Literaturverzeichnis

360Helios (2016): Operation Mermaid. Hg. v. 360 Core Security. Online verfügbar unter https://blogs.360.cn/post/operation-mermaid.html, zuletzt aktualisiert am 30.05.2016, zuletzt geprüft am 01.09.2021.

Achmatova, Nina (2012): Former oligarch appeals to the Patriarch for regime change in Russia. Hg. v. AsiaNews.it. Online verfügbar unter http://www.asianews.it/news-en/Former-oligarch-appeals-to-the-Patriarch-for-regime-change-in-Russia-23726.html, zuletzt aktualisiert am 18.01.2012, zuletzt geprüft am 29.04.2021.

Adams, Gordon; Williams, Cindy (2010): Buying national security: How America plans and pays for Its global role and safety at home. New York: Routledge.

Adamsky, Dmitry (2017): The Israeli Odyssey toward its National Cyber Security Strategy. In: The Washington Quarterly 40 (2), S. 113–127. DOI: 10.1080/0163660X.2017.1328928.

Agrafiotis, Ioannis; Bada, Maria; Cornish, Paul; Creese, Sadie; Goldsmith, Michael; Ignatuschtschenko, Eva et al. (2016): Cyber Harm: Concepts, Taxonomy and Measurement. Hg. v. SAID Business School. University of Oxford (Saïd Business School RP, 2016–23). Online verfügbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2828646.

Agrafiotis, Ioannis; Nurse, Jason R. C.; Goldsmith, Michael; Creese, Sadie; Upton, David (2018): A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. In: J Cyber Secur 4 (1). DOI: 10.1093/cybsec/tyy006.

Albert, Eleanor; Maizland, Lindsay; Xu, Beina (2021): The Chinese Communist Party. Hg. v. Council on Foreign Relations. Online verfügbar unter https://www.cfr.org/backgrounder/chinese-communist-party, zuletzt aktualisiert am 23.06.2021, zuletzt geprüft am 09.07.2021.

Alekseyeva, Anna (2015): The Russian politics of multiculturalism | openDemocracy. Hg. v. OpenDemocracy. Online verfügbar unter https://www.opendemocracy.net/en/odr/russian-politics-of-multiculturalism/, zuletzt aktualisiert am 30.03.2015, zuletzt geprüft am 05.05.2021.

Ali, Idrees; Stewart, Phil (2019): Exclusive: U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack: officials. Hg. v. Reuters. Online verfügbar un-

ter https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive-idUSKBN1WV0EK, zuletzt aktualisiert am 16.10.2019, zuletzt geprüft am 06.10.2021.

Alperovitch, Dmitri (2016): Bears in the Midst: Intrusion into the Democratic National Committee. Hg. v. CrowdStrike. Online verfügbar unter https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/, zuletzt geprüft am 15.12.2019.

Al-qatari, Hussain; Gambrell, Jon (2018): Iraq, Saddam and the 1991 Gulf War looms large over George H.W. Bush's legacy. Hg. v. Chicago Tribune. Online verfügbar unter https://www.chicagotribune.com/nation-world/ct-gulf-war-bush-legacy-20181201-story.html, zuletzt aktualisiert am 01.12.2018, zuletzt geprüft am 01.09.2021.

Al-Rawi; Ahmed K. (2014): Cyber warriors in the Middle East: The case of the Syrian Electronic Army. In: Public Relations Review 40 (3), S. 420–428. DOI: 10.1016/j.pubrev.2014.04.005.

Amos, Howard (2017): Vladimir Putin's man in the Balkans. Hg. v. Politico. Online verfügbar unter https://www.politico.eu/article/vladimir-putin-balkans-point-man-nikolai-patrushev/, zuletzt aktualisiert am 21.06.2017, zuletzt geprüft am 12.05.2021.

Anderlini, Jamil (2010): The Chinese dissident's ›unknown visitors‹. Hg. v. Financial Times. Online verfügbar unter https://www.ft.com/content/c590cdd0-016a-11df-8c54-00144feabdc0, zuletzt aktualisiert am 15.01.2010, zuletzt geprüft am 21.06.2021.

Anderson, Collin; Sadjadpour, Karim (2018): Iran's Cyber Threat: Espionage, Sabotage, and Revenge. Washington, D.C.: Carnegie Endowment for International Peace.

Andress, Jason (2014): The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Oxford: Syngress.

Appelbaum, Jacob; Gibson, Aaron, Guarnieri, Claudio; Müller-Maguhn, Andy; Poitras, Laura; Rosenbach, Marcel; Ryge, Leif et al. (2015): Die NSA rüstet zum Cyber-Feldzug. Hg. v. Spiegel Online. Online verfügbar unter https://www.spiegel.de/netzwelt/netzpolitik/snowden-dokumente-wie-die-nsa-digitale-kriege-vorbereitet-a-1013521.html, zuletzt aktualisiert am 18.01.2015, zuletzt geprüft am 10.12.2021.

Applegate, Scott (2011): Cybermilitias and Political Hackers: Use of Irregular Forces in Cyberwarfare. In: IEEE Secur. Privacy Mag. 9 (5), S. 16–22. DOI: 10.1109/MSP.2011.46.

Apuzzo, Matt; LaFraniere, Sharon (2018): 13 Russians Indicted as Mueller Reveals Effort to Aid Trump Campaign. Hg. v. The New York Times, zuletzt aktualisiert am 16.02.2018, zuletzt geprüft am 20.08.2021.

Arquilla, John (2012): Cool War. Foreign Policy. Online verfügbar unter https://foreignpolicy.com/2012/06/15/cool-war/, zuletzt aktualisiert am 15.06.2012, zuletzt geprüft am 25.06.2020.

Asher-dotan, Lital (2018): What Israel's Elite Defense Force Unit 8200 Can Teach Security about Diversity. Hg. v. Dark Reading. Online verfügbar unter https://www.darkreading.com/threat-intelligence/what-israel-s-elite-defense-force-unit-8200-can-teach-security-about-diversity, zuletzt aktualisiert am 21.05.2018, zuletzt geprüft am 25.10.2021.

Associated Press (2021): China tightens political control of internet giants. Hg. v. Politico. Online verfügbar unter https://www.politico.com/news/2021/10/03/china-control-internet-giants-514970, zuletzt aktualisiert am 03.10.2021, zuletzt geprüft am 11.10.2021.

Austin, Greg (2015): How China's Ministry of Public Security Controls Cyber Policy. Hg. v. The Diplomat. Online verfügbar unter https://thediplomat.com/2015/04/how-chinas-ministry-of-public-security-controls-cyber-policy/, zuletzt aktualisiert am 29.04.2015, zuletzt geprüft am 31.07.2021.

Austin, Greg (2016): International Legal Norms in Cyberspace: Evolution of China's National Security Motivations171CHAPTER 9International Legal Norms in Cyberspace: Evolution of China's National Security Motivations. In: Anna-Maria Osula und Henry Rõigas (Hg.): International Cyber Norms: Legal, Policy & Industry Perspectives. Tallinn, Estonia: NATO CCD COE Publications, S. 171–201. Online verfügbar unter https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch9.pdf.

Au-Yeung, Angel (2019): What We Know About CrowdStrike, The Cybersecurity Firm Trump Mentioned In Ukraine Call, And Its Billionaire CEO. Hg. v. Forbes. Online verfügbar unter https://www.forbes.com/sites/angelauyeung/2019/09/25/what-we-know-about-crowdstrike-the-cybersecurity-firm-mentioned-by-trump-in-his-call-with-ukraines-president-and-its-billionaire-ceo/?sh=65bbd8321c55, zuletzt aktualisiert am 26.09.2019, zuletzt geprüft am 20.08.2021.

Axelrod, Robert; Iliev, Rumen (2014): Timing of cyber conflict. In: Proceedings of the National Academy of Sciences of the United States of America 111 (4), S. 1298–1303. DOI: 10.1073/pnas.1322638111.

Babayan, Nelli (2015): The return of the empire? Russia's counteraction to transatlantic democracy promotion in its near abroad. In: Democratization 22 (3), S. 438–458. DOI: 10.1080/13510347.2014.993973.

Bachner, Michael (2020): Israeli websites hacked in cyberattack: ›Be ready for a big surprise‹. Hg. v. Times of Israel. Online verfügbar unter https://www.timesofisrael.com/israeli-websites-hacked-in-cyberattack-be-ready-for-a-big-surprise/, zuletzt aktualisiert am 21.05.2020, zuletzt geprüft am 12.02.2022.

Bajak, Frank (2019): Why Trump asked Ukraine's president about ›CrowdStrike‹. Hg. v. Associated Press. Online verfügbar unter https://apnews.com/article/trump-impeachment-inquiry-donald-trump-ap-top-news-politics-technology-aa1f66a1770d4995a6bada960a7d119e, zuletzt aktualisiert am 18.10.2019, zuletzt geprüft am 20.08.2021.

Balding, Christopher (2019): Huawei Technologies' Links to Chinese State Security Services. In: SSRN Journal. DOI: 10.2139/ssrn.3415726.

Ball, Desmond (2011): China's cyber warfare capabilities. In: Security Challenges 7 (2), S. 81–103.

Balmforth, Tom; Tsvetkova, Maria (2022): Russia takes down REvil hacking group at U.S. request – FSB. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/technology/russia-arrests-dismantles-revil-hacking-group-us-request-report-2022-01-14/, zuletzt aktualisiert am 14.01.2022, zuletzt geprüft am 24.01.2022.

Banse, Dirk (2009): Putins Konjunkturprogramm: Russische Agenten spionieren deutsche Energie-Unternehmen aus. Hg. v. Welt. Online verfügbar unter https://www.welt.de/wams_print/article3965455/Putins-Konjunkturprogramm-Russische-Agenten-spionieren-deutsche-Energie-Unternehmen-aus.html, zuletzt aktualisiert am 21.06.2009, zuletzt geprüft am 06.05.2021.

Bar, Tomer; Conant, Simon (2016): Infy Malware Active In Decade of Targeted Attacks. Hg. v. Palo Alto Networks. Online verfügbar unter https://unit42.paloaltonetworks.com/prince-of-persia-infy-malware-active-in-decade-of-targeted-attacks/, zuletzt aktualisiert am 02.05.2016, zuletzt geprüft am 01.09.2021.

Baram, Gil (2017): Israeli defense in the age of cyber war. In: Middle East Quarterly, S. 1–10.

Baram, Gil; Sommer, Udi (2019): Covert or not Covert: National Strategies During Cyber Conflicts. In: T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga und G. Visky (Hg.): 11th International Conference on Cyber Conflict: Silent Battle. Tallinn: NATO CCD COE Publications, S. 197–212.

Barboza, David (2012): Family of Wen Jiabao Holds a Hidden Fortune in China. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2012/10/26/business/global/family-of-wen-jiabao-holds-a-hidden-fortune-in-china.html?pagewanted=all, zuletzt aktualisiert am 25.10.2012, zuletzt geprüft am 02.08.2021.

Bar-eli, Avi (2021): Israel exports arms endangering human rights because it serves our interests, top defense official admits. Hg. v. Haaretz. Online verfügbar unter https://www.haaretz.com/israel-news/.premium.HIGHLIGHT.MAGAZINE-israel-exported-arms-that-endangered-human-rights-top-defense-official-admits-1.10445867, zuletzt aktualisiert am 07.12.2021, zuletzt geprüft am 06.01.2022.

Barlow, John Perry (1996): A Declaration of the Independence of Cyberspace. Hg. v. Electronic Frontier Foundation. Davos. Online verfügbar unter https://www.eff.org/cyberspace-independence, zuletzt aktualisiert am 07.04.2018, zuletzt geprüft am 09.06.2020.

Barnes, Julian E.; Gibbons-Neff, Thomas (2019): U.S. Carried Out Cyberattacks on Iran. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html, zuletzt aktualisiert am 22.06.2019, zuletzt geprüft am 03.01.2022.

Barr, Luke; Margolin, Josh (2022): DHS warns of Russian cyberattack on US if it responds to Ukraine invasion. Hg. v. ABC News. Online verfügbar unter https://abcnews.go.com/Politics/dhs-warns-russian-cyberattack-us-responds-ukraine-invasion/story?id=82441727, zuletzt aktualisiert am 24.01.2022, zuletzt geprüft am 10.02.2022.

Barrett, Brian (2018): How China's Elite APT10 Hackers Stole the World's Secrets. Hg. v. Wired. Online verfügbar unter https://www.wired.com/story/doj-indictment-chinese-hackers-apt10/?redirectURL=https%3A%2F%2Fwww.wired.com%2Fstory%2Fdoj-indictment-chinese-hackers-apt10%2F, zuletzt aktualisiert am 20.12.2018, zuletzt geprüft am 17.06.2021.

Barry, Rob; Volz, Dustin (2019): Ghosts in the Clouds: Inside China's Major Corporate Hack. Hg. v. Wall Street Journal. Online verfügbar unter https://robbarry.org/assets/pdfs/Ghosts%20in%20the%20Clouds.pdf, zuletzt aktualisiert am 30.12.2019, zuletzt geprüft am 29.12.2021.

Bar-Siman-Tov, Yaacov (1984): The strategy of war by proxy. In: Cooperation and Conflict 19 (4), S. 263–273.

Bartholomew, Brian; Guerrero-Saade, Juan Andres (2016): Wave your flags! Deception tactics muddying attribution in targeted attacks. q. Hg. v. Virus Bulletin Conference.

Bartlett, Jason (2020): Exposing the Financial Footprints of North Korea's Hackers. Hg. v. Center for a new Amercian Security. Online verfügbar unter https://www.cnas.org/publications/reports/exposing-the-financial-footprints-of-north-koreas-hackers , zuletzt aktualisiert am 18.11.2020, zuletzt geprüft am 08.02.2021.

Bättig, Michèle B.; Bernauer, Thomas (2009): National institutions and global public goods: are democracies more cooperative in climate change policy? In: International Organization, S. 281–308.

Baumgartner, Kurt; Garnaeva, Maria (2014): BE2 custom plugins, router abuse, and target profiles. Hg. v. Securelist. Kaspersky. Online verfügbar unter https://securelist.com/be2-custom-plugins-router-abuse-and-target-profiles/67353/, zuletzt aktualisiert am 03.11.2014, zuletzt geprüft am 18.04.2021.

BBC (2012): ›Hacking attacks‹ hit Russian political sites. Hg. v. BBC. Online verfügbar unter https://www.bbc.com/news/technology-16032402?print=true, zuletzt aktualisiert am 08.03.2012, zuletzt geprüft am 04.05.2021.

BBC (2016): Chinese hackers turn to ransomware. Hg. v. BBC. Online verfügbar unter https://www.bbc.com/news/technology-35811777, zuletzt aktualisiert am 15.03.2016, zuletzt geprüft am 17.06.2021.

Beaumont, Peter (2016): US abstention allows UN to demand end to Israeli settlements. Hg. v. The Guardian, zuletzt aktualisiert am 23.12.2016, zuletzt geprüft am 05.01.2022.

Behar, Richard (2016): Inside Israel's Secret Startup Machine. Hg. v. Forbes. Online verfügbar unter https://www.forbes.com/sites/richardbehar/2016/05/11/inside-israels-secret-startup-machine/?sh=27c295f61a51, zuletzt aktualisiert am 30.05.2016, zuletzt geprüft am 11.10.2021.

Bejtlich, Richard (2014): DoJ Indicts Chinese Military Hackers: First Impressions. Hg. v. FireEye. Online verfügbar unter https://www.fireeye.com/blog/executive-perspective/2014/05/doj-indicts-chinese-military-hackers-first-impressions.html, zuletzt aktualisiert am 20.05.2014, zuletzt geprüft am 12.08.2021.

Bendiek, Annegret; Schulze, Matthias (2021): Attribution als Herausforderung für EU-Cybersanktionen. Hg. v. Stiftung Wissenschaft Und Politik. Online verfügbar unter https://www.swp-berlin.org/publikation/attribution-als-herausforderung-fuer-eu-cybersanktionen.

Ben-Eliezer, Uri (2001): From Military Role-Expansion to Difficulties in Peace-Making: The Israel Defense Forces 50 Years on.«. In: Military, State and Society in Israel: Theoretical and Comparative Perspective, S. 137–172.

Benjakob, Omer; Yaron, Oded (2021): Substantial majority of Jewish Israelis feel unregulated cyberarm sales are ›immoral‹. Hg. v. Haaretz. Online verfügbar unter https://www.haaretz.com/israel-news/tech-news/.premium-majority-of-jewish-israelis-feel-unregulated-cyberarm-sales-are-immoral-1.10102292, zuletzt aktualisiert am 09.08.2021, zuletzt geprüft am 03.01.2022.

Benjamin, Henry (2011): Radware – Cyber Soldiers. Hg. v. J-Wire. Online verfügbar unter https://www.jwire.com.au/radware-cyber-soldiers/, zuletzt aktualisiert am 27.11.2011, zuletzt geprüft am 11.10.2021.

Benn, Aluf (2009): Why isn't Netanyahu backing two-state solution? Hg. v. Haaretz. Online verfügbar unter https://www.haaretz.com/1.5081572, zuletzt aktualisiert am 01.03.2009, zuletzt geprüft am 05.01.2022.

Bennett, Andrew (2004): Case study methods: Design, use, and comparative advantages. In: Detlef F. Sprinz und Yael Wolinsky-Nahmias (Hg.): Models, numbers, and cases. Methods for studying international relations. [Nachdr.]. Ann Arbor, Mich.: Univ. of Michigan Press, S. 19–55.

Ben-Porat, Guy (2005): Netanyahu's second coming: A neoconservative policy paradigm? In: Israel Studies 10 (3), S. 225–245.

Berghel, Hal (2017): On the Problem of (Cyber) Attribution. In: Computer 50 (3), S. 84–89. DOI: 10.1109/MC.2017.74.

Bergman, Michael K. (2001): White Paper: The Deep Web: Surfacing Hidden Value. In: The Journal of Electronic Publishing 7 (1). DOI: 10.3998/3336451.0007.104.

Bergman, Ronen (2019): Rise and Kill First: The Secret History of Israel's Targeted Assassinations. New York: Random House.

Bergmann, Max; Cicarelli, Siena (2021): NATO's Financing Gap. Hg. v. Center for American Progress. Online verfügbar unter https://www.americanprogress.org/article/natos-financing-gap/, zuletzt aktualisiert am 13.01.2021, zuletzt geprüft am 02.01.2022.

Bettiza, Gregorio; Lewis, David (2020): Authoritarian Powers and Norm Contestation in the Liberal International Order: Theorizing the Power Politics of Ideas and Identity. In: Journal of Global Security Studies 5 (4), S. 559–577. DOI: 10.1093/jogss/ogz075.

Betts, Richard K. (2007): Two Faces of Intelligence Failure: September 11 and Iraq's Missing WMD. In: Political Science Quarterly 122 (4), S. 585–606. Online verfügbar unter http://www.jstor.org/stable/20202928.

Beuth, Patrick; Biermann, Kai; Klingst, Martin; Stark, Holger (2017): Bundestags-Hack: So wurde das deutsche Parlament ausspioniert. Hg. v. Die Zeit. Online verfügbar unter https://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland?utm_referrer=https%3A%2F%2Fwww.google.com%2F, zuletzt aktualisiert am 11.05.2017, zuletzt geprüft am 18.04.2021.

BfV (2019): BfV Cyber – Brief Nr. 01/2019. Hinweis auf aktuelle Angriffskampagne. Hg. v. Bundesamt für Verfassungsschutz (BfV). Online verfügbar unter http://docs.dpaq.de/15627-cyber-brief_nr-6_06-12-19.pdf, zuletzt geprüft am 25.06.2021.

Bhattacharya, Abanti (2019): Chinese Nationalism Under Xi Jinping Revisited. In: India Quarterly 75 (2), S. 245–252. DOI: 10.1177/0974928419841789.

Biasini, Nick; Chen, Michael; Karkins, Alex; Khodjibaev, Azim; Neal, Chris; Olney, Matt (2022): Comprehensive Threat Intelligence: Ukraine Campaign Delivers Defacement and Wipers, in Continued Escalation. Hg. v. Talos. Online verfügbar unter https://blog.talosintelligence.com/2022/01/ukraine-campaign-delivers-defacement.html, zuletzt aktualisiert am 04.02.2022, zuletzt geprüft am 10.02.2022.

Bing, Chris (2017a): Security firms sometimes wreck FBI investigations. Here's how. Hg. v. Cyberscoop. Online verfügbar unter https://www.cyberscoop.com/security-researchers-occasionally-disrupt-fbi-investigations-heres-how/, zuletzt aktualisiert am 03.04.2017, zuletzt geprüft am 12.08.2021.

Bing, Chris (2017b): Ukraine blames infamous Russian hackers for ›BadRabbit‹ ransomware attack. Hg. v. Cyberscoop. Online verfügbar unter https://www.cyberscoop.com/fancy-bear-bad-rabbit-ransomware-security-service-of-ukraine/, zuletzt aktualisiert am 02.11.2017, zuletzt geprüft am 01.01.2022.

Bing, Chris (2018): China's government is keeping its security researchers from attending conferences. Hg. v. Cyberscoop. Online verfügbar unter https://www.cyberscoop.com/pwn2own-chinese-researchers-360-technologies-trend-micro/, zuletzt aktualisiert am 08.03.2018, zuletzt geprüft am 25.10.2021.

Bing, Christopher (2021): White House blames Russian spy agency SVR for SolarWinds hack: statement. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/business/white-house-blames-russian-spy-agency-svr-solarwinds-hack-statement-2021-04-15/, zuletzt aktualisiert am 15.04.2021, zuletzt geprüft am 12.05.2021.

Bing, Christopher; Taylor, Marisa (2020): Exclusive: China-backed hackers ›targeted COVID-19 vaccine firm Moderna‹. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-health-coronavirus-moderna-cyber-excl-idUSKCN24V38M, zuletzt aktualisiert am 30.07.2020.

Bisson, David (2018): New Gallmaker Attack Group Using Living-off-the-Land Tactics in Espionage Campaign. Hg. v. Security Intelligence. Online verfügbar unter https://securityintelligence.com/news/new-gallmaker-attack-group-using-living-off-the-land-tactics-in-espionage-campaign/, zuletzt aktualisiert am 19.10.2018.

Bitton, Raphael (2016): In law we trust: the Israeli case of overseeing intelligence. In: Zachary K. Goldman und Samuel James Rascoff (Hg.): Global intelligence oversight. Governing security in the twenty-first century. New York: Oxford University Press, S. 141–174.

Blank, Stephen (2017): Cyber and Information War à la Russe. In: George Perkovich und Ariel E. Levite (Hg.): Understanding cyber conflict. 14 analogies. Washington, D.C.: Georgetown University Press, S. 81–98.

Bloomberg News (2012): Xi Jinping Millionaire Relations Reveal Fortunes of Elite. Hg. v. Bloomberg. Online verfügbar unter https://www.bloomberg.com/news/articles/2012-06-29/xi-jinping-millionaire-relations-reveal-fortunes-of-elite, zuletzt aktualisiert am 29.06.2012, zuletzt geprüft am 02.08.2021.

Bob, Yonah Jeremy (2016): Islamic Jihad cyber terrorist indicted for hacking IDF drones over Gaza. Hg. v. The Jerusalem Post. Online verfügbar unter https://www.jpost.com/Arab-Israeli-Conflict/Islamic-Jihad-cyber-terrorist-indicted-for-hacking-IDF-drones-over-Gaza-448936, zuletzt aktualisiert am 23.03.2016, zuletzt geprüft am 06.01.2022.

Bob, Yonah Jeremy (2021): New Shin Bet head: Ready to take on Iran, Israeli-Arab violence. Hg. v. The Jerusalem Post. Online verfügbar unter https://www.jpost.com/middle-east/iran-news/new-shin-bet-head-ready-to-take-on-iran-israeli-arab-violence-681866, zuletzt aktualisiert am 13.10.2021, zuletzt geprüft am 06.01.2022.

Bodeen, Christopher (2007): New Chinese spy chief an expert on commercial intelligence, monitoring group says. Hg. v. Taiwan News. Online verfügbar unter https://www.taiwannews.com.tw/en/news/512740, zuletzt aktualisiert am 31.08.2007, zuletzt geprüft am 31.07.2021.

Boehm, Dana Carver (2009): China's Failed War on Terror: Fanning the Flames of Uighur Separatist Violence. In: Berkeley J. Middle E. & Islamic L. 2, S. 61.

Boeke, Sergei; Broeders, Dennis (2018): The Demilitarisation of Cyber Conflict. In: Survival 60 (6), S. 73–90. DOI: 10.1080/00396338.2018.1542804.

Borger, Julian (2006): Neocons turn on Bush for incompetence over Iraq war. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/world/2006/nov/04/iraq.midterms2006, zuletzt aktualisiert am 04.11.2006, zuletzt geprüft am 26.08.2021.

Borghard, Erica D. (2021): Time to End the Dual Hat? Hg. v. Council on Foreign Relations. Online verfügbar unter https://www.cfr.org/blog/time-end-dual-hat, zuletzt aktualisiert am 03.02.2021, zuletzt geprüft am 24.08.2021.

Borghard, Erica D.; Lonergan, Shawn W. (2016): Can States Calculate the Risks of Using Cyber Proxies? In: Orbis 60 (3), S. 395–416. DOI: 10.1016/j.orbis.2016.05.009.

Borghard, Erica D.; Lonergan, Shawn W. (2017): The Logic of Coercion in Cyberspace. In: Security Studies 26 (3), S. 452–481. DOI: 10.1080/09636412.2017.1306396.

Borghard, Erica D.; Lonergan, Shawn W. (2018): What Do the Trump Administration's Changes to PPD-20 Mean for U.S. Offensive Cyber Operations? Hg. v. Council on Foreign Relations. Online verfügbar unter https://www.cfr.org/blog/what-do-trump-administrations-changes-ppd-20-mean-us-offensive-cyber-operations, zuletzt aktualisiert am 10.09.2018, zuletzt geprüft am 24.08.2021.

Borghard, Erica D.; Lonergan, Shawn W. (2019): Cyber Operations as Imperfect Tools of Escalation. In: Strategic Studies Quarterly 13 (3), S. 122–145.

Bowen, Andrew S. (2021): Russian Cyber Units. Hg. v. Congressional Research Service (In Focus, IF11718). Online verfügbar unter https://crsreports.congress.gov/product/pdf/IF/IF11718, zuletzt geprüft am 14.04.2021.

Bradbury, Danny (2019): FSB hackers drop files online. Hg. v. Naked Security. Online verfügbar unter https://nakedsecurity.sophos.com/2019/07/23/fsb-hackers-drop-files-online/, zuletzt aktualisiert am 23.07.2019, zuletzt geprüft am 20.05.2021.

Branigan, Tania (2009): China restores limited internet access after Urumqi violence. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/world/2009/jul/28/china-restores-limited-internet-access, zuletzt aktualisiert am 28.07.2009, zuletzt geprüft am 27.07.2021.

Branigan, Tania; Halliday, Josh (2011): China hits back over US claims of satellite hacking. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/technology/2011/oct/31/china-us-claims-satellite-hacking, zuletzt aktualisiert am 31.10.2011, zuletzt geprüft am 29.07.2021.

Brantly, Aaron F. (2014): Cyber Actions by State Actors: Motivation and Utility. In: International Journal of Intelligence and CounterIntelligence 27 (3), S. 465–484. DOI: 10.1080/08850607.2014.900291.

Breland, Ali (2018): Trump broadens attack on Silicon Valley companies. Hg. v. The Hill. Online verfügbar unter https://thehill.com/policy/technology/404042-trump-broadens-attack-on-silicon-valley-companies, zuletzt aktualisiert am 28.08.2018, zuletzt geprüft am 02.09.2021.

Bremmer, Ian; Charap, Samuel (2007): The siloviki in Putin's Russia: who they are and what they want. In: The Washington Quarterly 30 (1), S. 83–92.

Brenner, Susan W. (2007): At light speed: attribution and response to cybercrime/terrorism/warfare. In: Journal of Criminal Law and Criminology 97 (2), S. 379–475.

Brewster, Thomas (2016a): Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones With A Single Text. Hg. v. Forbes. Online verfügbar unter https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/?sh=355b22d63997, zuletzt aktualisiert am 26.08.2016, zuletzt geprüft am 26.10.2021.

Brewster, Thomas (2016b): Ukraine Claims Hackers Caused Christmas Power Outage. Hg. v. Forbes. Online verfügbar unter https://www.forbes.com/sites/thomasbrewster/2016/01/04/ukraine-power-out-cyber-attack/?sh=56bb54836fa8, zuletzt aktualisiert am 04.01.2016, zuletzt geprüft am 18.04.2021.

Brichta, Avraham (1998): The new premier-parliamentary system in Israel. In: The Annals of the American Academy of Political and Social Science 555 (1), S. 180–192.

Broadhurst, Rod; Grabosky, Peter (2005): Cyber-crime: The challenge in Asia. Hong Kong: Hong Kong University Press.

Broadhurst, Roderic; Grabosky, Peter; Alazab, Mamoun; Bouhours, Brigitte; Chon, Steve (2014): An analysis of the nature of groups engaged in cyber crime. In: International Journal of Cyber Criminology 8 (1), S. 1–20.

Bronk, Christopher; Tikk-Ringas, Eneken (2013): Hack or attack? Shamoon and the Evolution of Cyber Conflict. Hg. v. James A. Baker III Institute for Public Policy. Rice University. Online verfügbar unter https://scholarship.rice.edu/bitstream/handle/1911/92672/ITP-pub-WorkingPaper-ShamoonCyberConflict-020113.pdf?sequence=1, zuletzt aktualisiert am 2013, zuletzt geprüft am 03.06.2020.

Brooks, Risa (2021): Through the Looking Glass: Trump-Era Civil-Military Relations in Comparative Perspective. In: Strategic Studies Quarterly 15 (2).

Brosgol, Dan (2019): Passover 5779: In Every Generation. Hg. v. The Bedford Citizen. Online verfügbar unter https://www.thebedfordcitizen.org/2019/04/passover-5779-in-every-generation/, zuletzt aktualisiert am 18.04.2019, zuletzt geprüft am 03.01.2022.

Brown, Kerry; Bērziņa-Čerenkova, Una Aleksandra (2018): Ideology in the Era of Xi Jinping. In: Journal of Chinese Political Science 23 (3), S. 323–339. DOI: 10.1007/s11366-018-9541-z.

BSI (2021): Social Engineering – der Mensch als Schwachstelle. Hg. v. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html, zuletzt aktualisiert am 21.05.2021, zuletzt geprüft am 17.01.2022.

Buchanan, Ben (2017): The cybersecurity dilemma. Hacking, trust and fear between nations. New York, NY: Oxford University Press.

Buckley, Noah; Reuter, Ora John (2019): Performance Incentives under Autocracy: Evidence from Russia's Regions. In: Comparative Politics 51 (2), S. 239–266. DOI: 10.5129/001041519X15647434969894.

Bugos, Shannon (2019): U.S. Completes INF Treaty Withdrawal | Arms Control Association. Hg. v. Arms Control Association. Online verfügbar unter https://www.armscon

trol.org/act/2019-09/news/us-completes-inf-treaty-withdrawal, zuletzt aktualisiert am 09.2019, zuletzt geprüft am 06.10.2021.

Bukkvoll, Tor; Østensen, Åse G. (2020): The Emergence of Russian Private Military Companies: A New Tool of Clandestine Warfare. In: Special Operations Journal 6 (1), S. 1–17. DOI: 10.1080/23296151.2020.1740528.

Burnell, Peter (2006): Autocratic opening to democracy: why legitimacy matters. In: Third World Quarterly 27 (4), S. 545–562.

Butt, Ahsan I. (2019): Why did Bush go to war in Iraq? Hg. v. Aj Jazeera. Online verfügbar unter https://www.aljazeera.com/opinions/2019/3/20/why-did-bush-go-to-war-in-iraq, zuletzt aktualisiert am 20.03.2019, zuletzt geprüft am 01.09.2021.

Cabestan, Jean-Pierre (2009): China's foreign-and security-policy decision-making processes under Hu Jintao. In: Journal of Current Chinese Affairs 38 (3), S. 63–97.

Calabresi, Massimo (2017): The Secret History of an Election. In: TIME Magazine 190 (5), S. 32–39.

