IMMEDIATE RELEASE

MEDIA CONTACT:
Gabriella Tejeda
+1 646-248-6486
Gaby.Tejeda@thesoufancenter.org

PRESS RELEASE

NEW REPORT EXAMINES HOW AMERICA'S SOFTWARE UNDERSTANDING GAP IS UNDERMINING NATIONAL SECURITY

The research finds that software is being produced faster than it can be understood, creating risks that adversarial states and criminal groups can exploit both today and in the future

LINK TO REPORT

(New York, NY – June 22, 2026) A new report from The Soufan Center (TSC) warns that software understanding blind spots in the United States present credible national security risks. The report, ***Closing the Gap: Software Understanding and U.S. National Security***, warns that as software expands faster than experts can fully understand the technology, dangerous gaps emerge that adversarial state actors and criminal groups are poised to exploit.

Software powers a range of military and civilian systems, from critical infrastructure and energy to financial systems and military technology. "The software understanding gap—that is, the delta between the proliferation of software-defined systems and our ability to understand them—is a major U.S. national security risk that needs to be prioritized, as America's adversaries continue to seek asymmetric means of challenging U.S. primacy," explains TSC's Executive Director Colin P. Clarke.

The report identifies six major areas of risk and highlights how all the areas have already been exploited by US adversaries, including Russia, Iran, and China, as well as criminal organizations and other non-state actors. The research argues that this growing gap between software production and knowledge of complex and evolving software systems presents a fertile terrain for bad actors to exploit and inhabit.

Knowledge over False Choices

Atalanta, a U.S.-founded mathematical AI company who supported the report, argues that it will be increasingly more difficult for actors to defend a software production landscape that they do not fully comprehend. "We are deploying AI systems that make consequential decisions at speeds no human can supervise," says Anjana Rajan, co-founder and CEO of Atalanta. "We keep being offered false choices about how to respond, and every one of them is a way of managing systems we cannot actually understand. There is another path. We can build the capability to understand these systems with mathematical certainty, before we deploy them. That capability exists today. The work now belongs to everyone who builds and defends these systems: to insist they be understood before they are ever trusted."

A core objective of the new report is to inform policymakers of the implications of the software understanding gap within a U.S. national security context. The report offers a series of recommendations

to help maintain U.S. dominance across operational domains and across geopolitical contexts. The report concludes with a set of recommendations designed to close the software understanding gap and mitigate the challenges and risks identified by the research team.

These recommendations include: the need for the U.S. government to empower coordinated interagency software understanding while classifying the topic as a mission requirement integrated into operational planning and acquisition; the need to realign market incentives by tying rigorous security standards to government software acquisition requirements; and, the need to reduce ambiguity and enforce accountability in the cyber domain at all levels and prepare for adaptive adversaries who will shift to lower-profile but higher-volume targets as major systems are hardened.

ABOUT THE SOUFAN CENTER (TSC)

The Soufan Center is an independent nonprofit organization based in New York City. Our mission is to provide cutting-edge research, analysis, and strategies to anticipate and counter the world's most urgent security challenges.

Follow us @TheSoufanCenter and visit our website http://thesoufancenter.org/