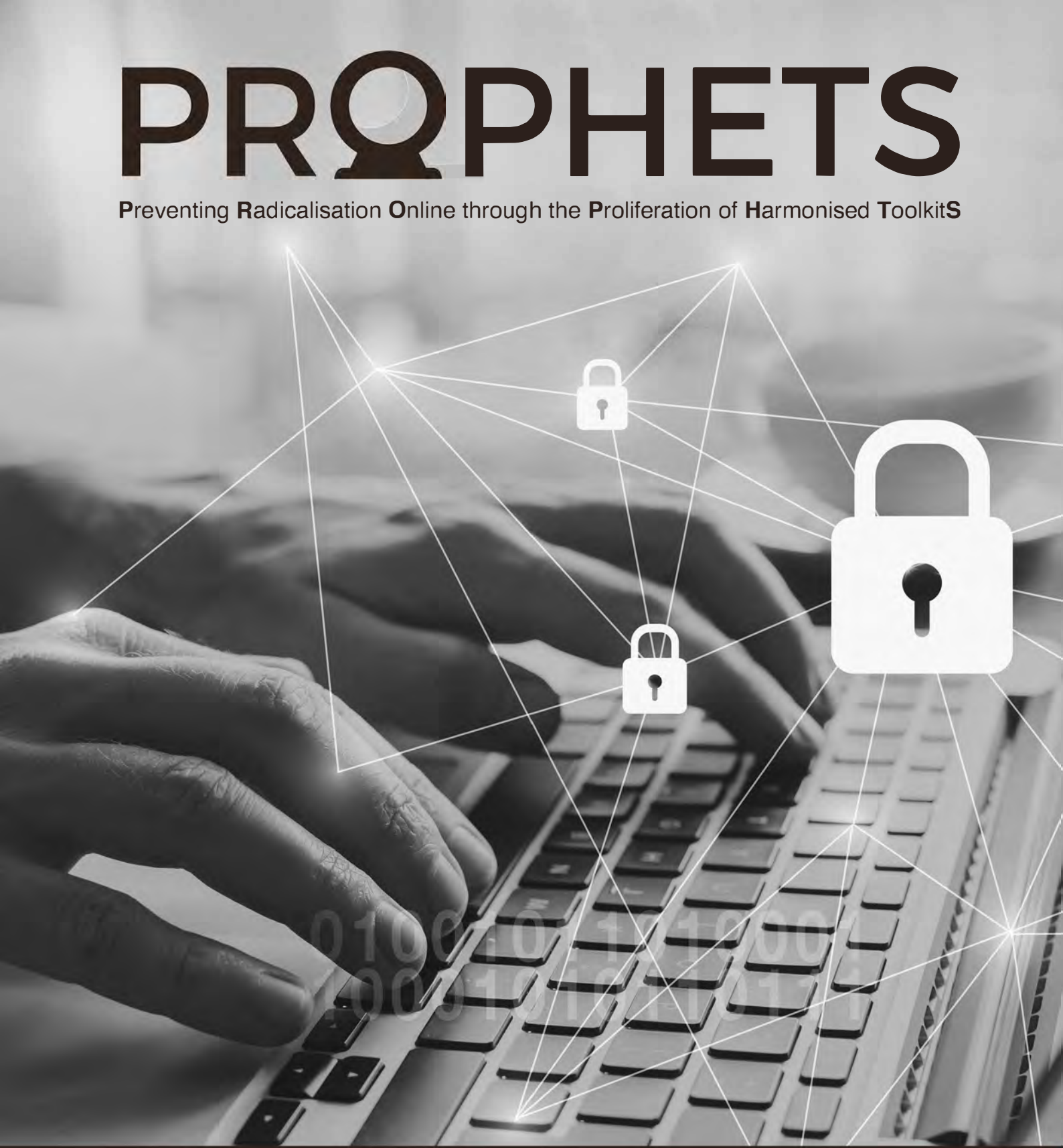
PROPHETS

Preventing **R**adicalisation **O**nline through the **P**roliferation of **H**armonised **T**oolkit**S**



Informationsblatt

Sicherheit im Internet

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786894.

Berlin, Dezember 2020

Freie Universität Berlin (FUB)

Arbeitsbereich Entwicklungswissenschaft und Angewandte Entwicklungspsychologie
Leiter: Univ. Prof. Dr. Herbert Scheithauer
Habelschwerdter Allee 45
14195 Berlin
Email: entwicklung@zedat.fu-berlin.de
Homepage: www.developmental-science.de

Projekt PROPHETS

Koordinator: Dr. Holger Nitsch
Hochschule für den öffentlichen Dienst in Bayern
Fachbereich Polizei
Fürstenfelder Str. 29
82256 Fürstenfeldbruck
Deutschland
Email: prophets@pol.hfoed.bayern.de
Webseite: www.prophets-h2020.eu

Autoren: Kristin Göbel, Antonia Schendel, Sven-Eric Fikenscher, Herbert Scheithauer
Layout: Jenny Köhler
Bildnachweise: istockphoto

Freie Universität Berlin

Das Internet wird zunehmend als Medium genutzt, um Personen zu Terroranschlägen zu motivieren beziehungsweise um terroristische Anliegen zu finanzieren, Einzelpersonen und / oder Gruppen für terroristische Zwecke zu rekrutieren und auszubilden sowie gegen europäische soziale und demokratische Ideale und Minderheiten aufzuhetzen.

