INTEGRATED SENSING AND COMMUNICATIONS REPORT

OFFICE OF RESEARCH, INNOVATION, AND ECONOMIC IMPACT
George Mason University®

MAY 2025

TABLE OF CONTENTS

PRINCIPAL INVESTIGATOR LETTER

On April 9–10, George Mason University's Office of Research, Innovation, and Economic Impact (ORIEI), in collaboration with the College of Engineering and Computing, hosted a national workshop on Integrated Sensing and Communications (ISAC). The event brought together leading researchers from premier academic institutions—including Arizona State University, Duke University, Georgia Tech, MIT, Michigan State University, Purdue University, Texas Tech University, UC San Diego, University of Hawai'i at Mānoa, UMass Dartmouth, University of Oklahoma, and Virginia Tech—alongside industry leaders from Ericsson Advanced Technologies, FT-Innovations, Nokia Federal Division, the Open RAN Policy Coalition, and SEMPRE.

Sponsored by the Office of the Under Secretary of Defense for Research and Engineering, FutureG Office, and the National Science Foundation, the workshop focused on charting a strategic roadmap for ISAC as an emerging technology with broad implications for Department of Defense (DoD) operations and national security. Participants conducted an in-depth analysis of the current landscape, including critical issues related to signal frequency, bandwidth, sensing and detection capabilities, electronic warfare, and precision trade-offs.

Key discussions examined how the DoD could enhance situational awareness by integrating ISAC with existing technologies such as radar, lidar, video, and novel sensing systems, as well as strategies to defend against adversarial use of similar technologies.

This report presents the findings and recommendations developed during the workshop, including key technical gaps, societal and regulatory challenges, a suggested research and development roadmap, and guidance to inform future defense technology investments and policy development related to ISAC.

Sarah P Campbell

SARAH P. CAMPBELL

Principal Investigator
Associate Vice President of Research for Defense and Security Initiatives
George Mason University

BACKGROUND

Integrated Sensing and Communications (ISAC) is rapidly emerging as a transformative integration of technologies at the intersection of commercial telecommunications and advanced sensing capabilities, including radar. Its ascent is attributable to several factors.

First, base stations and user equipment are ubiquitous and commercially critical pieces of infrastructure. Consequently, these systems will proliferate across the globe regardless of funding or interest from the public sector. Further, telecommunications companies have a strong customer demand for increasing swaths of the spectrum. Consequently, the telecommunications infrastructure of even underdeveloped countries offers widespread, persistent, wideband signals. Finally, due to commercial pressures on user equipment, protocols are standardized across the globe.
The result of this demand is a communications environment saturated with persistent, wideband signals—an environment that ISAC seeks to exploit for sensing purposes. Compounding this opportunity is the global standardization of protocols and hardware, a byproduct of commercial pressures for interoperability and efficiency. Consequently, ISAC technologies have a unique chance to piggyback on globally deployed, commercially sustained platforms, providing a scalable and cost-effective alternative to purpose-built sensing systems.

In this context, ISAC is no longer merely a speculative research topic but a strategic opportunity, holding the potential to redefine the future of wireless systems by integrating sensing capabilities into the very fabric of global communications infrastructure. It is also widely acknowledged within the academic community that the United States may be as much as a decade behind other leading countries in deploying this technology. Reports of other countries leveraging ISAC have emerged over the last 10 years describing systems already fielded in prototype form. Publicly available information indicates that certain countries have ISAC fully deployed in their commercial networks, with coverage across certain cities, and we can only assume the coverage is more widespread. It remains uncertain whether the U.S. military has developed the capability to create tactics, techniques, and procedures (TTPs) for potential future operations involving adversaries equipped with ISAC.

KEY TECHNICAL GAPS

Currently there are no meaningful theoretical foundations addressing global network resource optimization in joint radar-comms environments.

Such a foundation would enable ISAC systems to be efficient, scalable, and robust. It would also facilitate efficient resource allocation across entire networks and help manage the complex interactions between multiple ISAC nodes. The lack of theoretical foundations leads to a piecemeal effort of system design, developing and navigating large, dynamic networks through what is essentially trial and error. Similarly, there is no significant theory regarding spectrum efficiency models tailored to radar and/or multi-functional systems. Without it, there is no unified approach for how to define, measure, and optimize spectrum use in an ISAC setting.

Radar and communications have vastly different technical requirements and areas of emphasis to drive performance, which are constantly at odds with each other. A theoretical foundation tailored to spectrum efficiency in radar and multi-functional systems would enable coexistence, adaptability, and scalability in NextG systems. The development of a unified theory and approach would provide a foundation for the collaborative efforts required to close the gaps between current technical capabilities and the future of ISAC systems.

1 Signal Integrity and Interference Limits

ISAC system performance is fundamentally limited by how well it can preserve signal integrity in the presence of noise, interference, and environmental reflections. These systems' dual functionality makes it highly susceptible to data degradation. Such limitations can be categorized into the context(s) of signal-to-noise ratio (SNR) constraints and interference-related concerns.

High SNR is critical for accurate sensing and reliable communication as it enables effective detection, localization, and data decoding. However, the desired high SNR is undermined by practical constraints such as oscillator phase noise, radar cross-section (RCS) fluctuations, and short coherent integration times. Fast moving targets, including unmanned aerial vehicles (UAV), quickly enter and exit the sensing beam, limiting integration time and degrading the effective SNR for range-Doppler processing. Using the example of UAVs, this could lead to reduced detection range, classification errors and/or missed detections, and impaired tracking stability.


