THIRD WAY

Methodology for The Militarization of Cyberspace?

Cyber-Related Provisions in the National Defense Authorization Act

This methodology section details how the author of “The Militarization of Cyberspace? Cyber-Related Provisions in the National Defense Authorization Act” identified and categorized cyber-related provisions that were included in the National Defense Authorization Acts from Fiscal Year 2017 through Fiscal Year 2021.

To identify relevant provisions, the author searched for the following keywords: “cyber,” “fifth generation,” “supply chain,” “encryption,” and “election.” Once all relevant provisions were identified, they were placed into one of the following categories:

- *Civilian Workforce*: Provisions that seek to improve K-12 cyber education programs or the cybersecurity-workforce development pipeline.
- *Critical Infrastructure Protection*: Provisions that seek to improve the cybersecurity of critical infrastructure that fall outside of the Defense Industrial Base.
- *DHS Cyber Mission*: Provisions that provided new authorities to the Department of Homeland Security and the Cybersecurity Infrastructure Security Agency to fulfill their cybersecurity mandates.
- *DoD Organizational Processes and Structure*: Provisions that created cybersecurity positions within DoD; modified command operations; amended purchasing authorities; assessed DoD’s cyber capabilities; or changed authorities for various DoD units.
- *DoD Personnel*: Provisions that increase the number of cyber personnel in DoD and amend their roles and responsibilities.
- *Election Security*: Provisions that seek to improve the cybersecurity of US election infrastructure and to combat misinformation and disinformation directed at US elections.
- *Encryption*: Provisions that mandated the use of encryption to secure information.
- *International Engagement and Nation-State Deterrence*: Provisions that fostered engagement with international partners to improve their cybersecurity posture, as well as policies to deter nation-state actors from conducting cyberattacks.
- *Military Operations*: Provisions on how DoD should engage in offensive and defensive cyber operations; Congressional reporting and notifications requirements; the development of cyber weapons; and DoD exercises that test cyber plans and policies.
- *Miscellaneous*: Provisions that do not fall into the other 12 categories, such as a study on the cybersecurity insurance market, the creation of the National Cyber Director, and increased funds for the research and development of AI and quantum computing.
- *Protection of DoD Assets and Infrastructure*: Provisions that require DoD to protect weapon systems, the defense industrial base, and DoD’s information network.
- *Small Business*: Provisions that help small and medium-sized businesses improve their cybersecurity.
- *Supply Chain Security*: Provisions that protect and secure US information and communication technologies’ (ICT) supply chain, as well as provisions that promote domestic manufacturing of ICT hardware and software.

Conference reports for the five NDAAs were also examined to provide further context on cyber-related provisions.

Please direct any questions to Michael Garcia, senior policy advisor for Third Way’s National Security Program, at mgarcia@thirdway.org.