Calian (2020): The Breach Report – Issue 8. Hg. v. Calian. Online verfügbar unter https://www.calian.com/assets/downloads/The-Breach-Report-Issue-8-Scandalous-Hacking-Operation.pdf, zuletzt geprüft am 12.11.2021.

Canfil, Justin Key (2016): Honing Cyber Attribution. The Cyber Issue. In: Journal of International Affairs 70 (1), S. 217–226.

Canfil, Justin Key (2020): Outsourcing Cyber Power: Why Proxy Conflict in Cyberspace May No Longer Pay. Hg. v. SSRN. Online verfügbar unter https://ssrn.com/abstract=3611582, zuletzt geprüft am 27.04.2021.

Carmola, Kateri (2010): Private security contractors and new wars: risk, law, and ethics: Routledge.

Carnegie, Allison; Carson, Austin (2020): Secrets in Global Governance: Disclosure Dilemmas and the Challenge of International Cooperation: Cambridge University Press.

Carothers, Thomas (2007): US Democracy Promotion During and after Bush 2007. Hg. v. Carnegie Endowment for International Peace. Online verfügbar unter https://carnegieendowment.org/files/democracy_promotion_after_bush_final.pdf, zuletzt geprüft am 01.09.2021.

Carr, Jeffrey (2011): Inside cyber warfare. Mapping the cyber underworld. 2. Aufl. Sebastopol, CA: O'Reilly & Associates.

Carson, Austin; Yarhi-Milo, Keren (2017): Covert Communication: The Intelligibility and Credibility of Signaling in Secret. In: Security Studies 26 (1), S. 124–156. DOI: 10.1080/09636412.2017.1243921.

CBS News (2014): North Korea blames U.S. for Internet shutdown. Hg. v. CBS News. Online verfügbar unter https://www.cbsnews.com/news/north-korea-blames-u-s-for-internet-shutdown/, zuletzt aktualisiert am 27.12.2014, zuletzt geprüft am 08.09.2021.

CEIC (2021): China Foreign Direct Investment. Hg. v. CEIC. Online verfügbar unter https://www.ceicdata.com/en/indicator/china/foreign-direct-investment, zuletzt geprüft am 29.07.2021.

Cerulus, Laurens (2019): How Ukraine became a test bed for cyberweaponry. Unter Mitarbeit von Politico. Online verfügbar unter https://www.politico.eu/article/ukraine-cy

ber-war-frontline-russia-malware-attacks/, zuletzt aktualisiert am 14.02.2019, zuletzt geprüft am 16.04.2021.

CFR (2020): Cyber Operations Tracker. Hg. v. Council on Foreign Relations. Online verfügbar unter https://www.cfr.org/interactive/cyberoperations.

CFR (2021): Connect the Dots on State-Sponsored Cyber Incidents – Offensive cyber campaign against Georgia. Hg. v. Council on Foreign Relations. Online verfügbar unter https://microsites-live-backend.cfr.org/cyber-operations/offensive-cyber-campaign-against-georgia, zuletzt aktualisiert am 14.04.2021, zuletzt geprüft am 18.04.2021.

Chang, Wu-ueh; Chao, Chien-min (2009): Managing Stability in the Taiwan Strait: Non-Military Policy towards Taiwan under Hu Jintao. In: Journal of Current Chinese Affairs 38 (3), S. 98–118.

Chatzky, Andrew (2020): China's Massive Belt and Road Initiative. Hg. v. Council on Foreign Relations. Online verfügbar unter https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative, zuletzt aktualisiert am 28.01.2020, zuletzt geprüft am 04.08.2021.

Check Point (2021a): Check Point Company Overview. Hg. v. Check Point. Online verfügbar unter https://www.checkpoint.com/about-us/company-overview/#, zuletzt geprüft am 11.10.2021.

Check Point (2021b): Leadership. Hg. v. Check Point. Online verfügbar unter https://www.checkpoint.com/about-us/leadership/, zuletzt geprüft am 11.10.2021.

Chepikova, Ksenia; Leiße, Olaf (2010): Russlands simulierter Föderalismus: Regionalpolitik unter Putin und Medvedev. In: Osteuropa 60 (1), S. 15–25. Online verfügbar unter https://www.jstor.org/stable/44935441.

Cheravitch, Joe; Lilly, Bilyana (2020): Russia's Cyber Limitations in Personnel and Innovation, Their Potential Impact on Future Operations, and How NATO and Its Members Can Respond. In: A. Ertan, K. Floyd, P. Pernik und S. Stevens (Hg.): Cyber Threats and NATO 2030: Horizon Scanning and Analysis, S. 31–59.

Chernenko, Elena (2015): Terrorism, Ukraine and the American threat: the view from Russia. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/world/2015/jul/15/russia-terrorism-ukraine-america-putin, zuletzt aktualisiert am 15.07.2015, zuletzt geprüft am 12.05.2021.

Cheung, Tai Ming (2017): Xi Takes Charge: Implications of the 19th Party Congress for China's Future. Xi Jinping and the Remaking of Chinese Military Politics. 21st Century China Center. San Diego. Online verfügbar unter https://china.ucsd.edu/_files/2017_xi-briefing-web.pdf, zuletzt geprüft am 25.07.2021.

Chin, Josh (2017): Chinese Firm Behind Alleged Hacking Was Disbanded This Month. Hg. v. The Wall Street Journal. Online verfügbar unter https://www.wsj.com/articles/chinese-firm-behind-alleged-hacking-was-disbanded-this-month-1511881494, zuletzt aktualisiert am 29.11.2017, zuletzt geprüft am 29.06.2021.

China.org (2003): What Is »Three Represents« CPC Theory? Hg. v. China.org. Online verfügbar unter http://www.china.org.cn/english/zhuanti/3represents/68735.htm, zuletzt aktualisiert am 27.11.2003, zuletzt geprüft am 25.07.2021.

China.org (2006): Die 4. Tagung des 10. NVK und des 10. Landeskomitees der PKKCV findet feierlich statt. Hg. v. China.org. Online verfügbar unter http://german.china.o

rg.cn/politics/archive/lianghui06/txt/2006-03/10/content_2225597.htm, zuletzt aktualisiert am 14.12.2006, zuletzt geprüft am 27.07.2021.

Choi, Sung J.; Johnson, M. Eric; Lehmann, Christoph U. (2019): Data breach remediation efforts and their implications for hospital quality. In: Health services research 54 (5), S. 971–980. DOI: 10.1111/1475-6773.13203.

Cimpanu, Catalin (2016): Philippines Government Websites Hit by Massive DDoS Attacks, China Suspected. Hg. v. Softpedia. Online verfügbar unter https://news.softpedia.com/news/philippines-government-websites-hit-by-massive-ddos-attacks-china-suspected-506412.shtml#ixzz4EnloNxmF, zuletzt aktualisiert am 23.06.2021, zuletzt geprüft am 23.06.2021.

Cimpanu, Catalin (2019): In a first, Israel responds to Hamas hackers with an air strike. Hg. v. ZDnet. Online verfügbar unter https://www.zdnet.com/article/in-a-first-israel-responds-to-hamas-hackers-with-an-air-strike/, zuletzt aktualisiert am 05.05.2019, zuletzt geprüft am 13.10.2021.

Cimpanu, Catalin (2021a): China says a foreign spy agency hacked its airlines, stole passenger records. Hg. v. The Record. Online verfügbar unter https://therecord.media/china-says-a-foreign-spy-agency-hacked-its-airlines-stole-passenger-records/, zuletzt aktualisiert am 08.11.2021, zuletzt geprüft am 09.02.2022.

Cimpanu, Catalin (2021b): Japanese police say Tick APT is linked to Chinese military. Hg. v. The Record. Recorded Future. Online verfügbar unter https://therecord.media/japanese-police-say-tick-apt-is-linked-to-chinese-military/, zuletzt aktualisiert am 20.04.2021, zuletzt geprüft am 05.07.2021.

CISA (2018): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. Hg. v. Cybersecurity & Infrastructure Security Agency. Online verfügbar unter https://www.cisa.gov/uscert/ncas/alerts/TA18-074A, zuletzt aktualisiert am 16.03.2018, zuletzt geprüft am 01.01.2022.

CISA (2021): Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA) | CISA. Hg. v. Cybersecurity & Infrastructure Security Agency. Online verfügbar unter https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure, zuletzt aktualisiert am 01.10.2021, zuletzt geprüft am 01.10.2021.

Clark, David D.; Landau, Susan (2010): Untangling attribution. In: National Research Council (Hg.): Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. Washington, D.C.: The National Academies Press, S. 25–40.

Clayton, Mark (2012): Stealing US business secrets: Experts ID two huge cyber ›gangs‹ in China. Hg. v. The Christian Science Monitor. Online verfügbar unter https://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China, zuletzt aktualisiert am 14.09.2012, zuletzt geprüft am 02.07.2021.

Clayton, Mark (2013): Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage. Hg. v. The Christian Science Monitor. Online verfügbar unter https://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural

-gas-pipelines-vulnerable-to-sabotage, zuletzt aktualisiert am 27.02.2013, zuletzt geprüft am 25.05.2021.

ClearSky (2020): Operation ›Dream Job‹ Widespread North Korean Espionage Campaign. Hg. v. ClearSky. Online verfügbar unter https://www.clearskysec.com/operation-dream-job/, zuletzt aktualisiert am 13.08.2020, zuletzt geprüft am 12.02.2022.

ClearSky (2021): About ClearSky. Hg. v. ClearSky. Online verfügbar unter https://www.clearskysec.com/company/#block-0, zuletzt geprüft am 11.10.2021.

Cloherty, Jack; Thomas, Pierre (2014): ›Trojan Horse‹ Bug Lurking in Vital US Computers Since 2011. Hg. v. ABC News. Online verfügbar unter https://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476, zuletzt aktualisiert am 06.11.2014, zuletzt geprüft am 06.05.2021.

Clunan, Anne L. (2019): Russia's pursuit of great-power status and security. In: Roger E. Kanet (Hg.): Routledge Handbook of Russian Security. Milton: Routledge, S. 3–16.

Cohen, Stuart A. (2006): Changing Civil–Military Relations in Israel: Towards an Over-subordinate IDF? In: Israel Affairs 12 (4), S. 769–788. DOI: 10.1080/13533310600890091.

Cohen, Zachary (2020): US recently conducted cyber operation against Iran to protect election from foreign interference – CNNPolitics. Hg. v. CNN. Online verfügbar unter https://edition.cnn.com/2020/11/03/politics/us-cyber-operation-iran-election-interference/index.html, zuletzt aktualisiert am 03.11.2020, zuletzt geprüft am 06.10.2021.

Collier, David; Brady, Henry E.; Seawright, Jason (2004): Sources of Leverage in Casual Inference: Toward an Alternative View of Methodology. In: Henry E. Brady und David Collier (Hg.): Rethinking social inquiry. Diverse tools, shared standards. Lanham, Md.: Rowman & Littlefield, S. 229–266.

Collier, Kevin (2018): The Indictment Of North Korea For The Sony Hack Shows How Cybersecurity Has Evolved. Hg. v. BuzzFeed News. Online verfügbar unter https://www.buzzfeednews.com/article/kevincollier/the-indictment-of-north-korea-for-the-sony-hack-shows-how, zuletzt aktualisiert am 08.09.2018, zuletzt geprüft am 11.08.2021.

Collins, Sean; McCombie, Stephen (2012): Stuxnet: the emergence of a new cyber weapon and its implications. In: Journal of Policing, Intelligence and Counter Terrorism 7 (1), S. 80–91. DOI: 10.1080/18335330.2012.653198.

Connell, Michael; Vogler, Sarah (2017): Russia's Approach to Cyber Warfare. Hg. v. CNA. Online verfügbar unter https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf, zuletzt aktualisiert am März 2017, zuletzt geprüft am 10.06.2020.

Cooley, Alexander (2015): Countering Democratic Norms. Journal of Democracy, 26(3), 49–63. DOI: 10.1353/jod.2015.0049.

Cooper, Helene; Barnes, Julian E. (2021): U.S. Considers Warning Ukraine of a Russian Invasion in Real-Time. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2021/12/23/us/politics/russia-ukraine-military-biden.html, zuletzt aktualisiert am 23.12.2021, zuletzt geprüft am 13.01.2022.

Cooper, Cortez A., III (2018): PLA Military Modernization: Drivers, Force Restructuring, and Implications. Hg. v. RAND Corporation. Online verfügbar unter https://www.

rand.org/pubs/testimonies/CT488.html, zuletzt aktualisiert am 15.02.2018, zuletzt geprüft am 02.08.2021.

Copp, Tara (2019): The clash between Trump and his generals. Hg. v. Military Times. Online verfügbar unter https://www.militarytimes.com/news/your-military/2019/01/04/the-clash-between-trump-and-his-generals/, zuletzt aktualisiert am 04.01.2019, zuletzt geprüft am 30.08.2021.

Corbin, Kenneth (2013): Economic Impact of Cyber Espionage and IP Theft Hits U.S. Businesses Hard. Hg. v. CIO. Online verfügbar unter https://www.cio.com/article/2384269/economic-impact-of-cyber-espionage-and-ip-theft-hits-u-s--businesses-hard.html, zuletzt aktualisiert am 10.07.2013, zuletzt geprüft am 02.09.2021.

Cordey, Sean (2019): The Israeli Unit 8200 – An OSINT-based study: Trend Analysis. Unter Mitarbeit von Tim Prior, Myriam Dunn Cavelty und Andreas Wenger. Hg. v. ETH Zürich. Online verfügbar unter https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/389135/Cyber-Reports-2019-12-Unit-8200.pdf?sequence=1&isAllowed=y, zuletzt aktualisiert am 31.12.2019, zuletzt geprüft am 11.10.2019.

Corera, Gordon (2017): Cyber-attack: US and UK blame North Korea for WannaCry. Hg. v. BBC. Online verfügbar unter https://www.bbc.com/news/world-us-canada-42407488, zuletzt aktualisiert am 19.12.2017, zuletzt geprüft am 06.10.2021.

Corera, Gordon (2018): UK think tanks hacked by groups in China, cyber-security firm says. Hg. v. BBC. Online verfügbar unter https://www.bbc.com/news/uk-43172371, zuletzt aktualisiert am 26.02.2018, zuletzt geprüft am 17.06.2021.

Corera, Gordon (2019): Russian hackers cloak attacks using Iranian group. Hg. v. BBC. Online verfügbar unter https://www.bbc.com/news/technology-50103378, zuletzt aktualisiert am 21.10.2019.

Corera, Gordon (2020): Huawei: MPs claim ›clear evidence of collusion‹ with Chinese Communist Party. Hg. v. BBC. Online verfügbar unter https://www.bbc.com/news/technology-54455112, zuletzt aktualisiert am 08.10.2020, zuletzt geprüft am 04.08.2021.

Cormac, Rory; Aldrich, Richard J. (2018): Grey is the new black: covert action and implausible deniability. In: International Affairs 94 (3), S. 477–494.

Costello, John (2016): China's Intelligence Services and Espionage Operations. Hearing before the United States-China Economic and Security Review Commission. Hg. v. United States-China Economic and Security Review Commission. Online verfügbar unter https://www.uscc.gov/sites/default/files/transcripts/June%2009,%202016%20Hearing%20Transcript.pdf, zuletzt aktualisiert am 09.06.2016, zuletzt geprüft am 31.07.2021.

Costello, John; McReynolds, Joe (2018): China's strategic support force: A force for a new era. In: China Strategic Perspective 13.

Cox, Joseph (2018): Meet ›Intrusion Truth,‹ the Mysterious Group Doxing Chinese Intel Hackers. Hg. v. Vice. Online verfügbar unter https://www.vice.com/en/article/wjka84/intrusion-truth-group-doxing-hackers-chinese-intelligence, zuletzt aktualisiert am 21.08.2018, zuletzt geprüft am 29.06.2021.

Crawford, Emily (2013): Virtual Backgrounds: Direct Participation in Cyber Warfare. In: I/S: A Journal of Law and Policy for the Information Society 9 (1), S. 1–19. Online ver-

fügbar unter https://kb.osu.edu/bitstream/handle/1811/73306/1/ISJLP_V9N1_001.pdf, zuletzt geprüft am 18.05.2020.

Cristiano, Fabio (2021): Israel: Cyber Warfare and Security as National Trademarks of International Legitimacy. In: Scott N. Romaniuk und Mary Manjikian (Hg.): Routledge Companion to Global Cyber-Security Strategy. 1. Aufl.: Routledge. Online verfügbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3698972.

Cronin, Patrick (2021): How to Asymmetrically Out-Compete Xi Jinping's One Belt One Road Initiative. Hg. v. War on the Rocks. Online verfügbar unter https://warontherocks.com/2021/03/how-to-asymmetrically-out-compete-xi-jinpings-one-belt-one-road-initiative/, zuletzt aktualisiert am 02.03.2021, zuletzt geprüft am 04.08.2021.

CrowdStrike: 2015 Global Threat Report. Hg. v. Crowdstrike Intelligence Team. CrowdStrike. Online verfügbar unter https://go.crowdstrike.com/rs/281-OBQ-266/images/15GlobalThreatReport.pdf?_ga=2.262085646.2058489206.1618905672-118602449.1618212950, zuletzt geprüft am 20.04.2021.

CrowdStrike (2016): Bears in the Midst: Intrusion into the Democratic National Committee. Hg. v. CrowdStrike. Online verfügbar unter https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2016/2016.06.16.DNC/Bears%20in%20the%20Midst_%20Intrusion%20into%20the%20Democratic%20National%20Committee%20%C2%BB.pdf, zuletzt aktualisiert am 15.06.2016, zuletzt geprüft am 19.04.2021.

CrowdStrike (2020): Our Work with the DNC: Setting the record straight. Hg. v. CrowdStrike. Online verfügbar unter https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/, zuletzt aktualisiert am 05.06.2020, zuletzt geprüft am 14.04.2021.

CrowdStrike (2021a): Cozy Bear. Hg. v. CrowdStrike. Online verfügbar unter https://adversary.crowdstrike.com/adversary/cozy-bear/, zuletzt aktualisiert am 2021, zuletzt geprüft am 14.04.2021.

CrowdStrike (2021b): Venomous Bear. Hg. v. CrowdStrike. Online verfügbar unter https://adversary.crowdstrike.com/adversary/venomous-bear/, zuletzt aktualisiert am 07.04.2021, zuletzt geprüft am 14.04.2021.

Crowley, Michael (2020): Allies and Former U.S. Officials Fear Trump Could Seek NATO Exit in a Second Term. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2020/09/03/us/politics/trump-nato-withdraw.html, zuletzt aktualisiert am 03.09.2020, zuletzt geprüft am 06.10.2021.

Crowley, Michael; Glueck, Katie (2021): For Kamala Harris, an Influential Voice and a Decisive Vote. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2021/01/20/us/politics/kamala-harris-vice-president.html, zuletzt aktualisiert am 20.01.2021, zuletzt geprüft am 25.08.2021.

CSIS (2020): Significant Cyber Incidents. Hg. v. Center for Strategic and International Studies. Online verfügbar unter https://csis-prod.s3.amazonaws.com/s3fs-public/200108_Significant_Cyber_Events_List.pdf?aj4_VlDq2hSan2U8O5mS29Iurq3G1QKa.

Cyb3rsleuth (2013): Tracking Cybercrime. Hg. v. Cyb3rsleuth. Online verfügbar unter http://cyb3rsleuth.blogspot.com/search/label/Chinese%20Threats, zuletzt aktualisiert am 11.09.2013, zuletzt geprüft am 11.10.2021.

Cybereason (2022): About Dan Verton. Hg. v. Cybereason. Online verfügbar unter https://www.cybereason.com/blog/authors/dan-verton, zuletzt aktualisiert am 18.01.2022, zuletzt geprüft am 19.01.2022.

Cybereason Nocturnus (2021): Cybereason vs. DarkSide Ransomware. Hg. v. Cybereason. Online verfügbar unter https://www.cybereason.com/blog/cybereason-vs-darkside-ransomware, zuletzt aktualisiert am 01.04.2021, zuletzt geprüft am 02.01.2022.

da Conceição-Heldt, Eugénia; Mello, Patrick A. (2016): Two-Level Games in Foreign Policy Analysis. In: William R. Thompson (Hg.): Oxford research encyclopedias. Oxford.: Oxford University Press.

Daalder, Ivo H.; Lindsay, James M. (2003): America unbound: The Bush revolution in foreign policy: Brookings Institution Press.

Dahan, Michael (2013): Hacking for the Homeland: Patriotic Hackers versus Hacktivists. In: Douglas Hart (Hg.): CIW 2013 Proceedings of the 8th International Conference on Information Warfare and Security: ICIW 2013. ICIW 2013 Proceedings of the 8th International Conference on Information Warfare and Security: ICIW 2013: Academic Conferences Limited, S. 51–57, zuletzt geprüft am 15.05.2020.

Dark Reading (2017): FireEye Finds Russian Group APT28 Targeted Montenegro Government with Cyber Attacks. Hg. v. Dark Reading. Online verfügbar unter https://www.darkreading.com/threat-intelligence/fireeye-finds-russian-group-apt28-targeted-montenegro-government-with-cyber-attacks/d/d-id/1329060, zuletzt aktualisiert am 06.06.2017, zuletzt geprüft am 06.05.2021.

Dawisha, Karen (2015): Putin's kleptocracy: who owns Russia?: Simon and Schuster.

Debusmann, Bernd (2011): COLUMN – Goodbye to myth of Iran's ›mad mullahs‹? Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/usa-column-idINDEE7B80HN20111209, zuletzt aktualisiert am 09.12.2011, zuletzt geprüft am 03.01.2022.

Deibert, Ron (2015): Authoritarianism goes global: Cyberspace under siege. In: Journal of Democracy 26 (3), S. 64–78.

Deibert, Ronald J. (2009): The geopolitics of internet control: Censorship, sovereignty, and cyberspace. In: Routledge handbook of Internet politics, S. 323–336.

Delcour, Laure; Wolczuk, Kataryna (2015): Spoiler or facilitator of democratization?: Russia's role in Georgia and Ukraine. In: Democratization 22 (3), S. 459–478. DOI: 10.1080/13510347.2014.996135.

Demchak, Chris; Dombrowski, Peter (2013): Cyber Westphalia: Asserting state prerogatives in cyberspace. In: Georgetown Journal of International Affairs, S. 29–38.

Der Spiegel (2019): Benny Gantz: Hacker-Affäre torpediert Wahlkampf von Netanyahus ärgstem Widersacher. Hg. v. Der Spiegel. Online verfügbar unter https://www.spiegel.de/politik/ausland/israel-hacker-skandal-um-benjamin-netanyahus-gegner-benny-gantz-a-1258271.html, zuletzt aktualisiert am 17.03.2019, zuletzt geprüft am 05.01.2022.

Der Tagesspiegel (2021): Wegen Unterdrückung der Uiguren in Xinjiang: EU und USA verhängen Sanktionen gegen China – Vergeltung aus Peking folgt prompt. Hg. v. Der Tagesspiegel. Online verfügbar unter https://www.tagesspiegel.de/politik/wegen-unterdrueckung-der-uiguren-in-xinjiang-eu-und-usa-verhaengen-sankt

ionen-gegen-china-vergeltung-aus-peking-folgt-prompt/27027594.html, zuletzt aktualisiert am 22.03.2021, zuletzt geprüft am 27.07.2021.

Desai, Padma (2005): Russian retrospectives on reforms from Yeltsin to Putin. In: Journal of Economic Perspectives 19 (1), S. 87–106.

Deuber, Lea; Krüger, Paul-anton (2021): China und USA: Konfrontation um Taiwan. Hg. v. Süddeutsche Zeitung. Online verfügbar unter https://www.sueddeutsche.de/politik/china-usa-taiwan-militaeruebung-1.5187636, zuletzt aktualisiert am 28.01.2021, zuletzt geprüft am 30.07.2021.

Deutsche Welle (2008a): Chinas Kampf gegen die Uiguren. Hg. v. Deutsche Welle. Online verfügbar unter https://www.dw.com/de/chinas-kampf-gegen-die-uiguren/a-3245545, zuletzt aktualisiert am 11.04.2008, zuletzt geprüft am 27.07.2021.

Deutsche Welle (2008b): Medwedew nimmt Stellung zur Zukunft Russlands. Deutsche Welle (www.dw.com). Online verfügbar unter https://www.dw.com/de/medwedew-nimmt-stellung-zur-zukunft-russlands/a-3087458, zuletzt aktualisiert am 24.01.2008, zuletzt geprüft am 19.05.2021.

Deutsche Welle (2018): Niederlande vereiteln Cyber-Attacke russischer Spione auf OPCW. Deutsche Welle. Online verfügbar unter https://www.dw.com/de/niederlande-vereiteln-cyber-attacke-russischer-spione-auf-opcw/a-45751523, zuletzt aktualisiert am 04.10.2018, zuletzt geprüft am 12.05.2021.

Deutsche Welle (2020): Alexei Navalny dupes FSB agent into admitting role in poisoning. Deutsche Welle. Online verfügbar unter https://www.dw.com/en/alexei-navalny-dupes-fsb-agent-into-admitting-role-in-poisoning/a-56013446, zuletzt aktualisiert am 21.12.2020, zuletzt geprüft am 29.04.2021.

Deyermond, Ruth (2013): Assessing the reset: successes and failures in the Obama administration's Russia policy, 2009–2012. In: European Security 22 (4), S. 500–523. DOI: 10.1080/09662839.2013.777704.

Diamond, Jeremy (2016): Donald Trump: ›I'm afraid the election's going to be rigged‹ – CNNPolitics. Hg. v. CNN. Online verfügbar unter https://edition.cnn.com/2016/08/01/politics/donald-trump-election-2016-rigged/index.html, zuletzt aktualisiert am 03.08.2016, zuletzt geprüft am 27.09.2021.

Div, Lior (2018): Cybereason named Israel's most promising startup. Hg. v. Cyberreason. Online verfügbar unter https://www.cybereason.com/blog/calcalist-israel-most-proming-startup, zuletzt aktualisiert am 19.04.2018, zuletzt geprüft am 07.10.2021.

DoD (2020): Military and Security Developments involving the People's Republic of China 2020. Hg. v. Office of the Secretary of Defence (Annual Report to Congress). Online verfügbar unter https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF, zuletzt geprüft am 31.07.2021.

DoJ (2014a): U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage. Hg. v. Department of Justice. Online verfügbar unter https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor, zuletzt aktualisiert am 22.07.2015, zuletzt geprüft am 23.11.2020.

DoJ (2014b): U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage. Hg. v.

Department of Justice. Online verfügbar unter https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor, zuletzt aktualisiert am 22.07.2015, zuletzt geprüft am 29.07.2021.

DoJ (2017): U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts. Hg. v. Department of Justice. Online verfügbar unter https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions, zuletzt aktualisiert am 21.03.2017, zuletzt geprüft am 15.04.2021.

DoJ (2018a): Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years. Hg. v. Department of Justice. Online verfügbar unter https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal, zuletzt aktualisiert am 05.11.2018, zuletzt geprüft am 31.07.2021.

DoJ (2018b): Indictment against GRU Officers. Hg. v. Department of Justice. Online verfügbar unter https://int.nyt.com/data/documenthelper/80-netyksho-et-al-indictment/ba0521c1eef869deecbe/optimized/full.pdf?action=click&module=Intentional&pgtype=Article, zuletzt aktualisiert am 13.07.2018, zuletzt geprüft am 20.08.2021.

DoJ (2018c): Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information. Hg. v. Department of Justice. Online verfügbar unter https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion, zuletzt aktualisiert am 20.12.2018, zuletzt geprüft am 29.06.2021.

DoJ (2018d): U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations. Hg. v. Department of Justice. Online verfügbar unter https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and, zuletzt aktualisiert am 04.10.2018, zuletzt geprüft am 06.10.2021.

DoJ (2020a): Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax. Hg. v. Department of Justice. Online verfügbar unter https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking, zuletzt aktualisiert am 13.02.2020, zuletzt geprüft am 04.08.2021.

DoJ (2020b): Seven International Cyber Defendants, Including »Apt41« Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally. Hg. v. Department of Justice. Online verfügbar unter https://www.justice.gov/opa/press-release/file/1317206/download, zuletzt aktualisiert am 16.09.2021, zuletzt geprüft am 14.11.2021.

DoJ (2020c): Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace: Unsealed Indictment. Hg. v. US Department of Justice. Online verfügbar unter https://www.justice.gov/opa/press-release/file/1328521/download, zuletzt aktualisiert am 15.10.2020, zuletzt geprüft am 18.04.2021.

DoJ (2020d): Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Con-

fidential Business Information, Including COVID-19 Research. Hg. v. Department of Justice. Online verfügbar unter https://www.justice.gov/opa/press-release/file/1295981/download, zuletzt aktualisiert am 22.07.2020, zuletzt geprüft am 01.07.2021.

DoJ (2021): Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research. Hg. v. Department of Justice. Online verfügbar unter https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion, zuletzt aktualisiert am 19.07.2021, zuletzt geprüft am 01.10.2021.

Dollar, David; Petri, Peter A. (2018): Why it's time to end the tit-for-tat tariffs in the U.S.-China trade war. Hg. v. Brookings. Online verfügbar unter https://www.brookings.edu/blog/order-from-chaos/2018/10/05/why-its-time-to-end-the-tit-for-tat-tariffs-in-the-u-s-china-trade-war/, zuletzt aktualisiert am 05.10.2018, zuletzt geprüft am 06.10.2021.

Dor, Ofir (2021): Palo Alto Networks founder Nir Zuk moves back to Israel. Hg. v. Globes. Online verfügbar unter https://en.globes.co.il/en/article-palo-alto-networks-founder-nir-zuk-moves-back-to-israel-1001364231, zuletzt aktualisiert am 16.03.2021, zuletzt geprüft am 11.10.2021.

Dorfman, Zach (2020a): China's Secret War for U.S. Data Blew American Spies' Cover. Hg. v. Foreign Policy. Online verfügbar unter https://foreignpolicy.com/2020/12/21/china-stolen-us-data-exposed-cia-operatives-spy-networks/, zuletzt aktualisiert am 21.12.2020, zuletzt geprüft am 16.06.2021.

Dorfman, Zach (2020b): How China's Tech Giants Like Alibaba, Tencent, and Baidu Aid Spy Agencies. Hg. v. Foreign Policy. Online verfügbar unter https://foreignpolicy.com/2020/12/23/china-tech-giants-process-stolen-data-spy-agencies/, zuletzt aktualisiert am 23.12.2020, zuletzt geprüft am 19.01.2022.

DoT (2018): Treasury Sanctions Russian Federal Security Service Enablers | U.S. Department of the Treasury. Hg. v. US Department of Treasury. Online verfügbar unter https://home.treasury.gov/news/press-releases/sm0410, zuletzt aktualisiert am 11.06.2018, zuletzt geprüft am 28.04.2021.

DoT (2019): Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware |. Hg. v. Department of the Treasury. Online verfügbar unter https://home.treasury.gov/news/press-releases/sm845, zuletzt aktualisiert am 05.12.2019, zuletzt geprüft am 15.04.2021.

DoT (2021): Treasury Sanctions Russia with Sweeping New Sanctions Authority. Hg. v. US Department of Treasury. Online verfügbar unter https://home.treasury.gov/news/press-releases/jy0127, zuletzt aktualisiert am 15.04.2021, zuletzt geprüft am 28.04.2021.

Doubek, James (2018): China Removes Presidential Term Limits, Enabling Xi Jinping To Rule Indefinitely. Hg. v. NPR. Online verfügbar unter https://www.npr.org/sections/thetwo-way/2018/03/11/592694991/china-removes-presidential-term-limits-enabling-xi-jinping-to-rule-indefinitely?t=1627206194175, zuletzt aktualisiert am 11.03.2018, zuletzt geprüft am 25.07.2021.

Duchâtel, Mathieu (2009): Hu Jintao and the People's Liberation Army. In: China Perspectives (3 (79)), S. 110–111. Online verfügbar unter http://www.jstor.org/stable/24054356.

Dudney, Robert S. (2011): Rise of the Cyber Militias. In: Air Force Magazine, S. 88–89.

Dumbrell, John (2018): The neoconservative roots of the war in Iraq. In: Intelligence and national security policymaking on Iraq: Manchester University Press, S. 19–39. Online verfügbar unter https://www.manchesterhive.com/view/9781526130969/9781526130969.00008.xml.

Easton, David (1975): A re-assessment of the concept of political support. In: British journal of political science 5 (4), S. 435–457.

