

DAFTAR PUSTAKA

- AwanPintar.id. (2024). *Laporan ancaman digital di Indonesia semester 1 tahun 2024*. PT Prosperita Sistem Indonesia.
- Badan Riset dan Inovasi Nasional. (2019). *Laporan tahunan ICT / Digital Rights in Indonesia*. SAFENet.
- Badan Siber dan Sandi Negara. (2019). *Laporan hasil monitoring keamanan siber tahun 2019*. Jakarta: Badan Siber dan Sandi Negara.
- Badan Siber dan Sandi Negara. (2020). *Laporan hasil monitoring keamanan siber tahun 2020*. Jakarta: Badan Siber dan Sandi Negara.
- Badan Siber dan Sandi Negara. (2020). *Peraturan Badan Siber dan Sandi Negara Republik Indonesia Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber (CSIRT)*. Jakarta: BSSN. Diakses dari <https://peraturan.bpk.go.id/Details/174287/peraturan-bssn-no-10-tahun-2020>
- Badan Riset dan Inovasi Nasional. (2021). *Profil BRIN*. Diakses 24 Agustus 2025, dari <https://www.brin.go.id/page/6/profil-brin-1>
- Badan Siber dan Sandi Negara. (2021). *Laporan tahunan monitoring keamanan siber tahun 2021*. Jakarta: Badan Siber dan Sandi Negara.
- Badan Siber dan Sandi Negara. (2021). *Tentang BSSN*. Diakses pada 23 Agustus 2025, dari <https://bssn.go.id/tentang-bssn/>
- Badan Siber dan Sandi Negara. (2022). *Lanskap keamanan siber Indonesia tahun 2022*. Jakarta: Badan Siber dan Sandi Negara.
- Badan Siber dan Sandi Negara. (2023). *Lanskap keamanan siber Indonesia tahun 2023*. Jakarta: Badan Siber dan Sandi Negara.
- Badan Siber dan Sandi Negara. (2023, 20 Februari). *BSSN dan Huawei bahas kerja sama pengembangan keamanan siber di Indonesia*. Diakses 23 Agustus 2025, dari <https://bssn.go.id/bssn-dan-huawei-bahas-kerja-sama-pengembangan-keamanan-siber-di-indonesia/>

- Badan Siber dan Sandi Negara. (2023). *Peraturan Badan Siber dan Sandi Negara Republik Indonesia Nomor 7 Tahun 2023 tentang Identifikasi Infrastruktur Informasi Vital*. Jakarta: BSSN. Diakses dari <https://peraturan.bpk.go.id/Details/291263/peraturan-bssn-no-7-tahun-2023>
- Badan Siber dan Sandi Negara. (2023b). *Peraturan Badan Siber dan Sandi Negara Republik Indonesia Nomor 8 Tahun 2023 tentang Kerangka Kerja Pelindungan Infrastruktur Informasi Vital*. Jakarta: BSSN. Diakses dari <https://peraturan.bpk.go.id/Details/291265/peraturan-bssn-no-8-tahun-2023>
- Badan Siber dan Sandi Negara. (2023c). *Peraturan Badan Siber dan Sandi Negara Republik Indonesia Nomor 9 Tahun 2023 tentang Peningkatan Kapasitas Sumber Daya Manusia di Bidang Keamanan Siber dan Sandi*. Jakarta: BSSN. Diakses dari <https://peraturan.bpk.go.id/Details/291275/peraturan-bssn-no-9-tahun-2023>
- Badan Siber dan Sandi Negara. (2024). *Lanskap keamanan siber Indonesia tahun 2024*. Jakarta: Badan Siber dan Sandi Negara.
- Badan Siber dan Sandi Negara. (2024a). *Peraturan Badan Siber dan Sandi Negara Republik Indonesia Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber*. Jakarta: BSSN. Diakses dari <https://peraturan.bpk.go.id/Details/291240/peraturan-bssn-no-1-tahun-2024>
- Badan Siber dan Sandi Negara. (2024b). *Peraturan Badan Siber dan Sandi Negara Republik Indonesia Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber*. Jakarta: BSSN. Diakses dari <https://peraturan.bpk.go.id/Details/291245/peraturan-bssn-no-2-tahun-2024>
- Badan Siber dan Sandi Negara. (2024c). *Peraturan Badan Siber dan Sandi Negara Republik Indonesia Nomor 5 Tahun 2024 tentang Rencana Aksi Nasional Keamanan Siber Tahun 2024–2028 (RANKS)*. Jakarta: BSSN. Diakses dari <https://peraturan.bpk.go.id/Details/309728/peraturan-bssn-no-5-tahun-2024>

Badan Siber dan Sandi Negara. (2024d). *Peraturan Badan Siber dan Sandi Negara Republik Indonesia Nomor 8 Tahun 2024 tentang Standar dan Tata Cara Pelaksanaan Audit Keamanan Sistem Pemerintahan Berbasis Elektronik (SPBE)*. Jakarta: BSSN. Diakses dari <https://peraturan.bpk.go.id/Details/309821/peraturan-bssn-no-8-tahun-2024>

BBC News. (2019, May 20). *Google restricts Huawei's use of Android*. <https://www.bbc.com/news/technology-48363772>.