U.S. soldiers parachuting out of a plane..

Interference can take several different forms. In monostatic and full duplex configurations, in-band transmissions can leak into the receiver path, masking weak signals and limiting dynamic range. An example of this is a 5G base station that struggles to detect a UAV due to interference from its own downlink signal. This self-interference can be mitigated through strategies such as antenna separation, cancellation algorithms, and radio frequency (RF) isolation, but such measures introduce additional complexity and power considerations into the system. Additionally, reflections from non-target surfaces, such as buildings or terrain, can mask weak targets, especially when leveraging wide-beam antennas or operating in environments with unstable oscillators. Clutter and multiplicative interference are often encountered in urban deployments where multipath reflections obscure smaller moving targets but could also be seen in the operation of low-altitude surveillance radar in mountainous terrain where rock faces and vegetation could produce significant clutter returns. Finally, dense network deployments and overlapping RF systems promote cross-interference, further degrading ISAC performance. If not properly synchronized, co-located systems may interfere with each other, potentially disrupting secure communication channels or masking critical threat detection.

2 Architecture and System Design

Architectural and system design challenges must also be addressed in order to effectively scale ISAC systems in real-world deployments. As discussed, these deployments introduce a dual workload – sensing and communication – on network infrastructure designed for one dedicated purpose, either communication or sensing. System architecture must be reimagined to manage parallel data pipelines, support real-time inference, and coordinate across distributed nodes. Multi-static configurations require precise clock and oscillator alignment across nodes.

Significant benefits could be realized if ISAC base stations were able to efficiently collaborate to achieve comprehensive situational awareness. This requires advancing the traditional concept of a single node as a sensor to treating the entire network as a sensing platform. In this paradigm, the network gathers information from multiple inputs, fuses the information, and subsequently provides actionable data. Current architecture and design frameworks lack the capacity to consistently and efficiently enable network-wide sensing.

Phase noise and synchronization errors degrade signal coherence, affecting range and velocity estimation. In distributed urban deployments, such misalignment can lead to missed detections or false positives. These challenges are compounded in large-scale environments, where decisions must be made rapidly based on distributed, often imperfect information. This leads to barriers in demonstration and scalability. Large-scale ISAC testing is hampered by limited access to testbeds, standardized protocols, and scalable processing platforms. Most current systems remain constrained to laboratory environments, reducing their applicability to live networks.

3 Hardware

By nature, ISAC demands highly flexible and efficient edge computation, requiring low Size, Weight, Power, and Cost (SWaP-C) processors. In addition, it needs wide and tunable instantaneous bandwidth. Existing hardware generally lacks the technical capability for navigating the data throughput and latency requirements of ISAC.

ISAC deployment over existing infrastructure introduces additional hardware constraints. This is exacerbated by repurposing communication-based components for sensing tasks. Many current wireless systems, including 5G base stations, were designed solely with communication in mind. As a result, they are optimized according to comms-based metrics such as data throughput, spectral efficiency, and user coverage. Communication systems inherently lack an emphasis on target tracking or detection. Subsequently, repurposing of this infrastructure for ISAC creates a gap between available capabilities and the system’s sensing needs.

This dynamic manifests in hardware nonlinearities, antenna and beamforming constraints, and receiver architecture limitations. In the first instance, the requirements of integrating sensing capabilities into the existing system cause power amplifiers to operate near saturation, particularly with high Peak-to-Average Power Ratio (PAPR) waveforms such as Orthogonal Frequency Division Multiplexing (OFDM), introducing nonlinear distortions. The resulting “fake” harmonics generated by the base station impairs its accuracy in range-Doppler estimation. While such distortions can be addressed via strategies like predistortion and equalization, these require additional resources. Additionally, many Frequency Division Duplexing (FDD) base stations lack the receiving paths necessary for monostatic downlink sensing. The absence of switching mechanisms and filters further limits feasibility without substantial redesign and prevents such systems from detecting downlink echoes. While Time

Division Duplexing (TDD) systems can alternate between transmit and receive functionality, these systems are much less common than FDD systems, representing another constraint. Outside of hardware and architecture considerations, antenna systems represent potential constraints on beamforming capabilities. Antenna systems designed for communication typically emphasize ground-level coverage, sacrificing support for upward or omnidirectional sensing and reducing the sensing vectors in which the system can effectively detect. Dynamic beam pattern shifts, the result of load balancing and/or scheduling, further undermine sensing consistency.

Given current limitations in front-end hardware, improvements in amplification, filtering, and interference resilience are necessary. This is compounded by concerns about backward compatibility and coexistence issues with legacy hardware, especially regarding long radar system lifespans (e.g., radar altimeters and difficulties with 5G interference).