Es hat sich gezeigt, dass insbesondere Personen im Jugend- und jungen Heranwachsendenalter gefährdet sind, mit radikalen Gruppierungen und Inhalten im Netz konfrontiert zu werden. Diese Altersspanne, die auch als Phase der Identitätsfindung betrachtet werden kann, ist eine Zeit, in der die Offenheit für neue Inhalte, die Suche nach Orientierung und die Neugier groß ist. Gerade dies kann leider von radikalen Gruppierungen häufig ausgenutzt werden.

Das Internet wird häufig zur Förderung und Unterstützung von Terrorismus genutzt, wobei insbesondere die folgenden Aktivitäten von Bedeutung sind:

Online-Hassrede mit Terrorismusbezug

Terroristische Online-Inhalte

Online-Finanzierung von Terrorismus

Online-Rekrutierung und -Ausbildung von Terroristen

Da diese Aktivitäten oft nicht sofort als solche erkennbar sind, möchten wir im Folgenden einige Informationen und Hinweise bereitstellen, um Ihnen zu helfen, diese besser zu erkennen, um sich entsprechend davor schützen und davon abgrenzen zu können.

ONLINE-HASSREDE MIT TERRORISMUSBEZUG

Was ist Online-Hassrede im Zusammenhang mit Terrorismus?

Als Hassrede gelten alle Arten von Online-Kommunikation, welche Rassismus, Xenophobie, Antisemitismus oder andere Ansichten, die auf Intoleranz und Hass basieren, rechtfertigen, verbreiten oder befürworten. Dies schließt Diskriminierung und Feindseligkeit gegenüber Migranten, Minderheiten und Menschen mit Migrationshintergrund sowie aggressiven Nationalismus und Ethnozentrismus mit ein.[1]

Von Online-Hassrede mit Terrorismusbezug - sei es von Terrorgruppen direkt oder deren Sympathisanten - können Einzelpersonen, aber auch ganze Personengruppen betroffen sein. Diese erfahren dadurch beispielsweise:

Rassismus und Fremdenfeindlichkeit (Diskriminierung aufgrund der Abstammung),

z.B. lückenhafte/verfälschte Informationen über Personen oder Personengruppen wie Gerüchte über Straftaten sowie subjektiv gefilterte Berichterstattung zu anderen ethnischen Gruppen

Antisemitismus und Antimuslimischen Rassismus (Diskriminierung von Juden und Muslimen), häufig unter Verwendung von Stereotypen

z.B. Themenblogs, die von einer drohenden Islamisierung sprechen und dabei gegen Menschen muslimischen Glaubens hetzen oder ganze Verbände und Moscheegemeinden diffamieren

Wichtig: Sofern solchen Inhalten nicht widersprochen wird, fühlen sich die betroffenen Personen möglicherweise abgelehnt, ausgegrenzt und nicht respektiert aufgrund ihrer religiösen Zugehörigkeit oder familiären Herkunft.

Was ist nun typisch für Hassrede? Woran erkennt man diese Art der Kommunikation? [2]

Wir/Die-Rhetorik (sich auf eine Ingroup/Outgroup beziehend – z.B.: „Die bedrohen, unsere‘ Frauen.", „Der Staat unterstützt die Islamisierung Deutschlands.“)

Bewusste Verbreitung uninformierter oder falscher Aussagen (z.B. Aussagen wie: „Die Asylanten müssen beim Einkaufen nicht bezahlen.“) ☞ [Falschnachrichten]

Getarnt als Humor oder Ironie (z.B. Sätze wie: „Ich will auch ein neues Handy. Muss ich im nächsten Leben halt Asylant werden.“)

1 Für eine nähere Definition siehe: Council of Europe's Committee of Ministers: Recommendation No. R (97) 20 of the Committee of Ministers to Member States on 'hate speech

2 „Hate Speech – Hass im Netz Infobroschüre“ von Lsm, ajs & Kooperation mit klicksafe.de

(https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Eltern_Allgemein/Hate_Speech_lfm_ajs_klicksafe.pdf)

- **Herabsetzende und verunglimpfende Begriffe; rassistische und sexistische Beleidigungen** (z.B. Beleidigungen wie: „Kanake.“)

- **Bedienen von Stereotypen und Vorurteilen durch die Verwendung bestimmter Begriffe und Sprachmuster** (z.B. Begriffe wie: „Ausländer raus.“, „Drohende Islamisierung.“)

- **Verallgemeinerungen** (Aussagen wie: „Alle Griechen sind faul.“)

- **Plakative Bildsprache** (beispielsweise die rassistische Darstellung von schwarzen Menschen in Baströcken oder Bilder, die Stereotype reproduzieren)

Für weitere Informationen, Hilfe oder Meldungen, wenden Sie sich an: *https://no-hate-speech.de/*

TERRORISTISCH-GENERIERTE ONLINE-INHALTE

Der Begriff „Terroristische Online Inhalte“ bezieht sich auf die Verbreitung von Aussagen im Online-Raum, die zum Ziel haben, Personen indirekt oder indirekt zur Ausübung einer terroristischen Straftat zu motivieren (für eine nähere Definition siehe EU-Verordnung zur Bekämpfung von Terrorismus).[3]

Hauptsächlich nutzen Terroristen bzw. terroristische Vereinigungen das Internet für die **Verbreitung von Propaganda**. Allgemein geschieht dies mit Hilfe von Multimedia-Kommunikation, um Propaganda etwa über ideologische Anweisungen, Begründungen, Erklärungen oder die Förderung terroristischer Aktivitäten zu liefern. Das kann in Form von virtuellen Nachrichten, Präsentationen, Magazinen, Abhandlungen, Audio- und Videodateien als auch von terroristischen Organisationen oder Sympathisanten entwickelten Videospielen erfolgen.

