Darknet - Beim Surfen im Internet nicht in dunkle Kanäle geraten

Thomas Heinz, Oktober 2025

Alles fing mit der Erfindung des Computers an …

1941 Konrad Zuse stellt in seiner Werkstatt in der Methfesselstraße 7 in Berlin-Kreuzberg mit der Z3 einen der ersten funktionsfähigen Digitalrechner weltweit vor.

1943 „Ich denke, dass es einen Weltmarkt für vielleicht fünf Computer gibt."
Thomas Watson, Vorsitzender von IBM

1949 Edmund C. Berkeley stellt mit „Simon" den ersten digitalen, programmierbaren Computer für den Heimgebrauch vor.

1951 Remington Rand baut ihren ersten kommerziellen Röhrenrechner, den UNIVersal Automatic Computer I (UNIVAC I)

1956 der Begriff „Computer" taucht erstmals in der DDR-Presse auf,

1959 Siemens beginnt mit der Auslieferung des Siemens 2002, ihres ersten in Serie gefertigten Computers.

1960 DECs (Digital Equipment Corporation) erster Minicomputer, die PDP-1 (Programmierbarer Datenprozessor) erscheint.

1964 DEC baut den Minicomputer PDP-8 für unter 20.000 Dollar.

1973 mit Xerox Alto erscheint der erste Computer mit Maus, graphischer Benutzeroberfläche (GUI) und eingebauter Ethernet-Karte.

1975 IBM stellt mit der IBM 5100 den ersten tragbaren Computer vor.

1976 Zilog entwickelt den Z80-Prozessor und Apple Computer stellt den Apple I vor, den weltweit ersten Personal Computer, gefolgt 1977 vom Commodore PET und dem Tandy TRS-80.

1977 „Es gibt keinen Grund dafür, dass jemand einen Computer zu Hause haben will." *Ken Olsen, Gründer des Computer-Herstellers DEC*

1990 „Das Internet ist eine Spielerei für Computer-Freaks, wir sehen darin keine Zukunft. *Ron Sommer, ehemaliger Telekom-Chef*

1993 Das Internet ist nur ein Hype. *Bill Gates, Microsoft Gründer*

Das Gute am Internet: Du kommst mit Leuten zusammen und musst doch keinen ausgeben. *Klaus Klages, Abreißkalender-Verleger*

1978 Intel stellt den 8086 vor, ein 16-Bit-Mikroprozessor; er ist der Urvater der noch heute gebräuchlichen x86-Prozessor-Familie

Das Arpanet

Das ARPANET war ein Computernetzwerk das ursprünglich im Auftrag der US Air Force ab 1968 entwickelt wurde.

Es sollte ein dezentrales Netzwerk geschaffen werden, das unterschiedliche Universitäten, die für das Verteidigungs-ministerium forschten, miteinander über Telefonleitungen verband.

Anfangs waren lediglich vier Forschungseinrichtungen[1] in Kalifornien und Utah vernetzt.

Der erste Adressat und Empfänger einer Nachricht im Arpanet war am 29. Oktober 1969 das SRI. Im November 1977 führte das SRI den ersten Datentransfer über mehrere völlig unterschiedliche Netze hinweg durch, von einem Lieferwagen mit Funksender bei San Francisco aus über das University College London zur University of Southern California.

Das ARPANET wurde offiziell am 28. Februar 1990 stillgelegt.

Der Mythos, dass das ARPANET entwickelt worden sei, um nuklearen Angriffen zu widerstehen, ist nach wie vor eine dermaßen „gute Geschichte“, dass viele Leute nicht glauben, dass sie falsch ist.

Laut Aussagen der ARPA wurde vielmehr nach einer Methode gesucht, die damals knappen Rechenkapazitäten der einzelnen Hochschulen durch Datenaustausch besser auszunutzen.

Das Internet

In den 1970er Jahren wurden das Transmission Control Protocol (TCP) und das Internet Protocol (IP) entwickelt. Diese Protokolle ermöglichten es, verschiedene Netzwerke miteinander zu verbinden, wobei TCP dafür sorgt, dass die Daten richtig und vollständig ankommen und IP sich um die richtige Adresse kümmert.