4 Processing

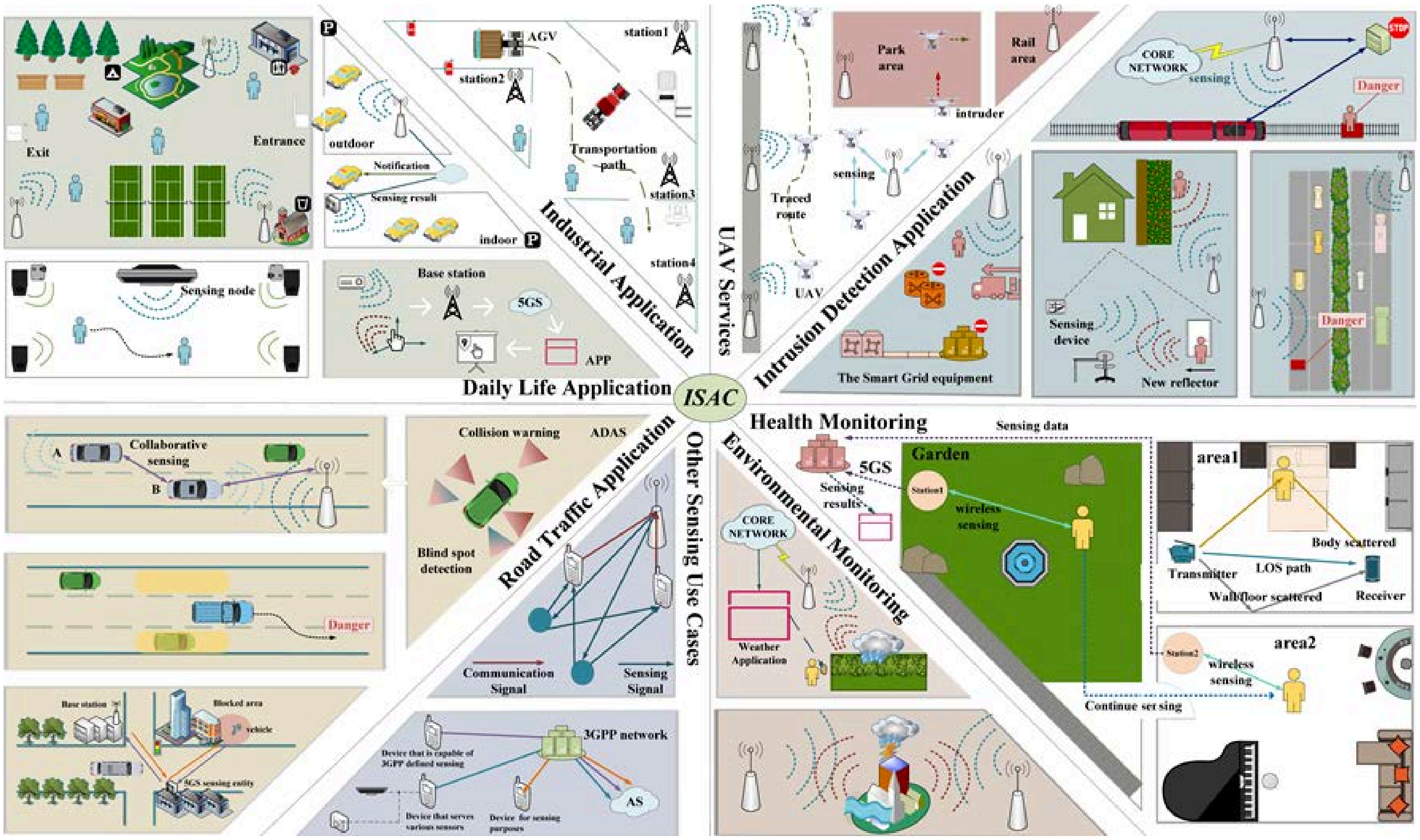
ISAC systems generate terabytes of data which must be processed and condensed quickly, with low latency, to capitalize on the intelligence provided by these systems. Computational constraints at the edge, as in base stations or vehicles, limit the feasibility of processing raw, high-rate In-phase and Quadrature (IQ) data streams. Without sufficient onboard processing or strategic data compression, systems risk becoming bandwidth- or latency-bound,

U.S. soldier in helicopter.

undermining real-time responsiveness. ISAC requires the allocation of resources between high-throughput communication and high-resolution sensing. On-device processing of raw IQ data is not feasible due to computation and power limits, necessitating localized filtering or prioritization. For example, a vehicular ISAC system might reduce sensing fidelity to prioritize safety-critical Vehicle-to-Everything (V2X) communication during peak traffic hours. But in a truly autonomous scenario, this could have significant repercussions as the system might have difficulty sensing potential risks or threats that do not, or are unable to, communicate directly with the vehicle.

Artificial intelligence (AI) is expected to play a transformative role in ISAC, particularly for complex sensing tasks. AI-based approaches could, additionally, support the potential for predictive sensing, enabling the system to anticipate changes in an environment based on historical data. However, current limitations in distributed processing capabilities, both in edge devices and across the network, hamstring the deployment of such advanced algorithms at scale.

