

Crypto Wars

Die Bürger sind gefordert – aber überfordert

Claus H. Godbersen
beim Kieler CryptoAdvent 2020

Agenda

Aktueller Anlass

Was die Bürgerinnen und
Bürger wissen sollten

Die aktuelle Debatte

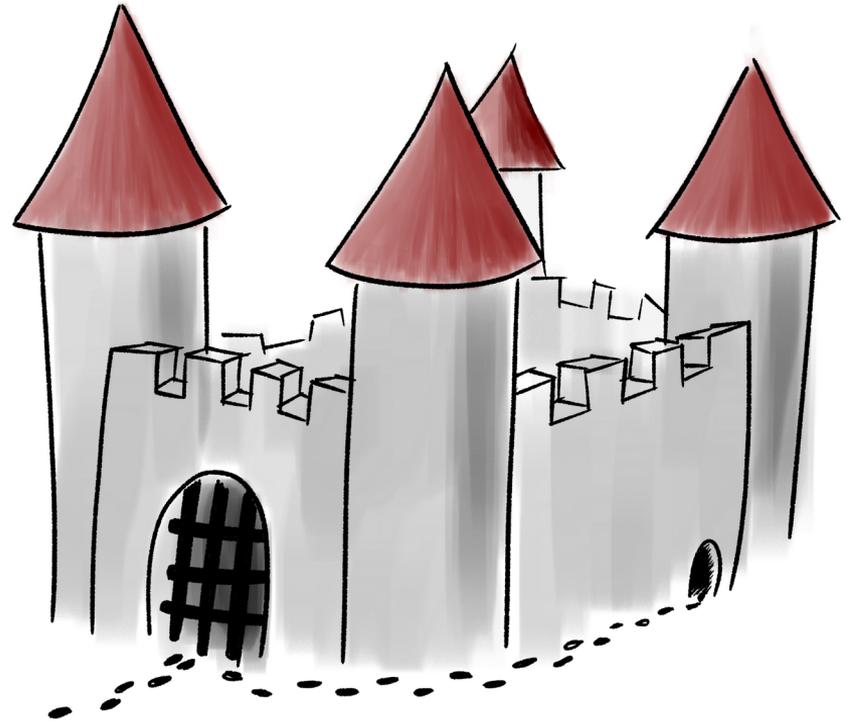
Bildungsoffensive

Was wir tun können

Quellen

Aktueller Anlass

Die EU-Regierungen planen offenbar, staatliche Zweitschlüssel oder “Hintertüren” zu verschlüsselten Kommunikationsangeboten gesetzlich vorzuschreiben.



Was die Bürgerinnen und Bürger wissen sollten

(Mindestens) fünf Themenblöcke bilden den Hintergrund der Crypto Wars:

- **Gründungsmythos und dunkle Machenschaften:**
Sind unsere Nachrichtendienste vertrauenswürdig?
- **Kontrolle ist besser:**
Wo stehen die Nachrichtendienste im Rechtsstaat?
- **Was dein Feind nicht wissen soll:**
Wie ticken Nachrichtendienste?
- **Schützenswertes:**
Sollen Bürger verschlüsseln (dürfen)?
- **Schlüssel und Zweitschlüssel:**
Hatten wird das nicht schonmal?



Gründungsmythos und dunkle Machenschaften:

Sind unsere Nachrichtendienste vertrauenswürdig?

Gründungen

1946	Bundesnachrichtendienst (BND)
1947	Central Intelligence Agency (CIA)
1950	Bundesamt für Verfassungsschutz (BfV)
1952	National Security Agency (NSA)
1956	Militärischer Abschirmdienst (MAD)

Gründungsmythos und dunkle Machenschaften:

Sind unsere Nachrichtendienste vertrauenswürdig?

