Institut für Technikfolgenabschätzung und Systemanalyse (ITAS)

Technologiemonitoring: Soziotechnische Innovationsdynamiken und systemische Resilienz

Alexandros Gazos, Octavia Madeira, Georg Plattner, Tim Röller, Christian Büscher

Phänomenmonitoring

Zusammenfassung

Die fortschreitende Digitalisierung führt zu einer zunehmenden Verfügbarkeit öffentlich zugänglicher Technologien, was sich immer deutlicher auf die Innovationsdynamik im Phänomenbereich Extremismus und Terrorismus auswirkt. Somit wird es für extremistische und terroristische Akteure zunehmend leichter, Technologien kreativ einzusetzen und umzufunktionieren. Eine solche Entwicklung verschärft die Herausforderungen im Umgang mit extremistischen Bedrohungsszenarien und beeinträchtigt die Fähigkeit, zukünftige Pfade der Technologienutzung verlässlich zu antizipieren. In diesem Beitrag sollen Forschungsergebnisse aus dem Bereich der kritischen Infrastrukturen Orientierung darüber geben, wie eine mögliche Bewältigungsstrategie mit vergleichbar schwer zu antizipierenden Herausforderungen aussehen kann. Es werden vier Aspekte einer systemischen Resilienz vorgestellt, die auch eine Erwartungsabhängigkeit des Konzepts berücksichtigen. Zudem werden erste Anknüpfungspunkte zur Übersetzung in den Bereich der Prävention und Mitigation extremistischer Bedrohungen exploriert und ein Ausblick auf die weitere Forschung zu den soziotechnischen Innovationsdynamiken malevolenter Akteure präsentiert.

Stichworte

Resilienz | *Kritische Infrastrukturen* | *Innovation* | *Technologien* | *Technikfolgenabschätzung* | *Terrorismus* | *Extremismus* | *Prävention*

Einführung

In typischer Weise nutzen Extremist*innen Technologien, die günstig, ohne Weiteres verfügbar, einfach zu handhaben – und im Fall von Propaganda, Kommunikation und Rekrutierung in weiten Kreisen zugänglich sind. Cronin (2020) legte eine Studie zu den Bedingungen einer todbringenden Ermächtigung (Lethal Empowerment) vor, in der begünstigende Faktoren für die Nutzung von Technologien durch Terrorist*innen ausgemacht wurden. Insbesondere die Digitalisierung brachte Open-Source- und Off-the-Shelf-Technologien hervor, die günstig, leicht zugänglich und einfach zu nutzen sind. Dies habe zur Herausbildung eines wirkmächtigen technologischen Kontexts für die gewaltförmige Mobilisierung durch die Kommunikation von Emotionen und Überzeugungen beigetragen (Cronin, 2020).

Technologie zu einem Zweck zu verwenden, der sich von dem durch die Technikentwickler*innen vorgesehenen Zweck unterscheidet, oder Technologie zu verwenden, um anderen zu schaden, ist inhärent kreativ. Cropley und Kollegen (2008) sprechen in diesem Zusammenhang von „malevolenter Kreativität". Diese Form der Kreativität speist sich aus einer Dynamik zwischen radikalen Motivlagen und dem Versuch, Handlungsfähigkeit zu generieren (Cropley et al., 2008). Dies gilt sowohl für gewaltförmige als auch für nicht gewaltförmige Handlungen wie interne oder externe Kommunikation oder auch Geldbeschaffung. Kreativität und Innovation sind keine spontanen Ideen, „they result from a well-aimed, intentional search for improvement" (Gill et al., 2013, S. 131).

Je kreativer Terrorist*innen sind, desto schwieriger ist es für deren Gegenpart, Handlungen vorherzusagen oder vorwegzunehmen. Wenn solche kreativen Problemlösungen in der Realität umgesetzt werden, handelt es sich um Innovationen (Argentino et al., 2021; Gill et al., 2013). Nicht selten werden die Terroranschläge vom 11. September 2001 als Beispiel hochgradiger Innovativität herangezogen. Obwohl es Flugzeugentführungen bereits zuvor gab, so war die Verwendung eines zivilen Passagierflugzeuges als Lenkflugkörperwaffe – „airplanes as weapons of mass destruction" (Fox, 2021) – etwas völlig Neuartiges. Dementsprechend reagierten die verantwortlichen Sicherheitsbehörden überrascht, sei es aufgrund von strukturellen Problemen in der nationalen Sicherheitsarchitektur (Sullivan &

Lester, 2022) oder aufgrund elaborierter Strategien der „intelligence and counterintelligence" aufseiten der Attentäter (Ilardi, 2009). Als eine Reaktion darauf wurde von den jeweiligen Militärs das Abschießen solcher als Waffen missbrauchter Flugzeuge trainiert – eine Entscheidung mit weitreichenden ethischen Implikationen. Die Verwendung bekannter Technologien zu anderen als den ursprünglich vorgesehenen Zwecken kann demnach auch als eine Form malevolenter Kreativität und Innovation betrachtet werden, die nicht nur Reaktionen auf der Gegenseite provozieren, sondern auch zur Nachahmung des *Modus Operandi* inspirieren (Demir & Guler, 2023).

Im Katz-und-Maus-Spiel zwischen extremistischen Kräften und Sicherheitsbehörden kann technologischer Fortschritt dazu führen, dass sich der Vorsprung im Wissen und Können immer wieder verändert, je nachdem, welche Seite aktuell ein innovatives Momentum organisieren kann. Die digitale Revolution hat Extremist*innen und Terrorist*innen mit einer noch nie da gewesenen Fülle an Werkzeugen ausgestattet, um ihre Agenda voranzubringen. Es ist zudem zu vermuten, dass sich die Innovationschancen erhöhen, da extremistische Akteure[1] rechtliche oder ethische Richtlinien außer Acht lassen können (Caviezel et al., 2022). Die Bandbreite der Verwendungszwecke dieser neuen Werkzeuge erstreckt sich von (verschlüsselter und unmittelbarer) Massenkommunikation für Propaganda oder Rekrutierung über die Finanzierung von Aktivitäten bis hin zur Ausübung von Gewalt oder gar Terror. Ferner haben das Web 2.0, die sozialen Medien und die unmittelbare Verfügbarkeit nahezu jeglicher Inhalte im Internet den Weg für malevolente Akteure bereitet, um sich mühelos mit Gleichgesinnten zu verbinden und diese Verbindungen über Raum und Zeit hinweg in einer kosteneffektiven und grenzenlosen Weise aufrechtzuerhalten (Zeiger & Gyte, 2020). Auf all diesen Gebieten waren extremistische Akteure unter den frühzeitigen Anwender*innen, die unter Ausnutzung der jeweiligen Affordanzen unterschiedlicher Plattformen (Schulze et al., 2024) neue Technik für ihre eigenen Zwecke kreativ umfunktionierten.

