Sicherheitsarchitektur eine zentrale Stellung ein und ist eng mit den umfassenden Befugnissen der Sicherheits- und Strafverfolgungsbehörden verknüpft. Das institutionelle Gefüge wird insbesondere durch den Komitee für Staatssicherheit (KGB), das Innenministerium, das Ermittlungskomitee, die Streitkräfte sowie weitere Sicherheitsorgane getragen, die im Rahmen eines stark zentralisierten Systems eng zusammenarbeiten. Regelmäßig durchgeführte Antiterrorübungen dienen der Überprüfung der Einsatzbereitschaft, der Koordination zwischen den Sicherheitsbehörden sowie der Erprobung gemeinsamer Reaktionsverfahren auf sicherheitsrelevante Lagen. Hierbei stehen insbesondere der Schutz kritischer Infrastruktur, die Bekämpfung bewaffneter Angriffe, die Sicherung urbaner Räume sowie die Abwehr hybrider Bedrohungen im Mittelpunkt.

Die praktische Anwendung der Anti-Terrorismusgesetzgebung geht jedoch über die Bekämpfung terroristischer Gewalt im engeren Sinne hinaus. Die belarussischen Behörden verwenden die Begriffe „Terrorismus“ und „Extremismus“ in einem deutlich erweiterten sicherheitspolitischen Kontext und beziehen darunter regelmäßig oppositionelle Organisationen, Exilstrukturen, unabhängige Medien, zivilgesellschaftliche Initiativen sowie einzelne Aktivisten ein. Dadurch verschwimmen die Grenzen zwischen klassischer Terrorismusbekämpfung und der strafrechtlichen Verfolgung politischer Gegner. Diese Ausweitung staatlicher Eingriffsbefugnisse stellt einen wesentlichen Unterschied zu den in den meisten europäischen Staaten angewandten Terrorismusdefinitionen dar und erschwert die Vergleichbarkeit offizieller Statistiken sowie die objektive Bewertung der tatsächlichen Bedrohungslage.

Die sicherheitspolitische Strategie verfolgt erkennbar das Ziel, potenzielle oppositionelle Netzwerke bereits in frühen Entwicklungsstadien zu identifizieren und ihre organisatorische Handlungsfähigkeit nachhaltig einzuschränken. Hierzu werden neben strafrechtlichen Maßnahmen umfangreiche Überwachungsinstrumente, digitale Kontrollmechanismen sowie präventive Sicherheitsmaßnahmen eingesetzt. Die hohe Kontrollintensität reduziert zwar die Wahrscheinlichkeit einer offenen Etablierung terroristischer Organisationsstrukturen, trägt zugleich jedoch dazu bei, dass politischer Widerstand zunehmend in konspirative, dezentrale oder digitale Formen ausweicht.

1.4 Akteurslandschaft

Die gegenwärtige Akteurslandschaft in Belarus unterscheidet sich grundlegend von Staaten mit einer ausgeprägten terroristischen Infrastruktur. Eine eigenständige jihadistische, separatistische oder ideologisch motivierte Terrororganisation mit dauerhafter operativer Präsenz und signifikanter Anschlagsfähigkeit innerhalb des Landes ist derzeit nicht erkennbar. Das sicherheitsrelevante Umfeld wird vielmehr von oppositionellen Exilstrukturen, dezentral organisierten Sabotagenetzwerken sowie politisch motivierten Cyberakteuren geprägt, deren Aktivitäten sich überwiegend gegen die belarussische Staatsführung und die militärische Zusammenarbeit mit der Russischen Föderation richten. Die Einordnung dieser Akteure wird zusätzlich dadurch erschwert, dass die belarussischen Behörden zahlreiche oppositionelle

Organisationen offiziell als terroristische Vereinigungen klassifizieren, während internationale Regierungen, Sicherheitsbehörden und wissenschaftliche Einrichtungen diese Bewertung überwiegend nicht übernehmen.

Zu den bedeutendsten oppositionellen Akteuren zählt BYPOL, eine Organisation ehemaliger Angehöriger der belarussischen Sicherheitsbehörden, die nach den Präsidentschaftswahlen 2020 im Exil gegründet wurde. Ziel der Organisation ist die Schwächung des bestehenden Machtapparates sowie die Unterstützung eines politischen Systemwechsels. Seit Beginn des russischen Angriffskrieges gegen die Ukraine wird BYPOL mit verschiedenen Sabotageaktionen gegen militärisch relevante Infrastruktur sowie mit Unterstützungsleistungen für belarussische Partisanennetzwerke in Verbindung gebracht. Die belarussischen Behörden stufen die Organisation als terroristische Vereinigung ein und verfolgen tatsächliche oder mutmaßliche Unterstützer strafrechtlich. Außerhalb Belarus wird BYPOL dagegen überwiegend als oppositionelle Exilorganisation bewertet, deren Aktivitäten primär im Bereich politischer und militärischer Sabotage verortet werden.