SOCIETAL AND REGULATORY CHALLENGES



Security and Privacy Challenges in ISAC Systems
1. *PHY Layer*: Passive Attacks (Eavesdropping/Passive Sensing); Active Attacks (Jamming and Spoofing Attacks, Inference and Cross-Domain Attacks, Adversarial Attacks on AI-Based ISAC); 2. *Data Layer*: User Privacy Protection during Collection, Sharing, Storage, and Usage; User Privacy; Protection during AI Model Training and Interference; Sense Data Falsification; 3. *Regulation and Policy*: User Consent; Spectrum Management; Compatibility and Interoperability (© 2025 Dr. Zai Zeng)

1 Privacy and Security

As shown in Figure 1, concerns around privacy straddle the line between technical and societal challenges with ISAC. Sensing, specifically, raises alarms on this front. The proliferation of mis- and dis-information has eroded public trust in many emerging technologies, negatively impacting public perception surrounding potential benefits to these advancements. Conspiracy theories about 5G, including claims that it triggered the COVID-19 pandemic or causes cancer, have spread quickly due to the widespread reach of social media. Additionally, ISAC has the potential to enable ubiquitous sensing.

Military command center.

Devices might be able to localize, track, and monitor individuals without their awareness. The surveillance potential of ISAC, particularly in the absence of clear regulations, could fuel even greater public distrust—both toward the government and the technology itself.

2 Regulatory Framework and Government

The disconnect among academia, government, and industry also represents a significant challenge. Academia tends to emphasize long-term, theoretical advancements and prioritizes open public publication of research. However, this research is frequently not easily commercialized or transitioned outside of the academic realm. Conversely, industry prioritizes near-term, product-driven goals that demand fast, scalable, and market-ready solutions. Government often acts as a as a driver for early research and innovation, including ISAC. Despite this foundational support, industry requires economic motivation and incentives to adopt, scale, and further refine these advancements.

ISAC operates by combining radar and communication functionalities, frequently leveraging shared, or overlapping, frequency bands, which is frequently at odds with current spectrum regulatory frameworks. These are built on rigid, service-specific allocations with oversight spread out across multiple government agencies depending on the use case. ISAC waveforms regularly do not fit conventional spectral allocations and in the current landscape, regulatory bodies are ill-equipped to handle novel spectrum-sharing schemes. Exacerbating this issue is concern about spectrum sharing between civilian communications and federal radar systems. While technically feasible, it remains politically complex due to national security concerns.

U.S. soldiers monitor barriers.

ISAC systems also face challenges related to public RF emission constraints and associated safety concerns. Emitting at non-standard frequencies and power levels raises legal and logistical concerns demanding further study and discussion. As noted, regulatory frameworks are generally service-specific, such as emission masks for Long Term Evolution (LTE) and radar peak power constraints. No such standards currently exist for multifunctional systems.

In unlicensed or lightly licensed frequency bands, radar signals used in ISAC could interfere with nearby consumer devices, creating issues, particularly in emergency situations. Given the ambiguous nature of the current landscape, real-world ISAC demonstrations are limited by both real and perceived regulatory barriers.

3 Standardization

In traditional wireless communication settings, standardization bodies drive unified benchmarking. ISAC, without such oversight, lacks the common datasets, simulation tools, and evaluation benchmarks of its predecessors. Communication datasets do not contain the sensing-relevant information necessary for ISAC and radar data is often sparse, classified, or proprietary in open datasets. The absence of such resources leads to fragmentation across (and within) academic and industry research and creates additional difficulty in fairly and accurately establishing minimum performance thresholds. As shown in Figures 2 and 3, sensing data requires unique approaches to security and privacy, which current standards do not address.

As a result, regulatory bodies and commercial entities lack a shared understanding of performance trade-offs across different system implementations and configurations. Research fragmentation, and the associated limitations in transparency and reproducibility, further fuels regulatory hesitation in this area.

