

Extremistische Online-Gemeinschaften und Massenmorde an Schulen und anderen Bildungseinrichtungen. Fortsetzung, Teil 3.

Fortsetzung: Vorherige Beiträge: [Teil 1](#), [Teil 2](#).

Einführung zusätzlicher Kontrollmechanismen sowie offener und verdeckter Maßnahmen zur Einflussnahme auf Jugendliche aus potenziellen Risikogruppen* in Bildungs- und Kinderbetreuungseinrichtungen. Dies dürfte sich erheblich auf die Gesamtzahl potenzieller Opfer von Anwerbern der «Todesgruppen» und damit auch auf die Zahl der Täter auswirken, die auf Anweisung und im Interesse dieser Gemeinschaften Straftaten begehen. Als Ergebnis: eine Verringerung der Aktivität solcher Gruppen, eine Verlangsamung der Verbreitung der von ihnen propagierten extremistischen Ideen und vor allem ein Rückgang der Zahl schwerer und besonders schwerer Straftaten, die von ihren Mitgliedern in den Ländern begangen werden, in denen diese Maßnahmen tatsächlich umgesetzt werden.

Wenn dieser Ansatz dauerhaft in die Arbeit von Psychologen und Soziologen in Bildungseinrichtungen und anderen Kinderbetreuungseinrichtungen integriert wird und die Arbeit einer internationalen Überwachungs- und Koordinierungsgruppe fortgesetzt wird, die die Entwicklung der Lage verfolgt und unter Berücksichtigung dieser Veränderungen die Taktik zur Aufdeckung und Bekämpfung entsprechend anpasst, wird dies als wirksamer Faktor zur Eindämmung der Bedrohung und langfristig zur Kontrolle der Situation dienen.

Als wirksame Ergänzung zu den zuvor genannten Präventionsmaßnahmen, die die Zahl potenzieller Opfer für Anwerber verringert, würde ich den Leitungen von Schulen, anderen Bildungseinrichtungen und Orten, an denen sich viele Kinder und Jugendliche aufhalten, vorschlagen, die Einführung eines Elements wie CPTED in Betracht zu ziehen.

CPTED: Das Konzept «Kriminalprävention durch Umweltgestaltung» (Crime Prevention Through Environmental Design) ist ein Ansatz, der darauf abzielt, die Kriminalität durch eine Veränderung der physischen Umgebung, in der sie stattfindet, zu verringern. Der Kern des Konzepts besteht darin, dass ein durchdachter physischer Raum dazu beitragen kann, Straftaten zu verhindern, unerwünschtes Verhalten einzudämmen und die Bindungen innerhalb der Gemeinschaft zu stärken.

Die Wirksamkeit dieser Methode zur Verringerung von Gewalt in Bildungseinrichtungen wurde durch langjährige Praxisstudien bestätigt, die von Safe Havens International (SHI) durchgeführt wurden – einer der ältesten und erfahrensten Fach- und Analyseorganisationen weltweit, die sich auf die Verbesserung der Sicherheit in Bildungseinrichtungen spezialisiert hat.

Ausführlichere Informationen zu den Methoden der CPTED-Anwendung und den erzielten Ergebnissen finden Sie in den [Artikeln](#) des Geschäftsführers von SHI, Michael Dorn, einem international anerkannten Experten auf dem Gebiet der Sicherheit an Bildungseinrichtungen.

Auch wenn die Schaffung eines angenehmeren moralisch-psychologischen Klimas nicht alle Sicherheitsprobleme löst und nicht garantiert auf alle Jugendlichen aus der Risikogruppe wirkt, kann der Einsatz solcher Methoden laut Forschungsergebnissen das Ausmaß an Angst, Anspannung und Aggression bei einem Teil der Jugendlichen um 10–15 % senken und somit die Zahl potenzieller Opfer verringern. Und je weniger es solcher moralisch und psychologisch verletzlichen Jugendlichen gibt, desto schwieriger wird es für die Anwerber der «Todesgruppen», sie für sich zu gewinnen und zu kontrollieren.