Bell, M., & Pavitt, K. (1993). Technological accumulation and industrial growth: Contrasts between developed and developing countries. *Industrial and Corporate Change*, 2(2), 157–210.

Beqa, M. (2017). Neoclassical realism: Its promises and limits as a theory of foreign policy. *European Academic Research*, 5(1), April.

BRIN dan Huawei Indonesia. (2019). *Huawei dan BRIN siapkan kerangka kerja sama untuk kembangkan riset dan inovasi*. Diakses (tanggal akses), dari <https://www.brin.go.id/news/95599/huawei-dan-brin-siapkan-kerangka-kerjasama-untuk-kembangkan-ri-set-dan-inovasi>.

BRIN & Huawei Indonesia. (2023). *Kolaborasi BRIN–Huawei perkuat ekosistem riset digital*. Diakses (tanggal akses), dari <https://www.brin.go.id/news/104822/kolaborasi-brin-huawei-perkuat-ekosistem-ri-set-digital>.

BRIN & Huawei Indonesia. (2024). *Dukung pengembangan 100.000 talenta digital Indonesia, BRIN terima apresiasi dari Huawei*. Diakses (tanggal akses), dari <https://www.brin.go.id/news/110997/dukung-pengembangan-100000-talenta-digital-indonesia-brin-terima-apresiasi-dari-huawei>.

Carnegie Endowment for International Peace. (2022). *How Huawei's Localization in North Africa Delivered Mixed Returns*.

Center for Indonesian Policy Studies. (2024). *ICT & security in Southeast Asia: Huawei and regional security concerns*. CIPS.

CNBC Indonesia. (2019, Februari 19). *Bos Huawei: Jika kami memata-matai, saya tutup perusahaan.* CNBC Indonesia.

<https://www.cnbcindonesia.com/tech/20190219115522-37-56341/bos-huawei-jika-kami-memata-matai-saya-tutup-perusahaan>

CNBC Indonesia. (2019, Juli 8). *Riset: Staf Huawei punya hubungan dengan intelijen China.* CNBC Indonesia.

<https://www.cnbcindonesia.com/tech/20190708162145-37-83420/riset-staf-huawei-punya-hubungan-dengan-intelijen-china>

CNN Indonesia. (2019, Oktober 29). *Gandeng Huawei, BSSN sebut tak perlu khawatir isu spionase.* CNN Indonesia.

<https://www.cnnindonesia.com/teknologi/20191029154752-185-443825/gandeng-huawei-bssn-sebut-tak-perlu-khawatir-isu-spionase>

Cyberthreat.id. (2019, Juni 24). *Isu spionase 5G, Chief RA: Itu peran BSSN.*

Cyberthreat.id. <https://cyberthreat.id/read/876/Isu-Spionase-5G-Chief-RA-Itu-Peran-BSSN>

Cyberthreat.id. (2021, 7 Januari). *Huawei: Aman itu standarnya teknologi, bukan opini.* Wawancara dengan VP Huawei Indonesia. Diakses dari

<https://cyberthreat.id/read/10657/huawei-aman-itu-standarnya-teknologi-bukan-opini>.

Dewan Perwakilan Rakyat Republik Indonesia. (2019). *Info Singkat: ASEAN, Indonesia, dan Perang Dagang Amerika Serikat–China.* Pusat Penelitian Badan Keahlian DPR RI.

Dewan Perwakilan Rakyat Republik Indonesia. (2020). *Info Singkat: ASEAN's Response to the Increasing of the US–China Rivalry.* Pusat Penelitian Badan Keahlian DPR RI.

Dewan Perwakilan Rakyat Republik Indonesia. (2020, 26 Februari). *Risalah Rapat Kerja Komisi I DPR RI dengan Wakil Menteri Pertahanan RI.* Jakarta: Sekretariat Jenderal DPR RI.