Gründungen

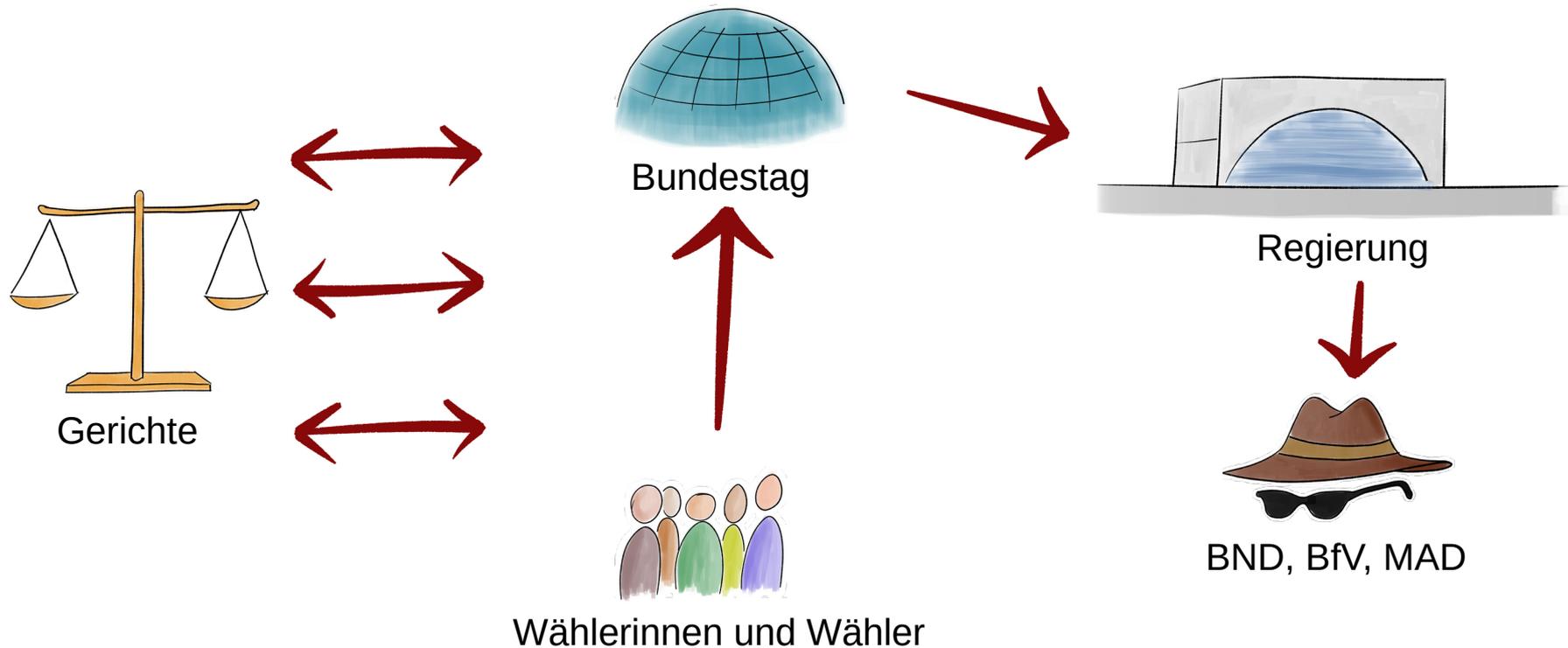
1946	Bundesnachrichtendienst (BND)
1947	Central Intelligence Agency (CIA)
1950	Bundesamt für Verfassungsschutz (BfV)
1952	National Security Agency (NSA)
1956	Militärischer Abschirmdienst (MAD)

besondere Ereignisse

1961	CIA lässt Patrice Lumumba ermorden
1970	CIA und BND kaufen Schweizer Crypto AG
1992	Hans Bühlen, Mitarbeiter der Crypto AG, wird im Iran verhaftet
2001	Terroranschläge vom 11. September
2008	BND erwirbt heimlich PRISM-Software der NSA
2011	Ende der NSU-Verbrechensserie
2013	Enthüllungen von Edward Snowden

Kontrolle ist besser:

