CohēCiv

Cyber Resilience for the People

AMBIENT DATA SURVEILLANCE, UBIQUITOUS TECHNICAL SURVEILLANCE, AND THE UBIQUITOUS SURVEILLANCE ECOSYSTEM:

National Security Implications and Strategic Countermeasures

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The modern digital ecosystem has facilitated a shift from traditional surveillance methods to an era of Ambient Data Surveillance (ADS) and Ubiquitous Technical Surveillance (UTS)—two key enablers of the broader Ubiquitous Surveillance Ecosystem (USE).

This paper explores the implications of these emerging surveillance paradigms and how they have fundamentally reshaped the operational security landscape, presenting unprecedented challenges for national security and military and federal operations. You will find that this pervasive data ecosystem also threatens covert military operations, critical infrastructure security, and the integrity of diplomatic and intelligence efforts abroad. The convergence of mass data collection and surveillance monetization has created an asymmetric threat environment where the U.S. must adapt or risk national security compromise. The Department of Defense and allied federal agencies must proactively secure digital identities, restrict adversarial access to data, and reinforce operational safeguards against the evolving threats posed by ADS, UTS, and USE.

1. INTRODUCTION

1.1 The New Data Battlefield

The modern battlespace is no longer confined to physical domains—it has expanded into a data-driven, AI-powered theater of continuous surveillance and exploitation. The unrestricted collection, aggregation, and weaponization of digital and physical surveillance data pose an escalating national security threat to the United States. In this era of hyperconnectivity, adversaries exploit data harvested from personal devices, smart infrastructure, social media platforms, and global information networks to gain strategic, military, and geopolitical advantages. This Ubiquitous Surveillance Ecosystem enables real-time intelligence gathering, precision cyber warfare, and large-scale cognitive influence operations, allowing hostile actors to infiltrate national decision-making processes, manipulate public perception, and erode U.S. military and government operational security (OPSEC).

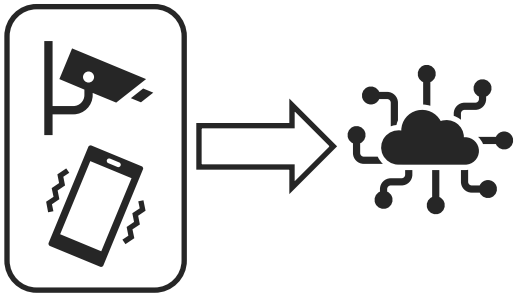
1.2 The ADS-UTS-USE Framework

Ambient Data Surveillance (ADS): Passive, continuous, and often unnoticed collection of personal and behavioral data from individuals through digital and physical environments. Driven by data monetization, this form of surveillance is embedded in everyday life, leveraging ubiquitous technology such as smartphones, IoT devices, social media, online browsing, and retail interactions to gather vast amounts of data without direct user input or explicit consent. This data is effective in mapping individual behavior, predicting trends, and informing influence operations. Advertising Technology (AdTech) platforms enable domestic and foreign entities, both commercial and governmental, to access this collected data.

Ubiquitous Technical Surveillance (UTS): Continuous, pervasive, and often covert monitoring of individuals, organizations, or environments through a wide array of technical means. This includes electronic, digital, and physical surveillance methods that operate across multiple domains- cyberspace, telecommunications, physical spaces, and even biological monitoring. The availability and use of sensors enable real-time monitoring and data collection. Both state actors and private industry engage in UTS for security, intelligence, commercial, or behavioral analytics purposes.

Ubiquitous Surveillance Ecosystem (USE): The global system where collected data is monetized and repurposed for commercial, political, and military exploitation. USE integrates ADS and UTS into a full-spectrum intelligence framework, allowing adversaries to manipulate economies, societies, and defense strategies based on extensive data sets.

Commercial data (ADS) & distributed sensors (UTS) feed into USE, an integrated system where surveillance is continuous, automated, and inescapable.



2. THE NATIONAL SECURITY RISKS OF ADS AND UTS

2.1 Foreign Data Exploitation and Intelligence Operations

The global proliferation of Ambient Data Surveillance and Ubiquitous Technical Surveillance has fundamentally reshaped the intelligence landscape, enabling foreign adversaries to conduct continuous, large-scale data exploitation with minimal risk of detection. Nation-state actors, leveraging vast surveillance ecosystems and AI-driven analytics, can transform seemingly innocuous commercial, digital, and biometric data into powerful intelligence assets for espionage, threat modeling, and strategic targeting of U.S. military, government, and critical infrastructure. As adversaries integrate commercial surveillance data with state-sponsored intelligence collection, traditional counterintelligence (CI) and OPSEC measures struggle to keep pace.

