08.03.2021

ABSCHLUSSBERICHT

RAN-Veranstaltung in kleiner Runde – EinzeltäterInnen im digitalen Raum
24. Februar 2021 15.00–18.00 Uhr MEZ, online

Digitaler Terrorismus und „EinzeltäterInnen"

Wichtige Ergebnisse

Leitfrage dieses ExpertInnentreffens war, wie sich terroristische EinzeltäterInnen im digitalen Raum finden und identifizieren lassen, bevor sie Gewalttaten begehen. Ein besonderer Fokus lag dabei auf der Rolle und den Funktionen von Social-Media- und Gaming-Plattformen. Der Begriff des „Einzeltäter-Terrorismus" hat sich im Laufe der Zeit als ein kontroverses und verwirrendes Konzept herausgestellt. Auch wenn bestimmte Personen auf operativer Ebene einzeln agieren, sind sie in der Regel Teil einer bestimmten Gruppe oder Bewegung bzw. fühlen sich dieser zugehörig. Gerade im digitalen Zeitalter sind sogenannte „EinzeltäterInnen" also in der Regel nicht vereinzelt. Manche AngreiferInnen schließen sich keiner Gruppe an, da sie davon ausgehen, von der Regierung überwacht zu werden; dennoch fühlen sie sich als Teil eines durch gemeinsame Werte, Aktionen und Feinde vereinten Kollektivs. Der Prozess gegen den Angreifer von Halle (2020) und der Bericht der Christchurch-Kommission (2020) haben gezeigt, dass weder die Nachrichtendienste noch die Strafverfolgungsbehörden oder die Tech-Industrie wussten, wo nach solchen digital agierenden EinzeltäterInnen zu suchen ist oder wie man sie online identifizieren kann. Zudem war man sich der grundlegenden Funktionsweise (und des Missbrauchs) von Plattformen, Websites und anderen Online-Diensten, die über Facebook, YouTube und Twitter hinaus von TäterInnen genutzt werden, kaum bewusst.

Einige der wichtigsten Erkenntnisse des Treffens waren:

- Sogenannte „EinzeltäterInnen" sind in der Regel nicht vereinzelt. Das Narrativ des „einsamen Wolfs" ist ungenau und potenziell schädlich, da es die Milieus und informellen Netzwerke unterschätzt, die den AngreiferInnen als ideologische, moralische und manchmal auch logistische Unterstützung dienen.

- Achten Sie auf bestimmte Warnzeichen, die darauf hindeuten, dass sich eine Person in Richtung Gewaltbereitschaft bewegt; zum Beispiel, wenn sie Hassreden oder Manifeste postet, in denen eine existenzielle Bedrohung ihrer Eigengruppe beschrieben und Gewalt gerechtfertigt oder gefordert wird; Anleitungen zum Selbstbau von Waffen weitergibt oder aktiv danach sucht; ein „Bedürfnis zu handeln" zum Ausdruck bringt; Beziehungen zu Personen beendet, die aufgrund ihrer Hautfarbe, ihres Glaubens, ihres Geschlechts oder anderer Eigenschaften als minderwertig betrachtet werden.

- Es werden Fördermittel für maßnahmenorientierte (kurzfristige) Forschungsvorhaben sowie für Projekte benötigt, die sich auf die digitalen (Teil-)Milieus konzentrieren, in denen potenzielle EinzeltäterInnen aktiv sein können.

Dieser Bericht beschreibt zunächst, welche Herausforderungen aus verschiedenen Perspektiven diskutiert wurden. Im zweiten Teil werden Empfehlungen sowohl für PraktikerInnen als auch für politische EntscheidungsträgerInnen präsentiert.

Kernpunkte der Diskussion

Die folgenden Herausforderungen wurden von FachexpertInnen vorgestellt.

- **EinzeltäterInnen sind nicht vereinzelt:** Sogenannte „EinzeltäterInnen" sind in der Regel nicht vereinzelt. Das Narrativ des „einsamen Wolfs" ist ungenau und potenziell schädlich, da es die Milieus und informellen Netzwerke unterschätzt, die den AngreiferInnen als ideologische, moralische und manchmal auch logistische Unterstützung dienen. In mehreren Fällen stellten sich TäterInnen, die als EinzeltäterInnen/einsamer Wolf bezeichnet wurden, als Teil einer Bewegung oder eines unorganisierten Kollektivs heraus. Eine Fehlinterpretation des Phänomens kann eine Fehleinschätzung der Größe und des Umfang der Bedrohung nach sich ziehen.