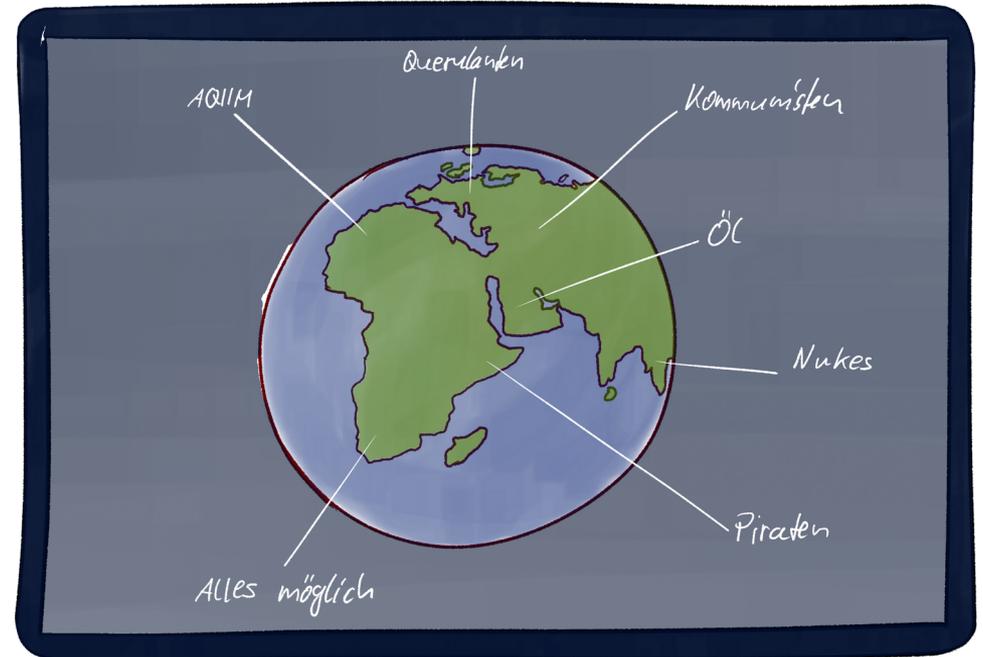
Wo stehen die Nachrichtendienste im Rechtsstaat?



Was dein Feind nicht wissen soll: Wie ticken Nachrichtendienste?

Freund-Feind-Schema

Alle überwachen als logische Konsequenz
andere Politik als einziger Ausweg



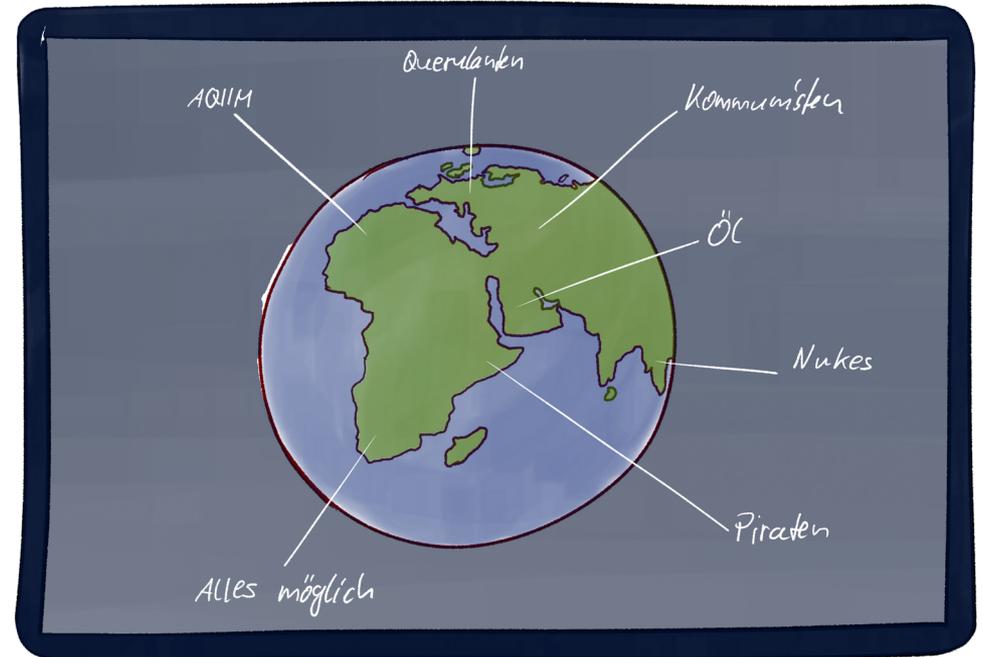
Was dein Feind nicht wissen soll: Wie ticken Nachrichtendienste?

Freund-Feind-Schema

Alle überwachen als logische Konsequenz
andere Politik als einziger Ausweg

“In God we trust,
all others we monitor.”