1983 wurde TCP/IP zum Standardprotokoll für Arpanet, was Arpanet in ein offenes Netzwerk umwandelte, das mit anderen Netzwerken kommunizieren konnte.

Dies war der erste Schritt in Richtung eines globalen Internets.

Der Begriff „Internet“ begann in den frühen 1990er Jahren populär zu werden

Das World Wide Web (WWW) ist seit 1991 öffentlich zugänglich. Es ermöglichte die einfache Anzeige und Interaktion mit Informationen und führte zu einer explosionsartigen Zunahme der Internet-Nutzung.

[1] Stanford Research Institute, California; University of Utah; University of California, Los Angeles; University of California, Santa Barbara

Eines Tages im Sommer 2008 überschritt Googles Suchmaschine still-schweigend einen Meilenstein. Sie fügte die Eine-Billionste Adresse zur Liste der Webseiten hinzu, die sie kennt. So unvorstellbar groß diese Zahl auch erscheinen mag, sie stellt nur einen Bruchteil des gesamten Webs dar.

Jenseits dieser Billion Seiten liegt ein noch weiträumigeres Web von verborgenen Daten: Finanzinformationen, Einkaufskataloge, Flugpläne, medizinische Forschungen und allerlei anderes Material, das in Datenbanken gespeichert ist und für Suchmaschinen weitgehend unsichtbar bleibt.

World Wide Web (Clear Web)

Das ist der Bereich des Internets, in dem wir surfen, shoppen, mit Freunden chatten oder Urlaubsfotos hochladen.

Dieser leicht zugängliche Teil des Internets ist jedoch nur ein kleines Fragment des gesamten Netzes.

In einer Untersuchung der University of California, Berkeley aus dem Jahr 2003 wurden folgende Werte als Umfang des Internets[2] ermittelt:
Surface Web – 167 Terabyte,
Deep Web – 91.850 Terabyte.

Die gedruckten Bestände der Library of Congress in Washington, eine der größten Bibliotheken der Welt, umfassen gerade einmal 10 Terabyte.

Es wird geschätzt, dass das Internet heute mehrere Zettabytes[3] an Daten umfasst.

2023 schätzte die International Data Corporation (IDC), dass das digitale Universum (die gesamte Menge an Daten, die weltweit erzeugt und gespeichert wird) etwa 120 Zettabytes erreichen könnte, und die Zahl wird mit zunehmender Digitalisierung weiter steigen.

Deep Web

In diesem mit Abstand umfangreichsten Bereich (ca. 90% des gesamten Internets) befinden sich Firmen-Datenbanken, Streaming-Server sowie Online-Speicher (z.B. Cloud-Speicher).

Grundsätzlich steht das Deep Web allen offen, viele Inhalte sind jedoch geschützt, um bspw. Unternehmensgeheimnisse zu schützen.

Die geschätzte Datenmenge des Deep Web ist etwa 400- bis 550-mal größer als die des Surface Web. Allein 60 der größten Websites im Deep Web enthalten etwa 7.500 Terabyte an Informationen, was die Menge des Surface Web um den Faktor 40 übersteigt. Es existieren angeblich mehr als 200.000 Deep-Websites. So haben laut der Studie Webseiten aus dem Deep Web durchschnittlich 50% mehr Zugriffe pro Monat und seien öfter verlinkt als Webseiten aus dem Surface Web. Das Deep Web sei auch die am schnellsten wachsende Kategorie von neuen Informationen im Web. Trotzdem sei der im Internet suchenden Öffentlichkeit das Deep Web kaum bekannt. Mehr als die Hälfte des Deep Web sei in themenspezifischen Datenbanken angesiedelt:

Datensammlung des National Climatic Data Center (361 Terabyte)

Daten der NASA (296 Terabyte)

weitere Datensammlungen (bspw. National Oceanographic Data Center & National Geophysical Data Center, Right to know Network, Alexa)

