Cryptowars 2021

Die Situation in Deutschland

Vortrag am 18.09.2021 im Rahmen der Kieler Linux Tage

zur Person

Claus Godbersen

- Jahrgang 1983
- Abschluss in Politikwissenschaft 2010 von der CAU Kiel
- Beauftragter für Qualitätsmanagement und Datenschutz
- seit 2005 begeistert für Mathe und IT
- seit 2020 Kryptologie-Enthusiast → https://aliceundbob.de

Agenda

Was bedeutet “Cryptowars”?

Wie ist die aktuelle Lage in Deutschland?
- Wofür stehen die zentralen Begriffe der Debatte?
- Was ist dieses Jahr passiert?
- Womit treten einige Parteien zur Bundestagswahl an?

Wie lautet mein persönliches Fazit?

Was bedeutet “Cryptowars”?

Was bedeutet “Cryptowars”?

Was bedeutet “Cryptowars”?

Verschlüsselung erlaubt?

Mitlesen erlaubt?

In aller Kürze: Die Lage in Deutschland

Bundes-
verfassungsschutz

Bundes-
nachrichtendienst

Bundes-
kriminalamt

Militärischer
Abschirmdienst

16 Landesbehörden für Verfassungsschutz

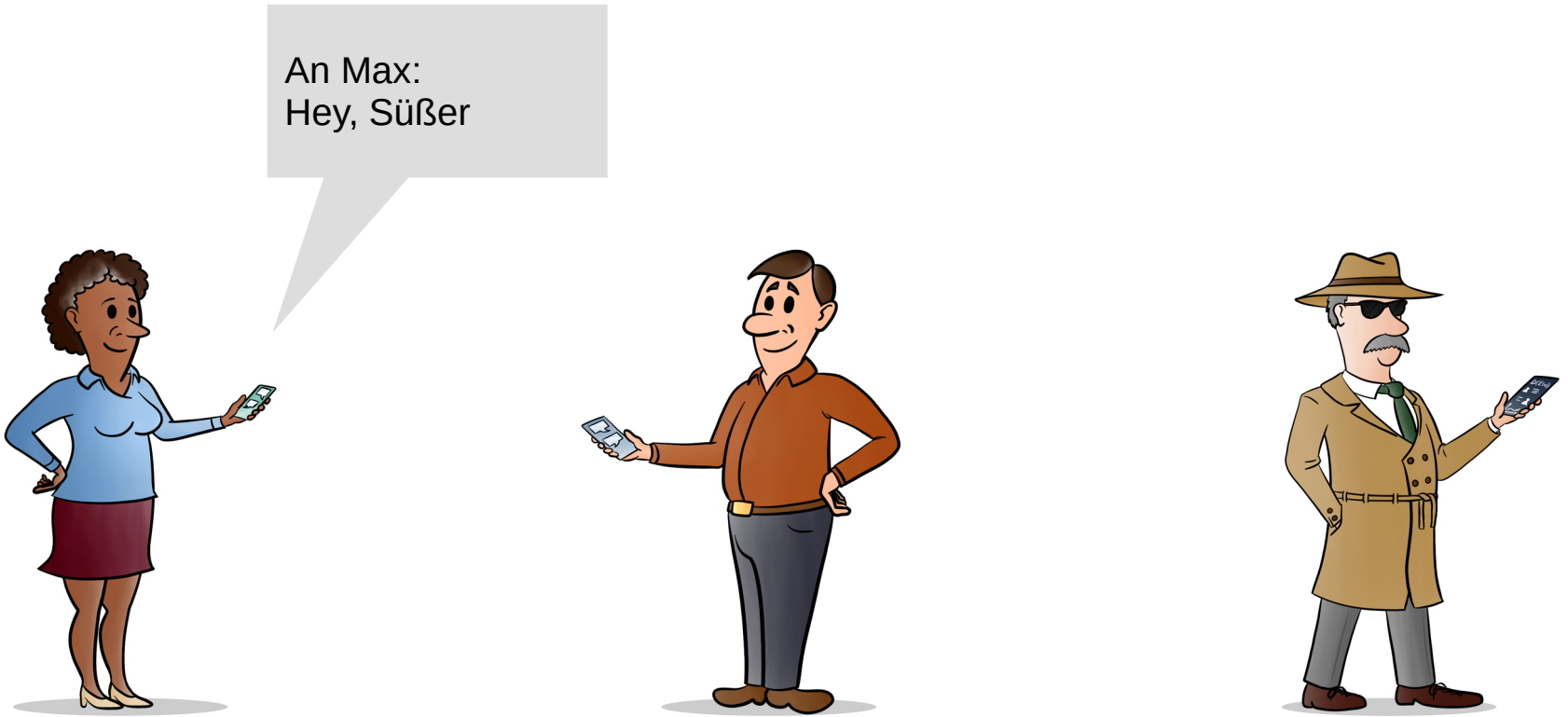
einige der 16 Landes-Polizeibehörden

zentrale Begriffe

Staatstrojaner
Quellen-TKÜ
Onlinedurchsuchung
Bestandsdatenauskunft
Hilfssherriffs
demokratische Kontrolle

zentrale Begriffe: Staatstrojaner

zentrale Begriffe: Staatstrojaner



zentrale Begriffe: Staatstrojaner

zentrale Begriffe: Staatstrojaner

zentrale Begriffe: Staatstrojaner

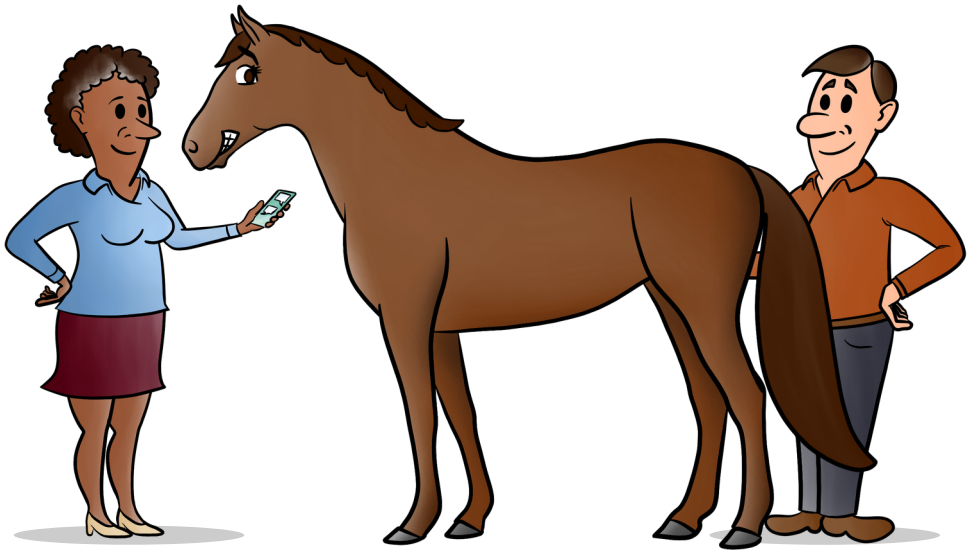
Klartext	Hey, Süßer
Bit-Klartext	01001000 01100101 01111001 00101100 00100000 01010011 11000011 10111100 11000011 10011111 01100101 01110010
Schlüssel	01011011 00111010 10101101 01110110 00110001 01111010 10101111 11000110 10101100 00000111 11010110 00110100
Chiffrat	00010011 01011111 11010110 01011010 00010001 00101001 01101100 01111010 01101111 10011000 10110011 01000110