Eine zentrale Rolle innerhalb der digitalen Widerstandsbewegung nimmt das Netzwerk der Cyber Partisans ein. Die Gruppe verfügt über ausgeprägte Fähigkeiten zur Durchführung komplexer Cyberoperationen gegen staatliche Informationssysteme und öffentliche Einrichtungen. Zu den bekanntesten Aktivitäten zählen Angriffe auf staatliche Datenbanken, die Veröffentlichung sensibler Regierungsinformationen sowie Cyberoperationen gegen russische Unternehmen und Behörden. Internationale Aufmerksamkeit erlangten insbesondere koordinierte Angriffe auf die IT-Infrastruktur russischer Unternehmen, die erhebliche betriebliche Einschränkungen verursachten. Während Belarus und Russland das Netzwerk als extremistische beziehungsweise terroristische Organisation einstufen, wird es international überwiegend als politisch motivierter Hacktivistenverbund betrachtet. Hinweise auf die Planung wahlloser Gewaltakte gegen die Zivilbevölkerung oder auf eine terroristische Zielsetzung im Sinne international anerkannter Definitionen liegen gegenwärtig nicht vor.

Von erheblicher sicherheitspolitischer Bedeutung sind darüber hinaus die sogenannten Eisenbahnpartisanen. Dabei handelt es sich um lose organisierte Sabotagenetzwerke, deren Aktivitäten sich auf die Beeinträchtigung militärisch bedeutsamer Eisenbahnverbindungen konzentrieren. Ziel dieser Aktionen ist die Störung russischer Truppen- und Materialtransporte über belarussisches Staatsgebiet. Die dokumentierten Vorfälle umfassen insbesondere Brandstiftungen an signaltechnischen Anlagen, die Beschädigung logistischer Infrastruktur sowie die zeitweilige Unterbrechung von Transportabläufen. Die Vorgehensweise richtet sich überwiegend gegen militärisch relevante Infrastruktur und weist keine systematische Ausrichtung auf wahllose Gewalt gegen die Zivilbevölkerung auf.

Neben diesen sicherheitsrelevanten Akteuren existieren politische Exilstrukturen wie der Koordinierungsrat unter Führung von Swjatlana Zichanouskaja. Diese Organisation verfolgt politische und diplomatische Zielsetzungen und konzentriert sich auf internationale Interessenvertretung, Menschenrechtsarbeit und die Unterstützung demokratischer Reformen. Trotz ihrer Einstufung als extremistisch oder terroristisch durch die belarussischen Behörden bestehen keine belastbaren Hinweise auf eine Beteiligung an

terroristischen Aktivitäten oder die Anwendung politisch motivierter Gewalt.

Insgesamt wird die gegenwärtige Akteurslandschaft weniger durch klassische terroristische Organisationen als durch ein Spektrum oppositioneller Widerstands-, Sabotage- und Cybernetzwerke geprägt. Eigenständige transnationale jihadistische Strukturen, separatistische Bewegungen oder dauerhaft operierende rechts- beziehungsweise linksterroristische Organisationen mit signifikanter Anschlagsfähigkeit innerhalb Belarus sind derzeit nicht feststellbar.

1.5 Nexus zwischen Terrorismus und organisierter Kriminalität

Belastbare Hinweise auf eine dauerhafte strukturelle Zusammenarbeit zwischen den gegenwärtig aktiven oppositionellen Sabotage- und Cybernetzwerken sowie der organisierten Kriminalität liegen derzeit nicht vor. Insbesondere bestehen keine gesicherten Erkenntnisse über eine systematische Finanzierung dieser Akteure durch Drogenhandel, Waffenhandel, Menschenhandel oder andere Formen transnationaler organisierter Kriminalität. Ebenso fehlen Hinweise auf eine institutionalisierte Kooperation mit kriminellen Netzwerken, wie sie aus verschiedenen Konfliktregionen des Nahen Ostens, Afrikas oder Lateinamerikas bekannt ist.