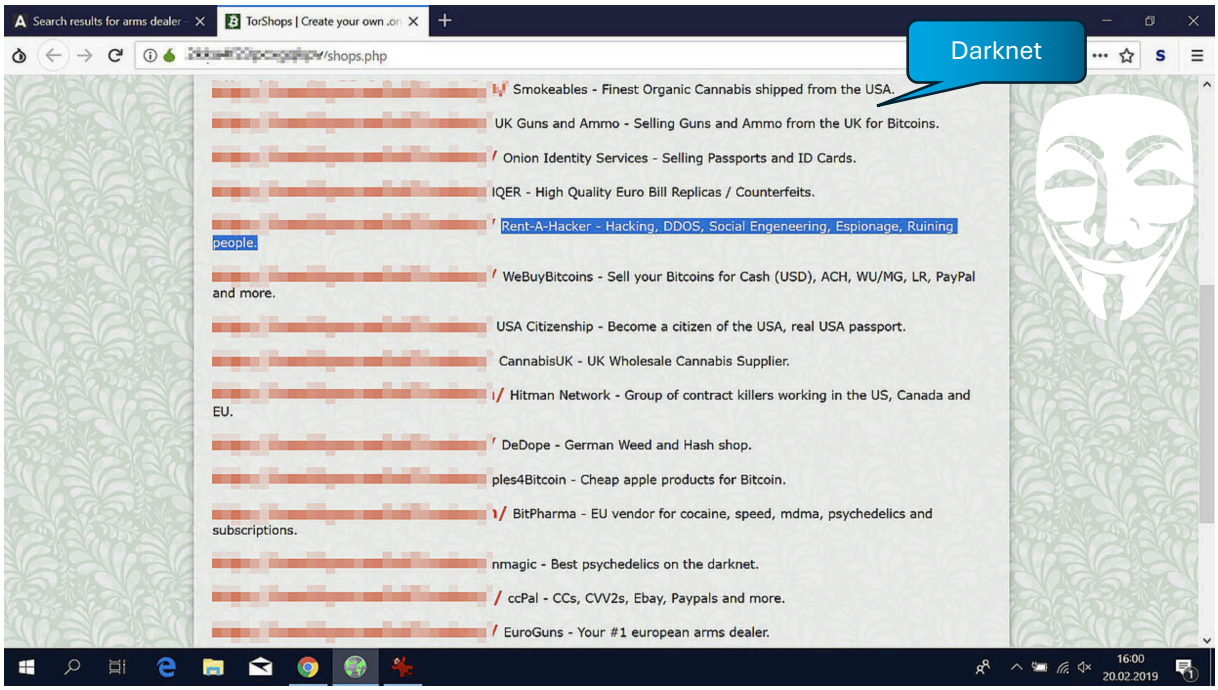
[2] https://de.wikipedia.org/wiki/Deep_Web.
Die Zahlen stimmen nicht exakt überein, da sie aus verschiedenen Quellen stammen. Sie geben aber eine Idee von den Verhältnissen.
[3] Ein Zettabyte (ZB) entspricht 1 Milliarde Terabytes (TB).

Das Deep Web besteht aus Datenbanken, Webseiten und Services, die zu Unternehmen, Behörden oder Universitäten gehören. Diese Inhalte sind meist zahlungspflichtig, vertraulich oder beispielsweise passwortgeschützt, aber harmlos, d.h. nicht illegal oder kriminell.

Dark Web

Dieser Raum des Internets ist ein vergleichsweise kleines Teilstück des Deep Webs.

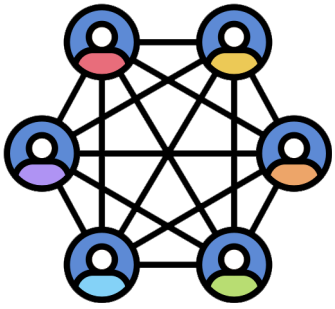
Es ist nicht auf herkömmliche Weise auffindbar, die Kommunikation wird verschlüsselt und die Urheber der Inhalte sowie seine Besucher wollen möglichst anonym bleiben.



Zugang zum Dark Web

Die gute Nachricht vorab:

Man kann sich nicht versehentlich auf eine illegale Seite im Dark Web verirren.