Hier greift einfache Mathematik. Derzeit rekrutieren «Betreuer» aus extremistischen Gemeinschaften über ihre Informationskanäle Hunderte und Tausende von Jugendlichen, doch zur

Teilnahme an aktiven Aktionen stimmen bestenfalls Dutzende zu, und zur Begehung besonders schwerer Straftaten nur Einzelne. Wenn wir die ursprüngliche Zahl reduzieren, reduzieren wir auch die übrigen. Selbst 10–15 % wären hier schon ein gutes Ergebnis.

Ein weiterer Schwerpunkt der Phase der Bedrohungs Eindämmung ist die Sperrung der von Kriminellen genutzten Netzwerkressourcen. Hierbei ist es wichtig zu verstehen, dass dieser Ansatz sowohl in technischer als auch in rechtlicher Hinsicht äußerst komplex ist. Die Sperrung muss punktgenau und zielgerichtet erfolgen und sich auf bestimmte Communities und einzelne Konten beziehen, über die extremistisches Material verbreitet und Jugendliche rekrutiert werden, um sie zu kriminellen und terroristischen Handlungen zu verleiten.

In dieser Situation nutzen Kriminelle mehrere bestehende Schwachstellen aus. Ich habe fünf Hauptprobleme herausgearbeitet, mit denen wir konfrontiert sind:

1. Die Schwierigkeit, einzelne Konten in sozialen Netzwerken und Messengern zu sperren.

Mit Hilfe technischer und programmtechnischer Sperrmaßnahmen ist es praktisch unmöglich, den Zugriff auf ein (oder mehrere) einzelnes Konto(s) einzuschränken, ohne dass die Verwaltung des sozialen Netzwerks oder des Messengers eingreift.

2. Die Komplexität und Dauer der rechtlichen und administrativen Verfahren zur Erlangung vollstreckbarer gerichtlicher Dokumente zur Sperrung solcher Websites sowie einzelner Profile und Gruppen.

In Anknüpfung an Punkt 1: Die Administrationen von sozialen Netzwerken und Messengern erkennen die Bedrohung in den meisten Fällen zwar an, verlangen jedoch im Rahmen ihrer internen Richtlinien sowie unter Berücksichtigung staatlicher und internationaler Rechtsvorschriften zur Meinungs- und Informationsfreiheit von den Strafverfolgungsbehörden die Vorlage von Beweisen und häufig auch gerichtliche Entscheidungen zur Sperrung von Konten. Eine solche Entscheidung zu erwirken, ist nicht so einfach und oft auch nicht so schnell möglich; manchmal dauert es Wochen oder Monate, bis die Mitarbeiter der Strafverfolgungsbehörden die Beweislage zusammengetragen haben, um sie dem Gericht vorzulegen.

3. Gerichtsbarkeit.

Wie ich bereits im ersten und zweiten Teil erwähnt habe, handelt es sich hierbei um eine internationale Bedrohung. In den letzten Jahren greifen Extremisten meist auf ein Schema zurück, bei dem sich der Anwerber in einem Land befindet, seine Opfer jedoch in einem anderen. Dabei wählt der Täter häufig Länder aus, zwischen denen diplomatische Differenzen bestehen und in denen eine Zusammenarbeit zwischen den Strafverfolgungsbehörden praktisch nicht stattfindet. Gerichtsentscheidungen eines Landes haben für ein anderes Land keinerlei Bedeutung.

4. Verfahrensrechtliche Unterschiede.

In verschiedenen Ländern gelten unterschiedliche Strafgesetze; verschiedene Straftatbestände weisen unterschiedliche Tatbestandsmerkmale, Arten (Kategorien), Merkmale und Schweregrade auf. Was in einem Land als besonders schweres Verbrechen gilt, kann in einem anderen als Ordnungswidrigkeit angesehen werden. Nach dem Recht eines Landes gelten bestimmte Gegenstände, Methoden zur Erfassung und Sicherstellung von Informationen als Beweismittel vor Gericht, in einem anderen Land hingegen nicht.

5. Unterschiede im verfahrensrechtlichen Dokumentenumlauf.

In verschiedenen Ländern gibt es unterschiedliche Arten, Formulare und Verfahren zur Erstellung von Verfahrensdokumenten, zur Erfassung und Registrierung von Beweismitteln, zur Vernehmung von Verdächtigen und Zeugen sowie zur Beschaffung und Aufnahme von Indizien in die Akte.