- **„Gamification" ist kein neues Phänomen:** Die Rolle von Gamification im Kontext des Einzeltäter-Terrorismus wird möglicherweise überbewertet, da der psychologische Rahmen der Förderung von Status und Belohnungen durch Wettbewerb eine gängige Praxis in (extremistischen/terroristischen) Gruppen ist. Bislang gibt es keine wissenschaftlichen Belege dafür, dass Online-Spiele (einschließlich sogenannter Ego-Shooter-Spiele) mit physischer Gewalt oder extremistischem/terroristischem Verhalten in Verbindung stehen.

- **Fehlende Governance auf Spieleplattformen schafft Raum für ExtremistInnen:** Einige Gaming-Plattformen/-Foren dienen als Treffpunkte, Propaganda-Outlets und Rekrutierungsplätze für ExtremistInnen oder TerroristInnen. Die meisten dieser Dienste verfügen über keine effektiven Governance- und Moderationssysteme, was sie zu leichten Zielen für extremistische und terroristische AkteurInnen und für das Erreichen bestimmter Zielgruppen macht.

- **Raum für Verbesserungen für Social-Media-Unternehmen:** Große Social-Media-Plattformen betonen, dass sie erhebliche Ressourcen in Tools und Verfahren zur Inhaltsmoderation investieren, behaupten aber, dass deren Effektivität aufgrund von Bedenken hinsichtlich der Meinungsfreiheit sowie der schieren Datenmenge begrenzt bleibt. Gleichzeitig werden alle Nutzerdaten ständig verarbeitet und analysiert, um das Geschäftsmodell der Plattform zu bedienen, welches darin besteht, den Zugang zu Nutzerprofilen zu Werbezwecken an Dritte zu verkaufen. Dies deutet darauf hin, dass Social-Media-Unternehmen mehr über extremistische oder terroristische AkteurInnen, die ihre Dienste missbrauchen, „wissen" (oder herausfinden) könnten, als sie es derzeit tun.

- **Kann gewaltbereites Verhalten vorhergesagt werden?** Die Frage, welches Online-Verhalten zukünftige gewaltbereite Handlungen signalisieren oder darauf hinweisen könnte, wurde aus verschiedenen Blickwinkeln diskutiert, wobei zwischen Personen, die sich online extremistisch äußern, und Personen, die „nur so tun, als ob", unterschieden wurde:

    - „Leaking" – Viele EinzeltäterInnen haben ihre Handlungen zuvor gegenüber Familienmitgliedern und FreundInnen oder auf bestimmten Social-Media-Plattformen oder Websites angekündigt. Wie können solche Informationen schneller verarbeitet werden?

    - Risikobewertungsinstrumente – Die Nützlichkeit von Risikobewertungsinstrumenten, die hauptsächlich für bereits bekannte Personen entwickelt wurden, wie VERA-2R, TRAP-18, ERG22+ und RADAR-iTE, sollte im Hinblick auf die Identifizierung „unbekannter" EinzeltäterInnen im digitalen Raum weiter untersucht werden.

    - Erkenntnisse aus Bewertungstools zu selbstverletzendem Verhalten (psychiatrische Erfahrungen) – Durch Bewertungstools zu selbstverletzendem Verhalten gewonnene Erkenntnisse könnten nützlich sein, um potenziell gewaltbereites Verhalten frühzeitig zu erkennen. Dies bedeutet nicht, dass EinzeltäterInnen notwendigerweise psychische Probleme haben, noch, dass wenn sie welche haben, diese in kausalem Zusammenhang zu ihren terroristischen Handlungen stehen.

- Wegfall von Schutzfaktoren – Die Online-Welt kann EinzeltäterInnen helfen, digitale soziale Bindungen aufzubauen, die sie in einem emotional sicheren Raum halten. Ein Gefühl der Dringlichkeit, zu handeln, kann durch den Wegfall von Schutzfaktoren oder durch apokalyptische Narrative entstehen, die eine existenzielle Bedrohung propagieren (z. B. „Bevölkerungsaustausch"/„weißer Genozid"/„Krieg gegen den Islam") und die Person dazu motivieren, vom Opfer zum Täter oder vermeintlichen „Helden" zu werden.