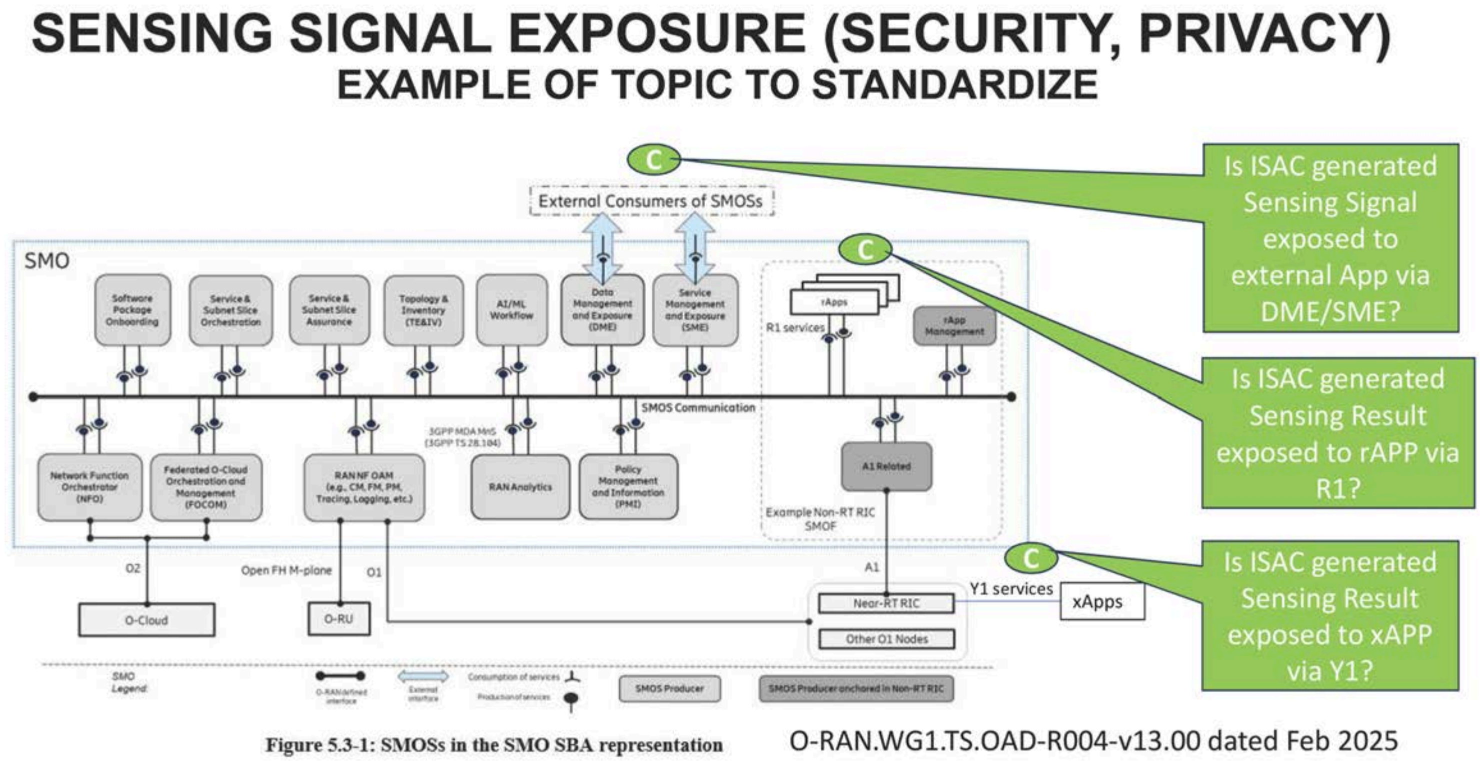


Figure 2: Standardization of Sensing Signal Exposure
Metadata standardization is necessary to effectively and efficiently identify characteristics of Sensing Signal stream to allow for multi-vendor interoperability and application digestibility. Sensing Signal stream information flows will require unique, comprehensive security and privacy architectures. (© 2025 Dr. Brenda Connor)