Amerikanische Neonazis (zum Beispiel mit der Schaffung des Stormfront-Forums in den frühen 1990er-Jahren) und islamistische Gruppen haben

[1] *Der Begriff ‚Akteure' meint hier nicht nur Personen, sondern auch Gruppen und Organisationen und wird daher bewusst nicht gegendert*

den Wert des Internets für alle möglichen Handlungen, von Propaganda bis zur Planung und Durchführung von Angriffen, gleichermaßen früh verstanden (Scrivens & Conway, 2019). Die Kampagne des sogenannten Islamischen Staates (IS) zur weltweiten Rekrutierung neuer Mitglieder (Piazza & Guler, 2021) ist nur eines von vielen Beispielen hochgradig erfolgreicher und innovativer Internetnutzung. „Violent non-state groups" wie der IS und Hezbollah werden als Beispiel für die Rolle der „early adopter" von kommerziellen Drohnen als Waffe herangezogen (Archambault & Veilleux-Lepage, 2024; Franke, 2014). Während des terroristischen Angriffs auf die israelische Bevölkerung am 7. Oktober 2023 hat die Hamas mithilfe solcher Drohnen die israelischen Verteidigungsstellungen ausgeschaltet, um ihre Grenzbefestigungen überwinden zu können (Harding et al., 2023).

Somit stellt das Phänomen der malevolenten Nutzung neuer Technologien durch extremistische Akteure die Gesellschaft vor die Herausforderung, sich unaufhörlich auf dadurch entstehende, bisher nicht bekannte Gefährdungen einstellen zu müssen.

Innovationsdynamik und Resilienz

Die bisherigen Forschungsergebnisse des Technologiemonitorings (Delphi-Befragung, Workshops und Interviews) erlauben eine Annäherung an die Strategien, Taktiken, Technologien, Methoden und Ziele malevolenter Akteure (Büscher et al., 2022; Madeira et al., 2023). Dennoch sind diese Annäherungen limitiert. So können die Ergebnisse solcher prospektiven Forschungen zu malevolenter Kreativität übersehen, was sich außerhalb des aufgespannten Möglichkeitsraums abspielt. Die Grundlage der von Expert*innen erwogenen Innovationsszenarien kann sich während des Forschungsprozesses weiterentwickeln, innerhalb weniger Jahre durch parallele Innovationen verändern oder Innovationstätigkeiten können klandestin verlaufen. Ein Teil der Innovationsdynamik malevolenter Akteure entzieht sich somit immer der Wahrnehmung und damit der Gewissheit, diese zuverlässig antizipieren zu können. Welche Strategie ist und bleibt dann noch in der Lage, mit derartigen Bedrohungsszenarien umzugehen?

Eine Facette des Technologiemonitorings umfasst das Thema der Resilienz und Vulnerabilität kritischer Infrastrukturen. Dabei wurde Resilienz als mögliche Bewältigungsstrategie und Antwort auf eine vergleichbar herausfordernde Landschaft aus unvorhersehbaren Bedrohungen untersucht. Kritische Infrastrukturbetreiber*innen, Dienstleister*innen und staatliche Institutionen sehen sich einer Fülle an Herausforderungen gegenüber (beispielsweise Terrorismus, Cyberangriffe, Extremwetterereignisse) und dennoch stellen sie überwiegend und über lange Zeiträume die Verfügbarkeit kritischer Infrastrukturen sicher. Aufgrund ihrer ausgewiesenen Zuverlässigkeit bieten ihre Bewältigungsstrategien Ansatzpunkte für eine Reihe anderer Bereiche und Akteure, die mit ähnlichen oder vergleichbaren Herausforderungen ringen. Die Erkenntnisse aus der Forschung an kritischen Infrastrukturen bieten sich daher auch als Orientierung für den Bereich der Prävention und Mitigation von extremistischen Bedrohungen an.

Im Weiteren präsentieren wir einen Teil der Forschungsergebnisse zu den erforderlichen Aspekten, die es soziotechnischen Systemen ermöglichen, einen gewissen Grad an Resilienz zu entwickeln und auch aufrechtzuerhalten. Bei soziotechnischen Systemen kann es sich um Organisationen, Institutionen, Unternehmen und/oder Infrastrukturen handeln, in denen soziale Akteure und technische Komponenten miteinander interagieren und gemeinsam bestimmte Leistungen oder Funktionen erfüllen (Büscher, 2022). Zunächst wird dabei die Bedrohungslage für jene Systeme skizziert, um zu verdeutlichen, wie ein transformatives Konzept der Resilienz auf diese Problemstellung Antworten finden kann. Im Anschluss wird dargelegt, inwieweit sich das Konzept auf die Prävention und Mitigation extremistischer Bedrohungen anwenden lässt.

Der resiliente Kern und dessen bedrohliche Umstände

Die hier vorgestellte Forschung konzentrierte sich auf die Resilienz kritischer Informationsinfrastrukturen im Angesicht terroristischer Bedrohungsszenarien. Resilienz ist als eine Fähigkeit zu verstehen, bei der erforderliche operative Vorgänge in einem soziotechnischen System unter erwarteten und unerwarteten Bedingungen aufrechterhalten werden

können. Die Bedingungen betreffen dabei nicht nur Bedrohungen und Störungen, sondern auch Veränderungen und Gelegenheiten (Hollnagel, 2013). Welche operativen Vorgänge dabei als erforderlich erachtet werden, wird im Rahmen kritischer Infrastrukturen gesellschaftlich verhandelt. Dies wird beispielsweise an dem Begriff der Kritikalität einer Infrastruktur deutlich, das heißt ihrer Bedeutsamkeit für gesellschaftliche Grundfunktionen und die damit einhergehende Verwundbarkeit bei einem Ausfall oder einer Beeinträchtigung (BMI, 2009). Dabei war die Begriffsgeschichte kritischer Infrastrukturen bereits eine Historie wandelnder Prioritäten (Folkers, 2018): von der militärisch-logistischen Kriegswichtigkeit über die lebenswichtige Daseinsvorsorge bis hin zu systemwichtigen Infrastrukturoperationen in einem Gesamtsystem aus kritischen Infrastrukturen.

Auch die Resilienz wird je nach beteiligten Akteuren unterschiedlich und konfliktreich verhandelt. So eigneten sich die Bewohner*innen eines Flutgebiets in Dresden Sandsäcke an, um ihre Wohngebiete zu schützen, anstatt die Katastrophenschutzpläne der lokalen Behörden zu befolgen (Krüger & Albris, 2020). Im Phänomenbereich der Radikalisierung kann Resilienz bedeuten, dass in einem dialogischen sowie vertrauensbasierten Ansatz die Position und Handlungsfähigkeit lokaler Gemeinschaften gestärkt werden (Community Policing), doch läuft dieser Fokus auch Gefahr, die Präventionsebene zu vernachlässigen (Wimelius et al., 2023). In der Terrorismusforschung wurde Resilienz hingegen für die Verlagerung auf die lokale Ebene kritisiert, da damit auch eine Verantwortungsabgabe einhergehen kann. Durch uneinheitliche und vage Verständnisse von Resilienz bleibt für Forscher*innen und Praktiker*innen zudem häufig fraglich, ob Resilienz möglich, wünschenswert oder vorteilhaft ist (Jore, 2023). Darüber hinaus ist Resilienz für viele Organisationen, Unternehmen und staatliche Institutionen nur ein mögliches Ziel unter vielen. Dabei müssen diese Ziele nicht einmal einem eindeutig rationalen Kalkül folgen, bei dem beispielsweise die Effizienz einer Maßnahme oder die Profitabilität eines Unternehmens gesteigert wird. Organisationen integrieren ebenfalls institutionelle Mythen ihrer Umwelt, um den Fortbestand ihrer eigenen Organisation sicherzustellen (Meyer & Rowan, 1977).