zentrale Begriffe: Staatstrojaner

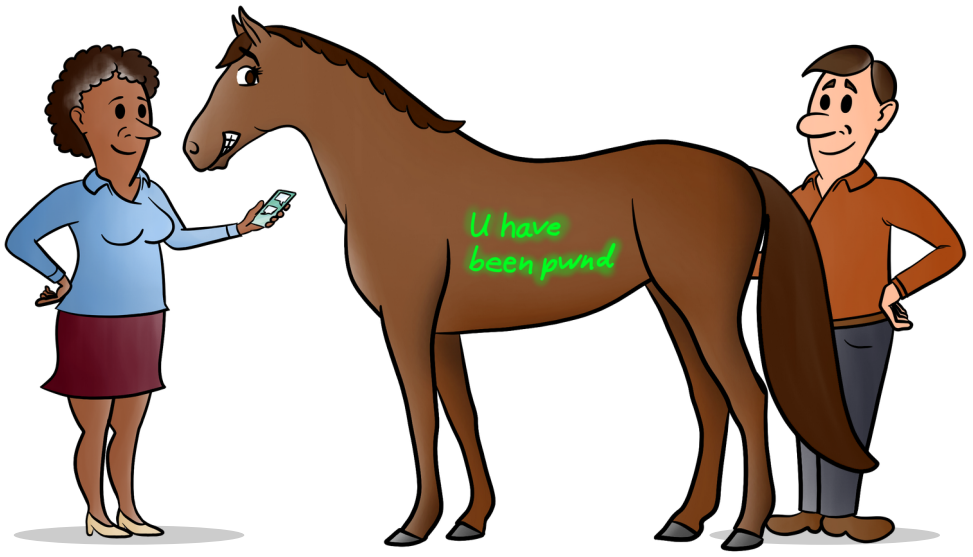
Klartext	Hey, Süßer
Bit-Klartext	01001000 01100101 01111001 00101100 00100000 01010011 11000011 10111100 11000011 10011111 01100101 01110010
Schlüssel	01011011 00111010 10101101 01110110 00110001 01111010 10101111 11000110 10101100 00000111 11010110 00110100
Chiffrat	00010011 01011111 11010110 01011010 00010001 00101001 01101100 01111010 01101111 10011000 10110011 01000110

zentrale Begriffe: Staatstrojaner

zentrale Begriffe: Staatstrojaner



zentrale Begriffe: Staatstrojaner



zentrale Begriffe: Quellen-TKÜ

Staatstrojaner ermöglichen die behördlichen Maßnahmen

> Quellen-Telekommunikationsüberwachung
> und
> Online-Durchsuchung

Quellen-TKÜ betrachtet Verlauf in Echtzeit.
Online-Durchsuchung betrachtet Inhalte auch rückwirkend.

§ 11 Artikel 10-Gesetz
§§ 100a, 100b Strafprozeßordnung

zentrale Begriffe: Hilfssherrifs

„Wer eine Telekommunikationsanlage betreibt, mit der öffentlich zugängliche Telekommunikationsdienste erbracht werden, hat ab dem Zeitpunkt der Betriebsaufnahme auf eigene Kosten technische Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation vorzuhalten und organisatorische Vorkehrungen für deren unverzügliche Umsetzung zu treffen.”

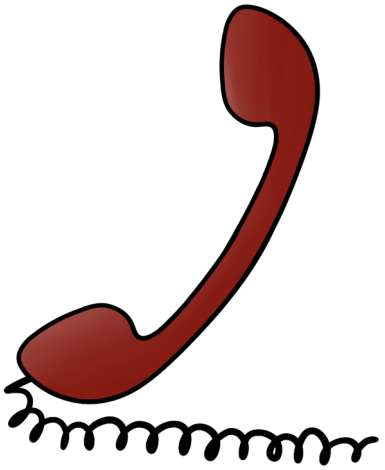
§ 110 Telekommunikationsgesetz

zentrale Begriffe: Bestandsdatenauskunft

Anbieter von Telekommunikationsdiensten und Telemediensten sind verpflichten, bestimmte Daten ihrer Kundinnen zu speichern und automatisch und/oder manuell an Behörden zu übermitteln.

Die betroffenen Nutzer dürfen nicht informiert werden.

§§ 110-113 Telekommunikationsgesetz
§§ 15a-15c Telemediengesetz

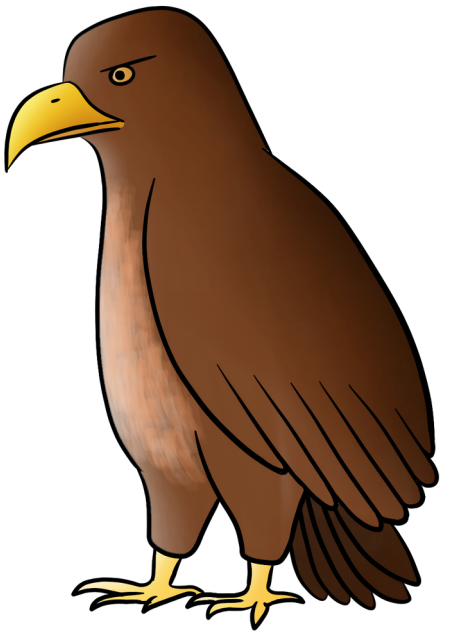


zentrale Begriffe: demokratische Kontrolle

Das **parlamentarische Kontrollgremium** ist eine Gruppe von Abgeordneten des Bundestages, die den Auftrag haben, die Nachrichtendienste der Bundesregierung zu kontrollieren.