Gleichwohl besitzt Belarus aufgrund seiner geographischen Lage zwischen der Europäischen Union und der Russischen Föderation weiterhin Bedeutung als Transitstaat für unterschiedliche Formen grenzüberschreitender Kriminalität. Schmuggelaktivitäten, Sanktionsumgehung sowie einzelne Formen illegaler Handelsströme stellen eigenständige sicherheitspolitische Herausforderungen dar. Eine belastbare Verbindung dieser Phänomene mit terroristischen Organisationsstrukturen lässt sich gegenwärtig jedoch nicht herstellen.

Aus strategischer Perspektive ergibt sich somit kein Hinweis auf einen ausgeprägten Terrorismus-Kriminalitäts-Nexus. Das gegenwärtige Sicherheitsumfeld wird vielmehr durch politische Opposition, hybride Bedrohungen, staatliche Repression sowie geopolitische Konfliktdynamiken bestimmt als durch die Verflechtung terroristischer und organisierter krimineller Strukturen.

2. Spezifische Risiken: Taktiken und Vulnerabilitäten

Die operative Bedrohungslage in Belarus unterscheidet sich deutlich von Staaten, in denen terroristische Organisationen regelmäßig komplexe Anschläge gegen die Zivilbevölkerung durchführen. Gegenwärtig existieren keine Hinweise auf eine etablierte terroristische Infrastruktur mit der Fähigkeit, koordinierte Anschlagsserien oder groß angelegte Massenanschläge innerhalb des Landes durchzuführen. Die sicherheitsrelevanten Aktivitäten konzentrieren sich vielmehr auf gezielte Sabotagehandlungen gegen militärisch bedeutsame Infrastruktur, Cyberoperationen sowie vereinzelte Angriffe auf staatliche Einrichtungen. Das Risikoprofil wird daher weniger durch wahllose Gewaltakte als durch selektive Aktionen mit politischer oder militärischer Zielsetzung bestimmt.

Vor dem Hintergrund der engen militärischen Kooperation zwischen Belarus und der Russischen Föderation hat sich insbesondere die kritische Infrastruktur zu einem zentralen sicherheitspolitischen Angriffsziel entwickelt. Besondere Bedeutung kommt hierbei dem Eisenbahnnetz zu, das seit Beginn des russischen Angriffskrieges gegen die Ukraine eine wesentliche Funktion für militärische Transport- und Versorgungsleistungen erfüllt. Wiederholt dokumentierte Sabotagehandlungen gegen signaltechnische Anlagen, Stellwerke und logistische Einrichtungen verdeutlichen, dass diese Infrastruktur aufgrund ihrer strategischen Bedeutung als besonders verwundbar gilt. Ziel derartiger Aktionen ist in erster Linie die Beeinträchtigung militärischer Bewegungsfreiheit und nicht die Verursachung möglichst hoher Opferzahlen unter der Zivilbevölkerung.

Neben der Eisenbahninfrastruktur besitzen militärische Einrichtungen, Kommunikationssysteme, staatliche Verwaltungsstrukturen sowie sicherheitsrelevante IT-Systeme eine erhöhte Gefährdung. Die zunehmende Digitalisierung staatlicher Verwaltungs- und Kommunikationsprozesse erweitert zugleich die Angriffsfläche für Cyberoperationen. Cyberakteure konzentrieren sich vor allem auf die Kompromittierung staatlicher Datenbanken, die Veröffentlichung vertraulicher Informationen sowie die zeitweilige Beeinträchtigung administrativer und logistischer Abläufe. Der Schwerpunkt liegt auf der Schwächung staatlicher Handlungsfähigkeit und der Erzeugung politischer sowie psychologischer Wirkung. Eine systematische Ausrichtung auf die Verursachung physischer Massenschäden oder langfristiger Zerstörung kritischer ziviler Infrastruktur ist bislang nicht erkennbar.

Das derzeitige Anschlagsprofil wird überwiegend durch niedrigschwellige Sabotageformen geprägt. Brandstiftungen, die Beschädigung technischer Einrichtungen, Eingriffe in Steuerungs- und Kommunikationssysteme sowie digitale Angriffe dominieren das operative Spektrum. Demgegenüber liegen keine belastbaren Hinweise auf einen regelmäßigen Einsatz komplexer improvisierter Sprengvorrichtungen, chemischer, biologischer, radiologischer oder nuklearer Kampfstoffe, koordinierter Schusswaffenangriffe oder Geiselnahmen vor. Ebenso fehlen Anzeichen für eine Entwicklung hin zu terroristischen Taktiken, die auf eine möglichst hohe Zahl ziviler Opfer abzielen.