- Dewan Perwakilan Rakyat Republik Indonesia. (2021, 1 Februari). *Risalah Rapat Kerja Komisi I DPR RI dengan Menteri Komunikasi dan Informatika RI*. Jakarta: Sekretariat Jenderal DPR RI.
- Dewan Perwakilan Rakyat Republik Indonesia. (2025). *Naskah Akademik Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber*. Jakarta: DPR RI.
- Dujarric, E. (2023, March 1). *Indonesia is hooked on Huawei*. The Strategist. Australian Strategic Policy Institute. <https://www.aspistrategist.org.au/indonesia-is-hooked-on-huawei/>.
- Dunn Cavelt, M., & Suter, M. (2009). Public–private partnerships in critical infrastructure protection: Governing critical infrastructures in the US and Europe. *International Affairs*, 85(1), 179–200. <https://doi.org/10.1111/j.1468-2346.2009.00791.x>
- European Commission. (2020). *Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures*. <https://digital-strategy.ec.europa.eu/en/policies/5g-toolbox>
- Fairclough, N. (1992). *Discourse and social change*. Polity Press.
- Federal Communications Commission. (2020, June 30). *FCC designates Huawei and ZTE as national security threats*. <https://www.fcc.gov/document/fcc-designates-huawei-and-zte-national-security-threats>.
- Goffman, E. (1974). *Frame analysis: An essay on the organization of experience*. Harvard University Press.
- Huawei Technologies Co., Ltd. (2021, 28 September). *Huawei Strengthens Contribution and Cooperation in Indonesia Cyber Security*. Diakses 23 Agustus 2025, dari <https://www.huawei.com/en/news/2021/9/tripartite-cooperation-agreement-indonesia-cyber-security>

- Huda, Miftahul & Al-Fadhat, Faris. (2022). The Political Economy of the US-China Cybersecurity Relations and Trade War Under the Trump Administration. *Journal of Islamic World and Politics*. 6. 188-206. 10.18196/jiwp.v6i2.15971.
- Indosat Ooredoo Hutchison. (2024, 3 Juni). Indosat Ooredoo Hutchison and Huawei consolidate core network to serve 100+ million subscribers. Siaran pers resmi. Diakses dari <https://www.huawei.com/en/news/2024/6/indosat-huawei-core-network>
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2018). *Peraturan Menteri Komunikasi dan Informatika Nomor 16 Tahun 2018 tentang Persyaratan Teknis Alat dan/atau Perangkat Telekomunikasi*. Jakarta: Kementerian Komunikasi dan Informatika.
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2021). *Peraturan Pemerintah Republik Indonesia Nomor 46 Tahun 2021 tentang Pos, Telekomunikasi, dan Penyiaran*. Jakarta: Kementerian Sekretariat Negara.
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2025). *Laporan Kinerja 2024: Kementerian Komunikasi dan Digital*. Jakarta: Kementerian Komunikasi dan Informatika Republik Indonesia.
- Kementerian Komunikasi dan Informatika Republik Indonesia – Balai Besar Pengujian Perangkat Telekomunikasi. (2024). *Laporan Kinerja 2024: Balai Besar Pengujian Perangkat Telekomunikasi*. Jakarta: Direktorat Jenderal Sumber Daya dan Perangkat Pos dan Informatika, Kementerian Komunikasi dan Informatika Republik Indonesia.
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2024). *Peraturan Menteri Komunikasi dan Informatika Nomor 3 Tahun 2024 tentang Penyelenggaraan Telekomunikasi*. Jakarta: Kementerian Komunikasi dan Informatika.

- Kementerian Komunikasi dan Informatika Republik Indonesia. (2024). *Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2024 tentang Balai Uji Alat Telekomunikasi*. Jakarta: Kementerian Komunikasi dan Informatika.
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2021). *Rencana Strategis Kementerian Komunikasi dan Informatika 2020–2024*. Jakarta: Kementerian Komunikasi dan Informatika.
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2007). Peraturan Menteri Komunikasi dan Informatika Nomor 26/PER/M.KOMINFO/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet. Jakarta: Kementerian Komunikasi dan Informatika.
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2010). Peraturan Menteri Komunikasi dan Informatika Nomor 16/PER/M.KOMINFO/10/2010 tentang Perubahan atas Peraturan Menteri Komunikasi dan Informatika Nomor 26/PER/M.KOMINFO/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet. Jakarta: Kementerian Komunikasi dan Informatika.
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2011). Peraturan Menteri Komunikasi dan Informatika Nomor 24/PER/M.KOMINFO/12/2011 tentang Perubahan Ketiga atas Peraturan Menteri Komunikasi dan Informatika Nomor 26/PER/M.KOMINFO/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet. Berita Negara Republik Indonesia Tahun 2011 Nomor 797. Jakarta: Kementerian Komunikasi dan Informatika.
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2017). Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2017 tentang Perubahan Keempat atas Peraturan Menteri Komunikasi dan Informatika Nomor 26/PER/M.KOMINFO/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet. Berita Negara Republik Indonesia Tahun 2017 Nomor 164. Jakarta: Kementerian Komunikasi dan Informatika.