Die Mitglieder haben umfangreiche Auskunftsrechte. Die Bundesregierung kann Auskünfte jedoch verweigern, wenn andere Interessen dagegenstehen.

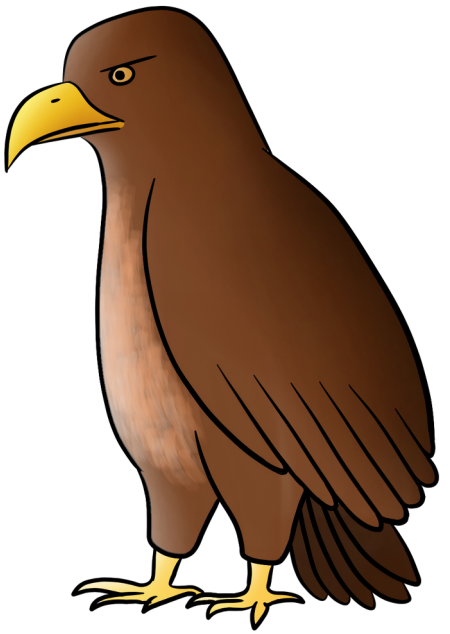
§§ 1, 4, 5, 6 Kontrollgremiumgesetz



zentrale Begriffe: demokratische Kontrolle

Die **G 10-Kommission** des Bundestages entscheidet über die Notwendigkeit und Zulässigkeit der Überwachungsmaßnahmen durch die Nachrichtendienste des Bundes. Möchte ein Nachrichtendienst beispielsweise ein Telefon abhören, wird die G10-Kommission eingeschaltet. Ohne ihre Zustimmung darf die Überwachungsmaßnahme nicht durchgeführt werden.

§ 15 Artikel 10-Gesetz

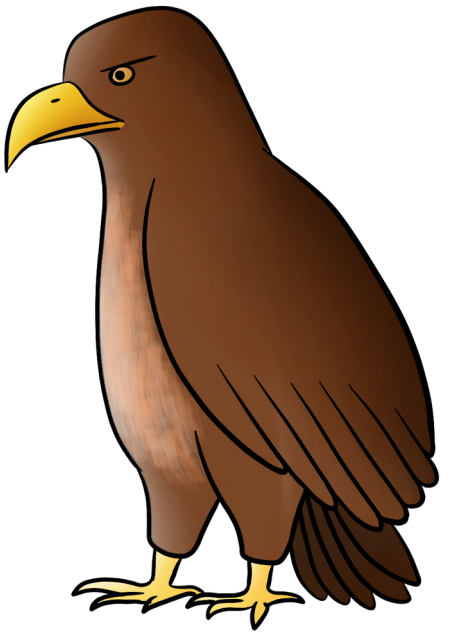


zentrale Begriffe: demokratische Kontrolle

BND-Gesetz:
Es werden vier spezielle Kontrollorgane genannt:

- das Unabhängige Gremium aus Richtern und Anwälten am Bundesgerichtshof
- der Unabhängige Kontrollrat; eine oberste Bundesbehörde, der die Kontrolle der technischen Aufklärung des BND obliegt
- das Gerichtsähnliche Kontrollorgan des Unabhängigen Kontrollrates, das aus ehemaligen Richtern beim Bundesgerichtshof und Bundesverwaltungsgericht besteht
- das Administrative Kontrollorgan