Zu den verbreitetsten Beispielen für Darknets gehören sogenannte Friend-to-Friend-Netzwerke, in denen geschützte Verbindungen nur mit ausgewählten Personen eingegangen werden. Das sind geschlossene Gesellschaften, zu denen man ausdrücklich eingeladen werden muss.

Der Unterschied zwischen beiden Prinzipien ist, dass sowohl die Nutzer als auch die Betreiber von Friend-to-Friend-Darknets genau einsehen können, wer außer ihnen an ihrem Netzwerk teilnimmt. In Peer-to-Peer-Netzwerken ist das üblicherweise nicht der Fall.

Das Darknet wird oft mit illegalen Aktivitäten in Verbindung gebracht.

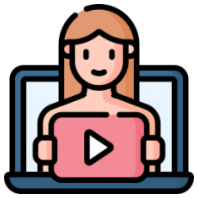
Drogen

Viren

Waffen

Auftragskiller

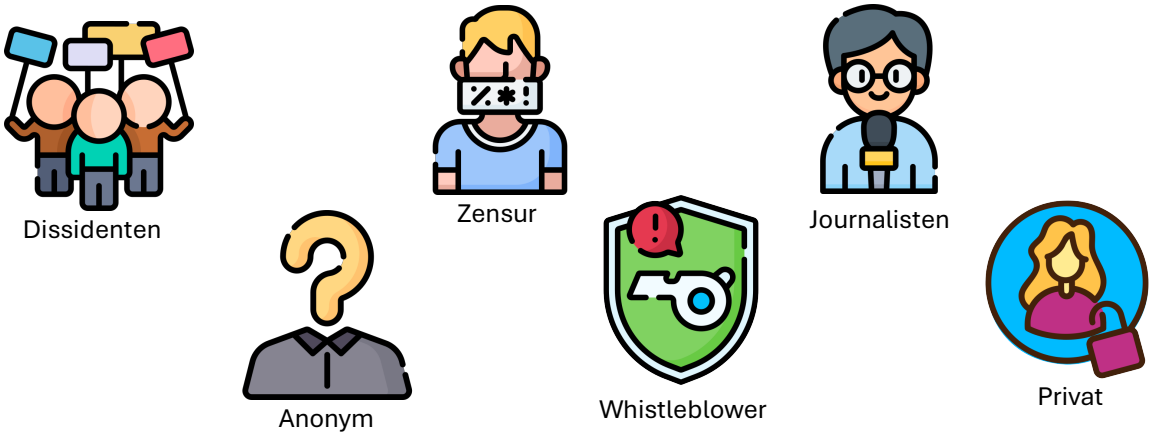
Cyberkriminalität



Pornografie

Gift

Es ist jedoch auch ein Zufluchtsort für Menschen, die Zensur und Überwachung entgehen möchten.



„Das Darknet ist das Internet, wie man es sich eigentlich wünschen würde. Ein Netz ohne Zensur und Überwachung, mit all seinen Vor- und Nach-teilen“. *(Linus Neumann, Sprecher des CCC)*

Anonymität und Privatsphäre: Für Menschen, die in Ländern leben, in denen Zensur oder Überwachung herrscht, bietet das Darknet einen Raum für freie Meinungs-äußerung und Zugang zu Informationen. Journalisten, Aktivisten oder Whistleblower nutzen es oft, um sicher zu kommunizieren und Informationen zu teilen, ohne ihre Identität preiszugeben oder Gefahr zu laufen, verfolgt zu werden.

Die Identität und Aktivitäten können Dritte nur sehr schwer nachverfolgen. Zum Beispiel können sich Journalisten und politisch Verfolgte unter diktatorischen Regimes aus diesem Grund dort bewegen und äußern, ohne Repressalien fürchten zu müssen.

Facebook hat z.B. einen Zugang im Dark Web.

Darknet - Die wichtigsten Fakten

Darknet-Netzwerke bestehen aus untereinander verlinkten Seiten, die nicht öffentlich einsehbar sind.