Internetpropaganda kann z.B. auch Inhalte wie Videomaterial von Gewalttaten oder von Terror-organisationen entwickelte Videospiele enthalten, die Terrorakte simulieren und den Benutzer dazu ermutigen, Rollenspiele zu spielen, in welchen er die Rolle eines virtuellen Terroristen einnimmt. Solche Inhalte können mithilfe einer Vielzahl von Tools verbreitet werden, z. B. über Websites, gezielte virtuelle Chatrooms und Foren, Online-Magazine, soziale Netzwerkplattformen sowie beliebte Video- und Filesharing-Websites. Insbesondere Social-Media-Plattformen wie Twitter und Facebook sowie beliebte Video- und Filesharing-Websites wie YouTube sind wichtige Bewegungsräume für radikale Gruppierungen, um ihre **Gewaltpropaganda, Hass und gefälschten Informationen** zu veröffentlichen.

☞ [Sicherheit und soziale Medien]

Ein häufig erwähntes Thema der terroristischen Propaganda ist die Förderung von Gewalt. Zudem erhöht die breite Reichweite von Inhalten, die über das Internet verbreitet werden können, das potenzielle Publikum erheblich. [4] Des Weiteren zielen extremistische Gruppen für Propagandazwecke überproportional oft auf **Jugendliche bzw. junge Heranwachsende** ab, da diese „anfälliger“ und empfänglicher für extremistische Ideen und gefährliche Verhaltensweisen sind.[5,6]

☞ [Kinderschutz im Internet]

Die grundlegende Bedrohung durch terroristische Propaganda hängt mit der Zielabsicht der Verbreitung und der Art und Weise ihrer Verwendung zusammen. Des Weiteren werden folgende Strategien oft eingesetzt:

[3] (Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism).

[4] United Nations Office on Drugs and Crime (2012). The use of the Internet for terrorist purposes. In collaboration with the United Nations Counter-Terrorism Implementation Task Force. Retrieved from: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

[5] Hassan, G., Brouillette-Alarie, S., Alava, S., Frau-Meigs, D., Lavoie, L., Fetiu, A., ... & Sieckelinck, S. (2018). Exposure to extremist online content could lead to violent radicalization: A systematic review of empirical evidence. International Journal of Developmental Science, 12, 71-88.

[6] Harpviken, A. N. (2019). Psychological vulnerabilities and extremism among wyestern outh: A literature review. Adolescent Research Review. doi:10.1007/s40894-019-00108-y

- Die Befürwortung von oder der Aufruf zu Gewalttaten (z.B. An den Galgen mit ihnen!“, „Die sollte man alle verbrennen/abknallen/vergasen.“)

- Die Glorifizierung von Terroranschlägen mit der Intention, andere Akteure zur Nachahmung zu bewegen (z. B. „9/11 war eine großartige Rache an den Ungläubigen. Es sollten weitere Strafaktionen folgen.“)

- Demonstration der wirksamen Durchführung von Terroranschlägen für diejenigen, die möglicherweise zur Nachahmung bereit sind [5] [6]

Wenn Sie eine Seite entdecken, die falsche Berichte oder diesbezüglich besorgniserregende Inhalte enthält, können Sie dies den entsprechenden Betreibern melden (z.B. Facebook, siehe https://de-de.facebook.com/help/212722115425932)

oder an folgende Meldestellen weitergeben:
https://www.internet-beschwerdestelle.de/de/index.html
https://www.jugendschutz.net/hotline/

*Wenn Sie **Verwandte, Freunde oder eine andere Person** haben, um welche Sie sich Sorgen machen, sehen Sie hier: **[Beratungshotline]***

Wenn Sie über irgendetwas reden möchten - ob große oder kleine Sorgen, können Sie sich an folgende Beratungsstelle wenden:
https://www.nummergegenkummer.de/kinder-und-jugendtelefon.html

ONLINE-FINANZIERUNG VON TERRORISMUS

Online-Finanzierung von Terrorismus umfasst die Bereitstellung oder Einwerbung von finanziellen Mitteln im Internet mit dem Ziel, dass diese in Gänze oder teilweise zur Durchführung von terroristischen Straftaten genutzt werden.[7]

Die Art und Weise, wie Terroristen das Internet nutzen, um Geld zu sammeln oder andere Ressourcen zu erlangen, kann in vier allgemeine Kategorien eingeteilt werden:[8]

Direktwerbung,
E-Commerce,
Nutzung von Online-Zahlungsinstrumenten und
über gemeinnützige Organisationen

Direktwerbung bezieht sich auf die Verwendung von Websites, Chat-Gruppen, Massenmailings und gezielter Kommunikation, um Spenden von Unterstützern anzufordern.

E-Commerce: Websites können auch als Online-Shops verwendet werden und bieten Unterstützern Bücher, Audio- und Videoaufzeichnungen und andere Artikel an.