Resilienz lässt sich somit auch als Identifikationsprozess verstehen, bei dem soziale Akteure stetig und dynamisch definieren, wie sich der Kern ihres Bestands zusammensetzt und wie er erhalten werden kann. Folglich

gestaltet sich etwas als resilient, wenn es sozialen Beobachter*innen (beispielsweise einer Organisation) gelingt, mit Bedrohungen, Störungen und Krisen so umzugehen, dass die Fähigkeit der Bestandsidentifikation erhalten bleibt oder neue Identifikationsoptionen entstehen (Endreß & Rampp, 2014). Für ein erwartungsabhängiges Verständnis von Resilienz ist somit bezeichnend, dass „Resilienz eben nicht die Bestandserhaltung eines Kerns trotz Transformation, sondern gerade durch Transformation bedeutet" (Endreß & Rampp, 2014, S. 94) und diese Fähigkeit zur Transformation erhalten bleibt.

Wie zuvor bereits ausgeführt, deuten aktuell beobachtbare Entwicklungen eine zunehmende Verfügbarkeit von Technologien durch Demokratisierungstendenzen an (Cronin, 2020). Für Angriffe auf kritische Infrastrukturen und deren Schutz sind jedoch weitere Innovationsfaktoren zu bedenken, die aus der Terrorismusforschung bekannt sind. In Anbetracht kontemporärer Beispiele aus der rechtsextremistischen Strömung des Akzelarationismus[2] (Loadenthal, 2021a, 2021b) sowie den Plänen dschihadistischer Salafist*innen (Krill & Clifford, 2022) lassen sich diese Innovationsfaktoren auch auf den Phänomenbereich organisierter extremistischer Gewalt und Kommunikation anwenden. Um in asymmetrischen Konflikten einen Schritt voraus zu sein, passen sich terroristische Organisationen dynamisch an staatliche Repression an. Ihre Innovationstätigkeiten müssen dementsprechend möglichst unberechenbar bleiben (Kron, 2007). Zudem entwickeln sich terroristische Gruppen in Abhängigkeit von Konfliktdynamiken (auch in Relation zu anderen Gruppen) und je nach Ideologie variiert ihre Fähigkeit, innovativ mit Technologie umzugehen (Dolnik, 2007). Demnach wird malevolente Kreativität nicht nur durch die Fähigkeiten der malevolenten Akteure selbst bestimmt oder durch technologische Verfügbarkeit begünstigt, sondern in entscheidender Weise von ideologischen Tendenzen vorgeprägt, während sie sich aufgrund von Repressions- und Konfliktdynamiken fortwährend verändert. Neuartige Entwicklungen deuten zudem einen Einfluss von Kommunikationsdynamiken in Online-Communities an (Basha, 2023).

[2] *Akzelerationist*innen streben danach, durch ihre Handlungen einen sozialen, politischen und/oder ökologischen Zusammenbruch zu beschleunigen beziehungsweise die Bedingungen für einen Zusammenbruch zu verschärfen (Loadenthal, 2022), indem sie die systeminhärenten Widersprüche ausbeuten (Parker, 2020).*

Eine derart komplexe und adaptive Bedrohungslage erschwert die ohnehin problematische Strategiefindung. Repressive Strategien oder Eingriffe in die dynamischen Faktoren malevolenter Kreativität riskieren weitere adaptive Innovationen extremistischer und terroristischer Organisationen. Es empfiehlt sich, eine Strategie zu wählen oder zumindest bestehende Strategien um Elemente zu ergänzen, bei denen Extremist*innen und Terrorist*innen, „die sich an dieses Verhalten anpassen, dies in einer gewissen Handlungs-Bandbreite tun, die allzu unerwünschte Handlungen weniger wahrscheinlich werden lassen“ (Kron, 2007, S. 113).

Ein transformatives Konzept der Resilienz bietet eine solche Strategie für soziotechnische Systeme. Dabei haben die vorangegangenen Ausführungen gezeigt, dass Resilienz von den Wahrnehmungen und Erwartungen sozialer Beobachter*innen abhängt. Für die Forschungsarbeit wurde eine synthetisierende Perspektive auf das Konzept entwickelt, die sowohl organisations- und techniksoziologische Elemente als auch Erkenntnisse aus der weiteren Sicherheitsforschung (Safety Management) heranzieht. Das Ergebnis dieser holistischen Konzeption sind vier Aspekte der Resilienz: (1) Systembeschaffenheit, (2) Systemkontrolle, (3) Systementwicklung und (4) Systemnetzwerk.

(1) Die *Systembeschaffenheit* umfasst vor allem, wie komplex Systemelemente (beispielsweise Menschen und Technik) miteinander interagieren und wie sie aneinandergekoppelt sind. Eine hohe Komplexität geht mit indirekten und unsicheren Informationslagen einher, die aus einer hohen Zahl potenzieller Interaktionen in dem System resultiert und die Gefahr unvorhersehbarer Rückkopplungseffekte birgt (Perrow, 1984). Während sich eng gekoppelte Systeme durch hohe interne Abhängigkeiten und begrenzte Möglichkeiten auszeichnen, erlauben lose Kopplungen Spielräume, ersetzbare Komponenten und alternative Möglichkeiten. Da in engen Kopplungen häufig ein Vorgang unmittelbar auf den anderen folgt (Hopkins, 1999) und komplexe Lagen die Ergründung der Prozesse erschweren, die zum Teil unvorhersehbare Effekte hervorbringen können, wohnt eng gekoppelten komplexen Systemen ein gewisses Katastrophenpotenzial inne (Perrow, 1984).

(2) Die *Systemkontrolle* umfasst überwachende, vorbereitende und intervenierende Maßnahmen, die der Stabilität eines Systems zuträglich

sein sollen und dessen Leistungen/Funktionen möglichst schnell wiederherstellen, wenn sie zuvor gestört wurden (beispielsweise durch einen Unfall oder einen Angriff). Dazu gehören Monitoringmaßnahmen, mit denen sich soziale Akteure ein kontinuierliches Bild der Lage – im eigenen System und der Umwelt – machen. Diese Akteure sollten zudem wissen, wie sie auf kleine Störungen und größere Disruptionen reagieren können, und für diese Fälle die Handlungs- und Entscheidungsfähigkeit aufrechterhalten (Hollnagel, 2013).

(3) Im Rahmen der *Systementwicklung* ist es von Bedeutung, mögliche Entwicklungspfade, Bedrohungen und Gelegenheiten antizipieren zu können. Auch wenn diese Fähigkeit, wie zuvor etabliert, in besonders komplexen Bedrohungslagen an ihre Grenzen stößt, kommt eine resiliente Strategie nicht ohne ein antizipatives Moment aus. Von entscheidender Bedeutung ist es jedoch, aus Fehlern und Erfolgen zu lernen und diese in weitere Antizipationen einfließen zu lassen (Hollnagel, 2013). Werden insbesondere die Mitglieder einer Organisation im Rahmen einer Fehlerkultur darin bestärkt, ihre Erfahrungen mit der Bewältigung eines disruptiven Ereignisses offen zu kommunizieren, ermöglichen sie wertvolle Lektionen für die gesamte Organisation (Weick et al., 2008).