Beweismaterial, das in einem Land gesammelt wurde, wird von einem Gericht eines anderen Landes allein aufgrund einer nicht konformen Formalisierung nicht anerkannt, was auf unterschiedliche prozessrechtliche Ansätze bei der Dokumentation von Tatsachen von prozessrechtlicher Bedeutung zurückzuführen ist.

All dies erschwert die Arbeit der Strafverfolgungsbehörden und erleichtert die Aktivitäten von Straftätern und kriminellen Vereinigungen. Andererseits darf man aber auch nicht das Verfahren zur Sperrung von Konten vereinfachen, indem man die Anzahl und die Qualität der rechtlichen Grundlagen dafür verringert. Dies würde sowohl Anlass für unbegründete und unbewiesene Einschränkungen der Informationsverbreitung allein auf der Grundlage von Verdächtigungen als auch für vorsätzlichen Missbrauch bieten. Das darf nicht zugelassen werden – die Rechtmäßigkeit ist eine grundlegende Säule und muss strikt eingehalten werden.

Aber wie lässt sich dann die operative Effizienz und die strikte Einhaltung der Rechtmäßigkeit gewährleisten? Ist ein solcher Kompromiss überhaupt möglich? Ja, das ist möglich, erfordert jedoch grundsätzliche Änderungen am bestehenden Ansatz.

Derzeit dauert die Übermittlung eines internationalen Ersuchens (selbst zwischen Ländern, die Abkommen geschlossen haben) Wochen und Monate; in dieser Zeit können Hunderte, wenn nicht Tausende von Jugendlichen in kriminelle Netzwerke hineingezogen und Dutzende schwerer Straftaten begangen werden. Es bedarf eines Systems zur operativen prozessualen Reaktion auf internationaler Ebene. Ein solches System würde es den Mitarbeitern der Strafverfolgungsbehörden jedes teilnehmenden Landes ermöglichen, operativ ein vollstreckbares prozessuales Dokument zu erhalten, auf dessen Grundlage die Betreiber von sozialen Netzwerken und Messengern die Sperrung von Gruppen und Nutzern vornehmen würden.

Für die praktische Umsetzung dieses Vorschlags müssen mehrere Voraussetzungen erfüllt sein:

1. Es muss ein hochspezialisiertes internationales Justizorgan geschaffen werden, das ausschließlich Fälle einer einzigen Kategorie** behandelt. Es muss nicht unbedingt als Gericht eingerichtet werden; in einer ersten Phase könnte es sich um eine internationale Organisation mit gerichtlichen Funktionen handeln, die im Rahmen eines gerichtlichen Verfahrens agiert, jedoch im rechtlichen Sinne kein Gericht darstellt.
2. Es muss ein einheitliches internationales Format für die Vorlage von Anklagen und Beweismitteln zur Prüfung durch diese gerichtliche Instanz entwickelt werden. Dieses Dokument muss klare Festlegungen enthalten darüber:
 - wer berechtigt ist, sich an diese gerichtliche Instanz zu wenden;
 - mit welchen Anklagepunkten und aus welchen Gründen;
 - welche Antragsunterlagen vorzulegen sind und wie diese abzufassen sind;
 - welche Beweismittel in welcher Form vorzulegen sind und wie diese zu beschaffen sind;
 - innerhalb welcher Fristen der Antrag geprüft werden muss;
 - welche Entscheidungen die gerichtliche Instanz treffen kann.
3. auf der Grundlage internationaler Verträge zumindest die größten internationalen Konzerne, die die wichtigsten sozialen Netzwerke, Messenger-Dienste und andere Informationsressourcen betreiben, die für kriminelle Zwecke genutzt werden, zur Zusammenarbeit mit dieser Organisation zu bewegen – wenn schon nicht alle, so doch zumindest die größten. Der Kern der Zusammenarbeit besteht in der Annahme und Umsetzung von Entscheidungen dieser Justizbehörde über die Sperrung (oder andere einschränkende Maßnahmen) von Konten, Nutzern oder Gemeinschaften, bei denen hinreichender Verdacht auf extremistische, terroristischer oder

sonstiger Aktivitäten im Zusammenhang mit der Begehung oder der Verwicklung anderer Personen (vor allem Minderjähriger) in besonders schwere Straftaten, die sich gegen die Person, das Leben oder die Gesundheit von Menschen richten.