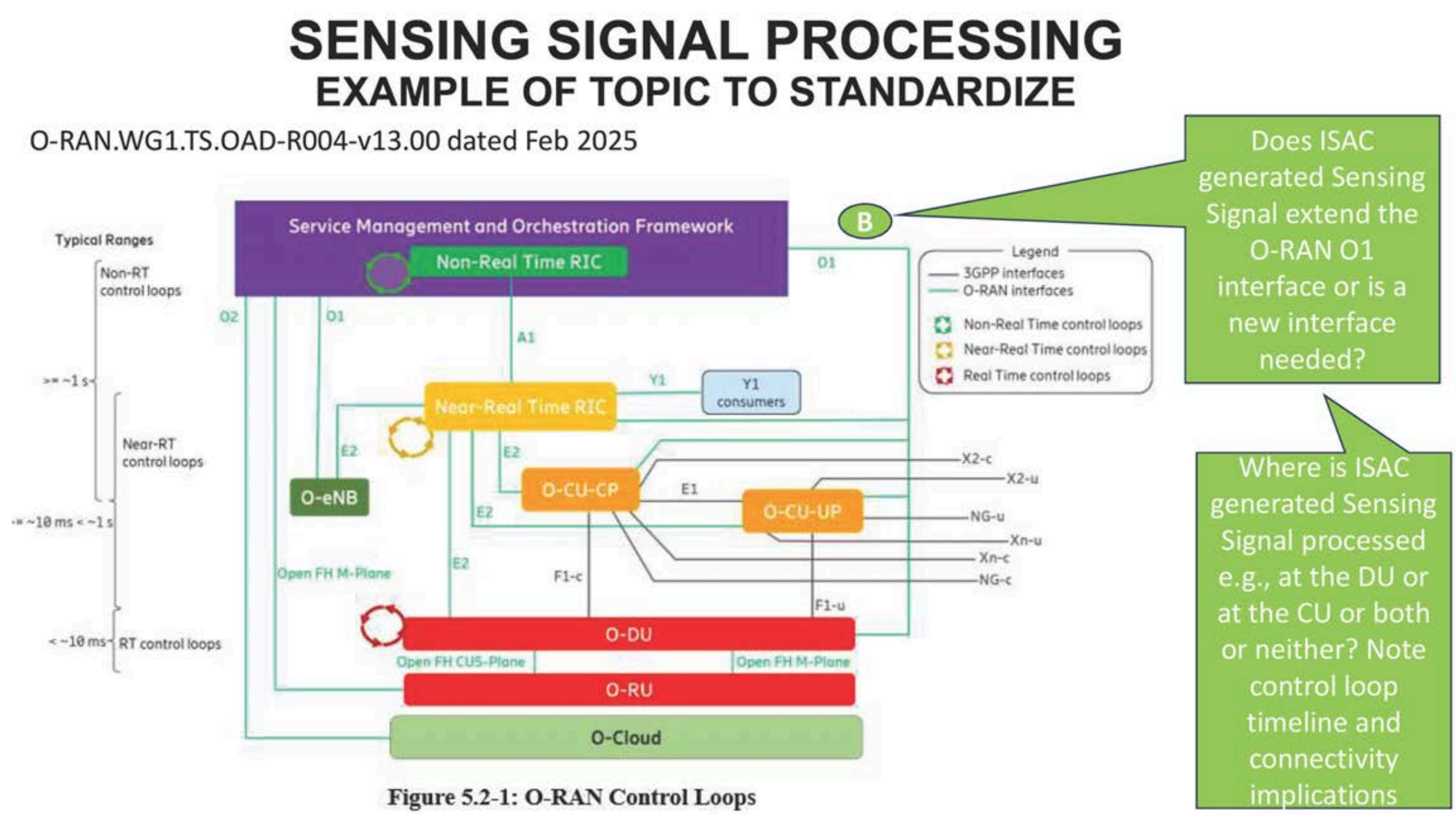


Figure 3: Standardization of Sensing Signal Processing
Security and privacy designed specifically for Sensing Signal stream is critical to ensuring the fidelity and trustworthiness of Sensing Signal-processed results, including the impact of data fusion from dual-use systems.
(© 2025 Dr. Brenda Connor)

RESEARCH AND DEVELOPMENT ROADMAP

ISAC holds transformative potential for not just next-generation communications, but public safety and defense as well.

As the U.S. explores ISAC capabilities, global competitors continue to aggressively invest in similar dual-use technologies, frequently integrating them into advanced military and surveillance systems. China, for example, has incorporated ISAC technology into its military modernization strategy, integrating dual-use systems for battlefield deployment. Its civil-military fusion enables coordinated access to critical infrastructure for ISAC testing at scale, amplifying advancement in areas such as smart city infrastructure and surveillance deployments. At the same time, firms such as Huawei and CETC are actively pursuing dual-use applications in both 6G development and electronic warfare, highlighting the country's defense-commercial synergy.

Simultaneously, U.S. allies have established collaborative research and development (R&D) frameworks and testbeds to ensure interoperability and leadership in emerging 6G and sensor-network domains. The European Union (EU) currently leads several well-funded, multinational ISAC-related projects and, given this multinational focus, is working to actively influence future ISAC standardization. Countries such as Germany and Finland were early actors in the deployment of 6G testbeds with integrated sensing capabilities. Finland has emphasized international collaboration on this front, fostering ecosystem-driven research and innovation in 6G technologies through infrastructure such as its 6G Flagship and 6G Test Centre and initiatives such as its 6G Bridge Program. Similarly, both Japan and South Korea are leveraging strong industry-government coordination to invest in 6G-era ISAC prototypes for autonomous vehicles, unmanned aerial systems, and smart infrastructure.

Ensuring U.S. leadership in ISAC is critical to both U.S. technological sovereignty and national security. It offers the potential to reshape battlefield awareness, secure communications, and autonomous operations in contested environments. As sensing and communication become increasingly inseparable in military and civilian infrastructure, dependency on foreign vendors or platforms could create strategic vulnerabilities. For instance, adversaries could exploit weaknesses in imported components, manipulate communication protocols, or deny access to critical subsystems in times of crisis. In terms of security, ISAC directly supports several key national priorities, offering the potential to reshape battlefield awareness, secure communications, and facilitate autonomous operations in contested environments. Failure to lead in ISAC could mean ceding battlefield advantages to adversaries who are more advanced in integrating sensing and communication into coordinated surveillance, strike, and electronic warfare systems.

Radar, RF, and Wireless Systems Synergies

Bridging the radar, RF, and wireless communities will unlock synergies. The workshop suggested concrete actions, including developing shared test platforms (e.g., software-defined radios that support radar waveforms and communications links); forming interdisciplinary research working groups; and organizing joint sessions at Institute of Electrical and Electronics Engineers (IEEE) radar, IEEE communications, and similar conferences. Such cross-pollination can harmonize signal models and measurement metrics across domains. For example, progress in RF hardware (like reconfigurable antennas) benefits both radar and cellular designs. Likewise, advances in wireless algorithms (e.g. Multiple-Input, Multiple-Output beamforming) have potential to be adapted for radar sensing. Encouraging such cross-community collaboration will accelerate innovation in both fields.

1 Strategic Research Design and Funding Models

Without a unified understanding, efforts to advance ISAC are fragmented, leading to inconsistent technical requirements, duplicative work, and slow progress. Establishing a standardized vocabulary across stakeholders is essential for effective collaboration, codifying how key concepts such as “sensing”, “communication”, and

U.S. soldier returns fire.

“integration” are defined. With a common language established, a clear scope of work can be developed, enabling strategic focus on the most promising use cases and informing investment priorities. This framework should consolidate theoretical underpinnings from its diverse inputs to guide ISAC analysis. Pulling from fields such as communication theory and estimation theory, this platform must further propel interdisciplinary innovation, serving as a conceptual bridge between sensing, communication, and control.

From here, the government should provide an initial concept of operations (CONOPS) for ISAC. Linking technical development with real-world utility, this guide will articulate how ISAC capabilities can be deployed in real-world use cases across domains and, by anchoring development within these use cases, ensure operational relevance and accelerate capability transition.