§§ 16, 41,43, 50 BND-Gesetz



zentrale Begriffe: demokratische Kontrolle

Artikel-10-Gesetz
§§ 5, 8

BND-Gesetz
§§ 6, 12, 14

Bundeskriminalamtgesetz
§ 2

Bundesverfassungsschutzgesetz
§§ 8a, 8b

Gerichtsverfassungsgesetz
§ 152

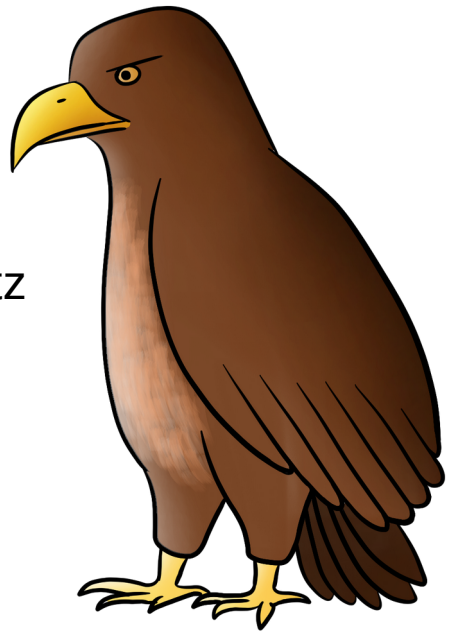
Kontrollgremiumsgesetz
§ 10

Strafprozessordnung
§§ 100a-100k

Telekommunikationsgesetz
§ §110, 112, 113

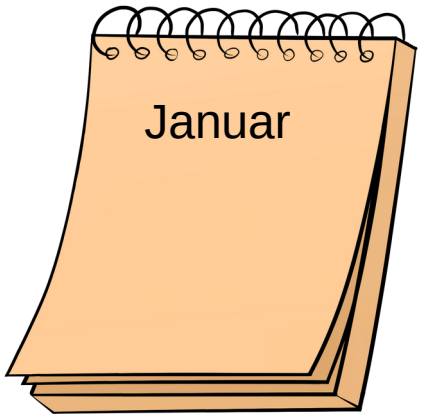
Telemediengesetz
§ 14, 15a, 15b

Zollfahnungsdienstgesetz
§§ 3, 72



Sonstige Ereignisse 2021

Bericht: Die Bundespolizei hat 2020 gute 100.000 stille SMS verschickt, um heimlich Mobiltelefone zu orten.



Sonstige Ereignisse 2021

Thomas Haldenwang, Präsident des Bundesamtes für Verfassungsschutz (BfV), erklärt, bei der eingeführten Befugnis des BfV zur Durchführung einer Quellen-Telekommunikationsüberwachung müssten keine neu erkannten IT-Sicherheitslücken ausgenutzt werden.

Die FDP-Bundestagsfraktion klagt beim Bundesverfassungsgericht gegen Staatstrojaner.

Spionagesoftware Pegasus wird bei ungarischen Journalisten gefunden.

Sonstige Ereignisse 2021

Nachdem die Taliban scheinbar überraschend wieder die Macht in Afghanistan übernehmen, erbeuten sie von der US-Armee und der ehemaligen afghanischen Regierung personenbezogene Daten vieler Bürger.

Sonstige Ereignisse 2021

September

Das Bundeskriminalamt berichtet im Bundestag, es habe die Spionagesoftware Pegasus erworben und im Einsatz. Der Bundesinnenminister sei nicht informiert gewesen.

Das Bundesamt für Sicherheit in der Informationstechnik warnt öffentlich, es gebe kaum eine Möglichkeit, sich vor Pegasus zu schützen.

Bundestagswahl

Wahlprogramme

Staatstrojaner etc einsetzen?


CDU-CSU


FDP


Grüne


Linke


Piraten


SPD


Volt


SSW


Fr. Wähler

Fazit

Ich wünsche mir

- mehr informierte Bürgerinnen
- mehr demokratische Kontrolle
- mehr Fachwissen in der CDU-CSU
- mehr Engagement zum Beispiel bei
  - Amnesty International
  - Transparency International
  - Electronic Frontier Foundation
  - Chaos Computer Club
  - Netzpolitik.org
  - Gesellschaft für Freiheitsrechte

Quellen

Bündnis 90 / Die Grünen: „Deutschland. Alles ist drin. Bundestagswahlprogramm 2021“, Berlin 2021.