Die in Absatz 1 genannte internationale Justizbehörde muss nicht unbedingt als eigenständiges Subjekt des Völkerrechts geschaffen werden; angesichts ihrer begrenzten Funktionen und rechtlichen Befugnisse kann sie durchaus als strukturelle Untereinheit einer der bestehenden internationalen Organisationen mit besonderem Rechtsstatus eingerichtet werden. Zum Beispiel wie die Vereinten Nationen. Die Finanzierung erfolgt durch die Teilnehmerstaaten im Rahmen eines gesonderten internationalen Vertrags. Jeder Teilnehmerstaat erhält das Recht, sich im Rahmen des Tätigkeitsbereichs dieser gerichtlichen Instanz an sie zu wenden, und verpflichtet sich, Mitgliedsbeiträge zu ihrem Unterhalt zu entrichten und die von ihr getroffenen Entscheidungen auf seinem Hoheitsgebiet zu vollstrecken. Beispielsweise indem die Entscheidung dieser internationalen Justizbehörde hinsichtlich der Einschränkung der Verbreitung von Informationen in verfahrensrechtlicher Hinsicht einer gerichtlichen Entscheidung des Justizsystems des jeweiligen Staates gleichgestellt wird.

Die Justizbehörde selbst wird hinsichtlich ihrer organisatorischen Struktur und Personalstärke nicht allzu groß sein. Die Prüfung der Anträge und die Entscheidungsfindung erfolgen kollegial; das Kollegium sollte meiner Meinung nach aus drei Richtern bestehen, die jeden eingereichten Antrag innerhalb von 60 Stunden entgegennehmen, prüfen, beurteilen und darüber entscheiden. In bestimmten Notfällen innerhalb von 12 Stunden. Dabei wird die Stichhaltigkeit der Vorwürfe und die Überzeugungskraft der Beweise im Hinblick auf die allgemein anerkannten Normen des nationalen und internationalen Rechts bewertet. Dementsprechend müssen die Richter über entsprechende Kenntnisse im Bereich des internationalen Rechts und ausreichende praktische Erfahrung in dessen Anwendung verfügen.

Im Durchschnitt wird ein Gremium bis zu vier Anträge pro Woche bearbeiten können. Unter den derzeitigen Umständen wird die durchschnittliche Auslastung bei etwa 100 Anträgen pro Monat liegen. Ich möchte daran erinnern, dass diese Behörde nur einen geringen Teil der Straftaten im Bereich der Informationssicherheit bearbeiten wird. Dabei handelt es sich um direkte, offensichtliche Bedrohungen extremistischer, terroristischer oder anderer Art, die mit der Begehung oder der Verwicklung anderer Personen (vor allem Minderjähriger) in besonders schwere Straftaten gegen die Person, das Leben oder die Gesundheit von Menschen verbunden sind. Derartige Straftaten sind bislang noch nicht sehr zahlreich, gehören jedoch zu den gesellschaftlich gefährlichsten und erfordern daher die schnellstmögliche Einleitung von Strafverfolgungsmaßnahmen.

Ausgehend von vorläufigen Zahlen wird die Gesamtpersonalstärke einer solchen Justizbehörde, die nicht nur Richter, sondern auch Verwaltungs- und technisches Personal umfasst, etwa 200 Mitarbeiter betragen. Für eine internationale Organisation ist dies nicht viel; bei mindestens 30 teilnehmenden Staaten wird die Finanzierung nicht kostspielig sein.

Die größte Herausforderung wird darin bestehen, die großen internationalen Konzerne, denen die wichtigsten sozialen Netzwerke, Messenger-Dienste und andere Informationsplattformen gehören – die in den meisten Fällen für kriminelle Zwecke genutzt werden –, von der Notwendigkeit einer Zusammenarbeit zu überzeugen. Denn nur so lässt sich der entscheidende Vorteil eines solchen Systems ausschöpfen: die Reaktionsgeschwindigkeit.