– NSA



Schützenswertes:

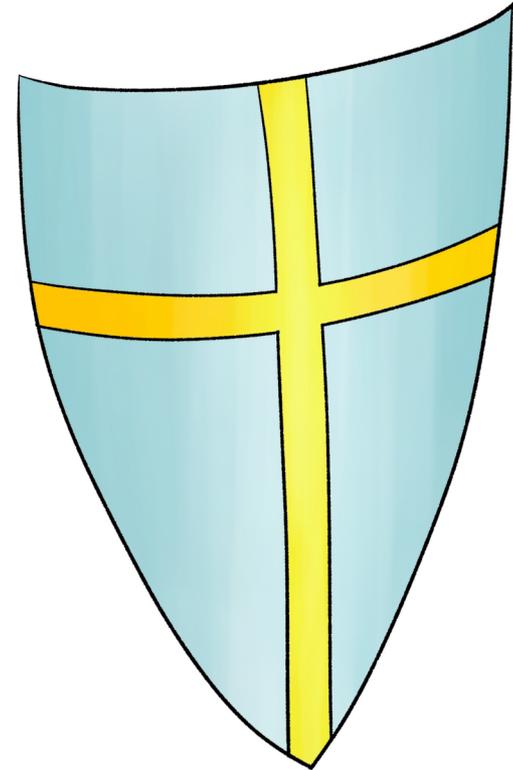
Sollen Bürger verschlüsseln (dürfen)?

starker Staat zum Schutz vor gefährlicher Anarchie

Grundrechte zum Schutz vor einem zu starken Staat u. a.

- Fernmeldegeheimnis (Grundgesetz)
- Privatsphäre (Allgemeine Erklärung der Menschenrechte)

digitale Privatsphäre



Schlüssel und Zweitschlüssel:

Hatten wir das nicht schonmal?

Cäsar-Verschlüsselung

von Linguistik zu Mathematik

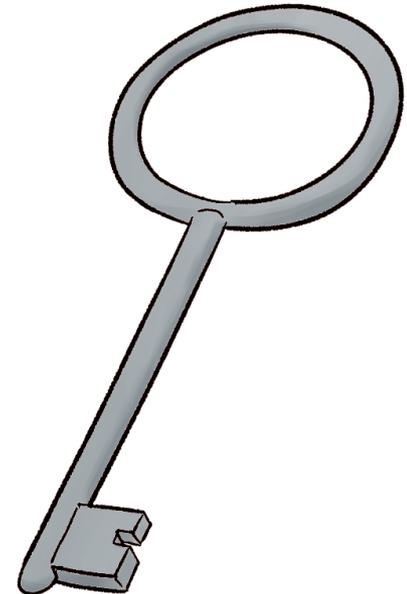
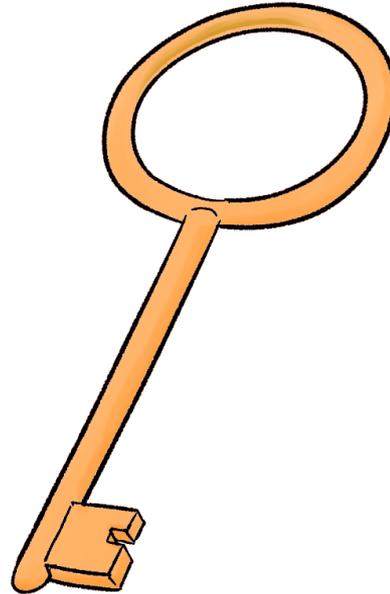
RSA