- **Informationsflut:** Die Unterscheidung, was lediglich als „Rauschen" zu werten ist und was ein relevantes Signal darstellt, wird immer schwieriger, da sich die extremistischen digitalen Landschaften diversifizieren und die Rolle von Organisationen weniger dominant ist – insbesondere im Bereich des gewaltbereiten Rechtsextremismus im Vergleich zum islamistischen Extremismus und Terrorismus.

- **Sich verändernde digitale Landschaften:** Infolge des Entfernens extremistischer/terroristischer Inhalte von den großen Social-Media-Plattformen verändern sich die digitalen Landschaften stetig. Extremistische/terroristische AkteurInnen bewegen sich oft auf und zwischen kleineren Social-Media- und Video-Sharing-Plattformen oder Messenger-Diensten wie Telegram und Chan-Boards. Diese digitalen Dienste werden von P/CVE-PraktikerInnen oft nicht ausreichend gut verstanden.

- **Spezialisierte Unterstützung:** Vielen P/CVE-PraktikerInnen, die online aktiv sind, fehlt ein tiefgreifendes Verständnis der verschiedenen (potenziell) extremistischen Subkulturen, ihres Gebrauchs von Sprache, Humor, Memes und anderen Arten von „Stammessymbolen". Spezialisierte zivilgesellschaftliche Organisationen können die für Analysen und digitale Outreach-Maßnahmen (z. B. Digital Streetwork) erforderlichen Erkenntnisse liefern.

Empfehlungen

Die Empfehlungen für PraktikerInnen lauten:

- Wenn Sie mit Personen oder den Familien von Personen arbeiten, die als EinzeltäterInnen eingestuft wurden, dann **erkunden und verstehen Sie deren soziales (Online-)Umfeld** sowie ihre Bezugsgruppe, um Fehleinschätzungen ihrer Motivationen, Werte und Unterstützungsstruktur zu vermeiden. **Lernen Sie aus Nachbesprechungen, Versuchen und Untersuchungen**, worauf Sie achten müssen, um sich ein vollständiges Bild zu machen. Idealerweise müssen bestimmte PraktikerInnen (glaubwürdige Quellen) in der Lage sein, **Gespräche zu führen**.

- Stellen Sie sicher, dass Sie die **relevanten und aktuellen Trends, Themen, Memes, Abzeichen und Marken der extremistischen (Online-)Milieus**, mit denen Sie sich beschäftigen, verstehen, indem Sie sich an spezialisierte zivilgesellschaftliche Organisationen und Forschende wenden, die über die entsprechende Expertise und Erfahrung verfügen. Es ist wichtig, PraktikerInnen wie PolizeibeamtInnen und JugendarbeiterInnen zu schulen, damit sie den spezifischen Humor und die online verwendete Sprache verstehen.

- Achten Sie auf **besondere Warnzeichen**, die darauf hindeuten, dass eine Person sich in Richtung Gewaltbereitschaft bewegt, wie zum Beispiel:

  - Posten von Hassreden oder Manifesten, in denen eine existenzielle Bedrohung der Eigengruppe beschrieben und Gewalt gerechtfertigt oder gefordert wird;

  - Weitergabe von oder aktive Suche nach Anleitungen zum Selbstbau von Waffen;

  - Ausdruck eines „Bedürfnisses zu handeln";

- Beendigung von Beziehungen zu Personen, die aufgrund ihrer Hautfarbe, ihres Glaubens, ihres Geschlechts oder anderer Eigenschaften als minderwertig betrachtet werden.

Um digitale Signale potenzieller EinzeltäterInnen zu identifizieren, **prüfen Sie**, ob existierende **Risikobewertungsinstrumente** wie VERA-2R, TRAP-18, ERG22+ oder RADAR-iTE aufschlussreich sein oder modifiziert werden können. Die Empfehlungen für politische EntscheidungsträgerInnen lauten:

- **Stellen Sie sicher, dass digitale extremistische/terroristische Milieus und Bewegungen, die EinzeltäterInnen leiten und motivieren könnten, richtig eingeschätzt und verstanden werden.** Eine Fehleinschätzung der Angriffe von EinzeltäterInnen als unzusammenhängende und isolierte Aktionen von Einzelpersonen kann zu irreführenden Statistiken und unvollständigen Bedrohungseinschätzungen führen.