- Le Thu, H. (2019). *A Collision of Cybersecurity and Geopolitics: Why Southeast Asia is Wary of a Huawei Ban*. Global Asia.
- Masyarakat Telematika Indonesia (MASTEL). (2021, 12 Agustus). MASTEL dorong operator memenuhi uji verifikasi keamanan NESAS/GSMA-3GPP. Siaran pers. Diakses dari <https://mastel.id/siaran-pers-nesas-gsma-3gpp>
- Mboya, E. (2023). *Huawei and Kenya's Digital Future: Between Connectivity and Control*. African Governance Papers.
- Nestoras, A., & Cappelletti, F. (2022). 5G, geopolitics and European strategic autonomy. *Future of Europe Online Journal*, 1. <https://feu-journal.eu/issues/issue-1/5g-geopolitics-and-european-strategic-autonomy>
- Paramitha Sandy, O. (2019, 24 Desember). *BSSN minta Huawei beri laporan detail soal backdoor*. Cyberthreat.id. <https://m.cyberthreat.id/read/4379/BSSN-Minta-Huawei-Beri-Laporan-Detail-Soal-Backdoor>
- Pierre, J., & Peters, B. G. (2000). *Governance, politics and the state*. Palgrave Macmillan.
- Ramba Santoso, Jascha. (2025, 29 April). *Indonesia is hooked on Huawei. The Strategist* (ASPI).
- Rhodes, R. A. W. (1996). The new governance: Governing without government. *Political Studies*, 44(4), 652–667. <https://doi.org/10.1111/j.1467-9248.1996.tb01747.x>
- Ripsman, N. M., Taliaferro, J. W., & Lobell, S. E. (2016). *Neoclassical realist theory of international politics*. Oxford University Press.
- Rose, G. (1998). Neoclassical realism and theories of foreign policy. *World Politics*, 51(1), 144–172.
- SAIS-CARI. (2020). *Southeast Asia and the Huawei Dilemma*. Johns Hopkins University.

- Sandle, P. (2019, May 16). *U.S. restricts Huawei access to American technology*. Reuters. <https://www.reuters.com/article/us-usa-trade-huawei-tech/u-s-restricts-huawei-access-to-american-technology-idUSKCN1SR1EU>
- Taliaferro, J. W., Lobell, S. E., & Ripsman, N. M. (2009). Introduction: Neoclassical realism, the state, and foreign policy. In J. W. Taliaferro, S. E. Lobell, & N. M. Ripsman (Eds.), *Neoclassical realism, the state, and foreign policy* (pp. 1–41). Cambridge University Press.
- Telkom Indonesia. (2023). *Laporan Tahunan 2023*. Jakarta: PT Telkom Indonesia (Persero) Tbk.
- Telkom Indonesia & Huawei. (2023, 5 Desember). *Telkom and Huawei signed a strategic collaboration to accelerate B2B IT capabilities and digital talent development*. Siaran pers resmi. Diakses dari <https://www.huawei.com/en/news/2023/12/telkom-huawei-b2b-it-digital-talent>
- Universitas Airlangga. (2020). *Alasan kebijakan restriktif Amerika Serikat terhadap Huawei*. Surabaya: Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Airlangga.
- Universitas Brawijaya. (2019). *Analisis yuridis larangan impor Huawei dan ZTE*. Malang: Fakultas Hukum, Universitas Brawijaya.
- Universitas Islam Indonesia. (2023). *Kebijakan sekuritisasi Amerika Serikat terhadap Huawei*. Yogyakarta: Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Islam Indonesia.
- Universitas Muhammadiyah Yogyakarta. (2023). *Analisis kebijakan pelarangan smartphone Huawei*. Yogyakarta: Universitas Muhammadiyah Yogyakarta.
- Universitas Negeri Islam Syarif Hidayatullah Jakarta. (2023). *Analisa kebijakan pelarangan Huawei di Inggris*. Jakarta: Fakultas Ilmu Sosial dan Ilmu Politik, UIN Jakarta.

Universitas Satya Negara Indonesia. (2023). *Implementasi Digital Silk Road (Huawei 5G di Indonesia)*. Jakarta: Universitas Satya Negara Indonesia.

Universitas 17 Agustus 1945 Jakarta. (2024). *Huawei dalam rivalitas Tiongkok–Amerika*. Jakarta: Universitas 17 Agustus 1945 Jakarta.

Universitas Udayana. (2024). *Dampak perkembangan teknologi Huawei China terhadap rivalitas global*. Denpasar: Universitas Udayana.

Universitas Langlangbuana. (2023). *Pembatasan teknologi Huawei oleh Amerika Serikat*. Bandung: Universitas Langlangbuana.

Wibel, A., & Löwenberg, C. (2024). *5G Geopolitics in Europe: Huawei, Sovereignty, and Strategic Autonomy*. Policy Insights Series.