Online-Zahlungsmöglichkeiten die über spezielle Websites oder Kommunikationsplattformen angeboten werden, erleichtern den elektronischen Geldtransfer zwischen Parteien. Überweisungen erfolgen häufig per elektronischer Überweisung, Kreditkarte oder alternativen Zahlungsmöglichkeiten, die über Dienste wie PayPal oder Skype verfügbar sind. Online-Zahlungsmöglichkeiten können auch durch terroristische Organisationen mittels betrügerischer Mittel wie Identitätsdiebstahl, Kreditkartendiebstahl, Überweisungsbetrug, Aktienbetrug, Verbrechen des geistigen Eigentums und Auktionsbetrug ausgenutzt werden.[8]

Allgemeine Hinweise zur Cybersicherheit und Tipps für ein sicheres Interneterlebnis finden Sie unter
☞ **[Selbstschutz im Internet]**

Finanzielle Unterstützung für illegale Zwecke kann auch durch scheinbar legitime Organisationen wie **Wohltätigkeitsorganisationen** erschlichen werden. Es ist bekannt, dass einige terroristische Organisationen gemeinnützige Unternehmen gründen, um Online-Spenden zu erbitten. Diese Organisationen können behaupten, humanitäre Ziele zu unterstützen, während Spenden tatsächlich zur Finanzierung von Terrorakten verwendet werden. Genauer gesagt weisen mehrere bekannte Fälle darauf hin, dass die Endverwendung von Geldern, die über soziale Netzwerke gesammelt wurden, den Geldgebern oft nicht bekannt war.[8]

Insbesondere auf Social-Media-Plattformen können von Benutzern bereitgestellte Informationen missbraucht und zum Nutzen krimineller Aktivitäten verwendet werden.
☞ **[Sicherheit und soziale Medien]**

[7] Eine vergleichbare Definition findet sich in der EU-Verordnung zur Bekämpfung von Terrorismus (Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating

[8] terrorism United Nations Office on Drugs and Crime (2012). The use of the Internet for terrorist purposes. In collaboration with the United Nations Counter-Terrorism Implementation Task Force. Retrieved from: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

ONLINE-REKRUTIERUNG UND AUSBILDUNG VON TERRORISTEN

Online-Rekrutierung bezeichnet das Anwerben einer anderen Person im Internet, um terroristische Straftaten zu begehen bzw. bei deren Durchführung mitzuwirken. Online-Training bezieht sich auf die Aus- und Fortbildung anderer Personen oder die Teilnahme an solchen Aus- und Fortbildungsmaßnahmen im Internet, z. B. mit nachfolgenden Inhalten: Herstellung bzw. Nutzung von Sprengsätzen, Schusswaffen oder anderer Waffen, giftiger oder gefährlicher Substanzen oder anderer Methoden und Techniken mit dem Ziel, eine terroristische Straftat zu begehen bzw. bei deren Durchführung mitzuwirken.[9]

Die Reichweite des Internets bietet terroristischen Organisationen und Sympathisanten einen globalen Pool potenzieller Rekruten. Diese Internetplattformen bieten z.B. auch detaillierte Anweisungen, häufig in leicht zugänglichem Multimedia-Format und in mehreren Sprachen, zu folgenden Themen: **wie man Sprengstoffe, Schusswaffen oder andere Waffen oder gefährliche Materialien baut; und wie man Terroranschläge plant und ausführt**. Solche Plattformen fungieren als virtuelles Trainingslager. Sie werden auch verwendet, um unter anderem spezifische Methoden, Techniken oder operatives Wissen zu teilen, um einen Terrorakt zu begehen.[8] Cyberforen mit beschränktem Zugang bieten Rekruten die Möglichkeit, sich über terroristische Organisationen zu informieren und diese zu unterstützen und direkte Maßnahmen zur Förderung terroristischer Ziele zu ergreifen.[8]

Terroristische Propaganda ist oft darauf zugeschnitten, schutzbedürftige und marginalisierte Gruppen in der Gesellschaft anzusprechen. Der Rekrutierungs- und Radikalisierungsprozess nutzt üblicherweise die Gefühle eines Individuums in Hinsicht auf Ausgrenzung, Ungerechtigkeit oder Demütigung aus. Propaganda kann so angepasst werden, dass demografische Faktoren wie Alter oder Geschlecht sowie soziale oder wirtschaftliche Umstände gezielt berücksichtigt werden.

Das Internet kann ein besonders wirksames Medium für die Rekrutierung von Minderjährigen und jungen Heranwachsenden sein, die einen hohen Anteil an Internet-Nutzern ausmachen. Propaganda, die über das Internet verbreitet wird, um Minderjährige und junge Heranwachsende zu rekrutieren, kann in Form von populären Musikvideos, Cartoons oder Computerspielen erfolgen. Zu den Taktiken, die auf Websites von Terrororganisationen oder ihren Mitgliedsorganisationen gezielt angewendet werden, gehören z. B. Botschaften in Zeichentrickfilme und Kindergeschichten unterzubringen, die Terrorakte und Selbstmordattentate fördern und verherrlichen.[8]

☞ [Kinderschutz im Internet]

[9] Eine vergleichbare Definition findet sich in der EU-Verordnung zur Bekämpfung von Terrorismus (Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism

BERATUNGSHOTLINE

Seit dem 01. Januar 2012 ist im Bundesamt für Migration und Flüchtlinge die „Beratungsstelle Radikalisierung“ eingerichtet, an die sich alle Personen wenden können, die sich wegen der Radikalisierung eines Angehörigen oder Bekannten sorgen und zu diesem Themenbereich Fragen haben.