Mit zunehmender Bedeutung digitaler Technologien gewinnen Cyberoperationen als Bestandteil hybrider Konfliktführung kontinuierlich an Relevanz. Belarus befindet sich aufgrund seiner strategischen Rolle im russisch-ukrainischen Konflikt in einem Umfeld intensiver nachrichtendienstlicher und cybergestützter Aktivitäten. Angriffe auf staatliche Netzwerke, Datenbanken und digitale Infrastrukturen sind deshalb fester Bestandteil des sicherheitspolitischen Lagebildes. Diese Aktivitäten verfolgen überwiegend politische oder militärische Zielsetzungen und unterscheiden sich hinsichtlich ihrer Motivation und Zielauswahl deutlich von klassischen Formen des Cyberterrorismus.

Auch unbemannte Luftfahrzeuge entwickeln sich zu einem zunehmend relevanten Element moderner Sicherheitsbedrohungen. Drohnen werden sowohl für militärische Aufklärung als auch für einzelne Sabotageoperationen eingesetzt und erweitern die operativen Möglichkeiten nichtstaatlicher Akteure erheblich. Ihre bisherige Verwendung beschränkt sich jedoch auf punktuelle Einsätze

gegen militärisch relevante Ziele. Hinweise auf einen systematischen Einsatz bewaffneter Drohnen im Rahmen terroristischer Anschläge gegen die Zivilbevölkerung bestehen derzeit nicht.

Geografisch konzentrieren sich sicherheitsrelevante Vorfälle vor allem auf den Großraum Minsk, bedeutende Eisenbahnknotenpunkte sowie Regionen entlang der Grenzen zu Polen, Litauen und der Ukraine. Diese Gebiete besitzen aufgrund ihrer militärischen, logistischen und politischen Bedeutung eine erhöhte strategische Relevanz. Gleichzeitig befinden sich dort zahlreiche Einrichtungen, die im Falle einer weiteren Eskalation des regionalen Konflikts potenzielle Ziele von Sabotage- oder Cyberoperationen darstellen könnten.

Aus sicherheitspolitischer Sicht ergibt sich somit ein Bedrohungsprofil, das sich grundlegend von klassischen terroristischen Szenarien unterscheidet. Die größten Risiken entstehen gegenwärtig durch hybride Operationsformen, gezielte Sabotage gegen militärisch bedeutsame Infrastruktur, Cyberangriffe sowie die zunehmende Verflechtung staatlicher und nichtstaatlicher Akteure im Kontext des russisch-ukrainischen Konflikts. Eine Entwicklung hin zu einer breit angelegten terroristischen Anschlagskampagne innerhalb Belarus ist derzeit nicht erkennbar.

3. Radikalisierungsprozesse

Die gegenwärtigen Radikalisierungsprozesse in Belarus unterscheiden sich deutlich von den in klassischen Terrorismuskontexten beobachteten Entwicklungen. Weder bestehen Hinweise auf eine nennenswerte jihadistische Rekrutierungsinfrastruktur noch auf ein systematisches Anwachsen gewaltorientierter extremistischer Milieus mit terroristischer Zielsetzung. Stattdessen wird das Radikalisierungsgeschehen maßgeblich durch die innenpolitische Entwicklung seit den Präsidentschaftswahlen 2020 sowie durch die Auswirkungen des russischen Angriffskrieges gegen die Ukraine beeinflusst. Politisch motivierte Radikalisierung entsteht überwiegend als Reaktion auf staatliche Repression, den eingeschränkten politischen Handlungsspielraum und die fortschreitende Polarisierung zwischen Staat und Opposition.

Die anhaltende Einschränkung politischer Freiheitsrechte, die strafrechtliche Verfolgung oppositioneller Aktivitäten sowie die umfassenden Überwachungsmaßnahmen der Sicherheitsbehörden bilden zentrale Faktoren, welche die Entstehung konspirativer Widerstandsstrukturen begünstigen. Die weitreichende Kriminalisierung oppositioneller Betätigung führt dazu, dass sich Teile der Opposition zunehmend außerhalb legaler politischer Räume organisieren. Daraus resultiert jedoch überwiegend keine Entwicklung hin zu wahlloser terroristischer Gewalt, sondern vielmehr die Verlagerung politischer Aktivitäten in den Bereich verdeckter Kommunikation, digitaler Vernetzung sowie gezielter Sabotagehandlungen gegen staatliche oder militärisch relevante Einrichtungen.