ECPR (2017): China's »New Era« with Xi Jinping Characteristics. Hg. v. European Council on Foreign Relations (China Analysis). Online verfügbar unter https://ecfr.eu/wp-content/uploads/ECFR240_China_Analysis_Party_Congress_Ideology_2.pdf, zuletzt aktualisiert am 15.12.2017, zuletzt geprüft am 30.07.2021.

Egloff, Florian J. (2018): Cybersecurity and non-state actors: a historical analogy with mercantile companies, privateers, and pirates. University of Oxford. Online verfügbar unter https://ora.ox.ac.uk/objects/uuid:77eb9bad-ca00-48b3-abcf-d284c6d27571, zuletzt aktualisiert am 2018, zuletzt geprüft am 08.06.2020.

Egloff, Florian J. (2020a): Contested public attributions of cyber incidents and the role of academia. In: Contemporary Security Policy 41 (1), S. 55–81. DOI: 10.1080/13523260.2019.1677324.

Egloff, Florian J. (2020b): Public attribution of cyber intrusions. In: Journal of Cybersecurity 6 (1), Artikel tyaa012, S. 484. DOI: 10.1093/cybsec/tyaa012.

Egloff, Florian J.; Smeets, Max (2021): Publicly attributing cyber attacks: a framework. In: Journal of Strategic Studies, S. 1–32. DOI: 10.1080/01402390.2021.1895117.

Eichensehr, Kristen (2017): Public-private cybersecurity. In: Texas Law Review 95, S. 467–538.

Eichensehr, Kristen (2020): The Law & Politics of Cyberattack Attribution. In: UCLA Law Review 67.

Eichensehr, Kristen E. (2019): Decentralized Cyberattack Attribution. In: AJIL Unbound 113, S. 213–217. DOI: 10.1017/aju.2019.33.

Eiran, Ehud; Malin, Martin B. (2013): The Sum of all Fears: Israel's Perception of a Nuclear-Armed Iran. In: The Washington Quarterly 36 (3), S. 77–89.

Eoyang, Carson (1994): Models of Espionage. In: Theodore R. Sarbin, Ralph M. Carney und Carson Eoyang (Hg.): Citizen espionage. Studies in trust and betrayal. Westport, Conn.: Praeger, S. 69–92.

Epifanova, Alena (2020): Deciphering Russia's »Sovereign Internet Law«. Hg. v. DGAP. DGAP (DGAP Analysis, 2), zuletzt aktualisiert am 16.01.2020.

Erb, Guy; Sommers, Scott (2020): Still Losing Ground: The Consequences of the Trump Administration's Bilateral Trade Policy. Hg. v. Washington International Trade Association. Online verfügbar unter https://www.wita.org/blogs/losing-ground-trump-administrations-bilateral-trade/, zuletzt aktualisiert am 09.07.2020, zuletzt geprüft am 06.10.2021.

Ermert, Monika (2016): Last Formal Tie To Historic US Internet Control Is Cut – Intellectual Property Watch. Hg. v. Intellectual Property Watch. Online verfügbar

unter http://www.ip-watch.org/2016/10/01/last-formal-tie-to-historic-us-internet-control-is-cut/, zuletzt aktualisiert am 01.10.2016, zuletzt geprüft am 09.06.2021.

EURACTIV (2017): Merkel bekräftigt: »Ausspähen unter Freunden geht gar nicht«. Hg. v. EURACTIV. Online verfügbar unter https://www.euractiv.de/section/eu-innenpolitik/news/merkel-bekraeftigt-ausspaehen-unter-freunden-geht-gar-nicht/, zuletzt aktualisiert am 17.02.2017, zuletzt geprüft am 27.09.2021.

Fainberg, Sarah (2017): Russian Spetsnaz, contractors and volunteers in the Syrian conflict. In: IFRI Proliferation Papers (105), S. 1–27.

Farrell, Henry; Newman, Abraham L. (2019): Weaponized Interdependence: How Global Economic Networks Shape State Coercion. In: International Security 44 (1), S. 42–79. DOI: 10.1162/isec_a_00351.

Farwell, James P.; Rohozinski, Rafal (2011): Stuxnet and the future of cyber war. In: Survival 53 (1), S. 23–40.

Fearon, James D. (1995): Rationalist explanations for war. In: International Organization 49 (3), S. 379–414.

Feng, Chen (1998): Rebuilding the Party's Normative Authority: China's Socialist Spiritual Civilization Campaign. In: Problems of Post-Communism 45 (6), S. 33–41. DOI: 10.1080/10758216.1998.11655812.

Filippov, Gabor (2021): Hungary: Nations in Transit 2020 Country Report. Hg. v. Freedom House. Online verfügbar unter https://freedomhouse.org/country/hungary/nations-transit/2020, zuletzt aktualisiert am 26.04.2021, zuletzt geprüft am 26.04.2021.

Finch III, Raymond C. (2018): Vladimir Putin and the Russian Military. In: South Central Review 35 (1), S. 48–73.

Finkelstein, Norman H. (2005): Ariel Sharon. Minneapolis: Lerner Publications Company.

Finkle, Jim; Polityuk, Pavel (2018): U.S. seeks to take control of infected routers from hackers. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-cyber-routers-ukraine/cyber-firms-ukraine-warn-of-planned-russian-attack-id USKCN1IO1U9, zuletzt aktualisiert am 23.05.2018, zuletzt geprüft am 19.04.2021.

Finnemore, Martha; Hollis, Duncan B. (2016): Constructing norms for global cybersecurity. In: American Journal of International Law 110 (3), S. 425–479.

Finnemore, Martha; Sikkink, Kathryn (1998): International norm dynamics and political change. In: International Organization, S. 887–917.

FireEye (2009): In-Q-Tel Invests in FireEye to Advance Cyber Security in the U.S. Intelligence Community. Hg. v. FireEye. Online verfügbar unter https://investors.fireeye.com/index.php/news-releases/news-release-details/q-tel-invests-fireeye-advance-cyber-security-us-intelligence, zuletzt aktualisiert am 18.11.2009, zuletzt geprüft am 12.08.2021.

FireEye (2014): APT28: A Window into Russia's Cyber Espionage Operations? | FireEye. Hg. v. FireEye. Online verfügbar unter https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf, zuletzt geprüft am 19.04.2021.

FireEye (2015a): APT30 and the Mechanics. Of a Long-Running Cyber Espionage Operation. Online verfügbar unter https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf, zuletzt geprüft am 02.07.2021.

FireEye (2015b): Hiding in Plain Sight: FireEye and Microsoft Expose Chinese APT Group's Obfuscation Tactic | FireEye Inc. Hg. v. FireEye. Online verfügbar unter https://www.fireeye.com/blog/threat-research/2015/05/hiding_in_plain_sigh.html, zuletzt aktualisiert am 14.05.2015, zuletzt geprüft am 25.06.2021.

FireEye (2016): Red Line Drawn: China Recalculates its Use of Cyber Espionage. Hg. v. FireEye. Online verfügbar unter https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf, zuletzt geprüft am 04.08.2021.

FireEye (2017): APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat | FireEye Inc. Hg. v. FireEye. Online verfügbar unter https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html, zuletzt aktualisiert am 06.04.2017, zuletzt geprüft am 25.05.2021.

Fish, M. Steven (2017): What Is Putinism? In: Journal of Democracy 28 (4), S. 61–75. DOI: 10.1353/jod.2017.0066.

Fisher, Max (2015): Did a Congressman just acknowledge the US took down North Korea's internet in December? Hg. v. Vox. Online verfügbar unter https://www.vox.com/2015/3/17/8235831/north-korea-internet-hack, zuletzt aktualisiert am 18.03.2015, zuletzt geprüft am 08.09.2021.

Flade, Florian; Mascolo, Georg (2021): Umstrittene Firma in Israel: BKA kaufte Spionagesoftware bei NSO. Hg. v. Tagesschau. Online verfügbar unter https://www.tagesschau.de/investigativ/ndr-wdr/spionagesoftware-nso-bka-101.html, zuletzt aktualisiert am 07.09.2021, zuletzt geprüft am 20.10.2021.

Floyd, Garry S. (2018): Attribution and Operational Art. Implications for Competing in Time. In: Strategic Studies Quarterly 12 (2), S. 17–55.

Ford, Matt (2019): The Trump Organization's Hostile Takeover of the U.S. Government | The New Republic. Hg. v. The New Republic. Online verfügbar unter https://newrepublic.com/article/155000/trump-organizations-hostile-takeover-us-government, zuletzt aktualisiert am 10.09.2021, zuletzt geprüft am 26.08.2021.

Frankenberg, Sydney (2020): Data-Driven Diplomacy: China's Growing Surveillance Industrial Complex | Stanford Rewired. Hg. v. Rewired (Issue One). Online verfügbar unter https://stanfordrewired.com/post/china-surveillance, zuletzt aktualisiert am 11.08.2020, zuletzt geprüft am 31.07.2021.

Fraser, Nalani; Plan, Fred; O'Leary Jacqueline; Cannon, Vincent; Leong, Raymond; Perez, Dan; Shen, Chi-en (2019): APT41: A Dual Espionage and Cyber Crime Operation. Hg. v. FireEye. Online verfügbar unter https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html, zuletzt aktualisiert am 07.08.2019, zuletzt geprüft am 10.06.2021.

Fravel, M. Taylor (2015): China's New Military Strategy: ›Winning Informationized Local Wars‹. In: China Brief 15 (13), S. 3–7.

Freedman, Robert O. (2020a): Introduction to Israel in the Netanyahu era. In: Robert O. Freedman (Hg.): Israel Under Netanyahu: Domestic Politics and Foreign Policy: Routledge, S. 1–8.

Freedman, Robert O. (2020b): Israel and the United States: An uncertain Relationship. In: Robert O. Freedman (Hg.): Israel Under Netanyahu: Domestic Politics and Foreign Policy: Routledge, S. 135–160.

Freedom House (2019): Freedom in the World Countries. Hg. v. Freedom House. Online verfügbar unter https://freedomhouse.org/report/countries-world-freedom-2019.

F-Secure (2015): The Dukes. 7 Years of Russian Cyberespionage. Hg. v. F-Secure (Whitepaper). Online verfügbar unter https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf.

Fukuyama, Francis (2006): The end of history and the last man. New York: Simon and Schuster.

G Data (2014): Uroburos – hochkomplexe Spionagesoftware mit russischen Wurzeln. Hg. v. G Data (Red Paper). Online verfügbar unter https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf, zuletzt aktualisiert am Februar 2014, zuletzt geprüft am 14.04.2021.

Gady, Franz-Stefan (2015): New Snowden Documents Reveal Chinese Behind F-35 Hack. Hg. v. The Diplomat. Online verfügbar unter https://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/, zuletzt aktualisiert am 27.01.2015, zuletzt geprüft am 25.05.2021.

Galeotti, Mark (2015): Putin's Spies and Security Men: His Strongest Allies, His Greatest Weakness. In: Stephen Aris, Matthias Neumann, Robert Orttung, Jeronim Perović, Heiko Pleines, Hans-Henning Schröder und Aglaya Snetkov (Hg.): Russia and Regime Security: ETH Zurich (RUSSIAN ANALYTICAL DIGEST, 173), S. 8–10.

Galeotti, Mark (2016a): Hybrid, ambiguous, and non-linear? How new is Russia's ›new way of war‹? In: Small wars & insurgencies 27 (2), S. 282–301.

Galeotti, Mark (2016b): Putin's hydra: inside Russia's intelligence services. Hg. v. European Council on Foreign Relations (Policy Brief). Online verfügbar unter https://ecfr.eu/archive/page/-/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf, zuletzt geprüft am 10.12.2021.

Galeotti, Mark (2017): Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe. European Council on Foreign Relations. Online verfügbar unter https://www.ecfr.eu/publications/summary/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe, zuletzt geprüft am 10.06.2020.

Galeotti, Mark (2019): The mythical ›Gerasimov Doctrine‹ and the language of threat. In: Critical Studies on Security 7 (2), S. 157–161. DOI: 10.1080/21624887.2018.1441623.

Gallagher, Sean (2018): Ukraine detects new Pterodo backdoor malware, warns of Russian cyberattack. Hg. v. Ars Technica. Online verfügbar unter https://arstechnica.com/information-technology/2018/11/ukraine-detects-new-pterado-backdoor-malware-warns-of-russian-cyberattack/, zuletzt aktualisiert am 20.11.2018, zuletzt geprüft am 01.01.2022.

Gareis, Sven Bernhard (2013): Taking off as a Global Power? China's Foreign Policy »Grand Strategy«. Hg. v. George C. Marshall European Center for Security Studies. Online verfügbar unter https://www.marshallcenter.org/en/publications/occasional-papers/taking-global-power-chinas-foreign-policy-grand-strategy, zuletzt aktualisiert am April 2013, zuletzt geprüft am 27.07.2021.

Gartzke, Erik (2000): Preferences and the democratic peace. In: International Studies Quarterly 44 (2), S. 191–212.

Gartzke, Erik (2013): The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. In: International Security 38 (2), S. 41–73. DOI: 10.1162/ISEC_a_00136.

Gechlik, Mei (2017): Appropriate Norms of State Behavior in Cyberspace: Governance in China and Opportunities for US Businesses. Hoover Institution (Aegis Series Paper, 1706).

Geddes, Barbara (1999): What Do We Know About Democratization After Twenty Years? In: Annual Review of Political Science 2 (1), S. 115–144. DOI: 10.1146/annurev.polisci.2.1.115.

Geddes, Barbara; Wright, Joseph; Frantz, Erica (2014): Autocratic breakdown and regime transitions: A new data set. In: Perspectives on Politics 12 (2), S. 313–331.

Geers, Kenneth; Kindlund, Darien; Moran, Ned; Rachwald, Rob (2014): World War C: Understanding nation-state motives behind today's advanced cyber attacks. In: FireEye, Milpitas, CA, USA, Tech. Rep., Sep.

Geller, Eric (2020): DHS cyber chief out after debunking Trump's election claims. Hg. v. Politico. Online verfügbar unter https://www.politico.com/news/2020/11/17/trump-fires-dhs-cybersecurity-chief-who-led-election-defense-437174, zuletzt aktualisiert am 18.11.2020, zuletzt geprüft am 06.10.2021.

Gel'man, Vladimir (2008): Party Politics in Russia: From Competition to Hierarchy. In: Europe-Asia Studies 60 (6), S. 913–930. DOI: 10.1080/09668130802161165.

George, Alexander L.; Bennett, Andrew (2005): The method of structured, focused comparison. In: Case studies and theory development in the social sciences, S. 67–73.

Georgieva, Ilina (2020): The unexpected norm-setters: Intelligence agencies in cyberspace. In: Contemporary Security Policy 41 (1), S. 33–54.

Gerschewski, Johannes (2013): The three pillars of stability: Legitimation, repression, and co-optation in autocratic regimes. In: Democratization 20 (1), S. 13–38.

Gertz, Bill (2014a): Chinese Military Creates High-Level Cyber Intelligence Center. Hg. v. The Washington Free Bacon. Online verfügbar unter https://freebeacon.com/national-security/chinese-military-creates-high-level-cyber-intelligence-center/, zuletzt aktualisiert am 03.07.2014, zuletzt geprüft am 07.07.2021.

Gertz, Bill (2014b): New Chinese Intelligence Unit Linked to Massive Cyber Spying Program. Hg. v. The Washington Free Beacon. Online verfügbar unter https://freebeacon.com/national-security/new-chinese-intelligence-unit-linked-to-massive-cyber-spying-program/, zuletzt aktualisiert am 31.10.2014, zuletzt geprüft am 01.07.2021.

Gertz, Bill (2015): FBI Alert Reveals ›Groups‹ Behind OPM Hack. Hg. v. The Washington Free Bacon. Online verfügbar unter https://freebeacon.com/national-security/fbi-alert-reveals-groups-behind-opm-hack/, zuletzt aktualisiert am 10.06.2015, zuletzt geprüft am 12.11.2021.

Gertz, Bill (2016a): Chinese Military Revamps Cyber Warfare, Intelligence Forces. Hg. v. The Washington Free Beacon. Online verfügbar unter https://freebeacon.com/national-security/chinese-military-revamps-cyber-warfare-intelligence-forces/, zuletzt aktualisiert am 27.01.2016, zuletzt geprüft am 07.07.2021.

Gertz, Bill (2016b): Pentagon Links Chinese Cyber Security Firm to Beijing Spy Service. Hg. v. The Washington Free Beacon. Online verfügbar unter https://freebeacon.com/national-security/pentagon-links-chinese-cyber-security-firm-beijing-spy-service/, zuletzt aktualisiert am 29.11.2016, zuletzt geprüft am 29.06.2021.

Gierow, Hauke (2018): Chinese hackers are expected to put their country first. Hg. v. Merics. Online verfügbar unter https://merics.org/de/analyse/chinese-hackers-are-expected-put-their-country-first, zuletzt aktualisiert am 18.04.2018, zuletzt geprüft am 11.10.2021.

Gilens, Martin; Page, Benjamin I. (2014): Testing theories of American politics: Elites, interest groups, and average citizens. In: Perspectives on Politics 12 (3), S. 564–581.

Giles, Keir (2011): »Information Troops«-A Russian Cyber Command? In: Christian Czosseck, E. Tyugu und T. Wingfield (Hg.): 2011 3rd International Conference on Cyber Conflict. Tallinn, Estonia: CCD COE Publications, S. 45–60.

Giles, Keir (2012): Russia's public stance on cyberspace issues. 4th International Conference on Cyber Conflict (CYCON 2012). Tallinn.

Gilli, Andrea; Gilli, Mauro (2019): Why China has not caught up yet: military-technological superiority and the limits of imitation, reverse engineering, and cyber espionage. In: International Security 43 (3), S. 141–189.

Gleicher, Nathaniel (2020): Taking Action Against Hackers in Bangladesh and Vietnam. Hg. v. Meta. Online verfügbar unter https://about.fb.com/news/2020/12/taking-action-against-hackers-in-bangladesh-and-vietnam/amp/, zuletzt aktualisiert am 11.12.2020, zuletzt geprüft am 11.01.2022.

Göbel, Christian (2015): Why does China Have Internet? Contagion, contingency and strategy in China's ICT management. Hg. v. Christian Göbel. Wien. Online verfügbar unter https://christiangoebel.net/why-does-china-have-internet-contagion-contingency-and-strategy-in-chinas-ict-management-2, zuletzt aktualisiert am 20.10.2015.

Göbel, Christian; Ong, Lynette H. (2012): Social unrest in China. Hg. v. Europe China Research and Advice Network. London. Online verfügbar unter https://d1wqtxts1xzle7.cloudfront.net/34690494/ECRAN_Social_Unrest_in_China__Christian_Gobel_and_Lynette_H._Ong-with-cover-page-v2.pdf?Expires=1627399212&Signature=XDKNZJrXDpR4GA5ITZBDMTizVlMBiiUixQYEyx6pScBf9n~GT-X-BTv0q2MNX2AraAQCFn5ZlvjTrCAg4Jumq4jF30D-q9W4m8TbPvqwf43OFIIW0Jnflxw~3WwThoetuOCA0SL8sx3l~pc0z5PSmkmKhnGae2cBLtu4TYuJ1ZR2E9eRmBnhX7FBPJda8iIWFXA6smAEM-NZL9IVNAH6LC8f92lIGvLVToKgqaVFxpkyEDsvu8Y7lLUn8dmf~oHMDpKHFeOSqFPy8HappPsk6a40bZZzZwvsiiRpwVit6~ylmZ~1auH3u5AQSC57obKOhdaynLExY3wSvqn27nkZOA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA, zuletzt geprüft am 27.07.2021.

Goertz, Gary (2012): Social science concepts: A user's guide. Princeton, Oxford: Princeton University Press.

Goldberg, Giora (2006): The Growing Militarization of the Israeli Political System. In: Israel Affairs 12 (3), S. 377–394. DOI: 10.1080/13537120600744594.

Goldstein, Judith; Keohane, Robert O. (1993): Ideas and foreign policy: beliefs, institutions, and political change: Cornell University Press.

Gorwa, Robert; Smeets, Max (2019): Cyber Conflict in Political Science: A Review of Methods and Literature (Working Paper Prepared for the 2019 ISA Annual Convention). Online verfügbar unter https://osf.io/preprints/socarxiv/fc6sg/, zuletzt geprüft am 05.08.2021.

Goulard, Sebastien (2020): The Impact of the US–China Trade War on the European Union. In: Global Journal of Emerging Market Economies 12 (1), S. 56–68. DOI: 10.1177/0974910119896642.

Gould-Davies, Nigel (2016): Russia's Sovereign Globalization: Rise, Fall and Future. Hg. v. Chatham House. Online verfügbar unter https://www.chathamhouse.org/2016/01/russias-sovereign-globalization-rise-fall-and-future, zuletzt aktualisiert am 06.01.2016, zuletzt geprüft am 05.05.2021.

Gov.UK (2018): Joint statement from Prime Minister May and Prime Minister Rutte. Hg. v. Government UK. Online verfügbar unter https://www.gov.uk/government/news/joint-statement-from-prime-minister-may-and-prime-minister-rutte, zuletzt aktualisiert am 04.10.2018, zuletzt geprüft am 06.10.2021.

Government of Canada (2018): Canada identifies malicious cyber-activity by Russia. Hg. v. Government of Canada. Online verfügbar unter https://www.canada.ca/en/global-affairs/news/2018/10/canada-identifies-malicious-cyber-activity-by-russia.html, zuletzt aktualisiert am 04.10.2018, zuletzt geprüft am 06.10.2021.

Gowan, Richard (2020): China's pragmatic approach to UN peacekeeping. Hg. v. Brookings. Online verfügbar unter https://www.brookings.edu/articles/chinas-pragmatic-approach-to-un-peacekeeping/, zuletzt aktualisiert am 14.09.2020, zuletzt geprüft am 30.07.2021.

Graff, Garrett M. (2018): Robert Mueller's Indictment Today of 12 Russian Hackers Could Be His Biggest Move Yet. Hg. v. Wired. Online verfügbar unter https://www.wired.com/story/mueller-indictment-dnc-hack-russia-fancy-bear/, zuletzt aktualisiert am 13.07.2018, zuletzt geprüft am 19.04.2021.

Graham, Alex (2019): State of the Venture Capital Industry in 2019 (with Infographic). Hg. v. Toptal. Online verfügbar unter https://www.toptal.com/finance/venture-capital-consultants/state-of-venture-capital-industry-2019, zuletzt aktualisiert am 20.06.2019, zuletzt geprüft am 26.10.2021.

Grant, Charles (2012): Russia, China and global governance. London: Centre for European Reform.

Grauvogel, Julia; Soest, Christian von (2014): Claims to legitimacy count: Why sanctions fail to instigate democratisation in authoritarian regimes. In: Eur J Polit Res 53 (4), S. 635–653. DOI: 10.1111/1475-6765.12065.

Green, James A. (Hg.) (2016): Cyber warfare. A multidisciplinary analysis. London: Routledge, Taylor & Francis Group (Routledge studies in conflict, security and technology, 2016: 1).

Greenberg, Andy (2018): The untold story of NotPetya, the most devastating cyberattack in history. Hg. v. Wired. Online verfügbar unter https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/, zuletzt aktualisiert am 22.08.2018.

Greenberg, Andy (2019a): Russia's ›Sandworm‹ Hackers Also Targeted Android Phones. Hg. v. Wired. Online verfügbar unter https://www.wired.com/story/sandworm-android-malware/, zuletzt aktualisiert am 21.11.2019, zuletzt geprüft am 10.06.2021.

Greenberg, Andy (2019b): Sandworm. A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. First edition. New York: Doubleday.

Greene, Abner S. (1994): Checks and Balances in an Era of Presidential Lawmaking. In: The University of Chicago Law Review 61 (1), S. 123. DOI: 10.2307/1600091.

Grey Goose (2009): Project Grey Goose Phase II Report: The evolving state of cyber warfare. Hg. v. GreyLogic. Online verfügbar unter https://www.nytimes.com/1992/03/08/world/us-strategy-plan-calls-for-insuring-no-rivals-develop.html, zuletzt aktualisiert am 20.03.2009, zuletzt geprüft am 26.08.2021.

Griffith, Melissa K. (2018): Why Cyber Conflict as an Academic Discipline Struggles to Make Its Mark in Political Sciene. Hg. v. Council on Foreign Relations. Online verfügbar unter https://www.cfr.org/blog/why-cyber-conflict-academic-discipline-struggles-make-its-mark-political-science, zuletzt aktualisiert am 06.09.2018.

Groll, Elias (2016): New Evidence Strengthens Guccifer 2.0's Russian Connections. Hg. v. Foreign Policy. Online verfügbar unter https://foreignpolicy.com/2016/07/26/new-evidence-strengthens-guccifer-2-0s-russian-connections/, zuletzt aktualisiert am 26.07.2016, zuletzt geprüft am 20.08.2021.

Gschwend, Thomas; Schimmelfennig, Frank (2007): Forschungsdesign in der Politikwissenschaft: ein Dialog zwischen Theorie und Daten 11. Online verfügbar unter https://www.ssoar.info/ssoar/handle/document/25827.

Guarnieri, Claudio (2015): Digitaler Angriff auf den Bundestag: Investigativer Bericht zum Hack der IT-Infrastruktur der Linksfraktion. Hg. v. netzpolitik.org. Online verfügbar unter https://netzpolitik.org/2015/digitaler-angriff-auf-den-bundestag-investigativer-bericht-zum-hack-der-it-infrastruktur-der-linksfraktion/, zuletzt aktualisiert am 10.07.2018, zuletzt geprüft am 19.04.2021.

Gueorguiev, Dimitar; Shao, Li; Crabtree, Charles (2018): Blurring the Lines: Rethinking Self-Censorship under Autocracy. Online verfügbar unter https://www.researchgate.net/profile/Dimitar_Gueorguiev2/publication/321636833_Blurring_the_Lines_Rethinking_Censorship_Under_Autocracy/links/5b418be0458515f71cb11ffb/Blurring-the-Lines-Rethinking-Censorship-Under-Autocracy.pdf, zuletzt aktualisiert am 09.05.2018.

Guerrero-Saade, Juan Andres; Raiu, Costin (2017): Walking in your enemy's shadow: when fourth-party collection becomes attribution hell. Virus Bulletin Conference. Virus Bulletin, 2017. Online verfügbar unter https://www.virusbulletin.com/uploads/pdf/magazine/2017/VB2017-Guerrero-Saade-Raiu.pdf.

Guitton, Clement; Korzak, Elaine (2013): The Sophistication Criterion for Attribution. In: The RUSI Journal 158 (4), S. 62–68. DOI: 10.1080/03071847.2013.826509.

Gunitsky, Seva (2015): Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability. Perspectives on Politics, 13(1), 42–54. DOI: 10.1017/S1537592714003120.

Haas, Ernst B. (1980): Why collaborate? Issue-linkage and international regimes. In: World politics 32 (3), S. 357–405.

Haberman, Maggie; Martin, Jonathan (2021): After the Speech: What Trump Did as the Capitol Was Attacked. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2021/02/13/us/politics/trump-capitol-riot.html?, zuletzt aktualisiert am 13.02.2021, zuletzt geprüft am 26.08.2021.

Hacker, Jacob S.; Pierson, Paul (2010): Winner-take-all politics: How Washington made the rich richer–and turned its back on the middle class: Simon and Schuster.

Hacquebord, Feike; Remorin, Alfred (2020): Pawn Storm's Lack of Sophistication as a Strategy. Hg. v. Trend Micro. Online verfügbar unter https://www.trendmicro.com/en_us/research/20/l/pawn-storm-lack-of-sophistication-as-a-strategy.html, zuletzt aktualisiert am 17.12.2020, zuletzt geprüft am 20.04.2021.

Haizler, Omry (2017): The United States' cyber warfare history: Implications on modern cyber operational structures and policymaking. In: Cyber, Intelligence, and Security 1 (1), S. 31–45.

Halchin, Elaine (2015): The Intelligence Community and Its Use of Contractors: Congressional Oversight Issues. Hg. v. Congressional Research Service. Online verfügbar unter https://sgp.fas.org/crs/intel/R44157.pdf, zuletzt aktualisiert am 18.08.2015, zuletzt geprüft am 27.09.2021.

Hale, Henry E. (2011): The Myth of Mass Russian Support for Autocracy: The Public Opinion Foundations of a Hybrid Regime. In: Europe-Asia Studies 63 (8), S. 1357–1375. DOI: 10.1080/09668136.2011.601106.

Hall, Peter A. (2003): Aligning Ontology and Methodology in Comparative Research. In: James Mahoney und Dietrich Rueschemeyer (Hg.): Comparative Historical Analysis in the Social Sciences. Cambridge, UK and New York: Cambridge University Press, 373–404.

Hanna, Andrew (2019): The Invisible U.S.-Iran Cyber War. Hg. v. United States Institute of Peace. Online verfügbar unter https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war, zuletzt aktualisiert am 25.10.2019, zuletzt geprüft am 06.10.2021.

Hansel, Mischa; Mutschler, Max; Dickow, Marcel (2018): Taming cyber warfare: lessons from preventive arms control. In: Journal of Cyber Policy 3 (1), S. 44–60. DOI: 10.1080/23738871.2018.1462394.

Hansel, Mischa; Nanni, Sara (2018): Quantitative Rüstungsanalysen im Zeichen von Digitalisierung und Automatisierung. In: ZIB Zeitschrift für Internationale Beziehungen 25 (1), S. 211–220. DOI: 10.5771/0946-7165-2018-1-211.

Harding, Luke (2007): Putin, the Kremlin power struggle and the $40bn fortune. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/world/2007/dec/21/russia.topstories3, zuletzt aktualisiert am 21.12.2007, zuletzt geprüft am 12.05.2021.

Harding, Luke; Borger, Julian; Sabbagh, Dan (2021): Kremlin papers appear to show Putin's plot to put Trump in White House. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/world/2021/jul/15/kremlin-papers-appear-to-show-putins-plot-to-put-trump-in-white-house, zuletzt aktualisiert am 15.07.2021, zuletzt geprüft am 29.07.2021.

Harel, Amos; Levinson, Chaim (2021): After NSO blacklisting, Israel fears U.S. targeting all Israeli offensive cyber firms. Hg. v. Haaretz. Online verfügbar unter https://www.haaretz.com/israel-news/not-just-nso-israel-fears-u-s-targeting-all-israeli-offensive-cyber-firms-1.10463087, zuletzt aktualisiert am 14.12.2021, zuletzt geprüft am 03.01.2022.

Harel, Amos; Levinson, Chaim; Kubovich, Yaniv (2021): Israeli authorities inspect NSO Group offices after Pegasus revelations. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/news/2021/jul/29/israeli-authorities-inspect-

nso-group-offices-after-pegasus-revelations, zuletzt aktualisiert am 29.07.2021, zuletzt geprüft am 03.01.2022.

Harnisch, Sebastian (2018): Deutschlands Politik gegenüber der Belt-and-Road-Initiative der Volksrepublik China 2013–2018. In: ASIEN: The German Journal on Contemporary Asia (148), S. 26–50.

Harnisch, Sebastian (2021): Spreading Cyber-Autocracy? The Shanghai Cooperation Organization and the Diffusion of Norms of »Internet Sovereignty«. In: Marianne Kneuer und Thomas Demmelhuber (Hg.): Authoritarian gravity centers. A cross-regional study of authoritarian promotion and diffusion. New York, London: Routledge (Conceptualising comparative politics, 11), S. 249–274.

Harnisch, Sebastian; Friedrichs, Gordon (2017): Alliances Rebalanced? The Social Meaning of the US Pivot and Allies' Responses in Northeast Asia. In: The Korean Journal of International Studies 15 (1), S. 1–39.

Harnisch, Sebastian; Zettl, Kerstin; Steiger, Stefan (2021): Heidelberg Cyber Conflict Dataset (HD-CY.CON). Unter Mitarbeit von Sebastian Harnisch. Hg. v. Institut für Politische Wissenschaft, Universität Heidelberg. Online verfügbar unter https://heidata.uni-heidelberg.de/dataset.xhtml?persistentId=doi:10.11588/data/KDSFRB, zuletzt aktualisiert am 2021, zuletzt geprüft am 27.12.2021.

Harris, Shane (2008): China's cyber-militia. In: National Journal Magazine 31.