Pretty Good Privacy

Zweitschlüssel-Initiative 1991 in USA

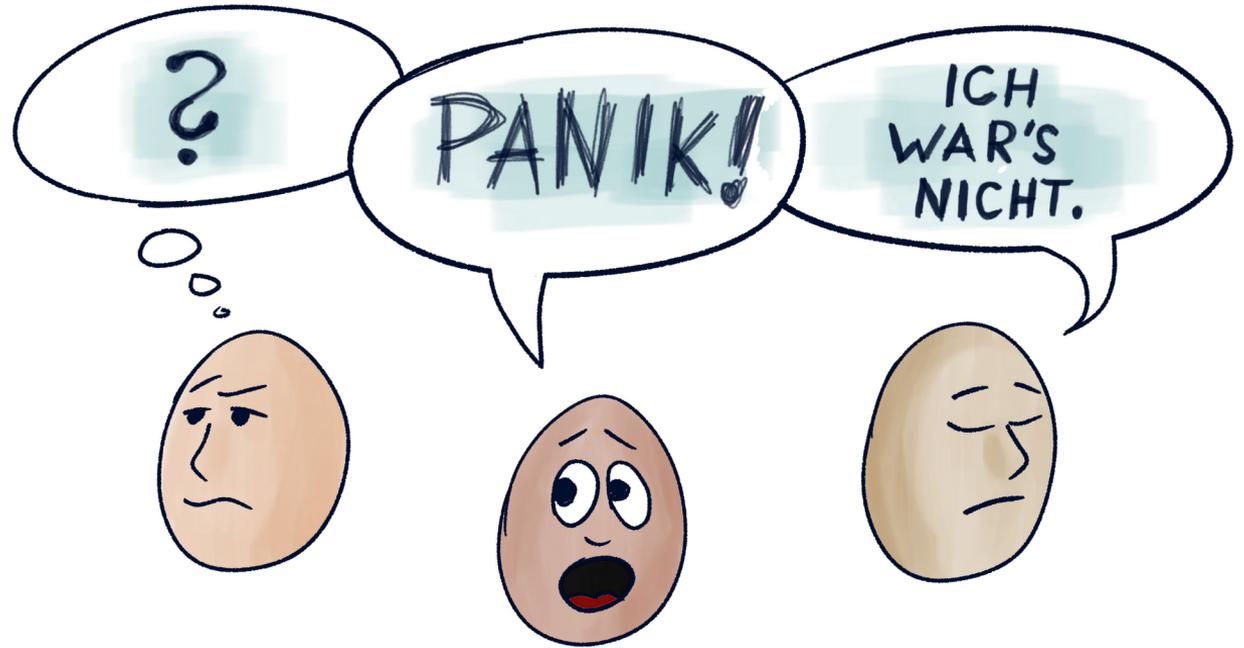
Capstone / Clipper

NSA, Juniper und Wannacry



Die aktuelle Debatte

hohe Bildungsvoraussetzungen
aneinander Vorbeireden
Emotionalität statt Sachlichkeit
Verantwortungslosigkeit



Bildungsoffensive

Ziel: Crypto Wars in
den Schulunterricht

Status quo:

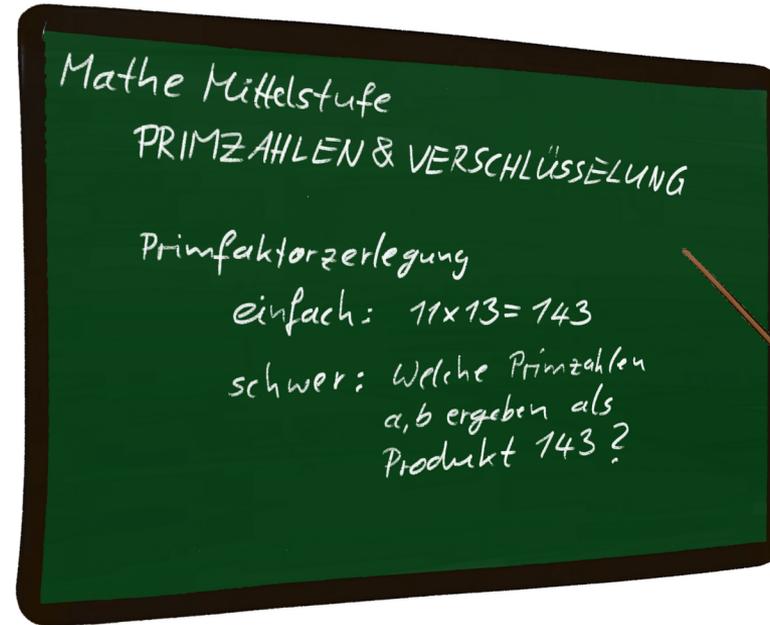
Zusatzangebote wie

z.B. Initiative "Chaos macht Schule"

z.B. Crypto Camp vom IPN

Ziel:

mehr lebenslanges Lernen



Was wir tun können

Veranstaltungen wie Crypto Advent

Parteimitgliedschaft

Botschaften an die Politik

Vereine

Weblog

Qualitätsjournalismus

soziales Umfeld

gute Laune



Quellen

ARD: Neues BND-Gesetz: Freibrief zur Überwachung?, Oktober 2020, <https://www.youtube.com/watch?v=E7x9iP09jbo>, abgerufen am 11.11.2020