Die Beratungsstelle ist Montag bis Freitag von 09.00 bis 15.00 Uhr erreichbar unter **Telefon: 0911/943 43 43.**

Für mehr Informationen:
https://www.beratungsstelle-radikalisierung.de/DE/Startseite/startseite_node.html
https://emel-onlineberatung.org/startseite.html

Falls Ihnen Hinweise zu den bisher beschriebenen Aktivitäten bekannt sind, können Sie sich bei der örtlichen Polizei melden, über die **110**.

Oder Sie können sich in Verbringung setzen mit dem Bundesamt für Verfassungsschutz über:
https://www.verfassungsschutz.de/de/hinweistelefon-gegen-extremismus-und-terrorismus

SICHERHEIT UND SOZIALE MEDIEN

Insbesondere im Zeitalter beliebter sozialer Netzwerkmedien wie *Facebook, Instagram, Twitter, YouTube, Flickr und Blogging-Plattformen* veröffentlichen Einzelpersonen freiwillig oder versehentlich eine beispiellose Menge sensibler Informationen im Internet. Während die Absicht derjenigen, die die Informationen verbreiten, darin bestehen kann, ihrem Publikum Nachrichten oder andere Aktualisierungen zu Informations- oder sozialen Zwecken zur Verfügung zu stellen, können einige dieser Informationen missbraucht und zum Nutzen krimineller Aktivitäten verwendet werden.

Grundlegende Überlegungen:

Vor der Anmeldung in einem sozialen Netzwerk sollten Sie sich fragen, welche Erwartungen Sie mit einer Teilnahme verbinden.

- Sollte Ihr Profil für den privaten Gebrauch sein, sodass es wichtig ist, dass nur Ihre Freunde Sie finden können?

- Was möchten Sie mit Ihrem Profil erreichen? Sollte es sich für Sie um ein rein privates Profil handeln oder ist es (auch) für den geschäftlichen Gebrauch bestimmt – sodass es möglich sein sollte, dass Sie auch von Dritten kontaktiert werden können?

Für Ihren Datenschutz:

- **Für jedes Netzwerk sollte eine separate E-Mail-Adresse** verwendet werden – dies ist anfangs ein größerer Aufwand, schützt aber Ihre Privatsphäre weitaus mehr

- Bedenken Sie – was soll für die Öffentlichkeit einsehbar sein? Möchten Sie unter einem Pseudonym oder mit Ihrem tatsächlichen Namen (Klarnamen) auftreten?

- Sollten Ihre Profilinhalte für alle (öffentlich) zugänglich oder nur für Personen zugänglich sein, die Sie kennen?

- Um **Fremden den Zugriff auf Ihre Daten** (wie Fotos und Profilinhalte) zu **erschweren**, widerstehen Sie der Versuchung, jede Freundschaftsanfrage anzunehmen oder selbst wahllos zu verschicken – Sie wissen nie, wer tatsächlich dahintersteckt.

Privatsphäre-Einstellungen bei Facebook, Twitter und Co.:

- Die Einstellungsoption *„Profil für Suchmaschinen unsichtbar machen“* bieten viele Social-Media-Plattformen an. Sie kann sehr hilfreich sein, wenn sie nicht auf den ersten Google-Treffer gefunden werden möchten. Wenden Sie sich dafür, falls nicht ersichtlich, ggf. an das Hilfecenter des Netzes.

- Überprüfen Sie die *„Privatsphäre-Einstellungen“*: Aktivieren Sie z.B. die "Markierungen Überprüfen"-Funktion bei Facebook - diese bewirkt, dass alle Beiträge und Markierungen, in denen Sie erscheinen, zuerst von Ihnen bestätigt werden müssen, bevor sie für die Öffentlichkeit einsehbar werden.

- *Sichtbarkeit von Kontaktdaten:* Sofern Sie Ihr Konto nicht geschäftlich nutzen, sollten Sie Ihre Kontaktdaten möglichst für niemanden sichtbar machen.

- Sichtbarkeit Ihrer Inhalte: Ob Profilbilder, Beiträge oder Fotoalben – in den meisten Netzwerken können Sie genau bestimmen, wer welche Inhalte sehen darf. Hier gilt: *Je weniger öffentlich ersichtlich ist, desto besser.*

Warum kann die Angabe personenbezogener Daten problematisch sein?

Viele Menschen veröffentlichen ihre personenbezogenen Daten noch zu leichtfertig, ohne sich dabei bewusst zu sein, wie viel diese für einzelne Unternehmen oder Behörden wert sein können (etwa um ihre Interessen und Aktivitäten besser vorhersagen und dementsprechend personalisierte Werbung oder Angebote schalten und präsentieren zu können).