Harrison, Virginia; Palumbo, Daniele (2019): China anniversary: How the country became the world's ›economic miracle‹. Hg. v. BBC. Online verfügbar unter https://www.bbc.com/news/business-49806247, zuletzt aktualisiert am 01.10.2019, zuletzt geprüft am 25.07.2021.

Healey, Jason (2011): The Spectrum of National Responsibility for Cyberattacks. In: The Brown Journal of World Affairs 18 (1), S. 57–70. Online verfügbar unter http://www.jstor.org/stable/24590776.

Healey, Jason (2018): The State of the Field of Cyber Conflict. Hg. v. Council on Foreign Relations. Online verfügbar unter https://www.cfr.org/blog/state-field-cyber-conflict, zuletzt aktualisiert am 12.11.2018.

Healey, Jason; Jervis, Robert (2020): The Escalation Inversion and Other Oddities of Situational Cyber Stability. In: Texas National Security Review 3 (4).

Healey, Jason; Piiparinen, Anni (2015): Did China Just Hack the International Court Adjudicating Its South China Sea Territorial Claims? Hg. v. The Diplomat. Online verfügbar unter https://thediplomat.com/2015/10/did-china-just-hack-the-international-court-adjudicating-its-south-china-sea-territorial-claims/, zuletzt aktualisiert am 27.10.2015, zuletzt geprüft am 23.06.2021.

Healey, Jason; Wilson, A. J. (2012): Cyber Conflict and the War Powers Resolution: Congressional Oversight of Hostilities in the Fifth Domain. In: Georgetown Journal of International Affairs, S. 59–69. Online verfügbar unter http://www.jstor.org/stable/43134339.

Hefele, Peter; Merkle, David; Zhivkov, Sasha (2015): Mit Konfuzius nach Afrika. Wie Auswärtige Kulturpolitik Chinas Simme und Sicht der Welt vermitteln soll. Hg. v. Konrad-Adenauer-Stiftung (KAS Auslandsinformationen, 05/2015). Online verfügbar unter https://www.kas.de/c/document_library/get_file?uuid=789580c9-5ef9-4e63-5731-038d86272d10&groupId=252038, zuletzt geprüft am 27.07.2021.

Hegel, Tom (2018): Burning Umbrella. An Intelligence Report on the Winnti Umbrella and Associated State-Sponsored Attackers. Hg. v. ProtectWise 401TRG.

Heilmann, Sebastian (2018): Charakteristika des politischen Systems. Hg. v. Bundeszentrale für Politische Bildung (Dossier China). Online verfügbar unter https://www.bpb.de/internationales/asien/china/44270/charakteristika-des-politischen-systems, zuletzt aktualisiert am 07.09.2018, zuletzt geprüft am 09.07.2021.

Henriksen, Anders (2019): The end of the road for the UN GGE process: The future regulation of cyberspace. In: Journal of Cybersecurity 5 (1). DOI: 10.1093/cybsec/tyy009.

Henry, Laura A.; Sundstrom, Lisa McIntosh (2012): Russia's Climate Policy: International Bargaining and Domestic Modernisation. In: Europe-Asia Studies 64 (7), S. 1297–1322. DOI: 10.1080/09668136.2012.701388.

Herd, Graeme P. (2019): Putin's Operational Code and Strategic Decision-Making in Russia. In: Roger E. Kanet (Hg.): Routledge Handbook of Russian Security. Milton: Routledge, S. 17–29.

Herpig, Sven; Morgus, Robert; Sheniak, Amit (2020): Active Cyber Defense- A comparative study on US, Israeli and German approaches. Hg. v. Konrad-Adenauer-Stiftung. Online verfügbar unter https://www.kas.de/documents/263458/263507/Active+Cyber+Defense+-+A+comparative+study+on+US,+Israeli+and+German+approaches.pdf, zuletzt geprüft am 06.01.2022.

HIIK (2016): Conflict Barometer 2016. Hg. v. Heidelberger Institut für internationale Konfliktforschung. Heidelberg. Online verfügbar unter http://hiik.de/de/konfliktbarometer/pdf/ConflictBarometer_2016.pdf, zuletzt geprüft am 20.12.2020.

Hill, Fiona (2021): The Kremlin's Strange Victory: How Putin Exploits American Dysfunction and Fuels American Decline. Hg. v. Foreign Affairs. Online verfügbar unter https://www.foreignaffairs.com/articles/united-states/2021-09-27/kremlins-strange-victory?utm_medium=promo_email&utm_source=lo_flows&utm_campaign=registered_user_welcome&utm_term=email_1&utm_content=20211006, zuletzt aktualisiert am 27.09.2021, zuletzt geprüft am 06.10.2021.

Hjortdal, Magnus (2011): China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. In: JSS 4 (2), S. 1–24. DOI: 10.5038/1944-0472.4.2.1.

Hoang, Viet (2020): The Code of Conduct for the South China Sea: A Long and Bumpy Road. Hg. v. The Diplomat. Online verfügbar unter https://thediplomat.com/2020/09/the-code-of-conduct-for-the-south-china-sea-a-long-and-bumpy-road/, zuletzt aktualisiert am 28.09.2020, zuletzt geprüft am 02.08.2021.

Hoffman, Ronen (2019): Israel's foreign policy under Benjamin Netanyahu. In: Foreign Policy Research Institute 18.

Hoffman, Samantha; Mattis, Peter (2016): Managing the Power Within: China's State Security Commission. Hg. v. War on the Rocks. Online verfügbar unter https://warontherocks.com/2016/07/managing-the-power-within-chinas-state-security-commission/, zuletzt aktualisiert am 20.07.2016, zuletzt geprüft am 16.06.2021.

Holbig, Heike (2009): Remaking the CCP's Ideology: Determinants, Progress, and Limits under Hu Jintao. In: Journal of Current Chinese Affairs 38 (3), S. 35–61.

Holbig, Heike; Gilley, Bruce (2010): Reclaiming legitimacy in China. In: Politics & policy 38 (3), S. 395–422.

Holbig, Heike; Mittelstaedt, Jean Christopher; Sautin, Yevgen; Stanzel, Angela (2017): China's »New Era« with Xi Jinping characteristics. Hg. v. European Council on Foreign Relations. Online verfügbar unter https://ecfr.eu/wp-content/uploads/ECFR240_China_Analysis_Party_Congress_Ideology_2.pdf, zuletzt aktualisiert am 15.12.2017, zuletzt geprüft am 10.02.2022.

Holt, Alexander (2020): A brief history of US-China espionage entanglements. Hg. v. MIT Technology Review. Online verfügbar unter https://www.technologyreview.com/2020/09/03/1007609/trade-secrets-china-us-espionage-timeline/, zuletzt aktualisiert am 03.09.2020, zuletzt geprüft am 27.07.2021.

Homolar, Alexandra (2011): Rebels without a conscience: The evolution of the rogue states narrative in US security policy. In: European Journal of International Relations 17 (4), S. 705–727. DOI: 10.1177/1354066110383996.

Horchert, Judith (2017): Kaspersky-Chef: »Wir schützen unsere Kunden vor Malware – sei sie nun russisch oder amerikanisch«. Hg. v. Der Spiegel. Online verfügbar unter https://www.spiegel.de/netzwelt/netzpolitik/kaspersky-firmenchef-eugene-kaspersky-verteidigt-sich-gegen-anschuldigungen-a-1167916.html, zuletzt aktualisiert am 16.09.2017, zuletzt geprüft am 21.03.2020.

Hovet, Jason (2018): Czech security service says Russia behind cyber attacks on ministry. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-czech-security-russia-idUSKBN1O21BN, zuletzt aktualisiert am 03.12.2018, zuletzt geprüft am 14.04.2021.

Hsiao, Russell (2010): China's Cyber Command? Hg. v. Jamestown Foundation. Online verfügbar unter https://jamestown.org/program/chinas-cyber-command/, zuletzt aktualisiert am 18.09.2016, zuletzt geprüft am 05.07.2021.

Hsu, Kimberly; Murray, Craig; Wild, Matt (2013): China's 2012 Defense White Paper: The Diversified Employment of China's Armed Forces. Hg. v. U.S.-China Economic and Security Review Commission Staff Research Backgrounder. Online verfügbar unter https://www.uscc.gov/sites/default/files/Research/China%E2%80%99s%202012%20Defense%20White%20Paper--The%20Diversified%20Employment%20of%20China%E2%80%99s%20Armed%20Forces.pdf, zuletzt geprüft am 05.07.2021.

Huetteman, Emmarie (2017): Obama White House Knew of Russian Election Hacking, but Delayed Telling. Hg. v. The Straits Times. Online verfügbar unter https://www.nytimes.com/2017/06/21/us/politics/jeh-johnson-testimony-russian-election-hacking.html, zuletzt aktualisiert am 21.06.2017, zuletzt geprüft am 08.09.2021.

Hulcoop, Adam; Scott-Railton, John; Tanchak, Peter; Brooks, Matt; Deibert, Ron (2017): Tainted leaks: Disinformation and phishing with a Russian nexus. University of Toronto (Citizen Lab Research Report, 92).

Human Rights Watch (2007): World Report 2007. Hg. v. Human Rights Watch. Online verfügbar unter https://www.hrw.org/sites/default/files/reports/wr2007master.pdf, zuletzt geprüft am 27.07.2021.

Hummel, Philipp (2017): Wie kann die Politik Hackerangriffen entgehen? Hg. v. Spektrum. Online verfügbar unter https://www.spektrum.de/news/stecken-russische-hacker-hinter-den-angriffen-auf-politiker/1485839, zuletzt aktualisiert am 27.07.2017, zuletzt geprüft am 05.05.2021.

Hunnicutt, Trevor (2021): Biden orders probe of latest ransomware attack. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/technology/biden-says-uncertain-who-is-behind-latest-ransomware-attack-2021-07-03/, zuletzt aktualisiert am 04.07.2021, zuletzt geprüft am 05.07.2021.

Iasiello, Emilio (2016): China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities. In: JSS 9 (2), S. 45–69. Online verfügbar unter http://www.jstor.org/stable/26466776.

IISS (2021a): Cyber Power – Tier One. Hg. v. International Institute for Strategic Studies. Online verfügbar unter https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-one, zuletzt aktualisiert am 28.06.2021, zuletzt geprüft am 24.08.2021.

IISS (2021b): Cyber Power – Tier Two. Russia. Hg. v. International Institute for Strategic Studies. Online verfügbar unter https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-two, zuletzt aktualisiert am 28.06.2021, zuletzt geprüft am 04.08.2021.

IISS (2021c): Cyber Power – Tier Two: Israel. Hg. v. International Institute for Strategic Studies. Online verfügbar unter https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-two, zuletzt aktualisiert am 28.06.2021, zuletzt geprüft am 25.10.2021.

Ilievski, Aleksandar; Bernik, Igor (2016): Social-economic aspects of cybercrime. In: Peer-reviewed academic journal Innovative Issues and Approaches in Social Sciences 9 (3), S. 8–22.

Inbar, Efraim (2020): Israel's pivot from Europe to Asia. In: Robert O. Freedman (Hg.): Israel Under Netanyahu: Domestic Politics and Foreign Policy: Routledge, S. 242–261.

Insikt Group (2017a): North Korea's ruling elite are not isolated. Hg. v. Recorded Future. Online verfügbar unter https://www.recordedfuture.com/north-korea-internet-activity/, zuletzt aktualisiert am 25.07.2017, zuletzt geprüft am 08.06.2020.

Insikt Group (2017b): Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3. Hg. v. Recorded Future. Online verfügbar unter https://www.recordedfuture.com/chinese-mss-behind-apt3/, zuletzt aktualisiert am 03.03.2021, zuletzt geprüft am 01.07.2021.

Insikt Group (2018a): Chinese Threat Actor TEMP.Periscope Targets UK-Based Engineering Company Using Russian APT Techniques. Hg. v. Recorded Future. Online verfügbar unter https://www.recordedfuture.com/chinese-threat-actor-tempperiscope/, zuletzt aktualisiert am 13.01.2021, zuletzt geprüft am 01.07.2021.

Insikt Group (2018b): RedAlpha: New Campaigns Discovered Targeting the Tibetan Community. Hg. v. Recorded Future. Online verfügbar unter https://www.recordedfuture.com/redalpha-cyber-campaigns/, zuletzt aktualisiert am 26.06.2018, zuletzt geprüft am 25.06.2021.

Insikt Group (2021a): China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions. Hg. v. Recorded Future. Online verfügbar unter https://www.recordedfuture.com/redecho-targeting-indian-power-sector/, zuletzt aktualisiert am 17.06.2021, zuletzt geprüft am 04.08.2021.

Insikt Group (2021b): China's PLA Unit is Purchasing Foreign Antivirus Products. Hg. v. Recorded Future. Online verfügbar unter https://www.recordedfuture.com/china-p

la-unit-purchasing-antivirus-exploitation/, zuletzt aktualisiert am 05.05.2021, zuletzt geprüft am 05.07.2021.

Insikt Group (2021c): Chinese State-Sponsored Activity Group TAG-22 Targets Nepal, the Philippines, and Taiwan Using Winnti and Other Tooling. Hg. v. Recorded Future. Online verfügbar unter https://www.recordedfuture.com/chinese-group-tag-22-targets-nepal-philippines-taiwan/, zuletzt aktualisiert am 28.07.2021, zuletzt geprüft am 14.11.2021.

Insikt Group (2021d): Threat Activity Group RedFoxtrot Targets Bordering Asian Countries. Hg. v. Recorded Future. Online verfügbar unter https://www.recordedfuture.com/redfoxtrot-china-pla-targets-bordering-asian-countries/?__hstc=156209188.afd5a56f082997c45b3ad6c0258a1b38.1625493199219.1625493199219.1625493199219.1&__hssc=156209188.1.1625493199219&__hsfp=1762131360, zuletzt aktualisiert am 17.06.2021, zuletzt geprüft am 05.07.2021.

Interfax (2015): Putin's electoral rating reaches new high in late March. Hg. v. Russia Beyond. Online verfügbar unter https://www.rbth.com/news/2015/03/27/putins_electoral_rating_reaches_new_high_in_late_march_44819.html, zuletzt aktualisiert am 27.03.2015, zuletzt geprüft am 10.06.2021.

Interfax (2017): В Минобороны РФ создали войска информационных операций [Im RF-Verteidigungsministerium wurden Truppen für Informationsoperationen eingesetzt]. Hg. v. Interfax.ru. Online verfügbar unter https://www.interfax.ru/russia/551054, zuletzt aktualisiert am 22.02.2017, zuletzt geprüft am 27.04.2021.

Intrusion Truth (2017): APT3 is Boyusec, a Chinese Intelligence Contractor. Hg. v. Intrusion Truth. Online verfügbar unter https://intrusiontruth.wordpress.com/2017/05/09/apt3-is-boyusec-a-chinese-intelligence-contractor/, zuletzt aktualisiert am 10.05.2017, zuletzt geprüft am 29.06.2021.

Intrusion Truth (2018a): APT10 was managed by the Tianjin bureau of the Chinese Ministry of State Security. Hg. v. Intrusion Truth. Online verfügbar unter https://intrusiontruth.wordpress.com/2018/08/15/apt10-was-managed-by-the-tianjin-bureau-of-the-chinese-ministry-of-state-security/, zuletzt aktualisiert am 15.08.2018, zuletzt geprüft am 29.06.2021.

Intrusion Truth (2018b): The destruction of APT3. Hg. v. Intrusion Truth. Online verfügbar unter https://intrusiontruth.wordpress.com/2018/05/22/the-destruction-of-apt3/, zuletzt aktualisiert am 22.05.2018, zuletzt geprüft am 29.06.2021.

Intrusion Truth (2019a): APT17 is run by the Jinan bureau of the Chinese Ministry of State Security. Hg. v. Intrusion Truth. Online verfügbar unter https://intrusiontruth.wordpress.com/2019/07/24/apt17-is-run-by-the-jinan-bureau-of-the-chinese-ministry-of-state-security/, zuletzt aktualisiert am 09.07.2019, zuletzt geprüft am 29.06.2021.

Intrusion Truth (2019b): Encore! APT17 hacked Chinese targets and offered the data for sale. Hg. v. Intrusion Truth. Online verfügbar unter https://intrusiontruth.wordpress.com/2019/07/25/encore-apt17-hacked-chinese-targets-and-offered-the-data-for-sale/, zuletzt aktualisiert am 24.07.2019, zuletzt geprüft am 29.06.2021.

Intrusion Truth (2019c): Who is Mr Guo? Hg. v. Intrusion Truth. Online verfügbar unter https://intrusiontruth.wordpress.com/2019/07/17/who-is-mr-guo/, zuletzt aktualisiert am 11.07.2019, zuletzt geprüft am 29.06.2021.

Intrusion Truth (2020): APT40 is run by the Hainan department of the Chinese Ministry of State Security. Hg. v. Intrusion Truth. Online verfügbar unter https://intrusiontruth.wordpress.com/2020/01/16/apt40-is-run-by-the-hainan-department-of-the-chinese-ministry-of-state-security/, zuletzt aktualisiert am 16.01.2020, zuletzt geprüft am 30.06.2021.

Intrusion Truth (2021): An APT with no name. Hg. v. Intrusion Truth. Online verfügbar unter https://intrusiontruth.wordpress.com/2021/05/06/an-apt-with-no-name/, zuletzt aktualisiert am 06.05.2021, zuletzt geprüft am 20.01.2022.

Ip, Greg (2020): Checks and Balances Erode as Trump Flexes Power of the Purse. Hg. v. The Wall Street Journal. Online verfügbar unter https://www.wsj.com/articles/checks-and-balances-erode-as-trump-flexes-power-of-the-purse-11597237218, zuletzt aktualisiert am 12.08.2020, zuletzt geprüft am 26.08.2021.

IT Times (2020): Microsoft schluckt israelisches Cybersecurity-Startup CyberX. Hg. v. IT Times. Online verfügbar unter https://www.it-times.de/news/microsoft-schluckt-israelisches-cybersecurity-startup-cyberx-135743/, zuletzt aktualisiert am 22.06.2020, zuletzt geprüft am 03.11.2021.

Jabareen, Hassan; Bishara, Suhad (2019): The Jewish Nation-State Law. In: Journal of Palestine Studies 48 (2), S. 43–57.

Jabareen, Yousef (2018): The nation-state Law and Jewish supremacy. In: Palestine-Israel Journal of Politics, Economics, and Culture 23 (4), S. 16–22.

Jacobs, Ben (2016): Obama says he warned Russia to ›cut it out‹ over election hacking. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/us-news/2016/dec/16/barack-obama-final-press-conference-election-hacking, zuletzt aktualisiert am 16.12.2016, zuletzt geprüft am 11.02.2022.

Jain-Chandra, Sonali; Khor, Niny; Mano, Rui; Schauer, Johanna; Wingender, Philippe; Zhuang, Juzhong (2018): Inequality in China – Trends, Drivers and Policy Remedies. Hg. v. International Monetary Fund (IMF Working Papers, 127). Online verfügbar unter https://books.google.de/books?hl=de&lr=&id=vzBlDwAAQBAJ&oi=fnd&pg=PR4&dq=imf+working+paper+Inequality+in+China+%E2%80%93+Trends,+Drivers+and+Policy+Remedies&ots=2v8qD9s4TN&sig=T9ZARVBWbL7DDWsIe3xK3s1sDCQ, zuletzt geprüft am 25.07.2021.

Jasper, Scott (2021): Assessing Russia's role and responsibility in the Colonial Pipeline attack. Hg. v. Atlantic Council. Online verfügbar unter https://www.atlanticcouncil.org/blogs/new-atlanticist/assessing-russias-role-and-responsibility-in-the-colonial-pipeline-attack/, zuletzt aktualisiert am 01.06.2021, zuletzt geprüft am 09.06.2021.

Jerusalem Center for Public Affairs (2012): Poll: 77 Percent of Israelis See Iran Nukes as Existential Threat. In: Jerusalem Issue Briefs 12 (4). Online verfügbar unter https://jcpa.org/article/poll-77-percent-of-israelis-see-iran-nukes-as-existential-threat/, zuletzt geprüft am 03.01.2022.

Jervis, Robert (2017): 7. Why Intelligence and Policymakers Clash. In: Robert Jervis (Hg.): How Statesmen Think. The Psychology of International Politics. Princeton: Princeton University Press, S. 148–168.

Jinping, Xi (2018): 习近平在全国组织工作会议上的讲话_共产党员网 [Rede von Xi Jinping auf der National Organization Work Conference]. Hg. v. 12371.CN. Online

verfügbar unter http://www.12371.cn/2018/09/17/ARTI1537150840597467.shtml, zuletzt aktualisiert am 03.07.2018, zuletzt geprüft am 09.07.2021.

Ji-Young, Kong; Jong In, Lim; Kyoung Gon, Kim (2019): The All-Purpose Sword: North Korea's Cyber Operations and Strategies. In: Tomáš Minárik, Siim Alatalu, Stefano Biondi, Massimiliano Signoretti, Ihsan Tolga und Gabor Visky (Hg.): 2019 11th International Conference on Cyber Conflict (CyCon). Tallinn, Estonia: IEEE, S. 1–20.

Johnson, A. L. (2017): BadRabbit: New strain of ransomware hits Russia and Ukraine. Hg. v. Symantec. Online verfügbar unter https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=39104bd6-008d-46a9-bf29-b061c8ecc815&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments, zuletzt aktualisiert am 27.10.2017, zuletzt geprüft am 19.04.2021.

Jones, Jeff (2020): Confronting China's Efforts to Steal Defense Information. Hg. v. Belfer Center for Science and International Affairs. Online verfügbar unter https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information, zuletzt geprüft am 31.07.2021.

Jones, William C. (1985): The Constitution of the People's Republic of China. In: Washington University Law Review 63 (4), S. 707–735.

Joshi, Sahil (2020): Mega Mumbai power outage may be result of cyber attack, final report awaited. Hg. v. India Today. Online verfügbar unter https://www.indiatoday.in/india/story/mumbai-power-outage-malware-attack-1742538-2020-11-20, zuletzt aktualisiert am 20.11.2020, zuletzt geprüft am 23.06.2021.

Kaczmarski, Marcin (2016): The asymmetric partnership? Russia's turn to China. In: International Politics 53 (3), S. 415–434. DOI: 10.1057/ip.2016.7.

Kahl, Colin H. (1998): Constructing a separate peace: Constructivism, collective liberal identity, and democratic peace. In: Security Studies 8 (2–3), S. 94–144. DOI: 10.1080/09636419808429376.

Kahl, Jürgen (2001): Großer Sprung in die Globalisierung: China vor dem Beitritt zur WTO. In: Internationale Politik und Gesellschaft (4), S. 423–434. Online verfügbar unter https://library.fes.de/pdf-files/ipg/ipg-2001-4/artkahl.pdf, zuletzt geprüft am 25.07.2021.

Kailitz, Steffen (2013): Classifying political regimes revisited: legitimation and durability. In: Democratization 20 (1), S. 39–60. DOI: 10.1080/13510347.2013.738861.

Kaminska, Monica (2021): Restraint under conditions of uncertainty: Why the United States tolerates cyberattacks. In: Journal of Cybersecurity 7 (1), Artikel tyab008. DOI: 10.1093/cybsec/tyab008.

Kania, Elsa B.; Costello, John K. (2018): The strategic support force and the future of chinese information operations. In: The Cyber Defense Review 3 (1), S. 105–122.

Kannunikova, Tatiana (2021): Gil Shwed, Co-Founder & CEO of Check Point Software Technologies Ltd | Company & CEO Profile. Hg. v. Gadgets Reviews. Online verfügbar unter https://gadgets-reviews.com/company-ceo-profiles/5706-heck-point-software-technologies.html, zuletzt aktualisiert am 12.05.2021, zuletzt geprüft am 11.10.2021.

Kant, Immanuel (1795): Zum ewigen frieden. In: Ein philosophischer Entwurf.

Kaspersky (2018): A Slice of 2017 Sofacy Activity. Hg. v. Securelist. Kaspersky. Online verfügbar unter https://securelist.com/a-slice-of-2017-sofacy-activity/83930/, zuletzt aktualisiert am 20.02.2018.

Kastein, Julia (2020): Endspurt im US-Wahlkampf – Trumps Versprechen für den Rust Belt. Hg. v. Deutschlandfunk Kultur. Online verfügbar unter https://www.deutschlandfunkkultur.de/endspurt-im-us-wahlkampf-trumps-versprechen-fuer-den-rust.979.de.html?dram:article_id=485779, zuletzt aktualisiert am 15.10.2020, zuletzt geprüft am 27.09.2021.

Katz, Yaakov (2010): ›Stuxnet virus set back Iran's nuclear program by 2 years‹. Hg. v. The Jerusalem Post. Online verfügbar unter https://www.jpost.com/iranian-threat/news/stuxnet-virus-set-back-irans-nuclear-program-by-2-years, zuletzt aktualisiert am 15.12.2010.

Kelle, Udo (2014): Mixed Methods. In: Nina Baur und Jörg Blasius (Hg.): Handbuch Methoden der empirischen Sozialforschung: Springer, S. 153–166.

Kenyon, Miles (2018): The NSO connection to Jamal Khashoggi. Hg. v. The Citizen Lab. Online verfügbar unter https://citizenlab.ca/2018/10/the-nso-connection-to-jamal-khashoggi/, zuletzt aktualisiert am 24.10.2018, zuletzt geprüft am 26.10.2021.

Keohane, Robert O. (1984): After hegemony: Cooperation and discord in the world political economy. Princeton, Oxford: Princeton University Press.

Keohane, Robert O.; Martin, Lisa L. (1995): The promise of institutionalist theory. In: International Security 20 (1), S. 39–51.

Keohane, Robert O.; Nye, Joseph S. (1987): Power and Interdependence revisited. In: International Organization 41 (4), S. 725–753.

Keohane, Robert O.; Nye, Joseph S.; Zakaria, Fareed (2012): Power and interdependence. 4. ed. Boston: Longman (Longman classics in political science).

Keohane, Robert O.; Nye Jr, Joseph S. (1998): Power and interdependence in the information age. In: Foreign Affairs 77, S. 81.

Keohane, Robert Owen (2002): Power and governance in a partially globalized world. London, New York: Routledge. Online verfügbar unter http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=96854.

Khan, Muqtedar (2018): Israel: No More the ›Only Democracy in the Middle East‹. Hg. v. Center for Global Policy. Online verfügbar unter https://www.cgpolicy.org/articles/israel-no-longer-the-only-democracy-in-the-middle-east/.

Kharpal, Arjun (2018): A major factor behind the US-China trade war is winning at a $12 trillion technology – 5G. Hg. v. CNBC. Online verfügbar unter https://www.cnbc.com/2018/07/06/a-major-factor-behind-the-us-china-trade-war-is-winning-in-a-crucial-t.html, zuletzt aktualisiert am 06.07.2018, zuletzt geprüft am 06.10.2021.

King, Gary; Keohane, Robert O.; Verba, Sidney (1994): Designing social inquiry: Scientific inference in qualitative research: Princeton University Press.

King, Gary; Pan, Jennifer; Roberts, Margaret E. (2013): How censorship in China allows government criticism but silences collective expression. In: American Political Science Review 107 (2), S. 326–343.

King & Spalding (2015): U.S. Business Groups Urge Obama Administration To Address Chinese Cybersecurity Rules | JD Supra. Hg. v. JD Supra. Online verfügbar unter

https://www.jdsupra.com/legalnews/u-s-business-groups-urge-obama-11440/, zuletzt aktualisiert am 20.08.2015, zuletzt geprüft am 02.09.2021.

Kingsley, Patrick (2021): Israel Security Chief Warns Against Incitement of Conflict as Tensions Mount Before Key Vote. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2021/06/06/world/israel-security-chief-warning-incitement.html, zuletzt aktualisiert am 06.06.2021, zuletzt geprüft am 05.01.2022.

Kirchgaessner, Stephanie; Lewis, Paul; Pegg, David; Cutler, Sam; Lakhani, Nina; Safi, Michael (2021): Revealed: leak uncovers global abuse of cyber-surveillance weapon. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus, zuletzt aktualisiert am 18.07.2021, zuletzt geprüft am 26.10.2021.

Kirkpatrick, David D.; Mazzetti, Mark (2018): How 2 Gulf Monarchies Sought to Influence the White House. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2018/03/21/us/politics/george-nader-elliott-broidy-uae-saudi-arabia-white-house-influence.html?mtrref=undefined&auth=login-email, zuletzt aktualisiert am 21.03.2018, zuletzt geprüft am 06.10.2021.

Kjøllesdal, Kristian Aamelfot; Welle-Strand, Anne (2010): Foreign Aid Strategies: China Taking Over? In: Asian Social Science 6 (10). DOI: 10.5539/ass.v6n10p3.

Klare, Michael T. (1989): Subterranean alliances: America's global proxy network. In: Journal of International Affairs, S. 97–118.

Kleinsteiber, Meghan (2013): Nationalism and Domestic Politics as Drivers of Maritime Conflict. In: The SAIS Review of International Affairs 33 (2), S. 15–19. Online verfügbar unter https://www.jstor.org/stable/26995397.

Klimburg, Alexander (2011): Mobilising Cyber Power. In: Survival 53 (1), S. 41–60. DOI: 10.1080/00396338.2011.555595.

Knake, Robert K. (2010): Untangling attribution: Moving to accountability in cyberspace. Hg. v. Council on Foreign Relations (Prepared Statement before the Subcommittee on Technology and Innovation, Committee on Science and Technology, Hearing: Planning for the Future of Cyber Attack.).

Knop, Dirk (2022): Cybergang Conti: Interne Daten geleakt – 2,8 Milliarden US-Dollar erbeutet. Hg. v. Heise Online. Online verfügbar unter https://www.heise.de/news/Cybergang-Conti-Interne-Daten-geleakt-2-8-Milliarden-US-Dollar-erbeutet-6529035.html, zuletzt aktualisiert am 03.01.2022, zuletzt geprüft am 15.12.2022.

Knott, Stephen F. (2014): The CIA's Greatest Fear: Being Thrown Under the Bus by Congress…Again. Hg. v. The National Interest. Online verfügbar unter https://nationalinterest.org/feature/the-cia%E2%80%99s-greatest-fear-being-thrown-under-the-bus-by-11034, zuletzt aktualisiert am 08.08.2014, zuletzt geprüft am 11.01.2022.

Koshkin, Roman (2021): Israeli Military Construction: The Financial Aspect. In: New Defence Order Strategy 69 (4). Online verfügbar unter https://dfnc.ru/en/journal/2021-4-69/israeli-military-construction-the-financial-aspect/, zuletzt geprüft am 02.01.2022.

Kostyuk, Nadiya; Zhukov, Yuri M. (2019): Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? In: Journal of Conflict Resolution 63 (2), S. 317–347. DOI: 10.1177/0022002717737138.

Kotkin, Joel (2012): Despite the Great Recession, Obama's New Coalition of Elites Has Thrived. Hg. v. The Daily Beast. Online verfügbar unter https://www.thedailybeast.com/despite-the-great-recession-obamas-new-coalition-of-elites-has-thrived, zuletzt aktualisiert am 14.07.2017, zuletzt geprüft am 02.09.2021.

Kovacs, Eduard (2016): Attack on Swiss Defense Firm Linked to Turla Cyberspies. Hg. v. Securityweek. Online verfügbar unter https://www.securityweek.com/attack-swiss-defense-firm-linked-turla-cyberspies, zuletzt aktualisiert am 23.05.2016, zuletzt geprüft am 14.04.2021.

Krebs, Brian (2014): Hackers Plundered Israeli Defense Firms that Built ›Iron Dome‹ Missile Defense System – Krebs on Security. Hg. v. Krebs on Security. Online verfügbar unter https://krebsonsecurity.com/2014/07/hackers-plundered-israeli-defense-firms-that-built-iron-dome-missile-defense-system/, zuletzt aktualisiert am 28.07.2014, zuletzt geprüft am 25.05.2021.

Krebs, Brian (2015): Premera Blue Cross Breach Exposes Financial, Medical Records. Hg. v. Krebs on Security. Online verfügbar unter https://krebsonsecurity.com/2015/03/premera-blue-cross-breach-exposes-financial-medical-records/, zuletzt aktualisiert am 17.03.2015, zuletzt geprüft am 19.08.2021.

Krebs, Brian (2017): A Shakeup in Russia's Top Cybercrime Unit. Hg. v. Krebs on Security. Online verfügbar unter https://krebsonsecurity.com/2017/01/a-shakeup-in-russias-top-cybercrime-unit/, zuletzt aktualisiert am 28.01.2017, zuletzt geprüft am 06.05.2021.