Arte: Nazis im BND - Neuer Dienst und alte Kameraden, <https://www.youtube.com/watch?v=bjI5t2hKGD4>, abgerufen am 25.11.2020

James Bamford: Body of Secrets, New York 2002

Bundesamt für Verfassungsschutz: Verfassungsschutzbericht 2019, Berlin 2019

Bundesverfassungsgericht: Urteil vom 19. Mai 2020 - 1 BvR 2835/17.

Bundeszentrale für politische Bildung: Vor 20 Jahren: Grundgesetzänderung für den "großen Lauschangriff", 15.01.2018, <https://www.bpb.de/politik/hintergrund-aktuell/262861/lauschangriff>, abgerufen am 21.11.2020

Jefferson Chase: German intelligence agency gets spy satellite system funds, 06.11.2017, <https://www.dw.com/en/german-intelligence-agency-gets-spy-satellite-system-funds/a-41244180>, abgerufen am 23.11.2020

Heise Online: Neuer Angriff auf Verschlüsselung, über Backdoors und andere Irrwege, 12.11.2020, <https://www.youtube.com/watch?v=jNiSIGkBT6To>, abgerufen am 27.11.2020

Martin Holland: Juniper-Skandal: China übernahm angeblich Hintertür in Netzhardware, 29.10.2020, <https://www.heise.de/news/Juniper-Skandal-China-uebernahm-angeblich-Hintertuer-4942914.html>, abgerufen am 27.11.2020

Jung & Naiv: Folge 104, 28.12.2013, <https://www.youtube.com/watch?v=5CvJbrmTv7c>, abgerufen am 05.12.2020

Stefan Krempel: Missing Link: Crypto Wars – der endlose Streit über sichere Verschlüsselung, 22.10.2020, <https://www.heise.de/hintergrund/Missing-Link-Crypto-Wars-der-endlose-Streit-ueber-sichere-Verschlueselung-4967574.html?seite=all>, abgerufen am 22.10.2020

Erich Moechel: Auf den Terroranschlag folgt EU-Verschlüsselungsverbot, 08.11.2020, <https://fm4.orf.at/stories/3008930/>, abgerufen am 29.11.2020

Quellen

Nicole Perlroth und Scott Shane: In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc, 25.05.2019, <https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html>, abgerufen am 27.11.2020

Marc Rotenberg auf dem Crypto Summit 2015 von Access Now, https://www.youtube.com/watch?v=_rD987SXoJI, abgerufen am 25.11.2020

Jeanne Sahadi: What the NSA costs taxpayers, 07.06.2013, <https://money.cnn.com/2013/06/07/news/economy/nsa-surveillance-cost/index.html>, abgerufen am 25.11.2020

Bruce Schneier: Data and Goliath, New York 2015.

Simon Singh: Geheime Botschaften, München 2001

SRF: SRF DOK - Wie CIA und BND mit Schweizer Hilfe weltweit spionierten, <https://www.youtube.com/watch?v=VWImO1Qz4Zo>, abgerufen am 16.11.2020

United Nations: Universal Declaration of Human Rights, <https://www.un.org/en/universal-declaration-human-rights/index.html>, abgerufen am 21.11.2020

SWR: Früh.Warn.System. – Brauchen wir diesen Verfassungsschutz?, 2020, <https://www.youtube.com/watch?v=D4-fWZyO2rM>, abgerufen am 24.11.2020

WDR: 26. Juli 1947 - Gründung des US-Geheimdienstes CIA, 26.07.2017, <https://www1.wdr.de/stichtag/stichtag-gruendung-der-cia-100.html>

Thorsten Wetzling und Daniel Moßbrucker: BND-Reform, die Zweite, Berlin 2020

Peter Wichmann: Genese der Al-Qaida, <https://www.kas.de/de/web/islamismus/al-qaida>, abgerufen am 29.11.2020

ZDF: Streng geheim! Cryptoleaks. Die große BND und CIA Spionage, 2020, <https://www.youtube.com/watch?v=jagiJ9YAqto>, abgerufen am 25.11.2020