(4) Der Aspekt des *Systemnetzwerks* beinhaltet die drei vorangegangenen Aspekte, verweist jedoch über die Systemgrenzen hinaus. Dies kann bedeuten, dass Organisationen, Institutionen und/oder Unternehmen (sowie ihre technischen Infrastrukturen) miteinander kommunizieren und interagieren. Die Kommunikations- und Interaktionsformen sollten dabei systemische Kapazitäten ergänzen und erweitern. Das Ziel sind koordinierende und kooperative Netzwerke aus Organisationen (La Porte, 2006) und ihren technischen Infrastrukturen, das heißt soziotechnische Systemnetzwerke. Auf diese Weise können zusätzliche Ressourcen als Puffer vorgehalten werden (lose gekoppelte Beschaffenheit) und die Systeme können sich in ihren Kontroll- und Entwicklungsmaßnahmen unterstützen. Konkret kann dies bedeuten, dass ein Unternehmen das Monitoring für ein anderes Unternehmen übernimmt (beispielsweise Cyber-Defence-Dienstleister*innen), erfahrene Organisationen weniger Erfahrene in der Vorbereitung eines Notfallplans unterstützen oder ihre Lern- und Antizipationsmethoden teilen.

Die vier Aspekte der Resilienz interagieren somit miteinander. Beschaffenheit, Kontrolle und Entwicklung spielen auch im Systemnetzwerkkontext eine Rolle und die verschiedenen Aspekte begünstigen oder benachteiligen einander. Die Erfahrungen und Einsichten aus der Entwicklung fließen in das Design der Beschaffenheit ein und informieren vorbereitende, überwachende und intervenierende Kontrollmaßnahmen. Eine weniger komplexe Beschaffenheit ist Monitoringmaßnahmen zuträglich und lose Kopplungen ermöglichen reibungsarme Wiederherstellungsprozesse. Aus den Informationen des Monitorings lässt sich ebenfalls lernen und antizipieren. Lose gekoppelte Beschaffenheiten ermöglichen auch Spielräume für lehrreiche Experimente. Systemnetzwerke stellen Kapazitäten für die Ausgestaltung der anderen Aspekte zur Verfügung und ermöglichen organisationsübergreifende Kontroll- und Entwicklungsmaßnahmen.

Vorläufige Ergebnisse der Studie und die Übersetzung in andere Problemkonstellationen

Die vier interagierenden Aspekte der Resilienz und ihre Rückbindung an die Erwartungen sozialer Beobachter*innen bildeten den theoretischen Ausgangspunkt und orientierten die empirische Arbeit des Forschungsprojekts. Im Laufe der Arbeit wurden fünf problemzentrierte Interviews (Witzel, 2000) mit relevanten Akteuren des Feldes kritischer Infrastrukturen (Betreiber*innen, Dienstleister*innen und staatliche Institutionen) geführt und mit der qualitativen Inhaltsanalyse ausgewertet (Mayring & Fenzl, 2019). Aufgrund des erschwerten Feldzugangs wurde das Material um 18 weitere Dokumente ergänzt (Gesetzestexte, Sicherheitsstandards, *White Paper* und Beratungsangebote sowie Positionspapiere einer zivilgesellschaftlichen Organisation). Die Dokumente wurden mithilfe von Kategorien und Erkenntnissen aus den Interviews, nach dem Repertoire der qualitativen Inhaltsanalyse, kodiert. Der Anspruch hinter diesem Vorgehen bestand darin, die theoretische Vorarbeit um empirische Einblicke kritisch zu erweitern.

Ein Teil der vorläufigen Zwischenergebnisse verweist auf bestimmte Erwartungshaltungen an die Ausprägungen der Aspektinteraktionen. Von Interesse sind hierbei einige Gemeinsamkeiten, welche im analysierten Material als eine Erwartungskontinuität auftraten. Die unterschiedlichen Akteure (Betreiber*innen, Dienstleister*innen, staatliche Institutionen

und zivilgesellschaftliche Organisationen) setzten zwar zum Teil deutlich variierende und konfligierende Akzente, doch wiesen ihre Erwartungen an die Aspekte eine gewisse Vergleichbarkeit auf. Im Folgenden werden die Zwischenergebnisse präsentiert und insoweit möglich in den Bereich der Prävention und Mitigation extremistischer Bedrohungen übersetzt:

Zu (1): Für die *Systembeschaffenheit* war von Bedeutung, dass Resilienz bereits bei der Konzeption oder dem Design ansetzt, also nicht erst bei der Implementation oder Umsetzung. So sollten beispielsweise technische Komponenten bestimmte Affordanzen aufweisen, das heißt aus der Sicht der späteren Nutzer*innen bestimmte Handlungsmöglichkeiten offerieren (Norman, 2013). Präferiert wurden hierbei Designs, die Interventionsmöglichkeiten erlauben und fehlertolerant sind. Wenn eine Komponente im System ausfällt, müssen andere Komponenten ihren Platz einnehmen können (beispielsweise Notstromversorgung). Auch in sozialer Hinsicht sollte genügend breit ausgebildetes Personal zur Verfügung stehen, um anderweitig verhinderte Mitarbeiter*innen in ihrer Funktion zu unterstützen. Derartige Überkapazitäten und Substitutionsmechanismen sollen eine lose Kopplung des Systems ermöglichen, um problematische Konsequenzen der steigenden Komplexität (beispielsweise eine undurchsichtige Informationslage) zu kompensieren. An dieser Stelle könnten ebenfalls Akteure, die sich mit der Prävention und Mitigation extremistischer Bedrohungen befassen, ansetzen, um kritische Kompetenzen bei mehreren Organisationsmitgliedern zu fördern. Plattformbetreiber*innen können hingegen konkret dazu beitragen oder regulatorisch dazu angehalten werden, die Affordanzen ihrer Plattform so zu überarbeiten, dass eine erweiterte Palette an Handlungsmöglichkeiten für Nutzer*innen in der *Content Moderation* besteht.[3] Hinsichtlich der Plattformen und neuer Technologien stellen Regularien und Zertifizierungskonzepte einen minimalen Standard des sicheren Gebrauchs her, wie das „IT-Sicherheitsgesetz 2.0“ (BSIG), die KI-Verordnung der Europäischen Union (Verordnung (EU) 2024/1689) oder Angebote diverser Anbieter von KI-Zertifizierungen (Schonschek, 2023).

[3] *Ein Teil des Transfers der Forschungsergebnisse auf den Bereich der Präventionsarbeit basiert auf den Ergebnissen des Technologiemonitorings, insbesondere den Workshops zum Metaverse und zu KI (Madeira et al., 2023), um die Ergebnisse besser an den Rahmen des Phänomenbereichs anzupassen.*

Zu (2): *Systemkontrolle* unterschied sich wie zuvor beschrieben in überwachende, vorbereitende und intervenierende Maßnahmen. Dabei sollte ein kontinuierliches Monitoring des eigenen Systems stattfinden, in dem aktuelle Entwicklungen und Vulnerabilitäten sichtbar werden. Für den Bereich der Prävention und Mitigation extremistischer Bedrohungen sind dabei mehrere Anwendungen denkbar. Während Sicherheitsbehörden vor allem die sichtbare Kommunikation und Handlungen malevolenter Akteure beobachten, so konzentriert sich die Forschung des Technologiemonitorings auf aktuelle Innovationsdynamiken. Darüber hinaus können gesellschaftliche Vulnerabilitäten identifiziert werden, wobei unterschiedliche Perspektiven und Erwartungshaltungen berücksichtigt werden sollten: die Ebene der intendierten Ziele (Sicherheitsbehörden), die Ebene der technologischen Affordanzen (Forschung) und die Ebene der Verletzlichkeit lokaler Gemeinschaften und demokratischer Werte (Zivilgesellschaft). Eine Beobachtbarkeit herzustellen kann auch durch Transparenz gewährleistet werden. Auf diese Weise können Nutzer*innen einer Plattform bestimmte Vorgänge durchschauen (beispielsweise durch eine Kennzeichnung von KI-generierten Inhalten). Vorbereiten können sich die Akteure aus der Präventionspraxis ebenfalls mit Notfallplänen, um auch in Krisensituationen auf einen Orientierungsrahmen zurückgreifen zu können und ein strukturiertes Vorgehen zu ermöglichen. Von einer resilienten Intervention wurde im untersuchten Material hingegen erwartet, dass die Entscheidungsfindung zu einem gewissen Grad mit den Problemen wandert (Weick et al., 2008), sodass lokal tätige Organisationsmitglieder beispielsweise in Krisensituationen schneller zu problemorientierten Lösungen finden. Die Organisationen der Präventionspraxis können dort ebenfalls ansetzen, indem sie auf die Fähigkeiten, Erfahrungen und Einsichten ihrer Mitglieder vertrauen und sie gleichzeitig durch Schulungen und Trainings fördern.