Beispiele für **personenbezogenen Daten:** Standort-, Aufenthaltsdaten, Kontaktdaten, Angaben zum Konsumverhalten

Mit solchen Daten können maßgeschneiderte Inhalte für Werbezwecke erstellt und angezeigt werden. Damit können Unternehmen Gewinne in Millionenhöhe erwirtschaften - **personenbezogene Daten sind entsprechend „bares Geld“ wert.**

Andererseits können diese sensiblen Informationen, wenn sie in die falschen Hände geraten, missbräuchlich verwendet werden und großen Schaden anrichten – hier können sich kriminelle Personen z. B. Bankdaten aneignen, um auf fremde Konten zuzugreifen oder etwa mit Personal- oder Ausweisnummern falsche Dokumente zu erstellen und zu verkaufen, um nur einige Beispiele zu nennen.

☞ **[Selbstschutz im Internet]**

Achten Sie also immer darauf, nicht zu viele persönliche Informationen preiszugeben, insbesondere wenn dies nicht unbedingt erforderlich ist!

Zusätzlich finden Sie hier ein kurzes YouTube-Tutorial darüber, warum Datenschutz und Privatsphäre in diesen Zeiten so wichtig sind:
https://www.youtube.com/watch?v=VF5A2JhiJug

Wie kann ich meine Datensicherheit gewährleisten?

Sichere https Verschlüsselung:
Sie sollten stets darauf achten, beim Surfen eine **sichere Datenverbindung zu wählen** (**https//: - das „s“ steht hierbei für „sicher**“). Hier werden die Daten verschlüsselt, sodass Ihre Online-Aktivitäten und die von Ihnen eingegebenen Informationen nicht durch Dritte eingesehen oder abgefangen werden können.

Mehr Informationen finden Sie hier: *https://www.youtube.com/watch?v=tW1-CmggG9s*

Inkognito surfen:
Der **Tor-Browser** ist weiterhin das Mittel der Wahl für anonymes Surfen. Hier genügt eine **einfache Installation des Programms.** Damit sind Sie etwas langsamer als sonst im Internet unterwegs. Sie verzichten für den Schutz und die Anonymität Ihrer Daten auf ein besonders schnelles Surferlebnis.
Aber auch mithilfe von **VPN-Clients** können Sie Ihre IP-Adresse verschleiern. Ganz anonym sind Sie damit jedoch nicht ç nichtsdestotrotz können Sie dadurch Ihrer Datenspur im Internet etwas entgegentreten.

Auch hier finden Sie ein kurzes Video-Tutorial zum anonymen Surfen:
https://www.youtube.com/watch?v=OpSUmuG3Bp8

Es gibt sehr einfache Möglichkeiten, mehr Sicherheit zu erlangen, die ohne großen Aufwand umgesetzt werden können. Cookies sind hierbei auch ein großes Thema.

Und was sind eigentlich Cookies?

Auf fast jeder Website werden Sie gefragt, ob Sie der Verwendung von Cookies zustimmen oder nicht. Dies sind Textdateien, die von Ihrem Browser an den entsprechenden Server auf der Seite gesendet werden. Auf diese Weise können die Seiten Informationen von Ihren vorherigen Besuchen abrufen und "speichern". Damit kann der Inhalt auf den Benutzer und seine typischen Surfgewohnheiten zugeschnitten werden. **Wenn Sie den Cookies zustimmen, werden Ihre persönlichen Daten gespeichert und beispielsweise von Online-Shops ausgewertet**. Dadurch kann vom Benutzer ein ziemlich genaues Bewegungsprofil erstellt werden.
Das Akzeptieren von Cookies kann jedoch auf Seiten hilfreich sein, die regelmäßig verwendet werden: Um zu vermeiden, dass Sie sich erneut anmelden oder wiederholt Formulare ausfüllen müssen.

Man unterscheidet zwei Arten von Cookies:

Session-Cookies (die eher von Online-Diensten verwendet werden, welche mit sensiblen Daten umgehen), die sich nach Beendigung des Browsers automatisch löschen.
Dauerhafte Cookies, die Monate bis hin zu Jahren im Computer vorhanden bleiben, wenn sie nicht durch den Nutzer gelöscht werden. Daher sollten **Sie immer darauf achten, die Cookies am Ende einer Browser-Sitzung zu löschen.**

Eine kurze Übersicht zum Thema “Cookies“ finden Sie in diesem YouTube-Aufklärungsvideo: *https://www.youtube.com/watch?v=R3RQ8ALa0g0*

KINDERSCHUTZ IM INTERNET: HINWEISE FÜR ELTERN

Mittlerweile bietet das Internet für viele Kinder und junge Menschen einen neuen Begegnungsraum, der vor allem für Eltern nicht immer leicht zu überblicken ist. Wahrscheinlich entsteht bei einigen von Ihnen die Sorge, wie Sie ihr Kind beispielsweise vor Angriffen durch radikale Gruppen oder ungeeignete Webinhalte schützen können. Hier finden Sie einige Informationen, wie Sie z. B. im Internet rechtsextreme Inhalte erkennen können und wie Sie Ihr Kind dafür sensibilisieren, kritisch mit für das Auge anfänglich unauffälligen, aber radikal geprägten Seiten umzugehen.