Eine besondere Bedeutung kommt den im Ausland befindlichen Exilgemeinschaften zu. Zahlreiche oppositionelle Akteure operieren mittlerweile außerhalb Belarus und koordinieren politische Aktivitäten, Informationskampagnen sowie technische Unterstützung über grenzüberschreitende Netzwerke. Dadurch entstehen transnationale

Kommunikationsstrukturen, welche die organisatorische Handlungsfähigkeit oppositioneller Gruppen stärken, ohne dass hieraus zwangsläufig eine terroristische Organisationsbildung hervorgeht. Die Exilstrukturen verfolgen überwiegend politische Zielsetzungen und nutzen digitale Plattformen zur Koordination, Mobilisierung und internationalen Öffentlichkeitsarbeit.

Die Rekrutierung oppositioneller Netzwerke erfolgt heute nahezu ausschließlich über digitale Kommunikationsräume. Verschlüsselte Messenger-Dienste, soziale Netzwerke sowie spezialisierte Kommunikationsplattformen bilden die wesentliche Infrastruktur für Informationsaustausch, organisatorische Abstimmung und technische Unterstützung. Diese Entwicklung trägt wesentlich dazu bei, dass klassische hierarchische Organisationsformen zunehmend durch flexible, dezentrale Netzwerkstrukturen ersetzt werden. Gleichzeitig erschwert diese Organisationsform den Sicherheitsbehörden die frühzeitige Identifizierung einzelner Akteure und erhöht die operative Resilienz oppositioneller Gruppen.

Hinweise auf eine systematische Rekrutierung durch jihadistische Organisationen oder andere transnationale terroristische Netzwerke liegen gegenwärtig nicht vor. Ebenso bestehen keine belastbaren Erkenntnisse über eine nennenswerte Verbreitung salafistisch-jihadistischer Ideologien oder über eine nachhaltige Etablierung entsprechender Unterstützerstrukturen innerhalb Belarus. Radikalisierungsprozesse werden daher gegenwärtig nahezu ausschließlich durch innenpolitische Konflikte, staatliche Repression sowie die sicherheitspolitischen Auswirkungen des Krieges in der Ukraine geprägt und nicht durch religiös motivierten Extremismus.

Die gegenwärtige Entwicklung deutet darauf hin, dass sich oppositionelle Aktivitäten auch künftig überwiegend auf Cyberoperationen, Informationsbeschaffung, digitale Einflussnahme sowie begrenzte Sabotageakte gegen militärisch bedeutsame Infrastruktur konzentrieren werden. Eine Entwicklung hin zu systematischen Anschlägen gegen die Zivilbevölkerung oder zur Bildung klassischer terroristischer Organisationen erscheint unter den derzeitigen Rahmenbedingungen weiterhin wenig wahrscheinlich. Das Risiko einer weiteren Radikalisierung besteht dennoch insofern, als eine anhaltende politische Eskalation, zunehmende Repression oder eine Ausweitung regionaler Konflikte einzelne Akteure zu gewaltorientierten Handlungsformen bewegen könnte. Gegenwärtig liegen jedoch keine belastbaren Hinweise auf eine solche Entwicklung vor.

4. Trends und Bedrohungsdynamiken

Die sicherheitspolitische Entwicklung in Belarus wird auch künftig in erster Linie durch geopolitische Veränderungen, die innenpolitische Stabilität sowie die Auswirkungen des russischen Angriffskrieges gegen die Ukraine bestimmt. Im Gegensatz zu Staaten mit dauerhaft aktiven terroristischen Organisationen zeichnet sich die Bedrohungsentwicklung nicht durch eine kontinuierliche Zunahme klassischer Anschlagsaktivitäten aus, sondern durch die fortschreitende Bedeutung hybrider Bedrohungsformen. Sabotage, Cyberoperationen, Desinformation und nachrichtendienstliche Aktivitäten prägen das sicherheitspolitische Umfeld

zunehmend stärker als terroristische Gewalt im engeren Sinne.

Seit den Präsidentschaftswahlen des Jahres 2020 hat sich das Verhältnis zwischen Staat und Opposition nachhaltig verändert. Die weitreichende Zerschlagung legaler Oppositionsstrukturen, umfangreiche Festnahmen sowie die Verlagerung zahlreicher oppositioneller Akteure ins Ausland haben klassische politische Handlungsspielräume erheblich eingeschränkt. Gleichzeitig hat sich ein dezentral organisiertes Widerstandsmilieu entwickelt, das sich überwiegend digital organisiert und seine Aktivitäten auf Informationsbeschaffung, Cyberoperationen sowie punktuelle Sabotage gegen militärisch bedeutsame Infrastruktur konzentriert. Diese Entwicklung deutet auf eine langfristige Transformation politischer Konflikte hin, ohne dass gegenwärtig eine Entwicklung hin zu einer breit angelegten terroristischen Kampagne erkennbar ist.