- **Priorisieren Sie die Finanzierung von maßnahmenorientierten (kurzfristigen) Forschungsvorhaben** sowie von Projekten, die sich auf die Identifizierung digitaler (Teil-)Milieus konzentrieren, in denen potenzielle EinzeltäterInnen aktiv sein könnten, d. h. Mapping von AkteurInnen, um internationale Verbindungen aufzuzeigen, Verfolgung von Unterhaltungen auf verschiedenen Plattformen, um potenzielle EinzeltäterInnen zu identifizieren und zu verstehen, welche prominenten Narrative für diese Online-AkteurInnen bedeutsam und relevant sind. Die Forschung kann in einem anonymisierten Format durchgeführt werden, um Trends und Unterhaltungen über Plattformen hinweg zu identifizieren.

- **Halten Sie den Dialog mit – und den Druck auf – Unternehmen aus den Bereichen soziale Medien, Video-Sharing und Online-Spiele aufrecht**, damit diese nicht nur terroristische Inhalte von den Plattformen entfernen, sondern sich auch bemühen, digital agierende potenzielle EinzeltäterInnen proaktiv zu identifizieren. Online-Plattformen und Forschende sollten Indikatoren zur Vorhersage von Verhalten (zum Beispiel Anzeichen für Hetze) entwickeln und deren Zusammenspiel mit anderen Indikatoren untersuchen, sowie Verhaltensmuster im Laufe der Zeit (zum Beispiel eine Verhaltenseskalation) untersuchen, um EinzeltäterInnen mittels solcher Verhaltensweisen zu identifizieren.

Investieren Sie in strukturierte und fortlaufende **Peer-Learning-Module**, die den Austausch von Erkenntnissen zwischen relevanten Akteuren (zivilgesellschaftliche Organisationen/Forschende/Regierung/Unternehmen) erleichtern.

Relevante Praktiken:

Es wurden einige Praktiken vorgestellt:

Die 1-2-1-Online-Interventionen des Institute for Strategic Dialogue sind ein experimenteller Ansatz, der die Lücke schließen soll, welche durch das Fehlen systematisierter Versuche entstanden ist, die Bemühungen zur Bekämpfung von Hetze durch direkte Online-Nachrichten und entsprechenden Austausch zu ergänzen. Das Programm, das bisher auf Facebook durchgeführt wurde und mit rechtsextremen und islamistischen Ideologien arbeitet, bietet Personen, die deutliche Anzeichen einer Radikalisierung aufweisen, die Möglichkeit, sich mit jemandem zu treffen und auszutauschen, der sie bei der Abkehr von Hass unterstützen kann.

Die Redirect-Methode von MoonshotCVE, die von Facebook und Google umgesetzt wird, kann hierbei als Inspiration dienen. Bei dieser Methode zur Bekämpfung von gewaltbereitem Extremismus und gefährlichen Organisationen werden Nutzer, die hass- oder gewaltbezogene Suchanfragen eingeben, zu Bildungsressourcen

und Hilfsgruppen umgeleitet. Ein Pilotprogramm wurde mit den Partnern Life After Hate in den USA (Mai 2019) sowie Exit Australia (September 2019) gestartet.

Das Projekt Good Gaming - Well Played Democracy der Amadeo Antonio Stiftung in Deutschland verbindet die Analyse von Gaming-Subkulturen aus einer P/CVE-Perspektive mit Digital Streetwork, indem es Online-Gamer anspricht und sie über schädliche Verschwörungsmythen aufklärt. Zudem werden im Rahmen des Projekts LehrerInnen, SozialarbeiterInnen und InfluencerInnen zu diesen Themen geschult.

Folgemaßnahmen

Ein strukturierter und kontinuierlicher Austausch zwischen ExpertInnen, die sich mit den digitalen Milieus von EinzeltäterInnen beschäftigen, sowie AusstiegshelferInnen, die Erfahrung mit Online-Interventionen haben, könnte zusätzliche praktische Erkenntnisse zum Verständnis, der Prävention und Bekämpfung dieses sich stetig weiterentwickelnden Phänomens generieren. Eine bereichsübergreifende Veranstaltung zum Thema „EinzeltäterInnen – gemeinsame Bestandsaufnahme der jüngsten Entwicklungen und Zusammenführung von Wissen" und ein Webinar zum Thema „Digitaler Terrorismus und EinzeltäterInnen" werden als Folgeveranstaltungen zu diesem Treffen dienen und eine weitere Sensibilisierung für das Thema anregen.