Zu (3): In der *Systementwicklung* standen die Mittel des Lernens und Antizipierens im Vordergrund. Die untersuchten Organisationen waren darauf bedacht, eine möglichst offene Kommunikationskultur zu entwickeln, in der Fehler offen kommuniziert werden. Erfahrungen und Einsichten sollten in regelmäßigen Lessons-Learned-Runden aufbereitet werden, wobei nicht nur außergewöhnliche Krisen, sondern auch alltägliche Ereignisse eine Rolle spielten. Für den Bereich der Prävention und Mitigation extremistischer Bedrohungen lassen sich in diesen Ergebnissen vor allem

Weiterbildungsangebote verorten. Unter Berücksichtigung der bisherigen Erkenntnisse des Technologiemonitorings sollten diese Angebote jedoch auch neue, vulnerable Gruppen erreichen (beispielsweise außerhalb des Bildungssystems). Den Herausforderungen neuer Technologien (wie des Metaverse oder der künstlichen Intelligenz) kann zudem in strukturierter Weise begegnet werden, indem Parallelen zu und Lehren aus vorangegangenen Technologien berücksichtigt werden (beispielsweise Gaming und Social Media). Werden die einzelnen Erfahrungen und Lehren aus den Technologien zudem über eine gemeinsame Plattform (beispielsweise ein organisationsinternes digitales Angebot) aufbereitet gesammelt und den Organisationsmitgliedern zugänglich gemacht, eignen sie sich für Antizipationen. Ein weiteres Mittel der Antizipation wären Simulationen und Planspiele oder auch Szenarien-Workshops und Vision Assessments (Madeira et al., 2023). Sie eignen sich für eine multiperspektivische Beleuchtung möglicher Entwicklungen sowie der darin enthaltenen Bedrohungen und Potenziale. Zum Teil regen solche Methoden dazu an, die eigene Erwartungshaltung temporär zu verlassen und sich in die Erwartungshaltung malevolenter Akteure zu versetzen. Zudem können auch Synergieeffekte zwischen aufkommenden Technologien exploriert werden (beispielsweise die Wechselwirkung zwischen künstlicher Intelligenz (KI) und Metaverse), die im organisationalen Alltag noch nicht sichtbar sind.

Zu (4): In der Forschung zu kritischen Infrastrukturen haben sich *Systemnetzwerke* als Kommunikations- und Kooperationsformen erwiesen, die über die individuellen Systemgrenzen hinaus Kapazitäten vorhalten. Demnach können einzelne Systeme in Krisensituationen oder im Allgemeinen in jeder Situation, die ihre eigenen Kapazitäten überfordert, von den Kapazitäten des Netzwerks Gebrauch machen. So können Netzwerke beispielsweise Erfahrungen und Einsichten (Expertise) bereitstellen, temporär unterstützende Fachkräfte mobilisieren und Ressourcen zur Verfügung stellen. Da in dem Bereich der Prävention und Mitigation von extremistischen Bedrohungen verschiedenste Organisationen mit unterschiedlichen Erwartungshaltungen und Herangehensweisen wirken, ist vor allem der Aspekt des Systemnetzwerks von besonderer Bedeutung. Konkret sind dabei transdisziplinäre Vernetzungen denkbar, also der Wissenstransfer aus der Forschung heraus, hin zu Praktiker*innen und zivilgesellschaftlichen Akteuren. Sicherheitsbehörden können die Resilienz der Zivilgesellschaft

beispielsweise mit Awareness-Workshops fördern oder ihre Erfahrung mit neuen Technologien mit weniger erfahrenen Präventionsakteuren teilen. Durch KI erleichterte Übersetzungen können dazu verwendet werden, um ressourcenärmere Sprachräume mit Informationsmaterial zu versorgen. Wenn sich zukünftige technologische Entwicklungen abzeichnen (beispielsweise das Metaverse), lassen sich zudem Stakeholder frühzeitig einbinden, um die Affordanzen zwischen demokratischen Akteuren, Plattformbetreiber*innen, Forscher*innen und potenziellen Nutzer*innen sozial zu verhandeln (Madeira & Plattner, 2023). Netzwerke spielen auch dann eine hervorgehobene Rolle, wenn extremistische Bestrebungen in organisierte Gewalt umschlagen. Untersuchungen des Katastrophenmanagements nach den terroristischen Anschlägen des 11. September 2001 haben gezeigt, dass Organisationen selbst abseits der formellen Strukturen in der Lage waren, spontan neue Netzwerke herauszubilden, um an notwendige Ressourcen und Expertise zu gelangen (Tierney, 2003).

Abschließend sollten einige Bedingungen der Resilienz im Rahmen der Prävention und Mitigation von extremistischen Bedrohungen nicht unerwähnt bleiben. Die hier erwähnten resilienzfördernden Maßnahmen bilden einen idealisierten Erwartungsgehalt ab, das heißt eine Ansammlung von Idealvorstellungen bezüglich des *Was* und *Wie* der Resilienz. Doch müssen diese Erwartungen nicht von allen (Mitgliedern der) Organisationen einstimmig getragen werden, sie können sich im Laufe der Zeit oder durch disruptive Ereignisse verändern und sind zudem nicht immer mit den anderen Zielen einer Organisation vereinbar (beispielsweise Gerechtigkeit, ethische Fragestellungen oder Geheimhaltung). In alltagspraktischen Angelegenheiten stellen vor allem Fragen der Effizienz und Effektivität eine nahezu konkurrierende Erwartungshaltung zur Resilienz dar. Maßnahmen sollten dementsprechend möglichst ressourcenschonend und wirksam sein. Selbst im Bereich der kritischen Infrastrukturen und den dort weitverbreiteten hohen Ansprüchen an die Verfügbarkeit systemischer Leistungen sind Resilienzstrategien letztendlich nicht nur von Erwartungen abhängig, sondern auch von verfügbaren Kapazitäten. Demzufolge sind die Aspekte der Resilienz nur im Rahmen der zur Verfügung stehenden Mittel möglich. Und dennoch sind sie in Anbetracht der Kernfunktionen, die resiliente Maßnahmen erhalten, eben nicht zu vernachlässigen. Vielmehr erfordern sie eine Neubewertung und gewinnen im Angesicht zunehmend komplexer Herausforderungen an Dringlichkeit.