Krebs, Brian (2022): Russia to Rent Tech-Savvy Prisoners to Corporate IT? Hg. v. Krebs on Security. Online verfügbar unter https://krebsonsecurity.com/2022/05/russia-to-rent-tech-savvy-prisoners-to-corporate-it/, zuletzt aktualisiert am 02.05.2022, zuletzt geprüft am 15.12.2022.

Krekel, Bryan (2009): Capability of the People's Republic of China to conduct cyber warfare and computer network exploitation. Northrop Grumman. Online verfügbar unter https://apps.dtic.mil/dtic/tr/fulltext/u2/a509000.pdf, zuletzt aktualisiert am 2009, zuletzt geprüft am 10.06.2020.

Kremlin.ru (2012): Заседание Совета по межнациональным отношениям [Sitzung des Rates für interethnische Beziehungen]. Hg. v. Kremlin.ru. Online verfügbar unter http://www.kremlin.ru/events/president/news/16292, zuletzt aktualisiert am 24.08.2012, zuletzt geprüft am 05.05.2021.

Kreps, Sarah; Schneider, Jacquelyn (2019): Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics. In: Journal of Cybersecurity 5 (1), Artikel tyz007. DOI: 10.1093/cybsec/tyz007.

Krumm, Reinhard (2010): Der Medwedew-Faktor. Russlands gewünschte Modernisierung. Hg. v. Friedrich-Ebert-Stiftung (Internationale Politikanalyse). Online verfügbar unter http://library.fes.de/pdf-files/id/ipa/07482.pdf, zuletzt aktualisiert am September 2010, zuletzt geprüft am 19.05.2021.

Kryshtanovskaya, Olga; White, Stephen (2003): Putin's militocracy. In: Post-Soviet Affairs 19 (4), S. 289–306.

Kshetri, Nir (2013): Cybercrimes in the Former Soviet Union and Central and Eastern Europe: current status and key drivers. In: Crime Law Soc Change 60 (1), S. 39–65. DOI: 10.1007/s10611-013-9431-4.

Kuhn, Johannes (2010): »Die Büchse der Pandora ist geöffnet«. Hg. v. Süddeutsche Zeitung. Online verfügbar unter https://www.sueddeutsche.de/digital/interview-zum-stuxnet-sabotagevirus-die-buechse-der-pandora-ist-geoeffnet-1.1005985, zuletzt aktualisiert am 03.10.2010, zuletzt geprüft am 26.08.2021.

Kuzio, Taras (2021): Five reasons why Ukraine rejected Vladimir Putin's »Russian World«. Hg. v. Atlantic Council. Online verfügbar unter https://www.atlanticcouncil.org/blogs/ukrainealert/five-reasons-why-ukraine-rejected-vladimir-putins-russian-world/, zuletzt aktualisiert am 26.03.2021, zuletzt geprüft am 06.05.2021.

Lacquement, Richard A. (2004): The casualty-aversion myth. In: Naval War College Review 57 (1), S. 38–58.

Lakshmanan, Ravie (2021): Ukraine Identifies Russian FSB Officers Hacking As Gamaredon Group. Hg. v. The Hacker News. Online verfügbar unter https://thehackernews.com/2021/11/ukraine-identifies-russian-fsb-officers.html, zuletzt aktualisiert am 10.02.2022, zuletzt geprüft am 05.11.2021.

Landler, Mark (2018): Trump Abandons Iran Nuclear Deal He Long Scorned. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2018/05/08/world/middleeast/trump-iran-nuclear-deal.html, zuletzt aktualisiert am 08.05.2018, zuletzt geprüft am 06.10.2021.

Laughlin, Shepherd (2008): Educational exchange between the United States and China. Hg. v. Institute of International Education (An IIE Briefing Paper), zuletzt geprüft am 05.07.2021.

Lebahn, Axel (2010): Modernisierer statt Marionette. Wie Dmitri Medwedew Russlands Politik sanft revolutioniert. In: Internationale Politik (September/Oktober). Online verfügbar unter https://internationalepolitik.de/system/files/article_pdfs/9_10_2010_Lebahn.pdf, zuletzt geprüft am 19.05.2021.

Lee, Heajune (2021): Strategic Publicity?: Understanding US Government Cyber Attribution. Stanford University. Online verfügbar unter https://stacks.stanford.edu/file/druid:py070wt8487/Lee_thesis.pdf, zuletzt geprüft am 08.02.2022.

Lee, John (2018): China's Trojan Ports. Hg. v. Hudson Institute. Online verfügbar unter https://www.hudson.org/research/14717-china-s-trojan-ports, zuletzt aktualisiert am 29.11.2018, zuletzt geprüft am 04.08.2021.

Lee, Robert (2016): The Problems with Seeking and Avoiding True Attribution to Cyber Attacks. Online verfügbar unter https://www.robertmlee.org/the-problems-with-seeking-and-avoiding-true-attribution-to-cyber-attacks/, zuletzt aktualisiert am 04.03.2016.

Lee, Yimou (2020): Taiwan says China behind cyberattacks on government agencies, emails. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-taiwan-cyber-china/taiwan-says-china-behind-cyberattacks-on-government-agencies-emails-idUSKCN25F0JK, zuletzt aktualisiert am 19.08.2020, zuletzt geprüft am 16.06.2021.

Legal Information Institute (2020): Separation of Powers and Checks and Balances. Hg. v. Cornell Law School. Online verfügbar unter https://www.law.cornell.edu/constitution-conan/article-1/section-1/separation-of-powers-and-checks-and-balances, zuletzt aktualisiert am 28.01.2020, zuletzt geprüft am 25.08.2021.

Legro, Jeffrey W. (1996): Culture and preferences in the international cooperation two-step. In: Am Polit Sci Rev 90 (1), S. 118–137.

Leiner, Barry M.; Cerf, Vinton G.; Clark, David D.; Kahn, Robert E.; Kleinrock, Leonard; Lynch, Daniel C. et al. (2009): A brief history of the Internet. In: ACM SIGCOMM Computer Communication Review 39 (5), S. 22–31.

Leipziger Volkszeitung (2018): Festakt im Alten Senatssaal – Konfuzius-Institut Leipzig feiert Zehnjähriges. Hg. v. Leipziger Volkszeitung. Online verfügbar unter https://www.lvz.de/Leipzig/Lokales/Konfuzius-Institut-Leipzig-feiert-Zehnjaehriges, zuletzt aktualisiert am 11.04.2018, zuletzt geprüft am 27.07.2021.

Levada (2021): Indicators. Putin's Approval Rating. Hg. v. Levada. Online verfügbar unter https://www.levada.ru/en/ratings/, zuletzt aktualisiert am 2021, zuletzt geprüft am 06.05.2021.

Levin, Dov H. (2020): Meddling in the Ballot Box: The Causes and Effects of Partisan Electoral Interventions: Oxford University Press.

Levitsky, Steven; Ziblatt, Daniel (2018): Wie Demokratien sterben. Und was wir dagegen tun können. München: Deutsche Verlags-Anstalt.

Levy, Ari (2021): Cybereason CEO told the world about DarkSide's hacking techniques from a bomb shelter in Israel. Hg. v. CNBC. Online verfügbar unter https://www.cnbc.com/2021/05/27/cybereason-ceo-was-in-israel-bomb-shelter-telling-world-about-darkside.html, zuletzt aktualisiert am 27.05.2021, zuletzt geprüft am 11.10.2021.

Levy, Jack S. (2008): Case studies: Types, designs, and logics of inference. In: Conflict Management and Peace Science 25 (1), S. 1–18.

Lewis, James (2011): Cyberwar Thresholds and Effects. In: IEEE Secur. Privacy Mag. 9 (5), S. 23–29. DOI: 10.1109/MSP.2011.25.

Lewis, James A. (2014): National perceptions of cyber threats. In: Strategic Analysis 38 (4), S. 566–576.

Lewis, Jason (2015): Cyber Espionage as a Component of Russian Modern Warfare. Hg. v. LookingGlass. Online verfügbar unter https://lookingglasscyber.com/blog/threat-intelligence-insights/operation-armageddon-cyber-espionage-as-a-strategic-component-of-russian-modern-warfare/, zuletzt aktualisiert am 28.04.2015, zuletzt geprüft am 01.01.2022.

Leyden, John (2013): APT1, that scary cyber-Cold War gang: Not even China's best. Hg. v. The Register. Online verfügbar unter https://www.theregister.com/2013/02/27/apt1_china_dark_visitor_b_team/, zuletzt aktualisiert am 27.02.2013, zuletzt geprüft am 14.11.2021.

Libicki, Martin C. (2018): Drawing Inferences from Cyber Espionage. In: T. Minárik, R. Jakschis und L. Lindström (Hg.): CyCon X: Maximising Effects. Tallinn: NATO CCD COE Publications (International Conference on Cyber Conflict, 10), S. 109–122.

Lijphart, Arend (2012): Patterns of democracy: Government forms and performance in thirty-six countries: Yale University Press.

Lim, Kheng Swe (2016): China's nationalist narrative of the South China Sea: A preliminary analysis. In: Enrico Fels und Truong-Minh Vu (Hg.): Power Politics in Asia's Contested Waters. Territorial Disputes in the South China Sea: Springer, S. 159–172.

Lin, Herbert (2016): From Soup to Nuts. Attribution of Malicious Cyber Incidents. In: Journal of International Affairs 70 (1), S. 75–137. Online verfügbar unter http://www.jstor.org/stable/90012598.

Lin, Herbert S. (2010): Offensive cyber operations and the use of force. In: Journal of National Security Law and Policy 4, S. 63–86.

Lindsay, Jon R. (2015): Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. In: Journal of Cybersecurity 1 (1), 53–67. DOI: 10.1093/cybsec/tyv003.

Lipman, Maria (2006): Putin's »Sovereign Democracy«. Hg. v. Carnegie Moscow Center – Carnegie Endowment for International Peace. Carnegie Moscow Center – Carnegie Endowment for International Peace. Online verfügbar unter https://carnegie.ru/2006/07/15/putin-s-sovereign-democracy-pub-18540, zuletzt aktualisiert am 15.07.2006, zuletzt geprüft am 05.05.2021.

Lipton, Eric; Sanger, David E.; Shane, Scott (2016): The Perfect Weapon: How Russian Cyberpower Invaded the U.S. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0, zuletzt aktualisiert am 13.12.2016, zuletzt geprüft am 20.08.2021.

Lloyd's Market Association (2021): Cyber War and Cyber Operation Exclusion Clauses. Hg. v. Lloyd's Market Association Bulletin. Online verfügbar unter https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx, zuletzt aktualisiert am 25.11.2021, zuletzt geprüft am 12.02.2022.

Lockheed Martin (2020): The Cyber Kill Chain. Hg. v. Lockheed Martin. Online verfügbar unter https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

Locks, Benjamin (2015): Asymmetric Warfare and the Third Offset – War on the Rocks. Hg. v. War on the Rocks. Online verfügbar unter https://warontherocks.com/2015/06/bad-guys-know-what-works-asymmetric-warfare-and-the-third-offset/, zuletzt aktualisiert am 23.06.2015, zuletzt geprüft am 01.09.2021.

Lohmann, Sarah (2018): Second Roundtable Looks at Role of Private Sector and Civil Society in Attribution – AICGS. Hg. v. American Institute for Contemporary German Studies. John Hopkins University. Online verfügbar unter https://www.aicgs.org/2018/06/second-roundtable-looks-at-role-of-private-sector-and-civil-society-in-attribution/, zuletzt aktualisiert am 28.06.2018, zuletzt geprüft am 18.Ma 2020.

Lohmann, Susanne (1997): Linkage Politics. In: Journal of Conflict Resolution 41 (1), S. 38–67. Online verfügbar unter http://www.jstor.org/stable/174486.

Lonergan, Erica D.; Lonergan, Shawn W. (2022): What do Russia's cyber moves mean for the Ukraine crisis? Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/politics/2022/01/12/what-do-russias-cyber-moves-mean-ukraine-crisis/, zuletzt aktualisiert am 12.01.2022, zuletzt geprüft am 13.01.2022.

Lonsdale, David J. (2019): We aren't in a cyber war – despite what Britain's top general thinks. Hg. v. The Conversation. Online verfügbar unter http://theconversation.com/we-arent-in-a-cyber-war-despite-what-britains-top-general-thinks-125578, zuletzt aktualisiert am 25.10.2019.

Lookout (2019): Monokle. The Mobile Surveillance Tooling of the Special Technology Center. Hg. v. Lookout (Security Research Report). Online verfügbar unter https://www.lookout.com/documents/threat-reports/lookout-discovers-monokle-threat-report.pdf?utm_source=BL&utm_medium=BL&utm_campaign=WW-MU-MU-MU-MU-P_NON-&utm_content=WP_Monokole%20.xml, zuletzt aktualisiert am Juli 2019.

Lösche, Peter (2008): Dossier USA. Hg. v. Bundeszentrale für Politische Bildung. Online verfügbar unter https://www.bpb.de/internationales/amerika/usa/10640/praesidial demokratie?p=all, zuletzt aktualisiert am 02.10.2008, zuletzt geprüft am 25.08.2021.

Lotrionte, Catherine (2014): Countering state-sponsored cyber economic espionage under international law. In: NCJ Int'l L. & Com. Reg. 40, S. 443.

Lupovici, Amir (2016): The »Attribution Problem« and the Social Construction of »Violence«: Taking Cyber Deterrence Literature a Step Forward. In: International Studies Perspectives 17, 322–342. DOI: 10.1111/insp.12082.

Lyngaas, Sean (2018): DOJ indictment spotlights China's civilian intel agency – and its hacker recruits. Hg. v. Cyberscoop. Online verfügbar unter https://www.cyberscoop.com/ministry-of-state-security-china-hacking-department-of-justice-indictment/, zuletzt aktualisiert am 01.11.2018, zuletzt geprüft am 30.06.2021.

MacAskill, Ewen (2005): George Bush: ›God told me to end the tyranny in Iraq‹. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/world/2005/oct/07/iraq.usa, zuletzt aktualisiert am 07.10.2005, zuletzt geprüft am 01.09.2021.

Machtiger, Peter (2020): The Latest GRU Indictment: A Failed Exercise in Deterrence. Hg. v. Just Security. Online verfügbar unter https://www.justsecurity.org/73071/the-latest-gru-indictment-a-failed-exercise-in-deterrence/, zuletzt aktualisiert am 29.10.2020, zuletzt geprüft am 20.08.2021.

Macias, Amanda (2020): Former cybersecurity chief says Russia, China, Iran and North Korea are trying to steal coronavirus vaccine IP. Hg. v. CNBC. Online verfügbar unter https://www.cnbc.com/2020/12/06/former-top-cybersecurity-chief-says-russia-china-iran-and-north-korea-are-trying-to-steal-coronoavir.html, zuletzt aktualisiert am 06.12.2020, zuletzt geprüft am 25.05.2021.

Magistretti, Bérénice (2017): Cybersecurity startup SentinelOne raises $70 million. Hg. v. Venture Beat. Online verfügbar unter https://venturebeat.com/2017/01/25/cybersecurity-startup-sentinelone-raises-70-million/, zuletzt aktualisiert am 25.01.2017, zuletzt geprüft am 03.11.2021.

Mahoney, James (2010): After KKV: The new methodology of qualitative research. In: World Pol 62, S. 120.

Makarin, Alexey (2019): Политический патриарх. Чего достиг и не достиг Кирилл за десять лет [Politischer Patriarch. Was Kyrill in zehn Jahren erreicht hat und was nicht]. Hg. v. Republic.ru. Online verfügbar unter https://republic.ru/posts/92948, zuletzt aktualisiert am 31.01.2019, zuletzt geprüft am 06.05.2021.

MANDIANT (2010): M-Trends. The Advanced Persistent Threat. Hg. v. Ryan Maness. Online verfügbar unter https://www2.fireeye.com/rs/fireye/images/PDF_MTrends_2010.pdf?mkt_tok=ODQ4LURJRCoyNDIAAAF-BTQAsGyLhrJemwrWOWxn9WjCCSlCipH5bPyPIGKwcu6YCacpq7YK5wqhilsvpj_tnTRGXXrbroP7mc1BAs3MIlRj7PUNiei8F1cnYVcaJoETOdY, zuletzt geprüft am 02.07.2021.

MANDIANT (2013): APT1: Exposing one of China's cyber espionage units. Hg. v. MANDIANT. Online verfügbar unter https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf, zuletzt aktualisiert am 19.02.2013, zuletzt geprüft am 25.05.2021.

Maness, Ryan; Valeriano, Brandon (2016a): Cyber spillover conflicts: transitions from cyber conflict to conventional foreign policy disputes? In: Karsten Friis und Jens Ringsmose (Hg.): Conflict in Cyber Space. Theoretical, Strategic and Legal Perspectives. London: Routledge, S. 45–64.

Maness, Ryan C.; Valeriano, Brandon (2016b): The Impact of Cyber Conflict on International Interactions. In: Armed Forces & Society 42 (2), S. 301–323. DOI: 10.1177/0095327X15572997.

Maness, Ryan C.; Valeriano, Brandon; Jensen, Benjamin (2019): Codebook for the Dyadic Cyber Incident and Campaign Dataset (DCID) Version 1.5. Online verfügbar unter http://www.brandonvaleriano.com/uploads/8/1/7/3/81735138/dcid_1.5_codebook.pdf, zuletzt aktualisiert am 01.06.2019.

Mangott, Gerhard (2012): Kommentar: Kampfrhetorik und »saubere Siege« Die ausgestreckte Hand Putins ist unabdingbar. Hg. v. Bundeszentrale für Politische Bildung. Online verfügbar unter https://www.bpb.de/internationales/europa/russland/analysen/135752/kommentar-kampfrhetorik, zuletzt aktualisiert am 11.05.2012, zuletzt geprüft am 29.04.2021.

Mankoff, Jeffrey (2014): Russia's latest land grab: How Putin won Crimea and lost Ukraine. In: Foreign Affairs (May/June), S. 60–68. Online verfügbar unter https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/fora93&ion=65.

Manutscharjan, Aschot L. (2017): Russlands Weg in die »postwestliche Welt«. In: Aus Politik und Zeitgeschichte 67 (21–22), S. 11–15.

Mao, Yexin (2021): Political institutions, state capacity, and crisis management: A comparison of China and South Korea. In: International Political Science Review (42), Artikel 3, 316–332.

Marczak, Bill; Anstis, Siena; Crete-Nishihata, Masashi; Scott-Railton, John; Deibert, Ron (2020): Stopping the Press: New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator – The Citizen Lab. Hg. v. The Citizen Lab. Online verfügbar unter https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/, zuletzt aktualisiert am 29.10.2020, zuletzt geprüft am 26.10.2021.

Marczak, Bill; Scott-Railton, John (2016): The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender – The Citizen Lab. Hg. v. The Citizen Lab. Online verfügbar unter https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/, zuletzt aktualisiert am 24.08.2016, zuletzt geprüft am 26.10.2021.

Maréchal, Nathalie (2017): Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy. In: MaC 5 (1), S. 29–41. DOI: 10.17645/mac.v5i1.808.

Maresca, Thomas (2014): Obama: Goal is not to ›contain‹ China. Hg. v. USA Today. Online verfügbar unter https://eu.usatoday.com/story/news/world/2014/04/28/obama

-philippines-china/8403801/, zuletzt aktualisiert am 28.04.2014, zuletzt geprüft am 02.08.2021.

Marks, Joseph (2019): The Cybersecurity 202: Russia's false flags in Winter Olympics cyberattack herald a more complicated future. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/10/21/the-cybersecurity-202-russia-s-false-flags-in-winter-olympics-cyberattack-herald-a-more-complicated-future/5dac9e2888e0fa3155a71266/, zuletzt aktualisiert am 17.07.2020, zuletzt geprüft am 18.04.2021.

Marks, Joseph (2020): The Cybersecurity 202: Chinese hackers could work for the government – or themselves. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/politics/2020/07/22/cybersecurity-202-chinese-hackers-could-work-government-or-themselves/, zuletzt aktualisiert am 22.07.2020, zuletzt geprüft am 01.07.2021.

Marks, Joseph (2022): The U.S.-Russia cyber relationship just got even more complicated. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/politics/2022/01/18/us-russia-cyber-relationship-just-got-even-more-complicated/, zuletzt aktualisiert am 18.01.2022, zuletzt geprüft am 24.01.2022.

Markus, Stanislav (2017): The Atlas That has Not Shrugged: Why Russia's Oligarchs are an Unlikely Force for Change. In: Daedalus 146 (2), S. 101–112.

Marquardt, Alex; Perez, Evan; Cohen, Zachary; Stracqualursi, Veronica (2020): Intel community's top election official: China and Iran don't want Trump to win reelection, Russia working to ›denigrate‹ Biden. Hg. v. CNN. Online verfügbar unter https://edition.cnn.com/2020/08/07/politics/2020-election-russia-china-iran/index.html, zuletzt aktualisiert am 08.08.2020, zuletzt geprüft am 07.01.2022.

Marshall, Alex (2016): From civil war to proxy war: past history and current dilemmas. In: Small wars & insurgencies 27 (2), S. 183–195. DOI: 10.1080/09592318.2015.1129172.

Marten, Kimberly (2017): The ›KGB State‹ and Russian Political and Foreign Policy Culture. In: The Journal of Slavic Military Studies 30 (2), S. 131–151. DOI: 10.1080/13518046.2017.1270053.

Marten, Kimberly (2019): Russia's use of semi-state security forces: the case of the Wagner Group. In: Post-Soviet Affairs 35 (3), S. 181–204. DOI: 10.1080/1060586X.2019.1591142.

Maschmeyer, Lennart; Deibert, Ronald J.; Lindsay, Jon R. (2020): A tale of two cybers – how threat reporting by cybersecurity firms systematically underrepresents threats to civil society. In: Journal of Information Technology & Politics, S. 1–20. DOI: 10.1080/19331681.2020.1776658.

Maschmeyer, Lennart; Kostyuk, Nadiya (2022): There Is No Cyber ›Shock and Awe‹: Plausible Threats in the Ukrainian Conflict. Hg. v. War on the Rocks. Online verfügbar unter https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/, zuletzt aktualisiert am 08.02.2022, zuletzt geprüft am 10.02.2022.

Mattes, Michaela; Rodríguez, Mariana (2014): Autocracies and International Cooperation. In: International Studies Quarterly 58 (3), S. 527–538. DOI: 10.1111/isqu.12107.

Mattingly, Daniel C. (2021): How the Party Commands the Gun: The Foreign-Domestic Threat Dilemma in China. Online verfügbar unter https://static1.squarespace.com/static/51cdc7e5e4b0d7474642bcb0/t/60f8809a47dddc167f011a3e/1626898586392/

Mattingly_PLA_Paper.pdf, zuletzt aktualisiert am 21.07.2021, zuletzt geprüft am 25.07.2021.

Mattis, Peter (2015a): A Guide to Chinese Intelligence Operations – War on the Rocks. Hg. v. War on the Rocks. Online verfügbar unter https://warontherocks.com/2015/08/a-guide-to-chinese-intelligence-operations/, zuletzt aktualisiert am 18.08.2015, zuletzt geprüft am 30.06.2021.

Mattis, Peter (2015b): Chen Wenqing: China's New Man for State Security. Hg. v. The National Interest. Online verfügbar unter https://nationalinterest.org/feature/chen-wenqing-china%E2%80%99s-new-man-state-security-14153, zuletzt aktualisiert am 23.10.2015, zuletzt geprüft am 25.07.2021.

Maull, Hanns W. (2022): Ukraine and Taiwan: two conflict zones with destabilizing potential. Hg. v. Merics. Online verfügbar unter https://merics.org/en/opinion/ukraine-and-taiwan-two-conflict-zones-destabilizing-potential, zuletzt aktualisiert am 04.02.2022, zuletzt geprüft am 10.02.2022.

Maurer, Tim (2011): Cyber norm emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security? Cambridge, Mass. (Discussion Paper, 2011–11).

Maurer, Tim (2016): ›Proxies‹ and Cyberspace. In: Journal of Conflict and Security Law 21 (3), S. 383–403. DOI: 10.1093/jcsl/krw015.

Maurer, Tim (2018a): Cyber Mercenaries. Cambridge: Cambridge University Press.

Maurer, Tim (2018b): Cyber Proxies and Their Implications for Liberal Democracies. In: The Washington Quarterly 41 (2), S. 171–188. DOI: 10.1080/0163660X.2018.1485332.

Mccrimmon, Ryan; Matishak, Martin (2021): Cyberattack on food supply followed years of warnings. Hg. v. Politico. Online verfügbar unter https://www.politico.com/news/2021/06/05/how-ransomware-hackers-came-for-americans-beef-491936, zuletzt aktualisiert am 05.06.2021, zuletzt geprüft am 02.09.2021.

McGuire, Michael (2021): Nation States, Cyberconflict and the Web of Profit. Hg. v. HP Threat Research. Online verfügbar unter https://threatresearch.ext.hp.com/web-of-profit-nation-state-report/.

McNamara, Luke (2021): The »Big Four«: Spotlight on Russia. Hg. v. FireEye. Online verfügbar unter https://www.fireeye.com/blog/executive-perspective/2021/04/the-big-four-spotlight-on-russia.html, zuletzt aktualisiert am 12.04.2021, zuletzt geprüft am 19.08.2021.

Mehrotra, Kartikay (2021): Microsoft Weighs Fixes to Code-Sharing Plan After Suspected Leak. Hg. v. Bloomberg. Online verfügbar unter https://www.bloomberg.com/news/articles/2021-04-27/microsoft-weighs-revamping-flaw-disclosures-after-suspected-leak, zuletzt aktualisiert am 27.04.2021, zuletzt geprüft am 02.07.2021.

Mell, Peter; Scarfone, Karen; Romanosky, Sasha (2007): A Complete Guide to the Common Vulnerability Scoring System. Version 2.0. FIRST.ORG, Inc. Online verfügbar unter https://www.first.org/cvss/v2/guide, zuletzt aktualisiert am 15.06.2019, zuletzt geprüft am 31.03.2020.

Melzer, Nils (2008): Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law. Hg. v. International Committee of the Red Cross. International Committee of the Red Cross. Genf. Online

verfügbar unter https://www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf, zuletzt geprüft am 18.05.2020.

Meng, Anne (2021): Winning the Game of Thrones: Leadership Succession in Modern Autocracies. In: Journal of Conflict Resolution 65 (5), S. 950–981.

Mercer, Andrew; Deane, Claudia; Mcgeeney, Kyley (2016): Why 2016 election polls missed their mark. Hg. v. Pew Research Center. Online verfügbar unter https://www.pewresearch.org/fact-tank/2016/11/09/why-2016-election-polls-missed-their-mark/, zuletzt aktualisiert am 09.11.2016, zuletzt geprüft am 08.09.2021.

Merkel, Wolfgang (1999): Die drei Demokratisierungswellen des 20. Jahrhunderts. In: Wolfgang Merkel (Hg.): Systemtransformation. Eine Einführung in die Theorie und Empirie der Transformationsforschung. Wiesbaden, s.l.: VS Verlag für Sozialwissenschaften (Beiträge zur Kenntnis des Rechtslebens, 2076), S. 173–184.

Merkel, Wolfgang (2004): Embedded and defective democracies. In: Democratization 11 (5), S. 33–58.

Merkley, Jeff; McGovern, James P. (2006): Ministry of Public Security Urges Use of »Strike Hard« to Counter Social Unrest. Hg. v. Congressional-Executive Commission on China. Online verfügbar unter https://www.cecc.gov/publications/commission-analysis/ministry-of-public-security-urges-use-of-strike-hard-to-counter, zuletzt aktualisiert am 22.05.2006, zuletzt geprüft am 27.07.2021.

Mesquita, Bruce Bueno de; Lalman, David (1990): Domestic Opposition and Foreign War. In: American Political Science Review 84 (3), S. 747–765. DOI: 10.2307/1962765.

Mesquita, Bruce Bueno de; Smith, Alastair; Siverson, Randolph M.; Morrow, James D. (2005): The logic of political survival: MIT press.

Meyer, Thomas (2009): Was ist Demokratie? Eine diskursive Einführung. Wiesbaden: VS Verlag für Sozialwissenschaften.

Meyers, Adam (2016): Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units. Hg. v. CrowdStrike. Online verfügbar unter https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/, zuletzt aktualisiert am 22.12.2016.

Michaels, Jon D. (2017): Trump and the »Deep State« The Government Strikes Back. In: Foreign Affairs 96 (5), S. 52–56. Online verfügbar unter http://www.jstor.org/stable/44821868.

Microsoft (2019): Government Security Program. Programmübersicht. Hg. v. Microsoft. Online verfügbar unter https://docs.microsoft.com/de-de/security/gsp/programoverview, zuletzt aktualisiert am 19.02.2019, zuletzt geprüft am 02.07.2021.

Microsoft Security (2021): HAFNIUM targeting Exchange Servers with 0-day exploits – Microsoft Security. Hg. v. Microsoft Security. Online verfügbar unter https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/, zuletzt aktualisiert am 26.03.2021, zuletzt geprüft am 25.05.2021.

Microsoft Threat Intelligence Center (2021): HAFNIUM targeting Exchange Servers with 0-day exploits. Hg. v. Microsoft Security. Online verfügbar unter https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/, zuletzt aktualisiert am 02.03.2021, zuletzt geprüft am 14.11.2021.

Militarist Monitor (2019): Projekt for the New American Century. Hg. v. Militarist Monitor. Online verfügbar unter https://militarist-monitor.org/profile/project_for_th

e_new_american_century/, zuletzt aktualisiert am 16.10.2019, zuletzt geprüft am 25.08.2021.

Miller, Maggie (2021): US concerns grow over potential Russian cyber targeting of Ukraine amid troop buildup. Hg. v. The Hill. Online verfügbar unter https://thehill.com/policy/cybersecurity/586033-us-concerns-grow-over-potential-russian-cyber-targeting-of-ukraine-amid/, zuletzt aktualisiert am 16.12.2021, zuletzt geprüft am 09.12.2022.

Ministry of Defense Israel (2020): Defense Establishment thwarts cyber-attack targeting defense industries 12 August 2020. Hg. v. Israel Ministry of Foreign Affairs. Online verfügbar unter https://mfa.gov.il/MFA/ForeignPolicy/Pages/Defense-Establishment-thwarts-cyber-attack-targeting-defense-industries-12-August-2020.aspx, zuletzt aktualisiert am 12.08.2020, zuletzt geprüft am 12.02.2022.

Mirski, Sean (2015): The South China Sea Dispute: A Brief History. Hg. v. Lawfare. Online verfügbar unter https://www.lawfareblog.com/south-china-sea-dispute-brief-history, zuletzt aktualisiert am 31.10.2019, zuletzt geprüft am 02.08.2021.

Mischke, Judith (2017): Russian hackers behind leak of UN diplomat's email: report. Hg. v. Politico. Online verfügbar unter https://www.politico.eu/article/russian-hackers-fancy-bear-behind-leak-of-un-diplomats-email-report/, zuletzt aktualisiert am 20.11.2017, zuletzt geprüft am 19.04.2021.

Mitchell, Sierra (2021): Profile of Group-IB CEO Ilya Sachkov, who is charged with treason in Russia, sources say for allegedly giving the US info about Fancy Bear's 2016 operation (Bloomberg). Hg. v. News AKMI. Online verfügbar unter https://newsakmi.com/news/tech-news/profile-of-group-ib-ceo-ilya-sachkov-who-is-charged-with-treason-in-russia-sources-say-for-allegedly-giving-the-us-info-about-fancy-bears-2016-operation-bloomberg/, zuletzt aktualisiert am 05.12.2021, zuletzt geprüft am 30.12.2021.

MOD (2011): Kontseptual'nye vzglyady na deyatel'nost‹ Vooruzhennykh Sil Rossiyskoy Federatsii v informatsionnom prostranstve [Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space]. Hg. v. Ministry of Defense of the Russian Federation. Online verfügbar unter http://www.pircenter.org/en/articles/532-conceptual-views-on-the-activity-of-the-armed-forces-of-the-russian-federation-in-information-space, zuletzt geprüft am 27.04.2021.

Moersen, Alex (2018): How Israel Became a Cybersecurity Powerhouse. Hg. v. Innovation & Tech Today. Online verfügbar unter https://innotechtoday.com/israel-cybersecurity-powerhouse/, zuletzt aktualisiert am 23.05.2018, zuletzt geprüft am 25.10.2021.