Darknet-Netzwerke sind aufwendig verschlüsselt, damit sich Außenstehende keinen Zugang verschaffen können.

Die Funktionsweise des Darknets macht es einfach, Vorgänge unter Ausschluss der Öffentlichkeit zu koordinieren. Viele Kriminelle verwenden daher das Darknet für illegale Aktivitäten.

Für den Zugang wird spezielle Software wie der TOR-Browser (The Onion Router) benötigt, der eine anonymisierte Verbindung herstellt.

Ist das Darknet illegal?

Besucher des Darknets müssen grundsätzlich mit strafrechtlichen Konsequenzen rechnen, sobald sie mit Anbietern illegaler Angebote in Kontakt treten. Wer sich nur aus Neugier kurz dort aufhält, hat nichts zu befürchten.

Wenn die Behörden bereits Ermittlungen gegen einen Händler illegaler Waren aufgenommen haben, können auch Nutzer zur Verantwortung gezogen werden, die sein Angebot nur aufgerufen haben.

Kinderpornografie: Bereits das Ansehen ist strafbar und kann eine Freiheitsstrafe von bis zu zehn Jahren nach sich ziehen. Daher können auch Darknet-Nutzer, die solche Seiten nur kurz besuchen, in Schwierigkeiten geraten.

Strafrechtliche Konsequenzen drohen also nicht durch die Nutzung des Darknets selbst. Gefährlich sind vielmehr die unseriösen Angebote im Darknet.

Wer ganz auf der sicheren Seite sein will, sollte auf keinen Fall auf einen Link klicken, wenn er auf solche Angebote stößt.

Vorsicht ist besser als Nachsicht.

Beispiel 1

Handel mit Passwörtern[4].


SPIEGEL Netzwelt

Gefährliche Cybercrime-Foren

S+ Passwörter Dutzender deutscher Politiker stehen im Darknet

Die Kennwörter von mehreren Dutzend Landtagsabgeordneten sind in kriminellen Foren gelandet, wie Recherchen des SPIEGEL zeigen. Hacker machen mit den privaten Daten ein gutes Geschäft.

Von Max Hoppenstedt und Roman Höfner
10.04.2025, 10.02 Uhr

[4] https://www.spiegel.de/netzwelt

Beispiel 2

Handel mit Kundendaten[5].

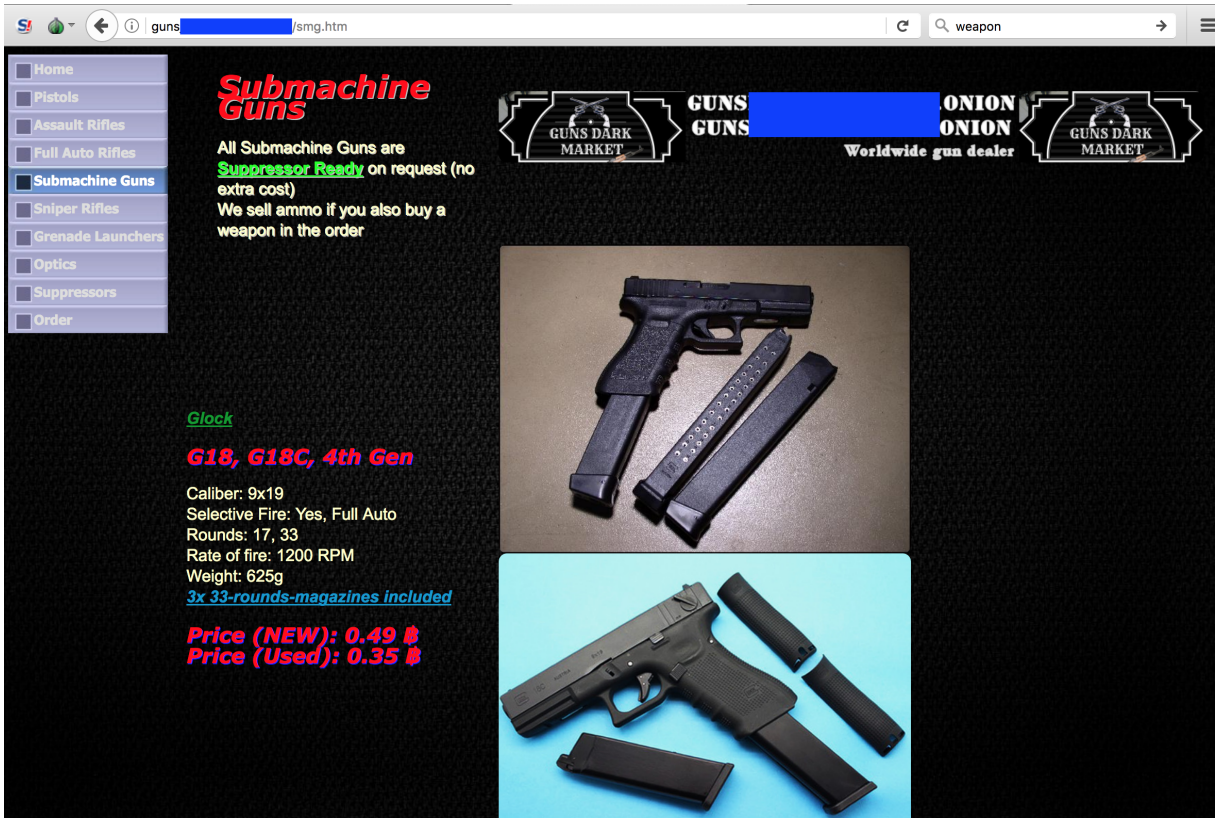
Unbefugte griffen auf persönliche Informationen von etwa 3,3 Millionen Nutzern zu. Dabei wurden laut dem Thermomix-Hersteller Vorwerk E-Mail-Adressen, Wohnorte und Geburtsdaten entwendet.