Es muss zunächst erst einmal grundsätzlich umgedacht werden, wenn vermutet wird, dass z.B. rechtsextreme Gruppierungen nur „typisch rechte" Themen behandeln. Es ist in der Regel oft anders herum: sie suchen sich (gesellschaftliche) Inhalte und Themenbereiche, die (oft auch junge Menschen) beschäftigen und die ggf. aktuell gerade intensiv diskutiert werden. Oft werden hier zunächst Meinungen präsentiert, die emotional sind und in der Gesellschaft auf breite Zustimmung treffen. Radikale Gruppen versuchen oft, extreme Meinungen versteckt zu verbreiten und sie sozial akzeptabel und normal erscheinen zu lassen. Es ist nicht ungewöhnlich, dass auf diese Weise auch Fehlinformationen (Fake News) verbreitet oder historische Ereignisse verzerrt werden. Dies sind Strategien, um Unmut gegenüber Minderheiten zu erzeugen. Darüber hinaus sind Seiten extremistischer Gruppen in der Regel sehr professionell gestaltet, um einen ernsthaften Eindruck zu erwecken.[11,12]

Daher ist und bleibt es unumgänglich, bei Beiträgen oder Webseiten genau – nach Möglichkeit gemeinsam mit Ihrem Kind – nachzuprüfen,welche Quelle den Informationen und der Seite zugrunde liegt.

Wie schütze ich mich und mein Kind?

Wesentlich ist, dass Sie Ihr Kind dabei unterstützten, Folgendes auseinanderhalten zu können: Welche Informationen sind echt? Welche nicht?

Zum Grundbaustein gehört

- früh schon mit Ihrem Kind über das Geschehen in der Welt zu sprechen und
- Ihr Kind zu ermutigen, eine differenzierte Betrachtungsweise zu entwickeln.

Tragendes Element ist hier, Informationen und die Quelle(n) dieser Information zu hinterfragen sowie Nachrichten und Meinungen einordnen zu können. Dabei sollte auch klar benannt werden, dass es Menschen gibt, die gezielt Falschinformationen verbreiten (etwa mit der Absicht, Meinungen zu beeinflussen oder Geld zu verdienen).

[11] Broschüre „Rechtsextremismus im Internet – Tipps für Eltern" von klicksafe.de & jugendschutz.net: https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Eltern_Allgemein/Rechtsextremismus_Internet_Eltern-Tipps_klicksafe.pdf

[12] SCHAU HIN!: https://www.schau-hin.info/sicherheit-risiken/fake-news-umgang-mit-falschmeldungen

Es bleibt unabdingbar, misstrauisch zu bleiben – auch wenn Informationen bereits (z.B. über soziale Medien) vielfach geteilt wurden oder eine Seite auf den ersten Blick seriös erscheint – beides ist keine Garantie dafür, dass die präsentierten Informationen wahr sein müssen.
Sie als Eltern können dafür sorgen, dass Ihre Kinder altersgemäße Erfahrungen im Internet sammeln. Begleiten Sie Ihre Kinder bei den ersten Schritten im Netz. Für weitere Information lesen Sie „Leitfaden: Internetkompetenz für Eltern“:
https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Eltern_Elternkurs/Internetkompetenz_f%C3%BCr_Eltern-Elternleitfaden_2014.pdf

Generelles Informationsmaterial zur Mediennutzung finden Sie auf *www.klicksafe.de*
Sie können Bedenken melden unter: *https://www.jugendschutz.net/hotline/*

Weitere Informationen finden Sie in folgendem Video:
https://www.youtube.com/watch?v=CKYFdNszQCs

FALSCHNACHRICHTEN

Jeder Onlinenutzer kann heutzutage über eigene Blogs, Kommentare oder in sozialen Medien ganz einfach eigene Beiträge verfassen und seine Meinung mitteilen. Die neu gewonnene Vielfalt stellt Onlinenutzer gleichzeitig stärker als bisher vor die Herausforderung, selbst entscheiden zu müssen, welche publizierte Information richtig oder falsch ist.

Vom Kettenbrief per Messenger oder E-Mail, bis zum Social-Media-Post mit verlinkten Falschinhalten: **alltäglich werden viele Onliner und Onlinerinnen mit zweifelhaften Inhalten im Netz konfrontiert.**

Welche Seiten helfen, über Fake News und Falschmeldungen aufzuklären?

- Überprüfen von Fake News & Falschmeldungen: *https://www.mimikama.at/*
- Dokumentation von Falschmeldungen über Geflüchtete: *https://hoaxmap.org/*
- Faktencheck der Tagesschau: *https://www.tagesschau.de/faktenfinder/*
- Altersgerechte Erklärung für Fragen im Netz durch ARD & ZDF: *https://www.br.de/sogehtmedien/index.html*

Umgang mit Fake News/menschenverachtenden Inhalten:
Sollten Sie auf eine Seite stoßen, auf welcher Falschmeldungen oder auch Inhalte verbreitet werden, die menschenverachtend sind, können Sie…

- **Die Inhalte** bei dem entsprechenden **Betreiber melden** (z.B. Facebook: *https://de-de.facebook.com/help/212722115425932*)
- oder (z.B. bei Verdacht auf eine Straftat) auch an **externe Beschwerdestellen** oder die Polizei senden (mit einem entsprechenden Screenshot)
- Sie sollten die betreffenden Falschmeldungen oder menschenverachtende Inhalte möglichst nicht weiterleiten/verbreiten

Beschwerdestellen sind z.B.