A system model for ISAC must also be developed, assuring that solutions are modular, scalable, and able to evolve with emerging technologies. This model should define architectural elements (such as nodes, links, and interfaces), data flows, and critical functions, and enable a structured approach to development. It should also identify tracks of innovation that can be pursued in parallel, enhancing agility while acknowledging necessary serial dependencies, to prevent bottlenecks. The establishment of such a system model must inform, and further grow, the research base. A broader, more comprehensive body of literature is needed to inform decision-making and attract new contributors to the field. Ultimately, bridging the current gaps and disconnects between radar, RF, and wireless sectors will unlock synergies that build upon and reinforce each other, fostering rapid advancement in ISAC research. This can be catalyzed by government sponsorship of technical symposia, funded research programs, and support of peer-reviewed publications. Expansion of the research base will accelerate innovation, foster cross-sector collaboration, and mitigate knowledge gaps.

As seen in Figure 4, challenges with ISAC span multiple domains; subsequently large-scale, interdisciplinary, cross-sector projects are essential to connect these fields and ensure that holistic solutions avoid the shortcomings of current, siloed advancement. Projects must also align with real-world mission profiles to ensure applicability. Moreover, early-stage innovation in ISAC demands a tolerance for failure. Programs must allow researchers to explore high-risk ideas without fear of project termination, particularly given academic hiring cycles and grant timelines.

A resilient model encourages bold exploration while protecting long-term viability. In addition, a phased funding approach with accountability and agility should balance discovery with direction in research. Phased funding can enable exploration in early stages while ensuring accountability through milestone-based progress tracking. This approach maintains flexibility while encouraging rapid iteration and tangible outcomes.

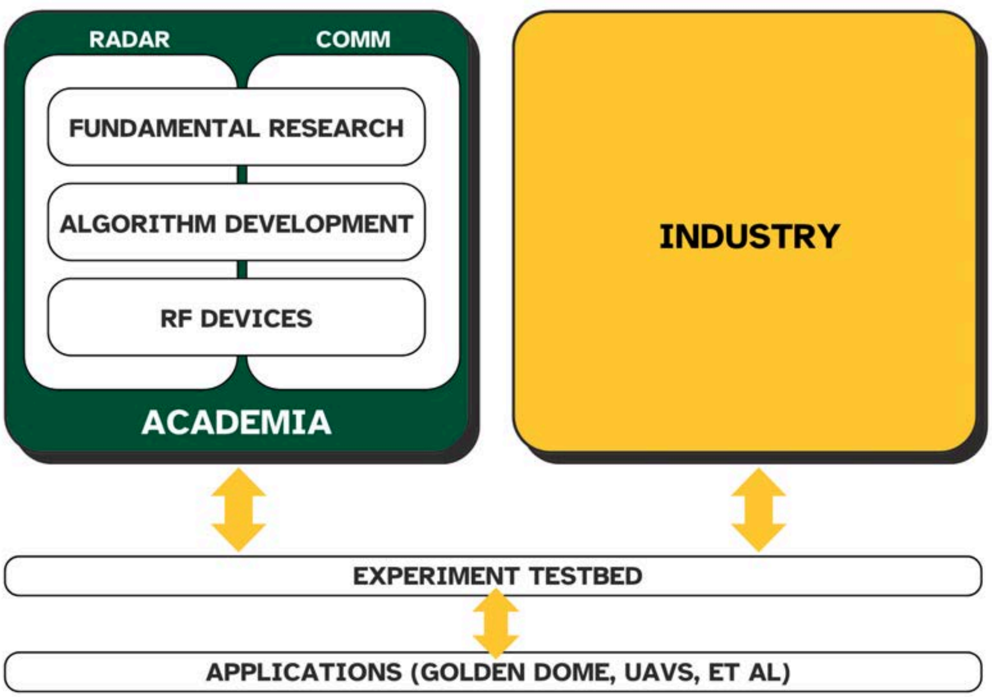


Figure 4: The ISAC Collaborative Ecosystem
In order to realize the transformative potential of ISAC capabilities, industry, academia, and government must partner to leverage their unique areas of expertise (@2025 Dr. Li Husheng).

U.S. Army ranger students provide security.

2 Technology Development and Enhancement

Artificial intelligence (AI) is expected to play a transformative role in ISAC, particularly for complex sensing tasks. Systems increasingly rely on intelligent processing for real-time sensing, adaptation, and decision-making. Integrating AI/Machine Learning (ML) models enables autonomous operations in complex, or contested, environments where human interaction and control might be limited or delayed. AI-based approaches could, additionally, support the potential for predictive sensing, enabling the system to anticipate changes in an environment based on historical data. However, current limitations in distributed processing capabilities, both in edge devices and across the network, hamstring the deployment of such advanced algorithms at scale. Algorithmic development might fall into these larger categories:

- Waveform design and optimization
- SNR optimization
- Dynamic multi-function network optimization
- Interference/clutter mitigation
- Distributed system/network data fusion

To facilitate and accelerate experimentation and system adaptation and scale, ISAC platforms should be built on modular, reconfigurable architectures. Such architectures enable components to be independently upgraded, switched out, or reprogrammed in isolation, with system-wide implications. This flexibility is critical in both operational and research settings, as technology advances quickly and mission requirements may change in real time. Similarly, the widespread implementation of open-source frameworks and plug-and-play components minimizes barriers to entry and promote rapid iteration. These tools facilitate broader participation across sectors by reducing costs and increasing transparency. They simplify integration between sensing, communication, and processing modules, allowing for the testing of new algorithms, protocols, and hardware configurations while minimizing downtime or system disruption. In concert, these features lower the economic and technical barriers to innovation, support rapid prototyping, and accelerate the transition of ISAC technologies from research environments to real-world deployment.