2.1.1 Adversarial Data Aggregation

Nation-state actors, including China and Russia, acquire, analyze, and weaponize commercial datasets to enhance intelligence operations. Data brokers, advertising platforms, and open-source intelligence (OSINT) tools provide adversaries with extensive information on U.S. government officials, military personnel, and private-sector defense contractors. This data enables foreign intelligence agencies to map strategic vulnerabilities, identify key decision-makers, and target high-value individuals for espionage.

2.1.2 Military Readiness & Operational Exposure

A. Fitness apps and social media geotagging have exposed military base locations and troop movements (ex. Strava Heat Map Leak, 2018).
B. IoT-enabled devices within military installations introduce vulnerabilities for real-time activity monitoring and network penetration.
C. Commercially available location and biometric data, typically gathered from mobile electronic devices, can be used to predict operational deployments and tactical movements (ex. One Nation Tracked, New York Times, 2019)

2.2 Cognitive Warfare and Influence Operations

ADS-derived data serves as a force multiplier for adversaries engaging in psychological operations (PsyOps) and digital influence campaigns, enabling highly targeted, scalable, and adaptive manipulation strategies. By leveraging real-time behavioral analytics, sentiment analysis, and AI-driven predictive modeling, adversaries can conduct mis- and disinformation campaigns, exploit cognitive biases, and shape public perception with unprecedented precision.

2.2.1 AI-Enhanced Mis/Disinformation Campaigns

ADS-derived data enables the creation of hyper-personalized misinformation and disinformation campaigns targeting service members, policymakers, and the general public, manipulating decision-making and public sentiment. Machine learning (ML) enables adversaries to adapt and refine these campaigns in real time, increasing their impact and effectiveness.

2.2.2 Behavioral Engineering & PsyOps

The fusion of ADS with machine learning models enables adversaries to predict and influence individual behavior, increasing the effectiveness of psychological operations, election interference, and radicalization efforts. Military personnel and their families are prime targets for adversarial cognitive attacks, like social engineering. This can be especially effective against part-time or transitioning service members, looking to enter the private sector. Examples include AI-powered phishing and deepfake threats and LinkedIn espionage.

2.3 Infrastructure and Cybersecurity Threats

ADS-derived intelligence provides adversaries with unprecedented access to the digital and operational backbone of national infrastructure, supply chains, research and development (R&D) efforts, and military networks. By continuously harvesting vast amounts of real-time data from commercial tracking systems, IoT devices, corporate metadata, and geospatial analytics, adversaries can map, analyze, and exploit vulnerabilities in critical infrastructure with surgical precision.

2.3.1 Supply Chain Intelligence Mapping

The globalization of defense and critical infrastructure supply chains has introduced significant vulnerabilities, allowing adversaries to exploit Ambient Data Surveillance and Ubiquitous Technical Surveillance to conduct real-time intelligence mapping of U.S. logistics, procurement networks, and industrial supply chains. By aggregating and analyzing commercial data, satellite imagery, IoT tracking, financial transactions, and corporate metadata, foreign intelligence services can identify, infiltrate, and manipulate critical supply networks supporting U.S. military operations and national security infrastructure. Additionally, backdoor vulnerabilities in foreign-made technology allow adversaries to exfiltrate sensitive data from critical industries.

2.3.2 Cyber Attack Surface Expansion

A vast network of interconnected devices creates an expanded attack surface for predictive social engineering, AI-driven phishing, and Kinetic Cyber Operations (KCO)— that is, the integration of cyberattacks with physical, real-world effects, where digital intrusions directly trigger damage, disruption, or destruction of tangible infrastructure, military assets, or human targets. These operations bridge the gap between cyberspace and kinetic warfare, using cyber means to manipulate, disable, or sabotage critical systems that control physical processes. Examples of KCO include Stuxnet (2010) and Russia's GPS spoofing and jamming in Ukraine (2022-present), where cyber operations have interfered with military drone guidance systems.

2.3.3 Critical Infrastructure Targeting

As critical infrastructure—such as power grids, transportation systems, water treatment facilities, and communication networks—becomes increasingly digitized, it also becomes more vulnerable to adversarial exploitation through ADS-derived intelligence. The vast amount of real-time data collected from smart meters, industrial IoT (IIoT) devices, traffic monitoring systems, and cloud-based control networks enables adversaries to model, predict, and potentially disrupt these essential services.