Ausblick Technologiemonitoring

Die Abschätzung zukünftiger Technologien ist und bleibt mit spezifischen epistemischen Unsicherheiten verbunden. Diesem Sachverhalt trägt das Technologiemonitoring Rechnung, indem es durch einen mehrstufigen Prozess das technologische Innovationsgeschehen im Phänomenbereich Extremismus beobachtet, um eine möglichst breite und verlässliche Wissensbasis für die fundierte Einschätzung zukünftiger technologischer Entwicklungen zu schaffen.

Den Ausgangspunkt in diesem Beobachtungsprozess bildet der sogenannte Grobradar, wobei mittels kontinuierlicher, systematischer Literaturrecherche eine umfassende Einsicht zu infrage kommenden neuen Technologien entsteht. In einem zweiten Schritt muss eine Auswahl getroffen werden, welche der potenziell relevanten zukünftigen Entwicklungen eingehender untersucht werden sollen. Für diese Selektion wird mithilfe geeigneter Methoden einschlägiges Expert*innenwissen herangezogen. In einem dritten Schritt, dem Feinradar, werden die zuvor identifizierten ausgewählten Technologien schließlich in Form von kurzen Vertiefungsstudien näher analysiert (Kusche et al., 2021).

Im bisherigen Verlauf des so konzipierten Technologiemonitorings wurden zwei Technologien ausgemacht, die in Bezug auf einen zukünftigen extremistischen Gebrauch einer vertiefenden Untersuchung unterzogen werden sollten. Dabei handelte es sich zum einen um die mittlerweile im Alltagsleben immer stärker präsent werdenden Anwendungen künstlicher Intelligenz. Dieser Befund stützt sich hauptsächlich auf die Ergebnisse einer Online-Delphi-Befragung und eines Expert*innen-Workshops. Zum anderen handelt es sich um die noch weiter in der Zukunft liegende Vision der auf virtueller Realität basierenden Weiterentwicklung des Internets zu einem Metaverse. Dieser Befund geht auf einen Expert*innen-Workshop zurück, der auf der Basis der am ITAS entwickelten Methode des Vision Assessments durchgeführt wurde (Büscher et al., 2022; Madeira et al., 2023).

Im Feinradar sollen nun die beiden für das Themenfeld Extremismus und Radikalisierung als besonders relevant identifizierten Technologiekomplexe der künstlichen Intelligenz und des Metaverse vertieft und detailliert ausgearbeitet werden. Hierbei werden die einzelnen Technologien

mithilfe weiterführender Recherchen (Literatur, Internetquellen) und einer Datenerhebung durch strukturierte Expert*innengespräche analysiert. Die daraus abgeleiteten Gefahren und Potenziale der Technologien werden entlang problemorientierter Kriterien bewertet, um mögliche Handlungsoptionen zu erarbeiten.

Als Datengrundlage für die vertiefenden Analysen dienen uns zwölf leitfadengestützte Interviews mit Expert*innen aus unterschiedlichen Bereichen (NGOs, Extremismusprävention, Sicherheitsbehörden, Extremismusforschung). Die Identifikation und Auswahl der Expert*innen basierte auf relevanten Wissensbeständen zu den Technologiekomplexen (KI und/oder Metaverse) sowie zu Phänomenen des Extremismus. Die durchgeführten Interviews orientieren sich an folgenden, aus dem Problembezug abgeleiteten Leitfragen:

- Welche Nutzung von Anwendungen künstlicher Intelligenz und/oder des Metaverse für extremistische Zwecke wird heute bereits beobachtet?
- Welche Nutzung von Anwendungen künstlicher Intelligenz und/oder des Metaverse für extremistische Zwecke wird zukünftig erwartet?
- Wie kann der extremistischen Nutzung von Anwendungen künstlicher Intelligenz und/oder des Metaverse begegnet werden?
- Welche Chancen bieten Anwendungen der künstlichen Intelligenz und/oder des Metaverse für die Prävention von Extremismus?

Die so erhobenen Daten wurden mit der Methode der qualitativen Inhaltsanalyse (Zhang & Wildemuth, 2009) ausgewertet. Die Grundlage der Auswertung bildete ein von Veilleux-Lepage und Rassler (2024) vorgeschlagener Analyserahmen, der das Zusammenspiel von vier Schlüsselfaktoren hervorhebt, welche die Nutzung neu entstehender Technologien durch terroristische Gruppen ermöglichen:

Die breite Verfügbarkeit von 1.) offenen Technologien, mit einem *Dual-Use-Potenzial* in Verbindung mit 2.) der *Demokratisierung* des notwendigen Wissens zu deren schadhafter Verwendung, senkt die technologischen Zugangshürden für terroristische Akteure. Auf diese Weise wird auch die

Wirkmächtigkeit derartiger Technologien gesteigert, indem 3.) deren breite *Diffusion* über Lernprozesse niederschwellig möglich wird und dadurch 4.) die Wahrscheinlichkeit für *Direktionalität*, das heißt die Entstehung neuer Richtungen terroristischer Technologieverwendung, erhöht wird.

Während sich die beiden Autoren mit ihren Überlegungen auf die terroristische Nutzung bestimmter Technologien beziehen, gehen wir davon aus, dass der Ansatz auch wertvolle Einsichten zur Technologienutzung durch extremistische Akteure im Allgemeinen (und dabei nicht gewalttätige Aktivitäten einschließend) bieten kann. Wir vermuten, dass sich sowohl die extremistische Nutzung neu aufkommender Anwendungen künstlicher Intelligenz als auch des Metaverse anhand der postulierten Schlüsselfaktoren beschreiben und analysieren lassen. Von der Analyse werden granulare Erkenntnisse für die Problemstellungen des Technologiemonitorings sowie ein validierter Leitfaden für die zeitnahe Bewertung des malevolenten Potenzials neuartiger Technologien erwartet. Diesen Leitfaden gilt es, mithilfe der Interviewdaten zu überprüfen und gegebenenfalls um weitere relevante Faktoren zu ergänzen. Eine Veröffentlichung der empirischen Forschungsdaten ist im ersten Halbjahr 2025 vorgesehen.

Schlussfolgerungen

Technologische Innovationsdynamiken wirken sich fortwährend auf die Fähigkeit malevolenter Akteure aus, kreative Nutzungsweisen zu erkunden und technologische Affordanzen für ihre Zwecke auszunutzen. Unser Beitrag hat dargelegt, dass diese Entwicklung die Antizipationsfähigkeit von Präventionsakteuren limitiert, aber nicht verunmöglicht. Vielmehr müssen die antizipativen Praktiken der Prävention und Mitigation extremistischer Bedrohungen in eine größere Bewältigungsstrategie integriert werden. Werden die vier Aspekte der Resilienz bedacht und bearbeitet, scheint eine erfolgreiche Bewältigung vergleichbarer Bedrohungen auch zukünftig aussichtsreich. Die verschieden involvierten gesellschaftlichen Akteure müssen in *Netzwerken* aus Systemen zusammenarbeiten, um die *Kontrolle* über die eigene *Beschaffenheit* zu bewahren, und diese einer kontinuierlichen *Entwicklung* unterziehen. Während Beschaffenheiten möglichst viel Spielraum und Handlungsmöglichkeiten erlauben sollten, so sollte Kontrolle entlang

vorbereitender, beobachtender und intervenierender Maßnahmen strukturiert werden. Für die Entwicklung muss in einer offenen Kommunikationskultur aus Ereignissen gelernt werden, Bedrohungen zu antizipieren. Vergangene und bestehende Polykrisen machen die Notwendigkeit einer erweiterten Kommunikation und Koordination unter verschiedensten Akteuren und ihren Erwartungen deutlich.