Die rasche Sperrung von Kommunikationskanälen und die Unterbindung der Verbreitung extremistischer Inhalte wird es ermöglichen, die Handlungsmöglichkeiten destruktiver Gemeinschaften erheblich einzuschränken und vor allem das System zur Steuerung und Koordination rechtswidriger Handlungen zu erschweren oder in manchen Fällen sogar zu zerstören. Dies ist gerade jetzt besonders aktuell, da Jugendliche zunehmend aktiv zur Organisation von Massenunruhen eingesetzt werden. Ich habe bereits im Jahr 2023 darüber geschrieben, als in Russland und einigen Nachbarländern Massenschlägereien und Pogrome verzeichnet wurden, die von Gruppen von Jugendlichen aus der Subkultur [«PMC Ryodan»](#) verübt wurden. Damals stellte ich die Vermutung an, dass diese Ereignisse kein Zufall seien und dass es sich bei dem, was wir beobachteten, nicht um spontane Ereignisse handele, sondern um geplante und gesteuerte Abläufe. Eine ähnliche Situation können wir heute in den USA beobachten, wo eine Welle solcher Straftaten grassiert, die sogar bereits den Namen «Teen Takeover» erhalten hat. Auch in Europa wurden ähnliche Massenangriffe verzeichnet, wenn auch in geringerem Ausmaß.

Wie die Analyse der begangenen Vorfälle gezeigt hat, erfolgten Aufrufe zu rechtswidrigen Handlungen, die Bekanntgabe von Treffpunkten sowie die Festlegung von Zielen, Zeitpunkten und Orten der Angriffe über Communities in sozialen Netzwerken, Chats und Kanäle in Messengern.

Zum Abschluss von Teil 3 möchte ich daran erinnern, dass die Bedrohung durch «Todesgruppen» und andere destruktive Gemeinschaften im Internet längst internationale Ausmaße angenommen hat. Die Entwicklung der Informationstechnologien sowie der Kommunikationsformen und -wege hat die Grenzen zwischen Ländern und Kontinenten aufgehoben. Leider machen sich Kriminelle und Extremisten dies aktiv zunutze, sodass ihre Gemeinschaften schnell transnational geworden sind. Unter solchen Umständen ist ein autonomes Sicherheitssystem, in dem jeder auf sich allein gestellt ist, nutzlos geworden. Diesen Bedrohungen kann man nur gemeinsam begegnen, indem man die Kräfte auf internationaler Ebene bündelt und offensiv, präventiv und vorausschauend handelt. In diesem Fall haben wir alle Chancen, diesen Kampf um eine sichere Zukunft für unsere Kinder zu gewinnen.

Im nächsten Artikel werde ich meine Vorschläge zum Thema der Bekämpfung der Aktivitäten der «Todesgruppen» weiter ausführen. Damit wird Phase 2 abgeschlossen, die der Entwicklung wirksamer praktischer Lösungen gewidmet ist, deren Anwendung die Verbreitung von Informationen und die Anwerbung erschweren und somit den Zustrom neuer Mitglieder in extremistische Gemeinschaften verringern soll, und es erfolgt der Übergang zu Phase 3, den konkreten taktischen Maßnahmen zur Bekämpfung.

** Der Psychotyp der Mitglieder dieser Gruppe sowie die Methoden zu seiner Erkennung und Beeinflussung werden gemeinsam mit Spezialisten für Verhaltensanalyse auf der Grundlage der Auswertung von personenbezogenen Daten entwickelt, die im Rahmen der Arbeit der internationalen Gruppe gesammelt wurden. Nähere Einzelheiten finden sich in Teil 2.*

*** In der Anfangsphase. Angesichts des Zuwachses und der Entwicklung transnationaler Bedrohungen im Bereich der Informationstechnologie hat die Schaffung einer solchen Justizbehörde jedoch ernstzunehmende Zukunftsperspektiven, wobei die Zuständigkeiten auf andere Straftatbestände ausgeweitet werden könnten.*

Veröffentlichungsdatum: 24. Juli 2026

Autor: Roman Grishin

[Profilseite des Autors auf dem Portal](#)