Bundesamt für Sicherheit in der Informationstechnik: „Smartphones weltweit von Pegasus überwacht“, 27.07.2021, https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-234348-1032.pdf;jsessionid=5562AFC8EDD53BF0D89E0B4A58168BB2.internet482?__blob=publicationFile&v=3 , abgerufen am 10.09.2021

Bundesgesetzblatt Jahrgang 2021 Teil I Nr. 40, Bonn, 08.07.2021, Seite 2274.

Bundestag: Drucksache 19/30797 vom 18.06.2021, Seite 6.

CDU-CSU: „Das Programm für Stabilität und Erneuerung“, Berlin und München ohne Datum.

Christian Baars, Florian Flade und Georg Mascolo: „Darf‘s ein bisschen mehr sein?“, 19.07.2021, https://www.tagesschau.de/investigativ/ndr-wdr/spaeh-software-pegasus-deutschland-101.html, abgerufen am 14.08.2021

Die Linke: „Zeit zu handeln! Für soziale Gerechtigkeit, Frieden und Klimagerechtigkeit“, Berlin 2021.

FDP: „Nie gab es mehr zu tun. Das Programm der Freien Demokraten zur Bundestagswahl 2021“, Berlin 2021.

Sebastian Grüner: Merkel verteidigt Einsatz von Pegasus-Trojaner, 10.09.2021, https://www.golem.de/news/spyware-merkel-verteidigt-einsatz-von-pegasus-trojaner-2109-159482.html, abgerufen am 10.09.2021

Sebastian Grüner und Moritz Tremmel: BKA hat Pegasus-Trojaner der NSO Group gekauft, 07.09.2021, https://www.golem.de/news/staatstrojaner-bka-hat-pegasus-trojaner-der-nso-group-gekauft-2109-159401.html, abgerufen am 10.09.2021

Bernd Heinrich und Tobias Reinbacher: „Examinatorium Strafprozessrecht – Arbeitsblatt Nr. 19: Quellen-TKÜ und Online-Durchsuchung”, 01.10.2020, https://www.jura.uni-wuerzburg.de/fileadmin/02150500/2020/19-quellentkue_online-durchsuchung.pdf, abgerufen am 15.08.2021.

Quellen

Martin Holland: „Afghanistan: Taliban erbeuten Biometrie-Geräte und -Datenbanken“, 18.08.2021, https://www.heise.de/news/Afghanistan-Biometrie-Geraete-und-Datenbanken-von-Taliban-erbeutet-6168158.html, abgerufen am 26.08.2021.

Johannes Jolmes: "NDR Morgenmagazin", 19.7.2021.

Kanzlei WBS: „Der Bundestrojaner kommt! Werden wir bald alle ausgespäht?“, 08.07.2017, https://www.youtube.com/watch?v=aTou4dbSbi0&t=339s, abgerufen am 28.08.2021.

Stefan Krempl: „Überwachung: Bundespolizei verschickte 2020 über 100.000 stille SMS“, vom 06.02.2021: https://www.heise.de/news/Ueberwachung-Bundespolizei-verschickte-2020-ueber-100-000-stille-SMS-5047855.html, abgerufen am 06.02.2021.

Netzpolitik: „Große Koalition einigt sich auf Staatstrojaner-Einsatz schon vor Straftaten”, 08.06.2021, https://netzpolitik.org/2021/bundespolizeigesetz-grosse-koalition-einigt-sich-auf-staatstrojaner-einsatz-schon-vor-straftaten/, abgerufen am 28.08.2021.

Phoenix: „Bundestag: Gesetzentwurf und Anträge zur Bundespolizei am 10.06.2021“, https://www.youtube.com/watch?v=VERtwFMLO2o , abgerufen am 11.08.2021.

Piratenpartei Deutschland: „Wahlprogramm zur Bundestagswahl 2021 der Piratenpartei Deutschland“, ohne Ort 2021.

Sonntagmorgen: „Staatstrojaner erkennen & entfernen 2021: Was hilft gegen Überwachungssoftware?“, 15.06.2021, https://www.sonntagmorgen.com/staatstrojaner-erkennen/, abgerufen am 07.09.2021

SPD: „Aus Respekt vor deiner Zukunft. Das Zukunftsprogramm der SPD“, ohne Ort 2021.