3. MITIGATION STRATEGIES FOR DOD AND FEDERAL AGENCIES

3.1 Data Sovereignty and Regulation of Data Brokers

A. Prevent foreign exploitation of servicemembers' data by implementing strict data sovereignty laws to prevent U.S. consumer and military personnel data from being sold to foreign entities. We should ensure that mission-critical, defense, and infrastructure data is not stored in jurisdictions with weak data protection laws or foreign government access.
B. Establish DoD-wide restrictions on third-party data sharing within the defense industry supply chain in order to secure cloud storage, IoT infrastructure, and AI training datasets from adversarial data harvesting. Restricting foreign-owned technology and cloud services as well as enhancing encryption to Post-Quantum Cryptology (PQC) standards are steps toward hardening our defenses against sensitive data exploitation.
C. Develop international alliances on data security, working with Five Eyes and NATO to standardize data sovereignty protections and intelligence-sharing protocols.
D. Promote public-private sector collaboration, engaging U.S tech companies and cloud providers to develop nationally secure data-handling practices that align with federal cybersecurity priorities.
E. Adopt a Whole-of-Government approach, coordinating efforts across the DoD, DHS, NSA, and NIST to create a unified data security framework.

3.2 Operational Security (OPSEC) Modernization

A. Implementation of policies accounting for ADS/UTS threats to mitigate association to sensitive sites and activities.
B. Employ Zero Trust Architecture (ZTA), requiring multi-factor authentication (MFA) for all networks and enabling a policy of least privilege for access compartmentalization.
C. Invest in DoD-wide ADS/UTS awareness training for service members on adversarial data exploitation tactics. This should expand beyond standard periodic IT and cybersecurity training, identifying threats that affect service members and contractors, not only at their duty station, but also while at home and away from station.
D. Implement automated threat intelligence monitoring for ADS-related vulnerabilities.

E. Update communication and data encryption standards to utilize secure, end-to-end encryption (E2EE) platforms
F. Transition to quantum-resistant encryption to counter emerging decryption threats.
G. Leverage OSINT capability to map individual and organizational digital footprints and profiles. This enables decision makers to conduct accurate risk assessments.
H. Regulate third-party software and hardware.
I. Conduct periodic testing and exercises, identifying vulnerabilities and improving resilience against real-world threats.

3.3 Counter-Influence and Cognitive Defense Strategies

A. Develop counter-PsyOps frameworks to neutralize adversarial influence campaigns targeting military personnel. This can include developing real-time threat assessments for emerging cognitive warfare tactics and adversarial disinformation trends to implementing cognitive security training to teach personnel how to recognize and resist PsyOps tactics.
B. With the employment of AI-generated deepfake videos, synthetic text, and social botnets allowing adversaries to manufacture highly persuasive and targeted propaganda, the DoD should consider investing in AI-driven misinformation detection systems to flag and disrupt foreign propaganda and cognitive attacks. This can include the integration of manipulated media detection tools into DoD cybersecurity frameworks.

3.4 Digital Threat Awareness Training

To fully address the threats posed by ADS, UTS, and USE, a comprehensive digital threat awareness training program should be implemented for all DoD personnel. This program should:

A. Educate personnel on why and how data is collected, sold, and weaponized.
B. Train service members on personal data hygiene and risk reduction strategies.
C. Provide real-world case studies on how adversaries have successfully used ADS/UTS-derived intelligence against military and governmental entities.
D. Develop a continuous education model to keep up with evolving surveillance and exploitation tactics.

4. CONCLUSION: ADS, UTS, AND USE AS THE NEXT SECURITY FRONTIER

Ambient Data Surveillance, Ubiquitous Technical Surveillance, and the Ubiquitous Surveillance Economy have transformed data collection from a commercial endeavor into a national security risk. In an era where every device, sensor, and digital platform serves as a potential surveillance node, the DoD and federal government must evolve beyond traditional security frameworks. The U.S. must control its digital footprint, neutralize data-driven threats, and leverage its own AI and cyber capabilities to maintain strategic superiority. By hardening defenses, modernizing policies, and fostering technological resilience, the U.S. can ensure that ADS, UTS, and USE technologies serve as tools of security—rather than vulnerabilities exploited by adversaries.

“Big data is both our greatest asset and our greatest liability in national security.”

— Gen. Paul Nakasone, Former Commander, U.S. Cyber Command & NSA Director (2021)

5. REFERENCES

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. arXiv.org. https://arXiv.org/pdf/1802.07228

Calo, R. (2017). Artificial Intelligence Policy: A Primer and Roadmap. UC Davis Law Review, 51(2), 399-435.

Chen, A., & Murdoch, S. J. (2020). Surveillance Capitalism: The Hidden Costs of Data Monetization. Journal of Digital Privacy & Security, 6(3), 112-128.

Hartzog, W., & Selinger, E. (2018). Surveillance as Loss of Obscurity. Washington University Law Review, 96(6), 1357-1402.

Hogan, M. (2022). Ubiquitous Surveillance and the Erosion of National Security: How Foreign Adversaries Weaponize Commercial Data. Georgetown Journal of International Affairs, 23(1), 77-94.

National Security Commission on Artificial Intelligence (NSCAI). (2021). Final Report: The Role of AI in National Security and Defense Operations. Washington, DC: U.S. Government.

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.