Die zunehmende Digitalisierung staatlicher Verwaltungs- und Sicherheitsstrukturen verändert zugleich die operative Bedrohungslage. Cyberoperationen entwickeln sich zu einem zentralen Instrument politischer Auseinandersetzungen und ermöglichen nichtstaatlichen Akteuren eine erhebliche Wirkung, ohne physische Gewalt anwenden zu müssen. Angriffe auf staatliche Informationssysteme, Datenbanken und Kommunikationsnetze werden voraussichtlich weiter an Bedeutung gewinnen. Gleichzeitig ist davon auszugehen, dass die belarussischen Sicherheitsbehörden ihre Fähigkeiten im Bereich Cyberabwehr, digitale Überwachung und elektronische Aufklärung kontinuierlich ausbauen werden. Daraus entsteht ein dauerhaftes Spannungsverhältnis zwischen staatlicher Kontrolle und den technischen Möglichkeiten oppositioneller Netzwerke.

Auch technologische Innovationen beeinflussen die zukünftige Sicherheitslage zunehmend. Die Verfügbarkeit kommerzieller Drohnensysteme, verbesserter Verschlüsselungstechnologien sowie künstlicher Intelligenz eröffnet sowohl staatlichen als auch nichtstaatlichen Akteuren neue operative Möglichkeiten. Während Drohnen bislang überwiegend zur Aufklärung und vereinzelt für Sabotagehandlungen eingesetzt werden, könnten technologische Weiterentwicklungen künftig die Reichweite und Präzision entsprechender Operationen erhöhen. Ebenso erleichtern moderne Kommunikationsplattformen die internationale Vernetzung oppositioneller Gruppen und erhöhen deren organisatorische Flexibilität.

Die strategische Bedeutung Belarus innerhalb der russischen Sicherheitsarchitektur dürfte auch künftig ein wesentlicher Einflussfaktor bleiben. Solange belarussisches Staatsgebiet für militärische Operationen, Truppenstationierungen und logistische Unterstützungsleistungen im Zusammenhang mit dem Krieg gegen die Ukraine genutzt wird, bleibt das Land Bestandteil einer angespannten sicherheitspolitischen Gesamtlage. Dadurch steigt insbesondere das Risiko weiterer Sabotagehandlungen gegen militärisch relevante Infrastruktur sowie einer Ausweitung hybrider Einflussoperationen. Diese Entwicklung betrifft vor allem staatliche Einrichtungen, Verkehrs- und Kommunikationsnetze sowie militärische Logistik und weniger zivile Ziele.

Eine zusätzliche Dynamik ergibt sich aus der fortschreitenden internationalen Isolation Belarus. Wirtschaftliche Sanktionen,

außenpolitischer Druck und die zunehmende Abhängigkeit von Russland verändern langfristig die innenpolitischen und wirtschaftlichen Rahmenbedingungen. Hieraus können gesellschaftliche Spannungen entstehen, die einzelne Formen politischer Radikalisierung begünstigen. Gegenwärtig bestehen jedoch keine belastbaren Hinweise darauf, dass sich hieraus eigenständige terroristische Organisationen mit nachhaltiger operativer Handlungsfähigkeit entwickeln.

Für die kommenden Jahre ist daher von einer weitgehenden Kontinuität des gegenwärtigen Bedrohungsbildes auszugehen. Die Wahrscheinlichkeit groß angelegter terroristischer Anschläge gegen die Zivilbevölkerung bleibt weiterhin gering. Demgegenüber ist mit einer anhaltenden Bedeutung hybrider Bedrohungen, cybergestützter Operationen, gezielter Sabotage gegen militärisch bedeutsame Infrastruktur sowie nachrichtendienstlicher Aktivitäten zu rechnen. Belarus entwickelt sich damit zunehmend zu einem sicherheitspolitischen Raum, in dem die Grenzen zwischen staatlichen und nichtstaatlichen Konfliktformen verschwimmen und klassische terroristische Gewalt gegenüber hybriden Operationsformen weiter an Bedeutung verliert.

TERRORISMUSBEDROHUNG

BELARUS

terrorismuswatch