Wahlprogramme

CDU-CSU

„Die Befugnisse von Polizei und Verfassungsschutz müssen auch in der digitalen Welt so wirksam sein, wie sie es in der analogen Welt sind. Wenn ein richterlicher Beschluss eine Telefonüberwachung oder die Durchsuchung einer Wohnung ermöglicht, muss Gleiches auch für verschlüsselte Nachrichten und Telefonate gelten, für das digitale Büro auf dem Computer oder Laptop. Die Voraussetzungen für die Quellen-TKÜ und Online-Durchsuchung – sowohl bei der Gefahrenabwehr als auch bei der Strafverfolgung – wollen wir bundesweit anpassen, sodass diese Instrumente rechtssicher und effektiv eingesetzt werden können.“ (CDU-CSU 2021, S. 116)

Wahlprogramme

FDP

„Wir Freie Demokraten setzen uns für ein Recht auf Verschlüsselung ein, und fordern eine grundsätzliche Verschlüsselung elektronischer Kommunikation. Jede Einschränkung des Einsatzes von Kryptografie und jede Verpflichtung zum Offenhalten von IT-Sicherheitslücken lehnen wir ab. […] Statt der Ausnutzung von Sicherheitslücken fordern wir eine Priorität für die IT-Sicherheit und ein klar geregeltes Schwachstellenmanagement. Der Staat darf keine Sicherheitslücken für Ermittlungszwecke aufkaufen. Wenn einer staatlichen Stelle Sicherheitslücken bekannt werden, muss sie diese umgehend dem Bundesamt für Sicherheit in der Informationstechnik (BSI) melden, das eine Schließung der Lücke durch den Hersteller herbeiführt oder, wenn dies nicht gelingt, die Lücke nach den allgemeinen Grundsätzen der Cybersicherheit koordiniert veröffentlicht.“ (FDP 2021, S. 35)

Wahlprogramme

Grüne

„Die [...] anlasslose Vorratsdatenspeicherung, generelle Hintertüren in digitalen Geräten und Anwendungen oder das Infiltrieren von technischen Geräten (Online-Durchsuchung bzw. Quellen-TKÜ) [lehnen wir] ab. Zudem soll eine Verpflichtung eingeführt werden, Sicherheitslücken zu melden und aktiv auf ihre Behebung hinzuwirken. Unternehmen dürfen nicht dazu verpflichtet werden, die IT-Sicherheit und Netzintegrität auf Kosten der Allgemeinheit zu gefährden.“ (Bündnis 90 / Die Grünen, S. 200)

„Wir fördern die Entkriminalisierung verschlüsselter Kommunikation, stellen uns der Schwächung von Verschlüsselungstechnologien und -standards entgegen und stärken die Multi-Stakeholder-Governance des Internets auf internationaler Ebene.“ (Bündnis 90 / Die Grünen 2021, S. 236)

Wahlprogramme

Linke

„Der Aufkauf von Informationen über und Beauftragung von Sicherheitslücken in IT-Systemen durch Geheimdienste muss verboten und unterbunden werden. […] Die Möglichkeit der Ende-zu-Ende-Verschlüsselung ist essenzieller Bestandteil des Grundrechts auf informationelle Selbstbestimmung. Quellen-Telekommunikationsüberwachung und Onlinedurchsuchung (Staatstrojaner) müssen verboten werden. Die Vorratsdatenspeicherung von IP-Verbindungen, Mobilfunkverbindungen und -standorten muss verboten werden. Eine Ausweispflicht für E-Mail-, Messengerdienste und Ähnliches lehnen wir ab.“ (Die Linke 2021, S. 95f)

Wahlprogramme

Piraten

„Für uns PIRATEN sind verdeckte Eingriffe in informationstechnische Systeme durch den Staat nicht mit Grundrechten und Rechtsstaat vereinbar. Wir setzen uns daher für die Abschaffung der Befugnisse für staatliche Behörden zum Verwanzen solcher Systeme ein.“

Wahlprogramme

SPD

„Wir wollen Hersteller darauf verpflichten, Softwareprodukte, digitale Dienste und technische Geräte so zu konzipieren, dass sie sicher sind (Security by Design) und dass sie bei den Standardeinstellungen die sicherste Variante wählen (Security by Default). Digitale Hintertüren sollen nicht offen gehalten werden. “