- *internet-beschwerdestelle.de*
- *jugendschutz.net*
- *hass-im-netz.info*

Online-Quellen überprüfen[13]

Wie stellen Sie fest, ob eine Quelle glaubwürdig ist? Mithilfe dieser Richtlinien können Sie die Zuverlässigkeit und Wissenschaftlichkeit von Informationen bewerten, die Sie sowohl online als auch in gedruckter Form finden:

- **Urheberschaft**

Wenn der Autor nicht identifizierbar ist, seien Sie vorsichtig. Wenn ein Artikel oder eine Website anonym verfasst wird, hat diese wenig Glaubwürdigkeit. Es sollte offensichtlich sein, wer den Inhalt erstellt hat. Was sind die Referenzen des Autors? Hat er / sie Fachwissen auf diesem Gebiet? Werden biografische Informationen bereitgestellt?

- **Herausgeber**

Überprüfen Sie den Herausgeber des Dokuments, z. B. ob es von einem etablierten Verlag, einer Regierungsbehörde, einer gemeinnützigen Organisation oder einer kommerziellen Website erstellt wurde. Berücksichtigen Sie den Ruf und die Vertrauenswürdigkeit des Herausgebers.

- **Genauigkeit und Objektivität**

Können die auf einer Website präsentierten Fakten an anderer Stelle verifiziert werden? Hüten Sie sich vor Informationen, die nicht bestätigt werden können oder die eine voreingenommene Sichtweise darstellen. Überprüfen Sie immer mehrere Quellen, um die Glaubwürdigkeit festzustellen.

- **Aktualität**

Beachten Sie, wann die Webseite erstellt wurde und ob sie kürzlich aktualisiert wurde. Sind die Informationen aktuell? Veraltete Informationen und fehlerhafte Links weisen darauf hin, dass die Seite nicht gepflegt wird.

- **Fußnoten und Bibliographien**

Verweise und Links zu anderen Quellen können die Glaubwürdigkeit und Wissenschaftlichkeit eines Dokuments erhöhen.

- **Förderung**

Einige Websites sind offiziell von einer übergeordneten Organisation genehmigt, mit der sie verbunden sind. Andere können sich auf einer übergeordneten Website befinden, jedoch nicht offiziell von dieser Organisation gefördert werden. Eine persönliche Homepage auf dem Server einer Universität verleiht nicht automatisch Glaubwürdigkeit.

[13] https://library.columbia.edu/libraries/undergraduate/evaluating_web.html

SELBSTSCHUTZ IM INTERNET

Möglicherweise ist es für Sie nicht immer einfach zu erkennen, welche Gefahren für Sie im Netz lauern und wie Sie ihnen begegnen können. Ein paar wichtige Tipps und Tricks haben wir für Sie parat, damit Sie sich sicherer und mit geschärftem Blick im Netz bewegen können.

Das Wichtigste zu sicheren Passwörtern in Kürze (Quelle: datenschutz.org)

Ein sicheres Passwort sollte:

- **mindestens acht Zeichen** lang sein (besser mehr)
- **Klein- und Großbuchstaben sowie eine Kombination aus Buchstaben, Zahlen und Sonderzeichen** enthalten

! Vermeiden Sie !

- Eine reine Wortkombination (z.B. rotes Haus)
- logische Zahlen- oder Buchstabenreihen (z.B. Geburtsdaten)

Kreieren Sie stattdessen solche Passwörter:

Versuchen Sie, Wort-, Zahlen und Sonderzeichen miteinander zu mischen, sodass das Passwort möglichst vielen Anforderungen entspricht - zum Beispiel „GroßesHau$_123“

Zeichenreihen, welche beispielsweise einen persönlichen **Merksatz** widerspiegeln (z.B. dbddhkP = „doof bleibt doof da helfen keine Pillen“)

Passwörter, die auf gänzlich **unreflektierten Zeichenreihen** beruhen (z.B. hdg6tzfrsgj5n6jlGHG)

Verwenden Sie möglichst

für jede Registrierung ein neues, sicheres Passwort.

Kein Passwort ist zu 100% sicher! Falls eins Ihrer Passwörter gehackt wird, behalten die verbleibenden Zugänge ihren Schutz bei.

Hier finden Sie das Erstellen und die Wichtigkeit von Passwörtern in einem kurzen YouTube-Video einfach erklärt:
https://www.youtube.com/watch?v=jtFc6B5ImIM

Außer einem sicheren Passwort sind die nachfolgenden Sicherheitsmaßnahmen ebenso wichtig:

Virenschutz
Firewall
sorgsamer Umgang mit den Login-Daten

Konsortium

Hochschule für den öffentlichen Dienst in Bayern
Fachbereich Polizei

CENTRIC
Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research

POLICE SERVICE NORTHERN IRELAND

POLICYJNA AKADEMIA

AGENFOR INTERNATIONAL

iti CENTRE FOR RESEARCH & TECHNOLOGY - HELLAS
Information Technologies Institute

Ministero della Giustizia

Freie Universität Berlin

europeaninstitute

Politsei- ja Piirivalveamet

UNIVERSIDAD DE GRANADA

RSM Erasmus

KEMEA

Politie
Voorkempen

Projekt PROPHETS

Koordinator

Dr. Holger Nitsch

Hochschule für den öffentlichen Dienst in Bayern — Fachbereich Polizei

Fürstenfelder Str. 29
82256 Fürstenfeldbruck
Germany

Prophets Project

www.prophets-h2020.eu

@H2020Prophets

Project-Prophets