MOFA (2000): NATIONAL SECURITY CONCEPT OF THE RUSSIAN FEDERATION. Hg. v. The Ministry of Foreign Affairs of the Russian Federation. Online verfügbar unter https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=en_GB, zuletzt aktualisiert am 10.01.2000, zuletzt geprüft am 27.04.2021.

MOFA (2010): Военная доктрина Российской Федерации [Militärdoktrin der Russischen Föderation]. Hg. v. The Ministry of Foreign Affairs of the Russian Federation. Online verfügbar unter http://kremlin.ru/supplement/461, zuletzt aktualisiert am 05.02.2010, zuletzt geprüft am 27.04.2021.

MOFA (2013): Concept of the Foreign Policy of the Russian Federation. Hg. v. The Ministry of Foreign Affairs of the Russian Federation. Online verfügbar unter https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/122186, zuletzt aktualisiert am 18.02.2013, zuletzt geprüft am 27.04.2021.

MOFA (2016): Doctrine of Information Security of the Russian Federation. Hg. v. The Ministry of Forein Affairs of the Russian Federation. Online verfügbar unter https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163, zuletzt aktualisiert am 05.12.2016, zuletzt geprüft am 27.04.2021.

Moghadam, Assaf; Wyss, Michel (2020): The Political Power of Proxies: Why Nonstate Actors Use Local Surrogates. In: International Security 44 (4), S. 119–157. DOI: 10.1162/ISEC_a_00377.

Mommsen, Margareta (2018): Verfassungsordnung versus politische Realität | Dossier Russland. Hg. v. Bundeszentrale für Politische Bildung. Online verfügbar unter https://www.bpb.de/internationales/europa/russland/47940/verfassungsordnung-versus-politische-realitaet, zuletzt aktualisiert am 26.03.2018, zuletzt geprüft am 28.04.2021.

Mommsen, Margareta; Nußberger, Angelika (2007): Das System Putin. Gelenkte Demokratie und politische Justiz in Russland. Originalausgabe ; 2. aktualisierte und erweiterte Auflage. München: Verlag C.H. Beck (Beck'sche Reihe, 1763).

Moran, Ned; Villeneuve, Nart (2013): Operation DeputyDog: Zero-Day (CVE-2013-3893) Attack Against Japanese Targets. Hg. v. FireEye. Online verfügbar unter https://www.fireeye.com/blog/threat-research/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html, zuletzt aktualisiert am 21.09.2013, zuletzt geprüft am 25.06.2021.

Moravcsik, Andrew (1993): Preferences and power in the European Community: a liberal intergovernmentalist approach. In: JCMS: Journal of Common Market Studies 31 (4), S. 473–524.

Moravcsik, Andrew (1997): Taking preferences seriously: A liberal theory of international politics. In: International Organization 51 (4), S. 513–553.

Moravcsik, Andrew (1998): The choice for Europe: Social purpose and state power from Messina to Maastricht: Routledge.

Moravcsik, Andrew (2000): The origins of human rights regimes: Democratic delegation in postwar Europe. In: International Organization, S. 217–252.

Moravcsik, Andrew (2003): Liberal international relations theory: a scientific assessment. In: Progress in international relations theory: appraising the field, S. 159–204.

Moravcsik, Andrew (2013): The New Liberalism. In: Robert E. Goodin (Hg.): The Oxford Handbook of Political Science. Oxford: Oxford University Press (Oxford Handbooks Online).

Morgan, Steve (2019): Hot 150 Cybersecurity Companies To Watch In 2021. Hg. v. Cybercrime Magazine. Online verfügbar unter https://cybersecurityventures.com/cybersecurity-companies-list-hot-150/#hot-150/?view_15_per_page=150&view_15_page=1, zuletzt aktualisiert am 06.01.2021, zuletzt geprüft am 25.08.2021.

Morgan, Steve (2020): China Cybersecurity Companies. Hg. v. Cybercrime Magazine. Online verfügbar unter https://cybersecurityventures.com/china-cybersecurity-companies/, zuletzt aktualisiert am 15.10.2020, zuletzt geprüft am 07.07.2021.

Moriuchi, Priscilla; Ladd, Bill (2017): China's Ministry of State Security Likely Influences National Network Vulnerability Publications. Hg. v. Recorded Future. Online verfügbar unter https://www.recordedfuture.com/chinese-mss-vulnerability-influence/, zuletzt aktualisiert am 16.11.2017, zuletzt geprüft am 25.06.2021.

Morozov, Evgeny (2011): The dark side of internet freedom: The net delusion. In: New York: Public Affairs.

Mshvidobadze, Khatuna (2011): The Battlefield On Your Laptop. Hg. v. Radio Free Europe. Online verfügbar unter https://www.rferl.org/a/commentary_battlefield_on_your_desktop/2345202.html, zuletzt aktualisiert am 21.03.2011, zuletzt geprüft am 27.04.2021.

Mudde, Cas (2004): The populist zeitgeist. In: Government and opposition 39 (4), S. 541–563.

Mueller, Milton (2017): Will the internet fragment? Sovereignty, globalization and cyberspace. Cambridge, Malden, MA: Polity. Online verfügbar unter https://ebookcentral.proquest.com/lib/gbv/detail.action?docID=4875231.

Mueller, Milton; Grindal, Karl; Kuerbis, Brenden; Badiei, Farzaneh (2019): Cyber Attribution. Can a New Institution Achieve Transnational Credibility? In: The Cyber Defense Review 4 (1), S. 107–122.

Mueller, Milton L. (2020): Against Sovereignty in cyberspace. In: International Studies Review 22 (4), S. 779–801.

Mueller, Robert S. (2019a): Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Volume II of II. Hg. v. Special Counsel's Office. Online verfügbar unter https://www.nytimes.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html, zuletzt geprüft am 20.08.2021.

Mueller, Robert S. (2019b): Report on the Investigation into Russian Interference in the 2016 Presidential Election. Volume I of II. Hg. v. Special Counsel's Office. Online verfügbar unter https://www.justice.gov/archives/sco/file/1373816/download, zuletzt geprüft am 20.08.2021.

Mulvad, Andreas Møller (2019): Xiism as a hegemonic project in the making: Sino-communist ideology and the political economy of China's rise. In: Review of International Studies 45 (3), S. 449–470. DOI: 10.1017/S0260210518000530.

Mumford, Andrew (2013): Proxy Warfare. Hoboken: Wiley.

Muncaster, Phil (2018): Five Eyes Nations United in Blaming Russia for NotPetya. Hg. v. Infosecurity Magazine. Online verfügbar unter https://www.infosecurity-magazine.com/news/five-eyes-united-blaming-russia/, zuletzt aktualisiert am 19.02.2018, zuletzt geprüft am 06.10.2021.

Muncaster, Phil (2019): Dutch Insider Deployed Stuxnet: Report. Hg. v. Infosecurity Magazine. Online verfügbar unter https://www.infosecurity-magazine.com/news/dutch-insider-deployed-stuxnet/, zuletzt aktualisiert am 04.09.2019, zuletzt geprüft am 02.07.2021.

Muth, Max (2019): Die Software, die Whatsapp hacken sollte. Hg. v. Süddeutsche Zeitung. Online verfügbar unter https://www.sueddeutsche.de/digital/spyware-pegasus-nso-group-whatsapp-hack-1.4447562.

Myre, Greg (2020): A ›Perception Hack‹: When Public Reaction Exceeds The Actual Hack. Hg. v. NPR. Online verfügbar unter https://www.npr.org/2020/11/01/929101685/a-perception-hack-when-public-reaction-exceeds-the-actual-hack, zuletzt aktualisiert am 01.11.2020, zuletzt geprüft am 20.05.2021.

Nakashima, Ellen (2013a): Chinese hackers who breached Google gained access to sensitive data, U.S. officials say. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html, zuletzt aktualisiert am 20.05.2013, zuletzt geprüft am 21.06.2021.

Nakashima, Ellen (2013b): Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html, zuletzt aktualisiert am 28.05.2013, zuletzt geprüft am 08.09.2021.

Nakashima, Ellen (2014): Iranian hackers target U.S. officials on Twitter, Facebook and other social networks. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/world/national-security/iranian-hackers-are-targeting-us-officials-through-social-networks-report-says/2014/05/28/7cb86672-e6ad-11e3-8f90-73e071f3d637_story.html?utm_term=.95e99b2d36f7, zuletzt aktualisiert am 29.05.2014, zuletzt geprüft am 12.08.2021.

Nakashima, Ellen (2016): Russian government hackers penetrated DNC, stole opposition research on Trump. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html, zuletzt aktualisiert am 14.06.2016, zuletzt geprüft am 20.08.2021.

Nakashima, Ellen (2017): New details emerge about 2014 Russian hack of the State Department: It was ›hand to hand combat‹. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/world/national-security/new-details-emerge-about-2014-russian-hack-of-the-state-department-it-was-hand-to-hand-combat/2017/04/03/d89168e0-124c-11e7-833c-503e1f6394c9_story.html, zuletzt aktualisiert am 03.04.2017.

Nakashima, Ellen (2020): U.S. undertook cyber operation against Iran as part of effort to secure the 2020 election. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/national-security/cybercom-targets-iran-election-interference/2020/11/03/aa0c9790-1e11-11eb-ba21-f2f001f0554b_story.html, zuletzt aktualisiert am 03.11.2020, zuletzt geprüft am 06.10.2021.

Naraine, Ryan (2010): Microsoft knew of IE zero-day flaw since last September. Hg. v. ZDnet. Online verfügbar unter https://www.zdnet.com/article/microsoft-knew-of-

ie-zero-day-flaw-since-last-september/, zuletzt aktualisiert am 21.01.2010, zuletzt geprüft am 21.06.2021.

NCSC (2018a): Joint US – UK statement on malicious cyber activity carried out by Russian government. Hg. v. National Cyber Security Centre. Online verfügbar unter https://www.ncsc.gov.uk/news/joint-us-uk-statement-malicious-cyber-activity-carried-out-russian-government, zuletzt aktualisiert am 15.11.2018, zuletzt geprüft am 06.10.2021.

NCSC (2018b): Reckless campaign of cyber attacks by Russian military intelligence service exposed. Hg. v. National Cyber Security Centre UK. Online verfügbar unter https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed, zuletzt aktualisiert am 18.03.2020, zuletzt geprüft am 19.04.2021.

Neuberger, Benyamin (2008): Staatsaufbau und politisches System. Hg. v. Bundeszentrale für Politische Bildung. Online verfügbar unter https://www.bpb.de/internationales/asien/israel/45024/das-politische-system, zuletzt aktualisiert am 10.06.2008, zuletzt geprüft am 02.01.2022.

Nevers, Renée de (2016): Private Security's Role in Shaping US Foreign Policy. In: Anna Leander und Rita Abrahamsen (Hg.): Routledge handbook of private security studies. London, New York: Routledge (Routledge handbooks), S. 168–176.

Newman, Lily Hay (2019): What Israel's Strike on Hamas Hackers Means For Cyberwar. Hg. v. Wired. Online verfügbar unter https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/, zuletzt aktualisiert am 06.05.2019, zuletzt geprüft am 13.10.2021.

Nichols, Michelle (2020): U.S. withdrawal from WHO over claims of China influence to take effect July 2021: U.N. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-health-coronavirus-trump-who-idUSKBN2482YZ, zuletzt aktualisiert am 07.07.2020, zuletzt geprüft am 06.10.2021.

Noack, Rick (2018): How a Dutch intelligence agency secretly hacked into the Kremlin's most notorious hacking group. Hg. v. Independent. Online verfügbar unter https://www.independent.co.uk/news/world/europe/netherlands-dutch-russia-kremlin-united-states-robert-mueller-intelligence-agencies-cozy-bear-aivd-a8181046.html, zuletzt aktualisiert am 27.01.2018.

Noble, Ben; Schulmann, Ekaterina (2021): Myth 15: »It's All About Putin – Russia is a manually run, centralized autocracy«. Hg. v. Chatham House. Online verfügbar unter https://www.chathamhouse.org/2021/05/myths-and-misconceptions-debate-russia/myth-15-its-all-about-putin-russia-manually-run, zuletzt aktualisiert am 13.05.2021, zuletzt geprüft am 18.05.2021.

Nossek, Hillel; Limor, Yehiel (2001): Fifty Years In A« Marriage Of Convenience«: News Media And Military Censorship In Israel. In: Communication Law & Policy 6 (1), S. 1–35.

Novetta (2014): Operation SMN: Axiom Threat Actor Group Report. Hg. v. Novetta. Online verfügbar unter http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf.

Novetta (2016): Operation Blockbuster. Unraveling the Long Thread of the Sony Attack. Hg. v. Novetta. Online verfügbar unter https://operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf.

Nye, Joseph S. (2011): Nuclear lessons for cyber security? In: Strategic Studies Quarterly 5 (4), S. 18–38.

Nye, Joseph S. (2017): Deterrence and Dissuasion in Cyberspace. In: International Security 41 (3), S. 44–71. DOI: 10.1162/ISEC_a_00266.

Nye, Joseph S. (2018): Protecting Democracy in an Era of Cyber Information War. Hg. v. Hoover Institution (Fall Series, Issue 318). Online verfügbar unter https://www.hoover.org/research/protecting-democracy-era-cyber-information-war, zuletzt aktualisiert am 13.11.2018, zuletzt geprüft am 12.05.2020.

O'Hara, Terence (2005): In-Q-Tel, CIA's Venture Arm, Invests in Secrets. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/wp-dyn/content/article/2005/08/14/AR2005081401108.html, zuletzt aktualisiert am 02.08.2016, zuletzt geprüft am 12.08.2021.

Obama, Barack (2011): Remarks By President Obama to the Australian Parliament. Hg. v. The White House. Online verfügbar unter https://eu.usatoday.com/story/news/world/2014/04/28/obama-philippines-china/8403801/, zuletzt aktualisiert am 17.11.2011, zuletzt geprüft am 02.08.2021.

O'Brien, Kevin J.; Li, Lianjiang (2000): Accommodating »Democracy« in a One-Party State: Introducing Village Elections in China. In: The China Quarterly 162, S. 465–489. DOI: 10.1017/s0305741000008213.

ODNI (2017): Background to »Assessing Russian Activities and Intentions in Recent US Elections«: The Analytic Process and Cyber Incident Attribution. Hg. v. Office of the Director of National Intelligence. Online verfügbar unter https://www.dni.gov/files/documents/ICA_2017_01.pdf, zuletzt aktualisiert am 06.01.2017, zuletzt geprüft am 19.04.2021.

ODNI (2018): A Guide to Cyber Attribution. Hg. v. Office of the Director of National Intelligence. Online verfügbar unter https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf, zuletzt aktualisiert am 14.09.2018.

Olson, Parmy (2014): The Largest Cyber Attack In History Has Been Hitting Hong Kong Sites. Hg. v. Forbes. Online verfügbar unter https://www.forbes.com/sites/parmyolson/2014/11/20/the-largest-cyber-attack-in-history-has-been-hitting-hong-kong-sites/?sh=722c95a838f6, zuletzt aktualisiert am 20.11.2014, zuletzt geprüft am 30.07.2021.

Oneal, John R.; Russet, Bruce M. (1997): The classical liberals were right: Democracy, interdependence, and conflict, 1950–1985. In: Int Stud Q 41 (2), S. 267–293.

Oneal, John R.; Russett, Bruce; Berbaum, Michael L. (2003): Causes of peace: Democracy, interdependence, and international organizations, 1885–1992. In: Int Stud Q 47 (3), S. 371–393.

O'Neill, Patrick Howell (2017): Report: Russian arrests allegedly tied to passing hacking information to U.S. Hg. v. Cyberscoop. Online verfügbar unter https://www.cyberscoop.com/russia-fsb-arrests-king-servers-threatconnect/, zuletzt aktualisiert am 26.01.2017, zuletzt geprüft am 06.05.2021.

O'Neill, Patrick Howell (2020a): Inside NSO, Israel's billion-dollar spyware giant. Hg. v. MIT Technology Review. Online verfügbar unter https://www.technologyreview.com/2020/08/19/1006458/nso-spyware-controversy-pegasus-human-rights/, zuletzt aktualisiert am 19.08.2020, zuletzt geprüft am 03.01.2022.

O'Neill, Patrick Howell (2020b): The NSA found a dangerous flaw in Windows and told Microsoft to fix it. Hg. v. MIT Technology Review. Online verfügbar unter https://www.technologyreview.com/2020/01/14/75069/the-nsa-found-a-dangerous-flaw-in-windows-and-told-microsoft-to-fix-it/, zuletzt aktualisiert am 15.01.2020, zuletzt geprüft am 01.10.2021.

O'Neill, Patrick Howell (2021): Google's top security teams unilaterally shut down a counterterrorism operation. Hg. v. MIT Technology Review. Online verfügbar unter https://www.technologyreview.com/2021/03/26/1021318/google-security-shut-down-counter-terrorist-us-ally/, zuletzt aktualisiert am 26.03.2021, zuletzt geprüft am 20.08.2021.

Orbach, Meir (2020): Microsoft in Negotiations to Acquire Israeli Cybersecurity Company CyberX. Hg. v. Calcalist. Online verfügbar unter https://www.calcalistech.com/ctech/articles/0,7340,L-3817591,00.html, zuletzt aktualisiert am 05.05.2020, zuletzt geprüft am 11.10.2021.

Oren, Ido (1995): The Subjectivity of the »Democratic« Peace: Changing U.S. Perceptions of Imperial Germany. In: International Security 20 (2), S. 147–184. DOI: 10.2307/2539232.

Orye, Erwin; Maennel, Olaf M. (2019): Recommendations for Enhancing the Results of Cyber Effects. In: Tomáš Minárik, Siim Alatalu, Stefano Biondi, Massimiliano Signoretti, Ihsan Tolga und Gabor Visky (Hg.): 2019 11th International Conference on Cyber Conflict (CyCon). Tallinn, Estonia: IEEE, S. 1–19.

Osborne, Charlie (2020): Microsoft has the highest rate of zero-days detected in the wild, but not all is as it seems. Hg. v. The Daily Swig. Online verfügbar unter https://portswigger.net/daily-swig/microsoft-has-the-highest-rate-of-zero-days-detected-in-the-wild-but-not-all-is-as-it-seems, zuletzt aktualisiert am 31.07.2020, zuletzt geprüft am 11.06.2021.

Østensen, Åse Gilje; Bukkvoll, Tor (2018): Russian Use of Private Military and Security Companies-the implications for European and Norwegian Security. In: FFI-rapport 18, S. 1–49. Online verfügbar unter https://open.cmi.no/cmi-xmlui/bitstream/handle/11250/2564170/Russian%20Use%20of%20Private%20Military%20and%20Security%20Companies%20-%20the%20implications%20for%20European%20and%20Norwegian%20Security?sequence=1, zuletzt geprüft am 19.05.2020.

Ottis, Rain (2010): Proactive Defence Tactics Against On-Line Cyber Militia. In: Joseph Demergis (Hg.): Proceedings of the 9th European Conference on Information Warfare and Security. Proceedings of the 9th European Conference on Information Warfare and Security. Thessaloniki, 01.-02. Juli 2010. Reading: Academic Publishing Limited, S. 233–237.

Owen, John M. (1994): How Liberalism Produces Democratic Peace. In: International Security 19 (2), S. 87. DOI: 10.2307/2539197.

Page, Carly (2021): EU warns Russia over ›Ghostwriter‹ hacking ahead of German elections. Hg. v. Techcrunch. Online verfügbar unter https://techcrunch.com/2021

/09/24/european-council-russia-ghostwriter/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAADuClHZMVk9Lh5I9ZZoF4hfr36d00c4fujTkb_ZJw1Lt9qcb2uphqRQkSk-I61cqEX4M8uOak5sxPZQrOPBf4ZdR8JbZOIlIPz7bsLq5vxpAjdKVKHVRJDOQSR9dprxGoQAxe1MkIxOgHx7OQ_XR10qQjFCu2szmXCtoxiM5Z48u, zuletzt aktualisiert am 24.09.2021, zuletzt geprüft am 10.02.2022.

Palm, Philip M.; Schulz, Daniel F. (2011): Die Beteiligung am Irak-Krieg – eine innenpolitische Frage? In: Markus M. Müller (Hg.): Casebook internationale Politik. 1. Aufl. Wiesbaden: VS Verl. für Sozialwiss (Lehrbuch), S. 64–87.

Palo Alto Networks (2021): Management. Hg. v. Palo Alto Networks. Online verfügbar unter https://www.paloaltonetworks.com/about-us/management, zuletzt geprüft am 11.10.2021.

Park, Donghui; Walstrom, Michael (2017): Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks – The Henry M. Jackson School of International Studies. Hg. v. The Henry M. Jackson School of International Studies. Online verfügbar unter https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/, zuletzt aktualisiert am 11.10.2017, zuletzt geprüft am 18.04.2021.

Parker, Ned; Landay, Jonathan; Walcott, John (2017): Putin-linked think tank drew up plan to sway 2016 US election – documents. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-usa-russia-election-exclusive/putin-linked-think-tank-drew-up-plan-to-sway-2016-us-election-documents-idUSKBN17L2N3, zuletzt aktualisiert am 19.04.2017, zuletzt geprüft am 14.04.2021.

Paul, Kari (2021): SolarWinds hack was work of ›at least 1,000 engineers‹, tech executives tell Senate. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/technology/2021/feb/23/solarwinds-hack-senate-hearing-microsoft, zuletzt aktualisiert am 24.02.2021, zuletzt geprüft am 12.05.2021.

Paul, Michael (2018): Chinas nukleare Abschreckung: Ursachen, Mittel und Folgen der Stationierung chinesischer Nuklearwaffen auf Unterseebooten. Hg. v. Stiftung Wissenschaft Und Politik. Berlin (SWP-Studie, 17). Online verfügbar unter https://www.ssoar.info/ssoar/handle/document/59759, zuletzt geprüft am 31.07.2021.

Pavur, James (2021): Securing new space: on satellite cyber-security. Hg. v. University of Oxford (A thesis submitted for the degree of Doctor of Philosophy). Online verfügbar unter https://ora.ox.ac.uk/objects/uuid:11e1b32a-8117-46b1-a0ce-9c485221d112, zuletzt geprüft am 23.11.2021.

Perez, Evan (2016): U.S. official blames Russia for power grid attack in Ukraine – CNNPolitics. Hg. v. CNN. Online verfügbar unter https://edition.cnn.com/2016/02/11/politics/ukraine-power-grid-attack-russia-us/index.html, zuletzt aktualisiert am 12.02.2016, zuletzt geprüft am 29.09.2021.

Peri, Yoram (1981): Political-Military Partnership in Israel. In: International Political Science Review 2 (3), S. 303–315. Online verfügbar unter http://www.jstor.org/stable/1601065.

Perlroth, Nicole (2012): In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2012/10/24

/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html, zuletzt aktualisiert am 23.10.2012.

Perlroth, Nicole (2013): Chinese Hackers Infiltrate New York Times Computers. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html, zuletzt aktualisiert am 30.01.2013, zuletzt geprüft am 02.08.2021.

Perlroth, Nicole (2021): This Is How They Tell Me the World Ends. London: Bloomsbury Publishing.

Pernik, Piret (2018): The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine. In: Nicu Popescu und Stanislav Secrieru (Hg.): Hacks, Leaks and Disruptions: Russian Cyber Strategies. Paris (Chaillot Papers, 148), S. 53–64.

Peters, Allison (2019): Russia and China Are Trying to Set the U.N.‹s Rules on Cybercrime. Hg. v. Foreign Policy. Online verfügbar unter https://foreignpolicy.com/2019/09/16/russia-and-china-are-trying-to-set-the-u-n-s-rules-on-cybercrime/, zuletzt aktualisiert am 16.09.2019.

Peters, Michael A. (2017): The Chinese Dream: Xi Jinping thought on Socialism with Chinese characteristics for a new era. In: Educational Philosophy and Theory 49 (14), S. 1299–1304. DOI: 10.1080/00131857.2017.1407578.

Peterson, Demosthenes James (2005): Russia and the information revolution. Santa Monica, Calif. (Rand Corporation monograph series, MG-422-CC).

Piiparinen, Anni (2016): China's Secret Weapon in the South China Sea: Cyber Attacks. Hg. v. The Diplomat. Online verfügbar unter https://thediplomat.com/2016/07/chinas-secret-weapon-in-the-south-china-sea-cyber-attacks/, zuletzt aktualisiert am 22.06.2016, zuletzt geprüft am 23.06.2021.

Pillar, Paul R. (2011): Intelligence and US foreign policy: Iraq, 9/11, and misguided reform: Columbia University Press.

Plan, Fred; Fraser, Nalani; O'Leary Jacqueline; Cannon, Vincent; Read, Ben (2019): APT40: Examining a China-Nexus Espionage Actor. Hg. v. FireEye. Online verfügbar unter https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html, zuletzt aktualisiert am 04.09.2019, zuletzt geprüft am 01.07.2021.

Poitras, Laura; Rosenbach, Marcel; Stark, Holger (2013): ›Follow the Money‹: NSA Monitors Financial World. Hg. v. Der Spiegel. Online verfügbar unter https://www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430.html, zuletzt aktualisiert am 16.09.2013, zuletzt geprüft am 26.08.2021.

Polaski, Sandra; Dollar, David (2020): How have Trump's trade wars affected Rust Belt jobs? Hg. v. Brookings. Online verfügbar unter https://www.brookings.edu/podcast-episode/how-have-trumps-trade-wars-affected-rust-belt-jobs/, zuletzt aktualisiert am 19.10.2020, zuletzt geprüft am 06.10.2021.

Pouliot, Vincent (2014): Setting Status in Stone: The Negotiation of International Institutional Privileges. In: T. V. Paul, Deborah Welch Larson und William C. Wohlforth (Hg.): Status in World Politics: Cambridge University Press, S. 192–218.

Pouliot, Vincent (2016): International Pecking Orders. The Politics and Practice of Multilateral Diplomacy: Cambridge University Press.

Pozen, David E. (2013): THE LEAKY LEVIATHAN: WHY THE GOVERNMENT CONDEMNS AND CONDONES UNLAWFUL DISCLOSURES OF INFORMATION. In: Harvard law review 127 (2), S. 512–635. Online verfügbar unter http://www.jstor.org/stable/23742018.

Poznansky, Michael; Perkoski, Evan (2018): Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution. In: Journal of Global Security Studies 3 (4), S. 402–416.

PRC Embassy Iraq (2017): Speech By President Xi Jinping At the United Nations Office at Geneva. Hg. v. Embassy of the People's Republic of China in the Republic of Iraq. Online verfügbar unter http://iq.chineseembassy.org/eng/zygx/t1432869.htm, zuletzt aktualisiert am 23.01.2017, zuletzt geprüft am 04.08.2021.

PRC Embassy Philippines (2016): Archaeological Findings Prove That Chinese People Are Real Owner of South China Sea Islands. Hg. v. Embassy of the People's Republic of China in the Rebublic of the Philippines. Online verfügbar unter http://ph.china-embassy.org/eng/sgdt/t1372445.htm, zuletzt aktualisiert am 15.06.2016, zuletzt geprüft am 02.08.2021.

Precht, Henry (1988): Ayatollah realpolitik. In: Foreign Policy (70), S. 109–128.

Proofpoint (2017): Leviathan: Espionage actor spearphishes maritime and defense targets | Proofpoint US. Hg. v. Proofpoint. Online verfügbar unter https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets, zuletzt aktualisiert am 27.01.2019, zuletzt geprüft am 01.07.2021.

Protasov, Vitaly (2010): EU-Russia Gas Relations: a View From Both Sides. Hg. v. International Association for Energy Economics. Online verfügbar unter https://www.iaee.org/en/publications/newsletterdl.aspx?id=115#:~:text=Dependence%20on%20Russian%20gas%20is,from%20Russia%20in%20prior%20years., zuletzt geprüft am 12.05.2021.

Ptak, Alicija; Pawlak, Justyna (2021): Polish trial begins in Huawei-linked China espionage case. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/world/china/polish-trial-begins-huawei-linked-china-espionage-case-2021-05-31/, zuletzt aktualisiert am 01.06.2021, zuletzt geprüft am 05.07.2021.

Putnam, Robert D. (1988): Diplomacy and domestic politics: the logic of two-level games. In: International Organization, S. 427–460.

Putnam, Tonya L.; Elliott, David D. (2001): International Responses to cyber crime. In: Transnational Dimension of Cyber Crime and Terrorism, S. 35–66.

Radio Free Europe (2017): Putin Compares Hackers To ›Artists,‹ Says They Could Target Russia's Critics For ›Patriotic‹ Reasons. Hg. v. Radio Free Europe. Online verfügbar unter https://www.rferl.org/a/russia-putin-patriotic-hackers-target-critics-not-state/28522639.html, zuletzt aktualisiert am 01.06.2017, zuletzt geprüft am 20.05.2021.

Rakuszitzky, Moritz; Romein, Daniel; Dobrokhotov, Roman (2018): MH17 – Russian GRU Commander ›Orion‹ Identified as Oleg Ivannikov. Hg. v. Bellingcat. Online verfügbar unter https://www.bellingcat.com/news/uk-and-europe/2018/05/25/mh17-russian-gru-commander-orion-identified-oleg-ivannikov/, zuletzt aktualisiert am 05.09.2018, zuletzt geprüft am 12.05.2021.

Ramadhani, Eryan (2019): Is Assertiveness Paying the Bill? China's Domestic Audience Costs in the South China Sea Disputes. In: Journal of Asian Security and International Affairs 6 (1), S. 30–54.

Rathbun, Brian C. (2010): Is anybody not an (international relations) liberal? In: Security Studies 19 (1), S. 2–25.

Raud, Mikk (2015): China and cyber: attitude, strategies, organisation. Hg. v. NATO CCD COE. Tallinn. Online verfügbar unter https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf, zuletzt aktualisiert am 2016, zuletzt geprüft am 10.01.2021.

Rauta, Vladimir (2020): Proxy Warfare and the Future of Conflict: Take Two. In: The RUSI Journal 165 (2), S. 1–10. DOI: 10.1080/03071847.2020.1736437.

Rauta, Vladimir (2021): ›Proxy War‹-A Reconceptualisation. In: Civil Wars 23 (1), S. 1–24.

Ray, Siladitya (2020): Report: CIA Conducted Cyber Attacks Against Iran, Russia After Secret Trump Order In 2018. Hg. v. Forbes. Online verfügbar unter https://www.forbes.com/sites/siladityaray/2020/07/15/report-cia-conducted-cyber-attacks-against-iran-russia-after-secret-trump-order-in-2018/?sh=22006c194600, zuletzt aktualisiert am 15.07.2020, zuletzt geprüft am 06.10.2021.

Recorded Future (2017): Recorded Future Launches Threat Research Arm to Enhance Threat Intelligence Offering. Hg. v. Recorded Future. Online verfügbar unter https://www.prnewswire.com/news-releases/recorded-future-launches-threat-research-arm-to-enhance-threat-intelligence-offering-300454937.html, zuletzt aktualisiert am 10.05.2017, zuletzt geprüft am 12.08.2021.

Reed, John (2015): Unit 8200: Israel's cyber spy agency. Hg. v. Financial Times. Online verfügbar unter https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c, zuletzt aktualisiert am 10.07.2015, zuletzt geprüft am 02.01.2022.

Reinhold, Thomas; Reuter, Christian (2021): Towards a Cyber Weapons Assessment Model -Assessment of the Technical Features of Malicious Software. In: IEEE Transactions on Technology and Society, S. 1. DOI: 10.1109/TTS. 2021.3131817.

Reuters (2011): Russia's Medvedev fires deputy FSB security chief. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/russia-medvedev-fsb-idUSLDE71K1NH20110221, zuletzt aktualisiert am 21.02.2011, zuletzt geprüft am 12.05.2021.

Reuters (2013): Iran ups cyber attacks on Israeli computers: Netanyahu. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-israel-iran-cyber-idUSBRE95808H20130609, zuletzt aktualisiert am 09.06.2013, zuletzt geprüft am 07.10.2021.

Reuters (2020a): ›There will be dad and mum‹: Putin rules out Russia legalizing gay marriage. Hg. v. NBC News. Online verfügbar unter https://www.nbcnews.com/feature/nbc-out/there-will-be-dad-mum-putin-rules-out-russia-legalizing-n1136936, zuletzt aktualisiert am 14.02.2020, zuletzt geprüft am 05.05.2021.