Aus der Beobachter*innenperspektive der Forschung ergeben sich bereits naheliegende Betätigungsfelder für ein Systemnetzwerk zur resilienten Bewältigung der Herausforderungen extremistischer Bedrohungen. Die Technikfolgenabschätzung richtet ihren Fokus auf die kontinuierliche Beobachtung und Antizipation der Entwicklungen technologischer Affordanzen und Schlüsselfaktoren malevolenter Kreativität. Im Sinne der Innovationsdynamik ist es zudem ratsam, weitere Einflussfaktoren zu beobachten, welche nicht nur die Verfügbarkeit und potenzielle Wirkung von Technologien im Blick behalten, sondern auch Repressions- und Konfliktdynamiken sowie die Variation und den Wandel von Einstellungen mit möglicherweise zugrunde liegenden Ideologien. Die MOTRA-Verbundpartner decken bereits einen Teil dieser Felder ab, indem sie das Protestgeschehen (vgl. Beitrag WZB ab Seite 154) , den Diskurs der Internet-Communities (vgl. Beitrag LMU ab Seite 50) und die Einstellungen der Menschen in Deutschland (vgl. Beitrag Universität Hamburg ab Seite 86) untersuchen. Das Ziel besteht jedoch darin, relevante Entwicklungen nicht nur zu beobachten, sondern die aus der Beobachtung gewonnenen Erkenntnisse für vorbereitende und intervenierende Maßnahmen aufzubereiten und sie innnerhalb von verschiedenen Netzwerken (transdisziplinär) offen zu kommunizieren. Demnach ist der Wissenstransfer an Präventionsakteure im Speziellen und an die Zivilgesellschaft im Allgemeinen entscheidend. Nur so kann es gelingen, auch aus dem Beobachteten antizipativ zu lernen und die Erfahrungen und Einsichten in die Ausgestaltung zukünftiger Beschaffenheiten (technische Plattformen, Organisationsnetzwerke, Kooperationsformate) einfließen zu lassen. Die systematische Integration der Präventionsperspektive ist daher ein unabdingbarer Bestandteil der Weiterentwicklung des Technologiemonitorings. Hierzu zählt ebenfalls die Konzeption eines validierten Leitfadens zur zeitnahen Bewertung neuartiger Technologien hinsichtlich ihres malevolenten Potenzials im Kontext von Radikalisierung und Extremismus. In diesem Sinne kann ein Technologiemonitoring, wie es im MOTRA-Verbund angelegt ist, einen gehaltvollen Beitrag zur Resilienz einer demokratisch verfassten Gesellschaft leisten.

Literatur

Archambault, E. & Veilleux-Lepage, Y. (2024). The Islamic State's drone innovation. In J. P. Rogers (Hrsg.), *De Gruyter Handbook of Drone Warfare*. De Gruyter.

Argentino, M.-A., Maher, S. & Winter, C. (2021). *Violent extremist innovation: a cross-ideological analysis*. International Centre for the Study of Radicalisation. https://icsr.info/wp-content/uploads/2021/12/ICSR-Report-Violent-Extremist-Innovation-A-Cross%E2%80%91Ideological-Analysis.pdf

Basha, S. (2023). "Death to the grid": ideological narratives and online community dynamics in encouraging far-right extremist attacks on critical infrastructure. *Counter Terrorist Trends and Analyses*, *15*(4), 17–24.

BMI (2009). *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie).* Bundesministerium des Innern. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.pdf?__blob=publicationFile&v=3

Büscher, C. (2022). The problem of observing sociotechnical entities in social science and humanities energy transition research. *Frontiers in Sociology*, *6*. https://doi.org/10.3389/fsoc.2021.699362

Büscher, C., Kusche, I., Röller, T., Andres, F., Gazos, A., Hahn, J., Ladikas, M., Madeira, O., Plattner, G. & Scherz, C. (2022). Trends der zukünftigen Technologienutzung im Kontext von Extremismus und Terrorismus: Erste Erkenntnisse aus dem MOTRA-Technologiemonitoring. In U. Kemmesies, P. Wetzels, B. Austin, C. Büscher, A. Dessecker, E. Grande & D. Rieger (Hrsg.), *MOTRA-Monitor 2021* (S. 248–281). MOTRA.

Caviezel, C., Hempel, L., Revermann, C. & Steiger, S. (2022). *Beobachtungstechnologien im Bereich der zivilen Sicherheit – Möglichkeiten und Herausforderungen. Endbericht zum TA-Projekt*. Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB). https://doi.org/10.5445/IR/1000153823

Cronin, A. K. (2020). *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists*. Oxford University Press.

Cropley, D. H., Kaufman, J. C. & Cropley, A. J. (2008). Malevolent creativity: a functional model of creativity in terrorism and crime. *Creativity Research Journal*, *20*(2), 105–115. https://doi.org/10.1080/10400410802059424

Demir, M. & Guler, A. (2023). The effects of the 9/11 terrorist attacks on suicide terrorism. *Behavioral Sciences of Terrorism and Political Aggression*, *15*(1), 24–41. https://doi.org/10.1080/19434472.2020.1866052

Dolnik, A. (2007). *Understanding terrorist innovation: Technology, tactics and global trends*. Routledge, Taylor & Francis Group.

Endreß, M. & Rampp, B. (2014). Resilienz als Prozess transformativer Autogenese. Schritte zu einer soziologischen Theorie. *BEHEMOTH – A Journal on Civilisation*, *7*(2), 73–102. https://doi.org/10.6094/behemoth.2014.7.2.834

Folkers, A. (2018). Was ist kritisch an Kritischer Infrastruktur? Kriegswichtigkeit, Lebenswichtigkeit, Systemwichtigkeit und die Infrastrukturen der Kritik. In J. I. Engels & A. Nordmann (Hrsg.), *Was heißt Kritikalität?* (S. 123–154). transcript Verlag. https://doi.org/10.1515/9783839442074-005

Fox, S. J. (2021). past attacks, future risks: where are we 20-years after 9/11? *Journal of Strategic Security*, *14*(3), 112–157. https://doi.org/10.5038/1944-0472.14.3.1964

Franke, U. E. (2014). The global diffusion of unmanned aerial vehicles (UAVs), or 'drones'. In M. Aaronson, R. Rauxloh, W. Aslam, T. Dyson, A. Barrinha, L. Alison & U. E. Franke (Hrsg.), *Precision strike warfare and international intervention: strategic, ethico-legal and decisional implications* (S. 52–73). Routledge.