Der oder die Angreifer bieten die Daten in einem einschlägigen Darknet-Forum für 1.500 US-Dollar zum Verkauf an, zeigen sich beim Preis aber verhandlungsbereit. Vermutlich vor allem, weil die Kronjuwelen eines Datenlecks – Passwörter – nicht Teil des Angebots sind.

[5] https://www.heise.de/news/Datenleck-bei-Thermomix-Daten-von-1-Million-deutscher-Nutzer-im-Darknet-10273696.html

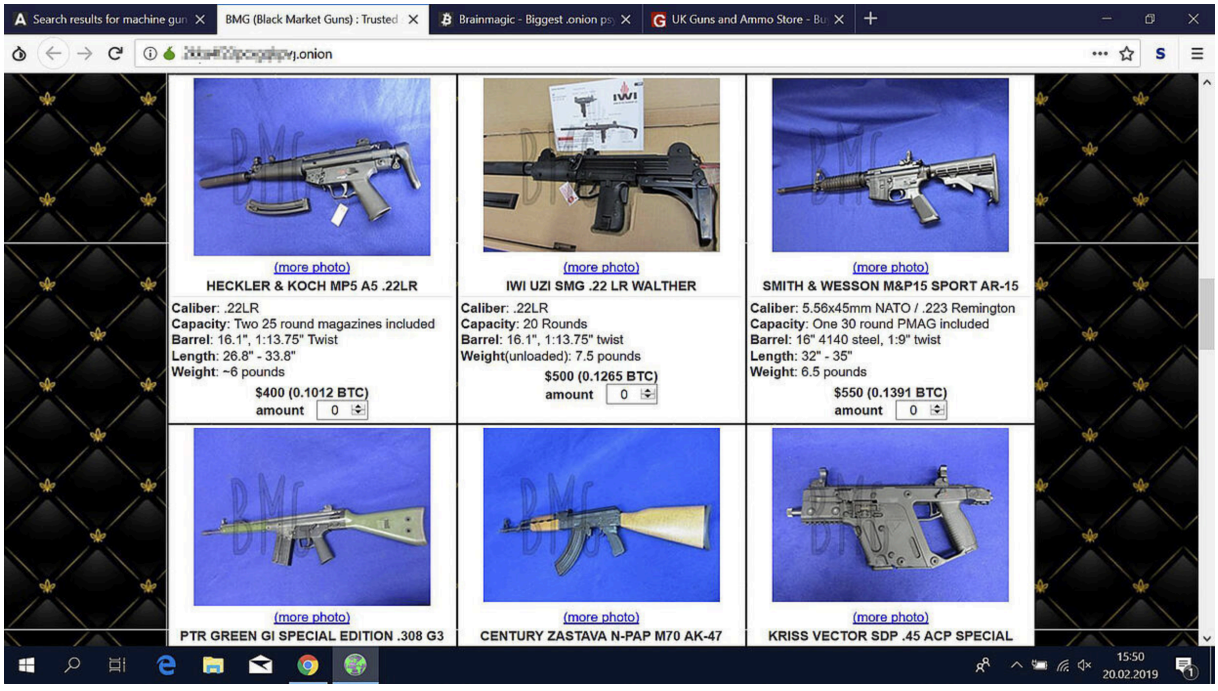
Beispiel 3

Handel mit Handfeuerwaffen und Munition.



Beispiel 4

Handel mit automatischen Waffen.



Beispiel 5

Kinderpornografie[6].

> **Schlag gegen Kindersex-Verbrecher**: Auch nach Hamburg, Bremen und Niedersachsen führten Ermittlungen der europäischen Polizeibehörde Europol gegen den wohl weltweit größten Streamingdienst für Pornografie mit Kindern. Behördenangaben zufolge konnten deutsche und internationale Ermittler die Darknet-Plattform „KidFlix“ abschalten und rund 1.400 Kunden identifizieren. Insgesamt hatten die Detektive 1,8 Millionen Nutzer in 31 Ländern im Visier. Die hatten Zugriff auf mehr als 91.000 Videos in technischer Top-Qualität. Den Angaben zufolge kümmerte sich die Kripo auch um den Schutz betroffener Kinder.
> polizei.bayern.de europol.europa.eu

- **Aktivisten und Journalisten**
  Menschenrechtsaktivisten, Journalisten und Dissidenten nutzen das Darknet oft, um sich vor Überwachung zu schützen, insbesondere in Ländern mit starken staatlichen Einschränkungen der Meinungsfreiheit.
- **Datenschutz-Enthusiasten**