Reuters (2020b): Timeline: Key dates in Hong Kong's anti-government protests. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-hongkong-protests-timeline-idUSKBN23608O, zuletzt aktualisiert am 30.05.2020, zuletzt geprüft am 30.07.2021.

Reuters (2020c): Timeline: Key dates in the U.S.-China trade war. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-usa-trade-china-timeline-idUSKBN1ZE1AA, zuletzt aktualisiert am 15.01.2020, zuletzt geprüft am 01.10.2021.

Richter, Steffen (2013): Bo Xilai-Urteil: Xi Jinping gnadenlos. Hg. v. Die Zeit. Online verfügbar unter https://www.zeit.de/politik/ausland/2013-09/xi-jinping-bo-xilai-reformen?utm_referrer=https%3A%2F%2Fwww.google.com%2F, zuletzt aktualisiert am 23.09.2013, zuletzt geprüft am 25.07.2021.

Rid, Thomas (2013): Cyberwar and Peace: Hacking Can Reduce Real-World Violence. In: Foreign Affairs 92 (6), S. 77–87.

Rid, Thomas; Buchanan, Ben (2015): Attributing Cyber Attacks. In: Journal of Strategic Studies 38 (1–2), S. 4–37. DOI: 10.1080/01402390.2014.977382.

Rivera, David W.; Rivera, Sharon Werning (2018): The Militarization of the Russian Elite under Putin. In: Problems of Post-Communism 65 (4), S. 221–232. DOI: 10.1080/10758216.2017.1295812.

Rivera, Jason (2015): Achieving cyberdeterrence and the ability of small states to hold large states at risk. In: M. Maybaum (Hg.): 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace (CyCon). 26–29 May 2015, Tallinn, Estonia. Piscataway, NJ: IEEE, S. 7–24.

Roberts, Samuel J. (2019): Party and policy in Israel: The battle between hawks and doves: Routledge.

Robinson, Glenn E. (2020): The death of the two-state solution. Israel, the Palestinians, and the Arab world in the age of Netanyahu. In: Robert O. Freedman (Hg.): Israel Under Netanyahu: Domestic Politics and Foreign Policy: Routledge.

Rød, Espen Geelmuyden; Weidmann, Nils B. (2015): Empowering activists or autocrats? The Internet in authoritarian regimes. In: Journal of Peace Research 52 (3), S. 338–351.

Röhl, Klaus-Heiner (2016): Unternehmensgründungen: Mehr innovative Startups durch einen Kulturwandel für Entrepreneurship? Hg. v. Institut für deutsche Wirtschaft Köln. Online verfügbar unter https://www.iwkoeln.de/fileadmin/publikationen/2016/262911/Unternehmensgruendungen_IW_policy_paper.pdf, zuletzt aktualisiert am 28.01.2016, zuletzt geprüft am 26.10.2021.

Rohlfing, Ingo (2014): Comparative Hypothesis Testing Via Process Tracing. In: Sociological Methods & Research 43 (4), S. 606–642. DOI: 10.1177/0049124113503142.

Romagna, Marco; van den Hout, Niek Jan (2017): Hacktivism and website defacement: motivations, capabilities and potential threats. Virus Bulletin Conference. Madrid. Online verfügbar unter https://www.virusbulletin.com/conference/vb2017/abstracts/hacktivism-and-website-defacement-motivations-capabilities-and-potential-threats, zuletzt aktualisiert am 2017, zuletzt geprüft am 11.06.2020.

Romanosky, Sasha (2017): Private-Sector Attribution of Cyber Attacks: A Growing Concern for the U.S. Government? Hg. v. Lawfare. Online verfügbar unter https://www.lawfareblog.com/private-sector-attribution-cyber-attacks-growing-concern-us-government, zuletzt aktualisiert am 21.12.2017, zuletzt geprüft am 13.07.2020.

Romanosky, Sasha; Boudreaux, Benjamin (2021): Private-Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government. In: Interna-

tional Journal of Intelligence and CounterIntelligence 34 (3), S. 463–493. DOI: 10.1080/08850607.2020.1783877.

Roncone, Gabriella; Wahlstrom, Alden; Revelli, Alice; Mainor, David; Riddell, Sam; Read, Ben (2021): UNC1151 Assessed with High Confidence to have Links to Belarus, Ghostwriter Campaign Aligned with Belarusian Government Interests | Mandiant. Hg. v. MANDIANT. Online verfügbar unter https://www.mandiant.com/resources/unc1151-linked-to-belarus-government, zuletzt aktualisiert am 16.11.2021, zuletzt geprüft am 10.02.2022.

Rondeaux, Candace (2019): Decoding the Wagner group: Analyzing the role of private military security contractors in Russian proxy warfare. Hg. v. Center on the Future of War. Arizona State University. Online verfügbar unter https://www.ohchr.org/Documents/issues/Mercenaries/WG/OtherStakeholders/candace-rondeux-submission-1.pdf.

Rosenbach, Eric; Chong, Shu Min (2019): Governing Cyberspace: State Control vs. The Multistakeholder Model. Hg. v. Belfer Center for Science and International Affairs. Online verfügbar unter https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model, zuletzt geprüft am 15.12.2022.

Ross, Ingrid (2005): Hijacking of the President? Die Neokonservativen und die Entscheidung zum Irakkrieg 2003. Göttingen, Berlin: Niedersächsische Staats- und Universitätsbibliothek; John-F.-Kennedy-Institut für Nordamerikastudien (Working paper/John-F.-Kennedy-Institut für Nordamerikastudien, 134). Online verfügbar unter http://webdoc.sub.gwdg.de/ebook/serien/p/jfk/workingpaper134.pdf.

Roth, Andrew (2019): Russia's great firewall: is it meant to keep information in – or out? Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/technology/2019/apr/28/russia-great-firewall-sovereign-internet-bill-keeping-information-in-or-out, zuletzt aktualisiert am 28.04.2019.

Roth, Andrew (2021): Ukraine still outgunned as Russia prepares for larger conflict. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/world/2021/apr/14/ukraine-still-outgunned-as-russia-prepares-for-larger-conflict, zuletzt aktualisiert am 14.04.2021, zuletzt geprüft am 18.05.2021.

Rousseau, David L.; Gelpi, Christopher; Reiter, Dan; Huth, Paul K. (1996): Assessing the dyadic nature of the democratic peace, 1918–88. In: Am Polit Sci Rev 90 (3), S. 512–533.

Rugge, Fabio (Hg.) (2018): Confronting an »axis of cyber«? China, Iran, North Korea, Russia in cyberspace. First edition. Milano: ISPI Ledizioni LediPublishing. Online verfügbar unter https://www.doabooks.org/doab?func=fulltext&uiLanguage=en&rid=29716.

Russett, Bruce (1994): Grasping the democratic peace: Principles for a post-Cold War world: Princeton University Press.

Rutland, Peter (2018): The Political Elite in Post-Soviet Russia. In: The Palgrave Handbook of Political Elites: Springer, S. 273–294.

Saalbach, Klaus-Peter (2019): Attribution of Cyber Attacks. In: Christian Reuter (Hg.): Information Technology for Peace and Security. Wiesbaden: Springer Vieweg, S. 279–303.

Saalman, Lora (2017): New domains of crossover and concern in cyberspace. Hg. v. Stockholm International Peace Research Institute. Online verfügbar unter https:/

/www.sipri.org/commentary/topical-backgrounder/2017/new-domains-crossover-and-concern-cyberspace, zuletzt aktualisiert am 26.07.2017, zuletzt geprüft am 11.01.2022.

Sadeh, Shuki (2021): Israeli military vs. NSO: The battle for talent is getting dark. Hg. v. Haaretz. Online verfügbar unter https://www.haaretz.com/israel-news/tech-news/idf-vs-nso-8200-battle-israel-cyber-talent-getting-dark-1.9929433, zuletzt aktualisiert am 29.06.2021, zuletzt geprüft am 02.01.2022.

Sakwa, Richard (2008): Putin and the Oligarchs. In: New Political Economy 13 (2), S. 185–191. DOI: 10.1080/13563460802018513.

Sakwa, Richard (2012): Party and power: between representation and mobilisation in contemporary Russia. In: East European Politics 28 (3), S. 310–327. DOI: 10.1080/21599165.2012.683784.

Sambaluk, Nick (2019): Conflict in the 21st Century. The Impact of Cyber Warfare, Social Media, and Technology. Santa Barbara, CA, Denver, CO: ABC-CLIO.

Sanchez, Julian (2020): No, The Presidential Election Was Not Rigged by Hacked Voting Machines. Hg. v. Cato Institute. Online verfügbar unter https://www.cato.org/blog/no-presidential-election-was-not-rigged-hacked-voting-machines, zuletzt aktualisiert am 13.11.2020, zuletzt geprüft am 05.05.2021.

Sanger, David E.; Perlroth, Nicole (2013): China's Army Is Seen as Tied to Hacking Against U.S. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html, zuletzt aktualisiert am 18.02.2013, zuletzt geprüft am 02.07.2021.

Sanger, David E.; Schmall, Emily (2021): China Appears to Warn India: Push Too Hard and the Lights Could Go Out. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html, zuletzt aktualisiert am 28.02.2021, zuletzt geprüft am 04.08.2021.

Sartori, Giovanni (1970): Concept misformation in comparative politics. In: American Political Science Review 64 (4), S. 1033–1053.

Satter, David (2003): Darkness at dawn: The rise of the Russian criminal state: Yale University Press.

Satter, Raphael (2020): Exclusive-Suspected Chinese hackers stole camera footage from African Union – memo. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/idUSKBN28Q1DB, zuletzt aktualisiert am 16.12.2020, zuletzt geprüft am 23.06.2021.

Schake, Kori (2020): The Military and the Constitution Under Trump. In: Survival 62 (4), S. 31–38. DOI: 10.1080/00396338.2020.1792096.

Schambra, William (2009): Obama and the Policy Approach. Hg. v. National Affairs. Online verfügbar unter https://www.nationalaffairs.com/publications/detail/obama-and-the-policy-approach, zuletzt geprüft am 02.09.2021.

Schelling, Thomas C. (1960): The Strategy of Conflict. Cambridge, Massachusetts: Harvard University Press.

Schepp, Matthias (2013): Bürgermeisterwahl in Moskau: Putin – der große Verlierer. Hg. v. Der Spiegel. Online verfügbar unter https://www.spiegel.de/politik/ausland/buergermeisterwahl-in-moskau-verlierer-putin-a-921104.html, zuletzt aktualisiert am 09.09.2013, zuletzt geprüft am 29.04.2021.

Schiermeier, Quirin (2014): Putin's Russia divides and enrages scientists. In: Nature 516 (7531), S. 298–299. DOI: 10.1038/516298a.

Schimmelfennig, Frank (2013): Internationale Politik. 3., aktualisierte Aufl. Paderborn: Schöningh (UTB, 3107 : Politikwissenschaft).

Schmidt, Michael S.; Sanger, David E.; Perlroth, Nicole (2014): Chinese Hackers Pursue Key Data on U.S. Workers. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html, zuletzt aktualisiert am 09.07.2014, zuletzt geprüft am 27.09.2021.

Schmitt, Michael N. (2015): The law of cyber targeting. In: Naval War College Review 68 (2), S. 10–29. Online verfügbar unter https://www.jstor.org/stable/26397834.

Schmitt, Michael N.; Vihul, Liis (2014): Proxy Wars in Cyberspace: The Evolving International Law of Attribution. In: Fletcher Security Review 1, S. 53.

Schneier, Bruce (2014): Essays: Did North Korea Really Attack Sony? – Schneier on Security. Hg. v. Schneier on Security. Online verfügbar unter https://www.schneier.com/essays/archives/2014/12/did_north_korea_real.html, zuletzt aktualisiert am 22.12.2014, zuletzt geprüft am 11.08.2021.

Schreyer, Söhnke (2017): Geteilte Herrschaft: Obama, die parteipolitische Polarisierung und der Kongress. In: Z Außen Sicherheitspolit 10 (S2), S. 25–38. DOI: 10.1007/s12399-017-0617-1.

Schröder, Hans-Henning (2018): Russland in der Ära Jelzin. Hg. v. Bundeszentrale für Politische Bildung. Online verfügbar unter https://www.bpb.de/internationales/europa/russland/47924/russland-in-der-aera-jelzin-1992-1999?p=2, zuletzt aktualisiert am 11.06.2018, zuletzt geprüft am 28.04.2021.

Schubarth, Cromwell (2021): What CrowdStrike CEO George Kurtz says about the controversy that got Donald Trump so angry. Hg. v. Silicon Valley Business Journal. Online verfügbar unter https://www.bizjournals.com/sanjose/news/2021/06/25/middle-market-75-crowdstrike-ukraine.html, zuletzt aktualisiert am 25.06.2021, zuletzt geprüft am 20.08.2021.

Schulze, Matthias (2019): Quo Vadis Cyber Arms Control? – A Sketch of an International Vulnerability Equities Process and a 0-Day Emissions Trading Regime. In: Christian Reuter, Jürgen Altmann, Malte Göttsche und Mirko Himmel (Hg.): Proceedings of the Interdisciplinary Conference on Technical Peace and Security Research. Science Peace Security '19. Darmstadt, 25.-27.9.2019. Darmstadt: TUprints, S. 24–40.

Schulze, Matthias (2020): The State of Cyber Arms Control. An International Vulnerabilities Equities Process as the Way to go Forward? In: S&F Sicherheit und Frieden 38 (1), S. 17–21.

Schulzke, Marcus (2018): The politics of attributing blame for cyberattacks and the costs of uncertainty. In: Perspectives on Politics 16 (4), S. 954–968.

Schünemann, Wolf J. (2020): Cybersicherheit. In: Tanja Klenk, Frank Nullmeier und Göttrik Wewer (Hg.): Handbuch Digitalisierung in Staat und Verwaltung. Wiesbaden: Springer Fachmedien Wiesbaden, S. 199–208.

Schwartz, Mathew J. (2017): French Officials Detail ›Fancy Bear‹ Hack of TV5Monde. Hg. v. Bankinfo Security. Online verfügbar unter https://www.bankinfosecurity.com

/french-officials-detail-fancy-bear-hack-tv5monde-a-9983, zuletzt aktualisiert am 12.06.2017, zuletzt geprüft am 19.04.2021.

Scobell, Andrew (2000): Chinese Army Building in the Era of Jiang Zemin. Carlisle: Strategic Studies Institute, U.S. Army War College.

Scott-Railton, John; Marczak, Bill; Anstis, Siena; Razzak, Bahr Abdul; Crete-Nishihata, Masashi; Deibert, Ron (2019): Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware. Hg. v. The Citizen Lab. Online verfügbar unter https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/, zuletzt aktualisiert am 20.03.2019, zuletzt geprüft am 26.10.2021.

Scott-Railton, John; Marczak, Bill; Razzak, Bahr Abdul; Crete-Nishihata, Masashi; Deibert, Ron (2017): Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware – The Citizen Lab. Hg. v. The Citizen Lab. Online verfügbar unter https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/, zuletzt aktualisiert am 19.06.2017, zuletzt geprüft am 26.10.2021.

Seals, Tara (2018): UK Launches Offensive Cyber-Weapons Against Islamic State. Hg. v. Infosecurity Magazine. Online verfügbar unter https://www.infosecurity-magazine.com/news/uk-launches-offensive-cyberweapons/, zuletzt aktualisiert am 12.04.2018.

Securelist (2013): Winnti. More than just a game. Hg. v. Kaspersky. Online verfügbar unter https://securelist.com/winnti-more-than-just-a-game/37029/, zuletzt aktualisiert am 11.04.2013, zuletzt geprüft am 25.06.2021.

Security Joes (2021): In the Media. News. Hg. v. Security Joes. Online verfügbar unter https://www.securityjoes.com/news, zuletzt aktualisiert am 26.09.2021, zuletzt geprüft am 06.01.2022.

Segal, Adam (2016): The U.S.-China Cyber Espionage Deal One Year Later. Hg. v. Council on Foreign Relations. Online verfügbar unter https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later, zuletzt aktualisiert am 28.09.2016, zuletzt geprüft am 04.08.2021.

Segal, Adam (2018): Cyber Week in Review: January 26, 2018. Hg. v. Council on Foreign Relations. Online verfügbar unter https://www.cfr.org/blog/cyber-week-review-january-26-2018, zuletzt aktualisiert am 26.01.2018, zuletzt geprüft am 20.08.2021.

Seybolt, Taylor B. (2007): Humanitarian military intervention: the conditions for success and failure: SIPRI Publication.

Shachtman, Noah (2010): Exclusive: Google, CIA Invest in ›Future‹ of Web Monitoring. Hg. v. Wired. Online verfügbar unter https://www.wired.com/2010/07/exclusive-google-cia/, zuletzt aktualisiert am 29.07.2010, zuletzt geprüft am 12.08.2021.

Shackelford, Scott J.; Sulmeyer, Michael; Deckard, Amanda N. Craig; Buchanan, Ben; Micic, Brian (2017): From Russia with Love: Understanding the Russian Cyber Threat to US Critical Infrastructure and What to Do about It. In: Nebraska Law Review 96 (2), S. 320–338.

Shafy, Samiha (2022): Sturm auf das Kapitol: Nach dem Sturm. Hg. v. Die Zeit. Online verfügbar unter https://www.zeit.de/2022/02/kapitol-sturm-donald-trump-anhaenger, zuletzt aktualisiert am 06.01.2022, zuletzt geprüft am 18.01.2022.

Shah, Anup (2004): The Bush Doctrine of Pre-emptive Strikes; A Global Pax Americana. Hg. v. Global Issues. Online verfügbar unter https://www.globalissues.org/article/4

50/the-bush-doctrine-of-pre-emptive-strikes-a-global-pax-americana, zuletzt aktualisiert am 24.04.2004, zuletzt geprüft am 01.09.2021.

Shamir, Eli (2005): Computer Science and Technology in Israel 1950–1980. Hg. v. Rutherford Journal. Online verfügbar unter http://rutherfordjournal.org/article030111.html, zuletzt geprüft am 21.10.2021.

Shanghai Cooperation Organization (2009): Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security, 16.06.2009. Online verfügbar unter https://ccdcoe-admin.aku.co/wp-content/uploads/2018/11/SCO-090616-IISAgreement.pdf.

Sherstobitoff, Ryan; Malhotra, Asheer (2018): ›Operation Oceansalt‹ Attacks South Korea, U.S., and Canada With Source Code From Chinese Hacker Group. Hg. v. McAfee. Online verfügbar unter https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf#:~:text=McAfee%C2%AE%20Advanced%20Threat%20Research%20and%20Anti-Malware%20Operations%20teams,described%20this%20implant%20in%20any%20of%20our%20analyses., zuletzt aktualisiert am 18.10.2018, zuletzt geprüft am 02.07.2021.

Sheva, Arutz (2020): Cybersecurity: Israel Aerospace Industries collaborates with Mellanox Technologies. Hg. v. Arutz Sheva – Israel National News. Online verfügbar unter https://www.israelnationalnews.com/News/News.aspx/274641, zuletzt aktualisiert am 16.01.2020, zuletzt geprüft am 11.10.2021.

Shih, Gerry; Kuo, Lily (2021): Trump upsets decades of U.S. policy on Taiwan, leaving thorny questions for Biden. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/world/asia_pacific/trump-biden-taiwan-china/2021/01/13/1bbadee0-53c0-11eb-acc5-92d2819a1ccb_story.html, zuletzt aktualisiert am 13.01.2021, zuletzt geprüft am 02.08.2021.

Shirk, Susan (2017): Trump and China: Getting to yes with Beijing. In: Foreign Affairs 96, S. 20–27. Online verfügbar unter https://www.washingtonpost.com/world/asia_pacific/trump-biden-taiwan-china/2021/01/13/1bbadee0-53c0-11eb-acc5-92d2819a1ccb_story.html.

Shirk, Susan L. (2018): The Return to Personalistic Rule. In: Journal of Democracy 29 (2), S. 22–36. DOI: 10.1353/jod.2018.0022.

Shorrock, Tim (2016): 5 Corporations Now Dominate Our Privatized Intelligence Industry. Hg. v. The Nation. Online verfügbar unter https://www.thenation.com/article/archive/five-corporations-now-dominate-our-privatized-intelligence-industry/, zuletzt aktualisiert am 08.09.2016, zuletzt geprüft am 25.08.2021.

Sigholm, Johan (2013): Non-state actors in cyberspace operations. In: Journal of Military Studies 4 (1), S. 1–37.

Simon, Herbert A. (1972): Theories of bounded rationality. In: Decision and organization 1 (1), S. 161–176.

Simpson, Dwight J. (1970): Israel: A Garrison State. In: Current History 58 (341), S. 1–47. Online verfügbar unter http://www.jstor.org/stable/45314003.

Singhofen, Sven (2010): Kapitel 11 Terrorbekämpfung in Tschetschenien und im Nordkaukasus: Mission accomplished or failed? In: Jahrbuch Terrorismus 4, S. 193–214. Online verfügbar unter http://www.jstor.org/stable/24916942.

Smeets, Max (2020): U.S. cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection. In: Intelligence and National Security 35 (3), S. 444–453. DOI: 10.1080/02684527.2020.1729316.

Smeets, Max (2022, forthcoming): No Shortcuts. Why States Struggle to Develop a Military Cyber-Force. London: Hurst Publishers.

Smith, Noah (2021): Why is China smashing its tech industry? Hg. v. Noahpinion. Online verfügbar unter https://noahpinion.substack.com/p/why-is-china-smashing-its-tech-industry?token=eyJ1c2VyX2lkIjozMTU4OSwicG9zdF9pZCI6MzkxNjg0MDcsIl8iOiJxUEx3dSIsImlhdCI6MTYyNzQxNDM0NywiZXhwIjoxNjI3NDE3OTQ3LCJpc3MiOiJwdWItMzUzNDUiLCJzdWIiOiJwb3NoLXJlYWNoaW9uIno.32h, zuletzt aktualisiert am 25.07.2021, zuletzt geprüft am 04.08.2021.

Snape, Holly; Wang, Weinan (2020): Finding a place for the Party: debunking the »party-state« and rethinking the state-society relationship in China's one-party system. In: Journal of Chinese Governance 5 (4), S. 477–502. DOI: 10.1080/23812346.2020.1796411.

Snowden, Edward (2019): Permanent record: Pan Macmillan.

Sobhani, Sohrab C. (1989): The pragmatic entente: Israeli-Iranian relations, 1948–1988. Dissertation. Georgetown University.

Soesanto, Stefan (2020): A one-sided Affair: Japan and the People's Republic of China in Cyberspace. In: CSS Cyberdefense Hotspot Analyses, S. 1–38. DOI: 10.3929/ethz-b-000389371.

Soesanto, Stefan (2021): The limits of like-mindedness in cyberspace. Hg. v. Elcano Royal Institute. Online verfügbar unter https://www.realinstitutoelcano.org/en/analyses/the-limits-of-like-mindedness-in-cyberspace/, zuletzt aktualisiert am 19.11.2021, zuletzt geprüft am 15.12.2022.

Soffer, Ari (2014): Report: IDF Foiled Massive Cyber-Attack on Israel. Hg. v. Israel National News. Online verfügbar unter https://www.israelnationalnews.com/News/News.aspx/184518#.U_, zuletzt aktualisiert am 28.08.2014, zuletzt geprüft am 07.10.2021.

Solomon, Lawrence (2012): Netanyahu's calculus. Hg. v. National Post. Online verfügbar unter https://nationalpost.com/opinion/lawrence-solomon-netanyahus-calculus, zuletzt aktualisiert am 19.08.2012, zuletzt geprüft am 03.01.2022.

Solomon, Shoshanna (2017): Israeli firm sees the spy agencies behind the sexy images. Hg. v. The Times of Israel. Online verfügbar unter https://www.timesofisrael.com/israel-firm-sees-the-spy-agencies-behind-the-sexy-images/, zuletzt aktualisiert am 28.08.2017, zuletzt geprüft am 11.10.2021.

Solomon, Shoshanna (2021): Alumni of 8200 unit win tender to boost women in R&D jobs. Hg. v. Times of Israel. Online verfügbar unter https://www.timesofisrael.com/alumni-of-8200-unit-win-tender-to-boost-women-in-rd-jobs/, zuletzt aktualisiert am 11.03.2021, zuletzt geprüft am 25.10.2021.

Sørli, Mirjam E.; Gleditsch, Nils Petter; Strand, Håvard (2005): Why is there so much conflict in the Middle East? In: Journal of Conflict Resolution 49 (1), S. 141–165.

Soschnikow, Andrej (2020): »Отключить интернет в небольшой стране«. Хакеры рассказали о новом кибероружии, заказанном ФСБ. Hg. v. BBC News Russia. Online verfügbar unter https://www.bbc.com/russian/news-51951933, zuletzt aktualisiert am 18.03.2020, zuletzt geprüft am 10.02.2022.

Sparks, C. (2003): Are the Western Media Really That Interested in China? In: Javnost – The Public 10 (4), S. 93–108.

Sperling, Valerie (2016): Putin's macho personality cult. In: Communist and Post-Communist Studies 49 (1), S. 13–23.

Spiegel, Steven L. (1983): Israel as a strategic asset. In: Commentary 75 (6), S. 51.

Spiegel Politik (2015): Russland erklärt US-Organisationen für unerwünscht. Hg. v. Spiegel Politik. Online verfügbar unter https://www.spiegel.de/politik/ausland/russland-erklaert-us-organisationen-fuer-unerwuenscht-a-1065291.html, zuletzt aktualisiert am 30.11.2015.

Spindler, Manuela (2014): Interdependence. In: Siegfried Schieder und Manuela Spindler (Hg.): Theories of international relations. London: Routledge, S. 56–75.

Staff, Toi (2020): Israel aghast at Iran cyberattack on civilian water infrastructure — TV report. Hg. v. Times of Israel. Online verfügbar unter https://www.timesofisrael.com/israel-aghast-at-iran-cyberattack-on-civilian-water-infrastructure-tv-report/, zuletzt aktualisiert am 09.05.2020, zuletzt geprüft am 07.10.2021.

Staniland, Paul (2015): Militias, Ideology, and the State. In: Journal of Conflict Resolution 59 (5), S. 770–793. DOI: 10.1177/0022002715576749.

Starks, Tim (2016): Obama administration accuses Russian government of election-year hacking. Hg. v. Politico. Online verfügbar unter https://www.politico.com/story/2016/10/obama-administration-accuses-russian-government-of-election-year-hacking-229296, zuletzt aktualisiert am 08.10.2016, zuletzt geprüft am 02.09.2021.

Stathis N. Kalyvas (1999): THE DECAY AND BREAKDOWN OF COMMUNIST ONE-PARTY SYSTEMS. In: Annual Review of Political Science 2 (1), S. 323–343. DOI: 10.1146/annurev.polisci.2.1.323.

Steffens, Timo (2018): Auf der Spur der Hacker. Wie man die Täter hinter der Computer-Spionage enttarnt. Berlin: Springer Vieweg.

Steffens, Timo (2020): Attribution of advanced persistent threats. How to identify the actors behind cyber-espionage. Berlin, Heidelberg: Springer Vieweg.

Steiger, Stefan; Harnisch, Sebastian; Zettl, Kerstin; Lohmann, Johannes (2018): Conceptualising conflicts in cyberspace. In: Journal of Cyber Policy 3 (1), S. 77–95. DOI: 10.1080/23738871.2018.1453526.

Stein, Jeff (2017): Exclusive: Russian Hackers Attacked the 2008 Obama Campaign. Hg. v. Newsweek. Online verfügbar unter https://www.newsweek.com/russia-hacking-trump-clinton-607956, zuletzt aktualisiert am 12.05.2017.

Stern (2019): Unit 8200 – diese Cyber-Soldaten sind der Motor für Israels Techboom. Hg. v. Stern. Online verfügbar unter https://www.stern.de/digital/online/unit-8200---diese-cyber-soldaten-sind-der-motor-fuer-israels-techboom-8757932.html, zuletzt aktualisiert am 18.06.2019, zuletzt geprüft am 25.10.2021.

Sternstein, Aliya (2016): DHS: Cyberattack on the Ukraine Power Grid Could Happen Here. Hg. v. Nextgov. Online verfügbar unter https://www.nextgov.com/cybersecurity/2016/04/dhs-ukraine-cyberattack-power-grid-could-happen-here/127262/, zuletzt aktualisiert am 06.04.2016, zuletzt geprüft am 29.09.2021.

Stewart, Will (2009): Were Russian security services behind the leak of ›Climategate‹ emails? Hg. v. Dailymail. Online verfügbar unter https://www.dailymail.co.uk/news/article-1233562/Emails-rocked-climate-change-campaign-leaked-Siberian-closed

-city-university-built-KGB.html, zuletzt aktualisiert am 06.12.2009, zuletzt geprüft am 19.05.2021.

Stoler, Yoav (2018): Israel to Train High Schoolers for Big Data Intelligence Jobs. Hg. v. Ctech. Online verfügbar unter https://www.calcalistech.com/ctech/articles/0,7340,L-3728778,00.html, zuletzt aktualisiert am 03.01.2018, zuletzt geprüft am 25.10.2021.

Stone, Jeff (2015a): Chinese Government Suspected In GitHub Hack, Evidence Links DDoS Attack To Censorship Push. Hg. v. International Business Times. Online verfügbar unter https://www.ibtimes.com/chinese-government-suspected-github-hack-evidence-links-ddos-attack-censorship-push-1863556, zuletzt aktualisiert am 30.03.2015, zuletzt geprüft am 02.08.2021.

Stone, Jeff (2015b): Meet CyberBerkut, The Pro-Russian Hackers Waging Anonymous-Style Cyberwarfare Against Ukraine. Online verfügbar unter https://www.ibtimes.com/meet-cyberberkut-pro-russian-hackers-waging-anonymous-style-cyberwarfare-against-2228902, zuletzt aktualisiert am 17.12.2015, zuletzt geprüft am 19.04.2021.

Stracqualursi, Veronica (2017): 10 times Trump attacked China and its trade relations with the US. Hg. v. ABC News. Online verfügbar unter https://abcnews.go.com/Politics/10-times-trump-attacked-china-trade-relations-us/story?id=46572567, zuletzt aktualisiert am 09.11.2017, zuletzt geprüft am 01.10.2021.

Strauss, Daniel (2016): Russian government hackers broke into DNC servers, stole Trump oppo. Hg. v. Politico. Online verfügbar unter https://www.politico.com/story/2016/06/russian-government-hackers-broke-into-dnc-servers-stole-trump-oppo-224315, zuletzt aktualisiert am 14.06.2016, zuletzt geprüft am 20.08.2021.

Stubbs, Jack; Bing, Christopher (2019): Hacking the hackers: Russian group hijacked Iranian spying operation, officials say. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-russia-cyber/hacking-the-hackers-russian-group-hijacked-iranian-spying-operation-officials-say-idUSKBN1X00AK, zuletzt aktualisiert am 21.10.2019, zuletzt geprüft am 14.04.2021.

Stykow, Petra (2006): Gesellschaft als staatliche Veranstaltung? Unternehmerverbände und Staat in Rußland. In: Osteuropa 56 (9), S. 25–42. Online verfügbar unter https://www.jstor.org/stable/44934083.

Sukhankin, Sergey (2018): ›Continuing War by Other Means‹: The Case of Wagner, Russia's Premier Private Military Company in the Middle East. Jamestown Foundation. Online verfügbar unter https://jamestown.org/program/continuing-war-by-other-means-the-case-of-wagner-russias-premier-private-military-company-in-the-middle-east/, zuletzt geprüft am 11.06.2020.

Swed, Ori; Butler, John Sibley (2015): Military Capital in the Israeli Hi-tech Industry. In: Armed Forces & Society 41 (1), S. 123–141. DOI: 10.1177/0095327X13499562.

Symantec (2018): Thrip: Espionage Group Hits Satellite, Telecoms, an Defense Companies. Hg. v. Symantec. Online verfügbar unter https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets, zuletzt aktualisiert am 19.06.2018.

Tagesschau (2009): Russland: Medwedjew kippt schärferes Mediengesetz. Hg. v. Tagesschau. Online verfügbar unter http://www.tagesschau.de/ausland/medwedew26.html, zuletzt aktualisiert am 12.12.2009, zuletzt geprüft am 19.05.2021.