Gill, P., Horgan, J., Hunter, S. T. & D. Cushenbery, L. (2013). Malevolent creativity in terrorist organizations. *The Journal of Creative Behavior*, *47*(2), 125–151. https://doi.org/10.1002/jocb.28

Harding, E., Leiter, M., & Byman, D. (2023, November 7). *Hamas' October 7 attack: the tactics, targets, and strategy of terrorists*. Center for Strategic and International Studies (CSIS). https://www.csis.org/events/hamas-october-7-attack-tactics-targets-and-strategy-terrorists

Hollnagel, E. (2013). Resilience engineering and the built environment. *Building Research & Information*, *42*(2), 221–228. http://dx.doi.org/10.1080/09613218.2014.862607

Hopkins, A. (1999). The limits of normal accident theory. *Safety Science*, *32*(2–3), 93–102. https://doi.org/10.1016/S0925-7535(99)00015-6

Ilardi, G. J. (2009). The 9/11 attacks – a study of Al Qaeda's use of intelligence and counterintelligence. *Studies in Conflict & Terrorism*, *32*(3), 171-187. https://doi.org/10.1080/10576100802670803

Jore, S. H. (2023). Is resilience a good concept in terrorism research? A conceptual adequacy analysis of terrorism resilience. *Studies in Conflict & Terrorism*, *46*(1), 1–20. https://doi.org/10.1080/1057610X.2020.1738681

Krill, I. & Clifford, B. (2022). Mayhem, murder, and misdirection: violent extremist attack plots against critical infrastructure in the United States, 2016–2022. P*rogram on Extremism,* George Washington University; and National Counterterrorism Innovation, Technology, and Education Center. https://digitalcommons.unomaha.edu/cgi/viewcontent.cgi?article=1009&context=ncitereportsresearch

Kron, T. (2007). Fuzzy-Terrorism – Zur Strategie-Evolution des transnationalen Terrorismus. In T. Kron & M. Reddig (Hrsg.), *Analysen des transnationalen Terrorismus: Soziologische Perspektiven* (S. 84–121). VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-531-90556-3_5

Krüger, M. & Albris, K. (2020). Resilience unwanted: Between control and cooperation in disaster response. *Security Dialogue*, *52*(4), 343–360. https://doi.org/10.1177/0967010620952606

Kusche, I., Andres, F., Büscher, C., Gazos, A., Hahn, J., Ladikas, M., Röller, T. & Scherz, C. (2021). MOTRA-Technologiemonitoring (S. 188–204). In U. Kemmesies, P. Wetzels, B. Austin, A. Dessecker, E. Grande, I. Kusche & D. Rieger (Hrsg.), *MOTRA-Monitor 2020.* MOTRA.

La Porte, T. M. (2006). organizational strategies for complex system resilience, reliability, and adaptation. In P. E. Auerswald, L. M. Branscomb, T. M. La Porte & E. O. Michel-Kerjan (Hrsg.), *Seeds of disaster, roots of response* (1. Aufl., S. 135–154). Cambridge University Press. https://doi.org/10.1017/CBO9780511509735.012

Loadenthal, M. (2021a, Januar 19). Anti-5G, Infrastructure Sabotage, and COVID-19. *GNET.* https://gnet-research.org/2021/01/19/anti-5g-infrastructure-sabotage-and-covid-19/

Loadenthal, M. (2021b, Februar 15). Infrastructure, Sabotage, and Accelerationism. *GNET.* https://gnet-research.org/2021/02/15/infrastructure-sabotage-and-accelerationism/

Loadenthal, M. (2022). Feral fascists and deep green guerrillas: Infrastructural attack and accelerationist terror. *Critical Studies on Terrorism*, *15*(1), 169–208. https://doi.org/10.1080/17539153.2022.2031129

Madeira, O. & Plattner, G. (2023). *A safe space for everyone – a plea for a democratic and participative metaverse*. https://www.metaverse-forschung.de/en/2023/08/22/a-safe-space-for-everyone-a-plea-for-a-democratic-and-participative-metaverse/

Madeira, O., Plattner, G., Gazos, A., Röller, T. & Büscher, C. (2023). Technologiemonitoring: Das Potenzial von Metaverse und KI für extremistische Verwendungszwecke (S. 226–252). In U. Kemmesies, P. Wetzels, B. Austin, C. Büscher, A. Dessecker, S. Hutter & D. Rieger (Hrsg.), *MOTRA-Monitor 2022.* MOTRA.

Mayring, P. & Fenzl, T. (2019). Qualitative Inhaltsanalyse. In N. Baur & J. Blasius (Hrsg.), *Handbuch Methoden der empirischen Sozialforschung* (S. 633–648). Springer VS. https://doi.org/10.1007/978-3-658-21308-4_42

Meyer, J. W. & Rowan, B. (1977). Institutionalized organizations: formal structure as myth and ceremony. *American Journal of Sociology*, *83*(2), 340–363.

Norman, D. (2013). *The design of everyday things. Revised and expanded edition*. Basic Books.

Parker, J. (2020, Februar 4). Accelerationism in America: threat perceptions. *GNET*. https://gnet-research.org/2020/02/04/accelerationism-in-america-threat-perceptions/

Perrow, C. (1984). *Normal accidents. Living with high-risk technologies*. Basic Books.

Piazza, J. A. & Guler, A. (2021). The online caliphate: internet usage and ISIS support in the arab world. *Terrorism and Political Violence*, *33*(6), 1256–1275. https://doi.org/10.1080/09546553.2019.1606801

Rassler, D. & Veilleux-Lepage, Y. (2024). The paradox of progress: How 'disruptive,' 'dual-use,' 'democratized,' and 'diffused' technologies shape terrorist innovation. *TATuP – Journal for Technology Assessment in Theory and Practice*, *33*(2), 22–28. https://doi.org/10.14512/tatup.33.2.22

Schonschek, O. (2023, April 17). *Was sich bei KI bereits zertifizieren lässt*. BigData-Insider. https://www.bigdata-insider.de/was-sich-bei-ki-bereits-zertifizieren-laesst-a-f40bad5afdc47d5df4662f2d58bfbad8/

Schulze, H., Greipl, S., Hohner, J. & Rieger, D. (2024). Social media and radicalization: an affordance approach for cross-platform comparison. *M&K Medien & Kommunikationswissenschaft*, *72*(2), 187–212. https://doi.org/10.5771/1615-634X-2024-2-187

Scrivens, R., & Conway, M. (2019). The roles of „old" and „new" media tools and technologies in the facilitation of violent extremism and terrorism. In R. Leukfeldt & T. J. Holt (Hrsg.), *The human factor of cybercrime* (S. 286–309). Routledge. https://doi.org/10.4324/9780429460593

Sullivan, J. & Lester, G. (2022). Revisiting domestic intelligence. *Journal of Strategic Security*, *15*(1), 75–105. https://doi.org/10.5038/1944-0472.15.1.1976

Tierney, K. J. (2003). *Conceptualizing and measuring organizational and community resilience: lessons from the emergency response following the September 11, 2001 attack on the World Trade Center*. University of Delaware. https://udspace.udel.edu/server/api/core/bitstreams/0c290331-74a5-4893-9986-d0614bd26c54/content

Weick, K. E., Sutcliffe, K. M. & Obstfeld, D. (2008). Organizing for high reliability: processes of collective mindfulness. In A. Boin (Hrsg.), *Crisis management* (S. 31–66). SAGE Publications.

Wimelius, M. E., Eriksson, M., Kinsman, J., Strandh, V. & Ghazinour, M. (2023). What is local resilience against radicalization and how can it be promoted? A multidisciplinary literature review. *Studies in Conflict & Terrorism*, *46*(7), 1108–1125. https://doi.org/10.1080/1057610X.2018.1531532

Witzel, A. (2000). Das problemzentrierte Interview. *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, *1*(1). https://doi.org/10.17169/fqs-1.1.1132

Zeiger, S. & Gyte, J. (2020). Prevention of radicalization on social media and the internet. In A. P. Schmid (Hrsg.), *Handbook of Terrorism Prevention and Preparedness* (S. 358–395). ICCT Press. https://doi.org/10.19165/2020.6.01

Zhang, Y. & Wildemuth, B. M. (2009). Qualitative analysis of content. In B. M. Wildemuth (Hrsg.), *Application of social research methods to questions in information and library science* (S. 308–319). Libraries Unlimited.