  Einige Nutzer verwenden das Darknet aus Gründen des Datenschutzes und der Anonymität. Sie können sensible Informationen austauschen, ohne dass Regierungen oder Unternehmen ihre Aktivitäten überwachen können.
- Auch viele ganz normale Webseiten haben Tor-Adressen, Facebook zum Beispiel ist unter https://facebookcorewwwi.onion/ zu erreichen.
- **Kriminelle**
  Das Darknet wird auch von kriminellen Gruppen genutzt, um illegale Waren und Dienstleistungen zu handeln. Dieser Aspekt des Darknets hat dazu geführt, dass es oft mit illegalen Aktivitäten in Verbindung gebracht wird.
- **Whistleblower**
  Personen, die Insiderinformationen über Unternehmen oder Regierungen veröffentlichen wollen, können das Darknet nutzen, um anonym zu bleiben und die Verbreitung ihrer Informationen zu ermöglichen.

[6] https://www.polizei.bayern.de/aktuelles/pressemitteilungen/082872/index.html

- **Umweltskandale:** Im November 2024 deckte ein Whistleblower bei Teslas Gigafactory in Texas gravierende Umweltverstöße auf, darunter ungefiltertes Abwasser und manipulierte Schadstoffprüfungen.
- **Gaza-Krieg:** Whistleblower der israelischen Armee enthüllten im April 2024, dass beim Einsatz einer Künstlichen Intelligenz namens „Lavender“ zur Identifizierung vermeintlicher Terroristen wissentlich hohe Zahlen ziviler Opfer in Kauf genommen wurde.
- **Risiken der Künstlichen Intelligenz (KI):** Ehemalige OpenAI-Mitarbeiter machten im Juni 2024 auf mangelnde Transparenz und potenzielle Gefahren von KI-Systemen aufmerksam und plädierten für ein „Right to Warn“.