Tanase, Stefan (2015): Turla in the Sky: Satelliten-C&C. Hg. v. Kaspersky. Online verfügbar unter https://de.securelist.com/satellite-turla-apt-command-and-control-in-the-sky/65255/, zuletzt aktualisiert am 09.09.2015, zuletzt geprüft am 14.04.2021.

Tang, Rose (2001): China-U.S. cyber war escalates. Hg. v. CNN. Online verfügbar unter https://edition.cnn.com/2001/WORLD/asiapcf/east/04/27/china.hackers/index.html, zuletzt aktualisiert am 01.05.2001, zuletzt geprüft am 02.07.2021.

Tanriverdi, Hakan (2018): »Der Mythos vom anonymen Hacken wankt«. Hg. v. Süddeutsche Zeitung. Online verfügbar unter https://www.sueddeutsche.de/digital/cyber angriffe-der-mythos-vom-anonymen-hacken-wankt-1.3868826, zuletzt aktualisiert am 16.02.2018, zuletzt geprüft am 20.04.2021.

Tanriverdi, Hakan; Eckert, Svea; Strozyk, Jan; Zierer, Maximilian; Ciesielski, Rebecca (2019): Winnti: Attacking the Heart of the German Industry. Hg. v. Bayerischer Rundfunk. Online verfügbar unter https://web.br.de/interaktiv/winnti/english/, zuletzt aktualisiert am 24.07.2019, zuletzt geprüft am 25.06.2021.

TeamPassword (2021): Who is Deep Panda and how can you protect yourself? Hg. v. TeamPassword. Online verfügbar unter https://www.teampassword.com/blog/who-is-deep-panda-and-how-can-you-protect-yourself, zuletzt aktualisiert am 31.08.2021, zuletzt geprüft am 12.11.2021.

Temple-Raston, Dina (2019): How the U.S. hacked ISIS. Hg. v. National Public Radio. Online verfügbar unter https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis?t=1576775524015.

Tendler, Idan (2015): From The Israeli Army Unit 8200 To Silicon Valley. Hg. v. Techcrunch. Online verfügbar unter https://techcrunch.com/2015/03/20/from-the-8200-to-silicon-valley/, zuletzt aktualisiert am 20.03.2015, zuletzt geprüft am 11.10.2021.

Tertytchnaya, Katerina (2020): Protests and Voter Defections in Electoral Autocracies: Evidence From Russia. In: Comparative Political Studies 53 (12), S. 1926–1956. DOI: 10.1177/0010414019843556.

The Bell (2017): Прототип космического корабля для полетов на Марс от SpaceX Илона Маска впервые совершил успешную посадку — The Bell [Wie Amerika von den »russischen Hackern« erfuhr]. Hg. v. The Bell. Online verfügbar unter https://thebell.io/prototip-kosmicheskogo-korablya-dlya-poletov-na-mars-ot-spacex-ilona-maska-vpervye-sovershil-uspeshnuyu-posadku, zuletzt aktualisiert am 05.12.2017, zuletzt geprüft am 06.05.2021.

The Guardian (2007): Barack Obama's campaign speech. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/world/2007/feb/10/barackobama, zuletzt aktualisiert am 10.02.2007, zuletzt geprüft am 27.09.2021.

The Hague Program on International Cyber Security (2022): Closing the Gap 2022 | Responsibility in Cyberspace: Narratives and Practice. Call for Papers. Hg. v. Leiden University. Online verfügbar unter https://www.thehagueprogram.nl/news/closing-the-gap-2022-responsibility-in-cyberspace-narratives-and-practice, zuletzt geprüft am 12.02.2022.

The Jerusalem Post (2012): Israel among top arms exporters and importers. Hg. v. The Jerusalem Post. Online verfügbar unter https://www.jpost.com/Defense/Israel-among-top-arms-exporters-and-importers, zuletzt aktualisiert am 28.08.2012, zuletzt geprüft am 02.01.2022.

The New York Times (2009): WikiLeaks Archive — A Selection From the Cache of Diplomatic Dispatches. China's Ties to the World of Computer Hackers. Hg. v. The New York Times. Online verfügbar unter https://archive.nytimes.com/www.nytimes.com/interactive/2010/11/28/world/20101128-cables-viewer.html#report/china-09STATE67105, zuletzt aktualisiert am 19.06.2011, zuletzt geprüft am 02.07.2021.

The Straits Times (2017): Having Chinese Communist Party membership is like having ›a diploma‹, ›opens doors‹. Hg. v. The Straits Times. Online verfügbar unter https://www.straitstimes.com/asia/east-asia/having-chinese-communist-party-membership-is-like-having-a-diploma-and-opens-doors, zuletzt aktualisiert am 21.10.2017, zuletzt geprüft am 09.07.2021.

The Wall Street Journal (2016): China's ›White-Hat‹ Hackers Fear Dark Times After Community Founder Is Detained. Hg. v. The Wall Street Journal. Online verfügbar unter https://www.wsj.com/articles/BL-CJB-29440, zuletzt aktualisiert am 01.08.2016, zuletzt geprüft am 11.10.2021.

The White House (2009a): Remarks by the President on Securing Our Nation's Cyber Infrastructure. Hg. v. The White House. Online verfügbar unter https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure, zuletzt aktualisiert am 02.03.2010, zuletzt geprüft am 24.08.2021.

The White House (2009b): The Comprehensive National Cybersecurity Initiative. Hg. v. The White House. Online verfügbar unter https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative, zuletzt geprüft am 24.08.2021.

The White House (2021): The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China. Online verfügbar unter https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/, zuletzt aktualisiert am 19.07.2021, zuletzt geprüft am 01.10.2021.

Thomas, Neil (2020): Members Only: A Look at Recruitment Trends in the CCP. Hg. v. MacroPolo. Online verfügbar unter https://macropolo.org/analysis/members-only-recruitment-trends-in-the-chinese-communist-party/, zuletzt aktualisiert am 15.07.2020, zuletzt geprüft am 09.07.2021.

Thomas Colatin, Samuele de (2019): Power grid cyberattack in Ukraine (2015) – International cyber law: interactive toolkit. Hg. v. CCDCOE. Online verfügbar unter https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015), zuletzt aktualisiert am 17.05.2019, zuletzt geprüft am 16.04.2021.

Threat Connect Research Team (2016): Does a BEAR Leak in the Woods? Hg. v. ThreatConnect. Online verfügbar unter https://threatconnect.com/blog/does-a-bear-leak-in-the-woods/#post_content, zuletzt aktualisiert am 12.08.2016, zuletzt geprüft am 20.08.2021.

ThreatConnect (2015): Project Camerashy. Closing the Aperture on China's Unit 78020. Hg. v. ThreatConnect. Online verfügbar unter https://cdn2.hubspot.net/hubfs/454298/Project_CAMERASHY_ThreatConnect_Copyright_2015.pdf, zuletzt geprüft am 02.07.2021.

ThreatConnect (2016): Belling the BEAR. Hg. v. ThreatConnect Insights. ThreatConnect. Online verfügbar unter https://threatconnect.com/blog/russia-hacks-belling cat-mh17-investigation/, zuletzt aktualisiert am 28.09.2016, zuletzt geprüft am 20.04.2021.

ThreatExpert (2008): ThreatExpert Blog: Agent.btz – A Threat That Hit Pentagon. Hg. v. ThreatExpert. Online verfügbar unter http://blog.threatexpert.com/2008/11/agen tbtz-threat-that-hit-pentagon.html, zuletzt aktualisiert am 28.02.2020, zuletzt geprüft am 14.04.2021.

TMG (2014): About Us. Hg. v. Tianji Media Group. Online verfügbar unter http://www.ti anjimedia.com/english/.

Tobin, Liza (2018): Xi's Vision for Transforming Global Governance: A Strategic Challenge for Washington and Its Allies (November 2018). In: Texas National Security Review 2 (1). DOI: 10.26153/TSW/863.

Top Universities (2020): Computer Science and Information Systems 2020. Hg. v. Top Universities. Online verfügbar unter https://www.topuniversities.com/university-r ankings/university-subject-rankings/2020/computer-science-information-system s, zuletzt aktualisiert am 24.08.2021, zuletzt geprüft am 24.08.2021.

Torbati, Yeganeh (2016): Trump election puts Iran nuclear deal on shaky ground. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-usa-election-t rump-iran-idUSKBN13427E, zuletzt aktualisiert am 09.11.2016, zuletzt geprüft am 06.10.2021.

Treisman, Daniel (2007): Putin's silovarchs. In: Orbis 51 (1), S. 141–153.

Tress, Luke (2021): Chinese group carried out widespread cyber espionage campaign in Israel. Hg. v. The Times of Israel. Online verfügbar unter https://www.timesofisrael .com/chinese-group-carried-out-widespread-cyber-espionage-campaign-in-israel -report/, zuletzt aktualisiert am 10.08.2021, zuletzt geprüft am 12.02.2022.

Troianovski, Anton (2021): China Censors the Internet. So Why Doesn't Russia? Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2021/02/21 /world/europe/russia-internet-censorship.html, zuletzt aktualisiert am 10.03.2021, zuletzt geprüft am 05.05.2021.

Troianovski, Anton; Nakashima, Ellen (2018): How Russia's military intelligence agency became the covert muscle in Putin's duels with the West. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/world/europe/ho w-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-du els-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html, zuletzt aktualisiert am 28.12.2018, zuletzt geprüft am 12.05.2021.

Tse, Don (2018): Why General Fang Fenghui Was Purged. Hg. v. The Diplomat. Online verfügbar unter https://thediplomat.com/2018/01/why-general-fang-fenghui-was-pur ged/, zuletzt aktualisiert am 14.01.2018, zuletzt geprüft am 31.07.2021.

Tsygankov, Andrei P. (2019): Russia and America. The asymmetric rivalry. Cambridge, UK, Medford, MA, USA: Polity.

Tucker, Patrick (2018): Russia Launched Cyber Attacks Against Ukraine Before Ship Seizures, Firm Says. Hg. v. DefenseOne. Online verfügbar unter https://www.defen seone.com/technology/2018/12/russia-launched-cyber-attacks-against-ukraine-shi

p-seizures-firm-says/153375/, zuletzt aktualisiert am 07.12.2018, zuletzt geprüft am 28.04.2021.

U.S. Government (2007): Blackwater USA. Hearing before the Committee on Oversight and Government Reform. Hg. v. U.S. Government Printing Office. House of Representatives. Washington, D.C. Online verfügbar unter https://oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/20071127131151.pdf, zuletzt aktualisiert am 02.10.2007, zuletzt geprüft am 23.04.2020.

U.S. Mission Korea (2017): Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea. Hg. v. U.S. Embassy & Consulate in the Republic of Korea. Online verfügbar unter https://kr.usembassy.gov/121917-press-briefing-attribution-wannacry-malware-attack-north-korea/, zuletzt aktualisiert am 19.12.2017, zuletzt geprüft am 07.01.2022.

Umland, Andreas (2021): Würde ein Präsident Alexei Nawalny die Krim zurückgeben? Hg. v. Neue Züricher Zeitung. Online verfügbar unter https://www.nzz.ch/meinung/wuerde-ein-praesident-alexei-nawalny-die-krim-zurueckgeben-ld.1600611, zuletzt aktualisiert am 10.02.2021, zuletzt geprüft am 06.05.2021.

Ungerleider, Neal (2013): How Check Point Became The Fortune 500's Cybersecurity Favorite. Hg. v. Fast Company. Online verfügbar unter https://www.fastcompany.com/3012414/how-check-point-became-the-fortune-500s-cybersecurity-favorite, zuletzt aktualisiert am 04.06.2013, zuletzt geprüft am 11.10.2021.

UNODC (2019): Cyberespionage. Hg. v. United Nations Office on Drugs and Crime (E4J University Module Series: Cybercrime. Module 14: Hacktivism, Terrorism, Espionage, Disinformation Campaigns and Warfare in Cyberspace). Online verfügbar unter https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberespionage.html, zuletzt aktualisiert am Juni 2019.

US Cyber Command (o.J.): Command History. Hg. v. US Cyber Command. Online verfügbar unter https://www.cybercom.mil/About/History/, zuletzt aktualisiert am 25.08.2021, zuletzt geprüft am 25.08.2021.

US Government (2014): H. R. 5103. Hg. v. U.S. Government Publishing Office. US Congress. Online verfügbar unter https://www.govinfo.gov/content/pkg/BILLS-113hr5103ih/html/BILLS-113hr5103ih.htm, zuletzt aktualisiert am 14.07.2014, zuletzt geprüft am 12.08.2021.

US Joint Chiefs of Staff (1998): Joint Pub 3–13: Joint Doctrine for Information Operations, October 9, 1998. Hg. v. US Joint Chiefs of Staff US Joint Chiefs of Staff. Online verfügbar unter https://www.hsdl.org/?abstract&did=3759, zuletzt geprüft am 24.08.2021.

US Senate (o.J.): About Treaties. Hg. v. United States Senate. Online verfügbar unter https://www.senate.gov/about/powers-procedures/treaties.htm, zuletzt geprüft am 25.08.2021.

Valache, Carmen (2020): Israel's Unit 8200 trains highly skilled entrepreneurs, who move on to set up cyber defense and autonomous veh. Hg. v. Interesting Engineering. Online verfügbar unter https://interestingengineering.com/israels-unit-8200-a-conveyor-belt-of-high-tech-startups, zuletzt aktualisiert am 17.08.2020, zuletzt geprüft am 25.10.2021.

Valeriano, Brandon (2021): Does the Cyber Offense Have the Advantage? Hg. v. Offensive Cyber Working Group. Online verfügbar unter https://offensivecyber.org/2021/12/2

o/does-the-cyber-offense-have-the-advantage/, zuletzt aktualisiert am 20.12.2021, zuletzt geprüft am 17.01.2022.

Valeriano, Brandon; Jensen, Benjamin (2019): The Myth of the Cyber Offense: The Case for Cyber Restraint. In: Cato Institute Policy Analysis (862).

Valeriano, Brandon; Jensen, Benjamin M.; Maness, Ryan C. (2018): Cyber strategy. The evolving character of power and coercion. New York, NY: Oxford University Press. Online verfügbar unter http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&AN=1776310.

Valeriano, Brandon; Maness, Ryan (2015): Cyber war versus cyber realities. Cyber conflict in the international system. Oxford, New York: Oxford University Press.

Valeriano, Brandon; Maness, Ryan C. (2014): The dynamics of cyber conflict between rival antagonists, 2001–11. In: Journal of Peace Research 51 (3), S. 347–360. DOI: 10.1177/0022343313518940.

Valeriano, Brandon; Maness, Ryan C. (2018): How We Stopped Worrying about Cyber Doom and Started Collecting Data. In: PaG 6 (2), S. 49. DOI: 10.17645/pag.v6i2.1368.

Välisluureamet (2018): International Security and Estonia 2018. Hg. v. Estonian Foreign Intelligence Service. Online verfügbar unter https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf, zuletzt geprüft am 14.04.2021.

Value (2021): World Top Technology Companies by Market Value as on 2020. Hg. v. Value. Online verfügbar unter https://www.value.today/world-top-companies/technology?title=&field_headquarters_of_company_target_id&field_company_category_primary_target_id&field_market_value_jan_2020_value_1=&page=0, zuletzt geprüft am 25.08.2021.

van Apeldoorn, Bastiaan; Graaff, Naná de (2014): Corporate elite networks and US post-Cold War grand strategy from Clinton to Obama. In: European Journal of International Relations 20 (1), S. 29–55. DOI: 10.1177/1354066111433895.

van Apeldoorn, Bastiaan; Graaff, Naná de (2017): Obama's economic recovery strategy open markets and elite power: business as usual? In: Int Polit 54 (3), S. 356–372. DOI: 10.1057/s41311-017-0030-3.

van Rosenthal, Eelco Bosch (2018): Dutch intelligence first to alert U.S. about Russian hack of Democratic Party. Hg. v. NOS. Online verfügbar unter https://nos.nl/nieuwsuur/artikel/2213767-dutch-intelligence-first-to-alert-u-s-about-russian-hack-of-democratic-party.html, zuletzt aktualisiert am 25.01.2018, zuletzt geprüft am 14.04.2021.

vander Straeten, Pascal (2020): Treatise On China's Clandestine Financial Warfare: China's Intelligence Community And The Communist Party As Key Players In Geofinance In The 21st Century«. Dallas Fort Worth, Texas: Value4Risk LLC.

Vavra, Shannon (2019): How did a Chinese APT get a U.S. hacking tool before it was leaked? Check Point has a theory. Hg. v. Cyberscoop. Online verfügbar unter https://www.cyberscoop.com/apt3-nsa-tools-smb-check-point/, zuletzt aktualisiert am 05.09.2019, zuletzt geprüft am 30.06.2021.

Voo, Julia; Hemani, Irfan; Jones, Simon; DeSombre, Winnona; Cassidy, Daniel; Schwarzenbach, Anna (2020): National Cyber Power Index 2020. Methodology and Analytical Considerations. Hg. v. Harvard Kennedy School, Belfer Center for Science and International Affairs. Online verfügbar unter https://www.belfercenter.org/p

ublication/national-cyber-power-index-2020#:~:text=The%20Belfer%20National%20Cyber%20Power,collected%20from%20publicly%20available%20data., zuletzt aktualisiert am 2020, zuletzt geprüft am 25.01.2021.

Walker, Shaun (2017): Ex-minister's harsh jail sentence sends shockwaves through Russian elite. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/world/2017/dec/15/russia-jails-former-economy-minister-alexei-ulyukayev-for-corruption, zuletzt aktualisiert am 15.12.2017, zuletzt geprüft am 12.05.2021.

Walton, Calder (2018): Russia has a long history of eliminating ›enemies of the state‹. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/news/monkey-cage/wp/2018/03/13/russia-has-a-long-history-of-eliminating-enemies-of-the-state/, zuletzt aktualisiert am 13.03.2018, zuletzt geprüft am 14.04.2021.

Wang, Zheng (2014): The Chinese dream: Concept and context. In: Journal of Chinese Political Science 19 (1), S. 1–13.

Warrick, Joby; Nakashima, Ellen (2020): Officials: Israel linked to a disruptive cyberattack on Iranian port facility. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html, zuletzt aktualisiert am 18.05.2020, zuletzt geprüft am 07.10.2021.

Wassermann, Felix (2014): Asymmetrische Kriege. Dissertation. Humboldt-Universität, Berlin.

Watanabe, Daisuke; Schmitz, Peter (2021): 4 Tipps zur Bekämpfung von »Living-off-the-Land«-Angriffe. Hg. v. Security-Insider. Online verfügbar unter https://www.security-insider.de/4-tipps-zur-bekaempfung-von-living-off-the-land-angriffe-a-1046009/, zuletzt aktualisiert am 10.08.2021, zuletzt geprüft am 17.01.2022.

Watkins, Ali (2017): Obama team was warned in 2014 about Russian interference. Hg. v. Politico. Online verfügbar unter https://www.politico.com/story/2017/08/14/obama-russia-election-interference-241547, zuletzt aktualisiert am 14.08.2017, zuletzt geprüft am 08.09.2021.

Waxman, Dov (2009): From Jerusalem to Baghdad? Israel and the War in Iraq. In: International Studies Perspectives 10 (1), S. 1–17. Online verfügbar unter http://www.jstor.org/stable/44218575.

Wehle, Kimberly (2020): The Checks and Balances That Trump Has Swept Away. Hg. v. The Atlantic. Online verfügbar unter https://www.theatlantic.com/ideas/archive/2020/02/checks-and-balances-trump-has-swept-away/606013/, zuletzt aktualisiert am 04.02.2020, zuletzt geprüft am 26.08.2021.

Weiss, Michael (2020): AQUARIUM LEAKS Inside the GRU's Psychological Warfare Program. Hg. v. Free Russia Foundation. Washington, DC. Online verfügbar unter https://www.4freerussia.org/aquarium-leaks-inside-the-gru-s-psychological-warfare-program/.

WeLiveSecurity (2019): Operation Ghost: The Dukes aren't back – they never left | WeLiveSecurity. Hg. v. ESET. Online verfügbar unter https://www.welivesecurity.com/2019/10/17/operation-ghost-dukes-never-left/, zuletzt aktualisiert am 01.10.2020, zuletzt geprüft am 13.04.2021.

Wen, Philip (2017): China denies links to alleged cyber attacks in United States targeting exiled tycoon Guo. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-china-corruption-tycoon-idUSKBN1CD0AP, zuletzt aktualisiert am 08.10.2017, zuletzt geprüft am 04.08.2021.

Whyte, Christopher (2018): Dissecting the Digital World: A Review of the Construction and Constitution of Cyber Conflict Research. In: International Studies Review 20 (3), S. 520–532. DOI: 10.1093/isr/viw013.

Wiegand, Dorothee (2014): Milliardendeal: Sicherheitsfirma FireEye übernimmt Mandiant. Hg. v. Heise Online. Online verfügbar unter https://www.heise.de/security/meldung/Milliardendeal-Sicherheitsfirma-FireEye-uebernimmt-Mandiant-2075120.html, zuletzt aktualisiert am 04.01.2014, zuletzt geprüft am 12.08.2021.

Wilkie, Christina (2021): Biden presses Putin to disrupt cybercriminals in Russia as U.S. grapples with latest ransomware attacks. Hg. v. CNBC. Online verfügbar unter https://www.cnbc.com/2021/07/09/ransomware-biden-presses-putin-to-disrupt-cybercriminals-in-russia.html, zuletzt aktualisiert am 09.07.2021, zuletzt geprüft am 05.08.2021.

William J. Lynn III (2010): Defending a New Domain. The Pentagon's Cyberstrategy. Hg. v. Foreign Affairs. Online verfügbar unter https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain, zuletzt aktualisiert am 01.09.2010, zuletzt geprüft am 14.04.2021.

Williams, Nick (2020): Rockwell to expand cyber services through acquisition of Israeli company. Hg. v. Milwaukee Business Journal. Online verfügbar unter https://www.bizjournals.com/milwaukee/news/2020/01/08/rockwell-to-expand-cyber-services-through.html, zuletzt aktualisiert am 08.01.2020, zuletzt geprüft am 03.11.2021.

WinTotal (2020): Einfach erklärt: Was ist ein Root-Server? Hg. v. WinTotal.de. Online verfügbar unter https://www.wintotal.de/root-server/, zuletzt aktualisiert am 06.08.2021, zuletzt geprüft am 16.01.2022.

Wipperfürth, Christian (2011): Außenpolitik unter Präsident Dmitri Medwedew (2008–2011). In: Christian Wipperfürth (Hg.): Russlands Außenpolitik. 1. Aufl. Wiesbaden: VS Verl. für Sozialwiss (Lehrbuch), S. 101–119.

Wong, Edward; Buckley, Chris (2021): U.S. Says China's Repression of Uighurs Is ›Genocide‹. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2021/01/19/us/politics/trump-china-xinjiang.html, zuletzt aktualisiert am 19.01.2021, zuletzt geprüft am 30.07.2021.

Woo, Stu; Wexler, Alexandra (2021): U.S.-China Tech Fight Opens New Front in Ethiopia. Hg. v. The Straits Times. Online verfügbar unter https://www.wsj.com/articles/u-s-china-tech-fight-opens-new-front-in-ethiopia-11621695273, zuletzt aktualisiert am 22.05.2021, zuletzt geprüft am 04.08.2021.

Work, J. D. (2021): China Flaunts Its Offensive Cyber Power – War on the Rocks. Hg. v. War on the Rocks. Online verfügbar unter https://warontherocks.com/2021/10/china-flaunts-its-offensive-cyber-power/, zuletzt aktualisiert am 22.10.2021, zuletzt geprüft am 25.10.2021.

Work, J. D.; Harknett, Richard (2020): Troubled vision: Understanding recent Israeli–Iranian offensive cyber exchanges. Hg. v. Atlantic Council. Online verfügbar unter https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/trouble

d-vision-understanding-israeli-iranian-offensive-cyber-exchanges/, zuletzt aktualisiert am 22.07.2020, zuletzt geprüft am 03.01.2022.

World Bank (2020): High-technology exports (% of manufactured exports) – China. Hg. v. World Bank. Online verfügbar unter https://data.worldbank.org/indicator/TX.VAL.TECH.MF.ZS?locations=CN, zuletzt geprüft am 26.04.2021.

World Bank (2021a): High-technology exports (% of manufactured exports). Hg. v. World Bank. Online verfügbar unter https://data.worldbank.org/indicator/TX.VAL.TECH.MF.ZS, zuletzt geprüft am 28.04.2021.

World Bank (2021b): High-technology exports (% of manufactured exports) – United States, China. Hg. v. World Bank. Online verfügbar unter https://data.worldbank.org/indicator/TX.VAL.TECH.MF.ZS?locations=US-CN, zuletzt geprüft am 25.08.2021.

World Bank (2021c): Research and Development Expenditure. Hg. v. World Bank. Online verfügbar unter https://databank.worldbank.org/reports.aspx?source=2&series=GB.XPD.RSDV.GD.ZS#, zuletzt aktualisiert am 26.04.2021, zuletzt geprüft am 26.04.2021.

World Bank (2021d): Research and development expenditure (% of GDP) – United States, China. Hg. v. World Bank. Online verfügbar unter https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS?locations=US-CN, zuletzt geprüft am 25.08.2021.

World Bank (2022a): High-technology exports (% of manufactured exports) – Israel. Hg. v. World Bank. Online verfügbar unter https://data.worldbank.org/indicator/TX.VAL.TECH.MF.ZS?locations=IL, zuletzt aktualisiert am 02.01.2022, zuletzt geprüft am 02.01.2022.

World Bank (2022b): Research and development expenditure (% of GDP) – Israel. Hg. v. World Bank. Online verfügbar unter https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS?locations=IL, zuletzt aktualisiert am 02.01.2022, zuletzt geprüft am 02.01.2022.

Wortham, Jenna (2016): Obama Brought Silicon Valley to Washington. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2016/10/30/magazine/barack-obama-brought-silicon-valley-to-washington-is-that-a-good-thing.html?, zuletzt aktualisiert am 25.10.2016, zuletzt geprüft am 02.09.2021.

Wright, Thomas (2017): All measures short of war: the contest for the twenty-first century and the future of American power: Yale University Press.

Wuthnow, Joel; Saunders, Phillip Charles (2017): Chinese military reform in the age of Xi Jinping: Drivers, challenges, and Implications. Hg. v. Institute for National Strategic Studies. Center for the Study of Chinese Military Affairs. Washington, D.C. (China Strategic Perspectives, 10). Online verfügbar unter https://apps.dtic.mil/sti/pdfs/AD1030342.pdf, zuletzt geprüft am 02.08.2021.

Xinhua (2013): Xi Jinping leitete das Treffen, um die Entwicklung und das Management der Parteimitglieder unter der neuen Situation zu stärken. Hg. v. The Central People's Government of the People´s Republic of China. Online verfügbar unter http://www.gov.cn/ldhd/2013-01/28/content_2321165.htm, zuletzt aktualisiert am 28.01.2013, zuletzt geprüft am 09.07.2021.

Yakovlev, Andrey (2020): The Dark Side of Russia: How New Internet Laws and Nationalism Fuel Russian Cybercrime. Hg. v. IntSights. Online verfügbar unter https://int

sights.com/resources/how-new-internet-laws-and-nationalism-fuel-russian-cyber crime, zuletzt aktualisiert am 20.05.2021, zuletzt geprüft am 20.05.2021.

Yeisley, Mark O. (2011): Bipolarity, proxy wars, and the rise of China. In: Strategic Studies Quarterly 5 (4), S. 75–91.

Yerman, Jordan (2019): A Startup Nation: Why Israel Has Become The New Silicon Valley. Hg. v. APEX. Online verfügbar unter https://apex.aero/articles/startup-nation-israel-become-silicon-valley/, zuletzt aktualisiert am 22.05.2019, zuletzt geprüft am 26.10.2021.

Yozma (2021): Overview. Hg. v. Yozma. Online verfügbar unter https://www.yozma.com/overview/, zuletzt geprüft am 26.10.2021.

Zacher, Mark W.; Matthew, Richard A. (1995): Liberal international theory: common threads, divergent strands. In: Charles W. Kegley (Hg.): Controversies in international relations theory. Realism and the neoliberal challenge. New York, NY: St. Martin's Press, S. 107–149.

Zarroli, Jim (2018): It Was A Company With A Lot Of Promise. Then A Chinese Customer Stole Its Technology. Hg. v. NPR. Online verfügbar unter https://www.npr.org/2018/04/09/599557634/it-was-a-company-with-a-lot-of-promise-then-a-chinese-customer-stole-its-technol, zuletzt aktualisiert am 09.04.2018, zuletzt geprüft am 27.07.2021.

Zegart, Amy B. (2000): Flawed by design. The evolution of the CIA, JCS, and NSC. [Nachdr.]. Stanford, California: Stanford University Press.

Zerachovitz, Omri (2021): Israeli hi-tech startups are booming. This is what it takes to raise a unicorn. Hg. v. Haaretz. Online verfügbar unter https://www.haaretz.com/israel-news/business/.premium.MAGAZINE-israeli-hi-tech-startups-are-booming-this-is-what-it-takes-to-raise-a-unicorn-1.9662215, zuletzt aktualisiert am 30.03.2021, zuletzt geprüft am 26.10.2021.

Zetter, Kim (2014): Russian ›Sandworm‹ Hack Has Been Spying on Foreign Governments for Years. Hg. v. Wired. Online verfügbar unter https://www.wired.com/2014/10/russian-sandworm-hack-isight/?redirectURL=https%3A%2F%2Fwww.wired.com%2F2014%2F10%2Frussian-sandworm-hack-isight%2F, zuletzt aktualisiert am 14.10.2014, zuletzt geprüft am 19.05.2021.

Zetter, Kim (2017a): The Ukrainian Power Grid Was Hacked Again. Hg. v. Vice. Online verfügbar unter https://www.vice.com/en/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report, zuletzt aktualisiert am 10.01.2017, zuletzt geprüft am 16.04.2021.

Zetter, Kim (2017b): WikiLeaks Files Show the CIA Repurposing Hacking Code to Save Time, Not to Frame Russia. Hg. v. The Intercept. Online verfügbar unter https://theintercept.com/2017/03/08/wikileaks-files-show-the-cia-repurposing-foreignhacking-code-to-save-time-not-to-frame-russia/.

Zetter, Kim (2019): How Close Did Russia Really Come to Hacking the 2016 Election? Hg. v. Politico. Online verfügbar unter https://www.politico.com/news/magazine/2019/12/26/did-russia-really-hack-2016-election-088171, zuletzt aktualisiert am 26.12.2019, zuletzt geprüft am 05.05.2021.

Zettl, Kerstin (2019): Lesson learned? Demokratische Resilienz gegenüber digitaler Wahlbeeinflussung in den USA und Deutschland. In: Zeitschrift für Außen- und Sicherheitspolitik 12 (4), S. 429–451. DOI: 10.1007/s12399-020-00789-7.

Zettl, Kerstin (2022): Der Einsatz von Cyberproxies zur Wahrung autokratischer Regimesicherheit – Iran und Nordkorea im Vergleich. In: Kerstin Zettl, Sebastian Harnisch und Mischa Hansel (Hg.): Asymmetrien in Cyberkonflikten. Wie Attribution und der Einsatz von Proxies die Normentwicklung beeinflussen. Baden-Baden: Nomos, S. 69 – 104.

Zezula, Ladislav; Kroustek, Jakub; Hron, Martin (2017): It's Rabbit season: BadRabbit ransomware infects airports and subways. Hg. v. Threat Intelligence Team. Avast. Online verfügbar unter https://blog.avast.com/its-rabbit-season-badrabbit-ransomware-infects-airports-and-subways, zuletzt aktualisiert am 25.10.2017, zuletzt geprüft am 19.04.2021.

Zheng, Yongnian; Tok, Sow Keat (2007): Harmonious society and harmonious world: China's policy discourse under Hu Jintao. In: Briefing Series 26, S. 1–12.

Zhou, Taomo (2015): Ambivalent Alliance: Chinese Policy towards Indonesia, 1960–1965. In: The China Quarterly 221, S. 208–228. DOI: 10.1017/s0305741014001544.

Zhu, Zhiqun (2020): Interpreting China's ›Wolf-Warrior Diplomacy‹. Hg. v. The Diplomat. Online verfügbar unter https://thediplomat.com/2020/05/interpreting-china s-wolf-warrior-diplomacy/, zuletzt aktualisiert am 15.05.2020, zuletzt geprüft am 17.06.2021.