Enhancing sidelink communication would strengthen operational continuity in disconnected, disrupted, or denied environments. The development of hardware and protocols that enable direct device-to-device communication without infrastructure support is critical for operational coordination in GPS-denied or infrastructure-degraded environments, such as in disaster recovery operations or emergency response coordination. Likewise, reliable positioning and timing are foundational to operations that depend on precise timing, such as autonomous vehicle navigation, military operations, and management of critical infrastructure. Investment in compact, ruggedized modules – such as chip-scale atomic clocks – and inertial navigation systems will enable independent time/position estimation, while enhanced calibration methods will reduce error accumulations and improve system accuracy across distributed platforms.

Distributed sensing can enrich urban planning, traffic monitoring, and spectrum management in networks. It can also increase resilience, enhance threat detection, and support adaptive operations in complex environments. To this end, base stations that have the capacity to autonomously sense environmental and signal conditions, without input from user equipment (UE), must be developed. Mobile UEs should be enabled to contribute sensor data, creating a collective that improves overall situational awareness.

Enhanced communications are critical to the functionality of smart cities, telemedicine, and mobile networks, especially in densely populated or environmentally challenging environments. Using data from a network of existing sensors (e.g., cameras, inertial measurement units, temperature sensor) can optimize communication parameters for better performance. Multi-sensor fusion can mitigate signal loss and improve robustness in cluttered, or contested, environments.

Quantum technology represents a significant driver for breakthrough improvements in sensitivity, precision, and security. Quantum-enhanced communications could have major impacts on sectors such as healthcare, transportation, and finance. While still an immature field, quantum computing,

High Mobility Artillery Rocket System.

sensing, and key distribution should be monitored, and incrementally tested, for potential ISAC integration.

Systems increasingly rely on intelligent processing for real-time sensing, adaptation, and decision-making. Integrating AI/ML models enables autonomous operations in complex, or contested, environments where human interaction and control might be limited or delayed. Autonomy amplifies ISAC by reducing human workload and accelerating response in time-critical scenarios. It improves efficiency in disaster response, logistics, and transportation networks by interpreting sensor data, making decisions, and initiating response without human intervention, thereby reducing latency. The development and integration of trusted autonomous systems within ISAC frameworks facilitates rapid, adaptive responses in dynamic settings.

3 Experimentation, Prototyping, and Scaling

Many promising innovations stall due to a lack of operational demonstration and/or user engagement. Directly funding prototyping and field evaluations with

U.S. soldiers stand in front of a self-propelled Howitzer.

military and public safety users can help bridge the gap between lab work and fielded systems. A philosophy of "prototype early and often" should be embraced. Frequent prototyping cycles reduce technical risk and help identify integration challenges early in-process. These prototypes should be tested in conditions that mirror operational complexity, including spectrum congestion and adversarial activity. The approach of iterative prototyping fosters user feedback speeds up learning cycles and improves technological maturity.

Pilot programs should be leveraged to provide actionable insights on usability, performance, and potential use-impact before broad deployment. These pilots should validate ISAC systems in use-relevant exercises, such as Project Convergence or EDGE, measuring key outcomes like communication reliability, sensor-to-shooter latency, and resilience in degraded or contested domains.

Furthermore, public-private testbeds mitigate risk, pool resources, and validate emerging solutions in lifelike environments, supporting real-time feedback, iterative development, and accelerating integration readiness. Examples such as the collaborative testbed Campfire provide a blueprint as to how academia-government-industry partnerships can fast-track innovation.

Similarly, a modular testing architecture would drive flexibility, reduce the cost of integration, and accelerate acquisition timelines. Modular testbeds would enable plug-and-play evaluation of novel components, driving competition and innovation. Such environments would also enable the standardized comparison of differing products, allowing decision makers to make more informed choices in terms of acquisition.

As quality data is the backbone of AI-enabled sensing and communication, a dedicated data working group should be created. Without quality data, models are unable to scale to meet demand. Access to high-quality datasets is essential for algorithm development, validation, and simulation. This formal working group would oversee the collection, standardization, and distribution of representative ISAC data, safeguarding secure and open collaboration.

U.S. soldier uses handheld transceiver.

4 Partnerships, Ecosystem Building, and Alignment

An active, diverse, and vibrant innovation base powers disruptive technologies and fosters a pipeline of novel ideas and capabilities. Programs such as Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) can attract small businesses with fresh solutions to system challenges and should continue to be supported. Additionally, active involvement in 5G/6G standards bodies allows the U.S. to advocate for ISAC-relevant features and interoperability. Cross-sector and international collaboration should be intentionally and aggressively pursued as it builds resilience, enables innovation, and enhances strategic alignment. Such coordination aligns efforts, mitigates redundancy, and leverages a wider base of expertise to drive advancement.

Allied collaboration also ensures interoperability in coalition operations, while simultaneously defraying the cost of development. Allied R&D partnerships enhance scalability and security in ISAC deployments, and the implementation of multilateral testbeds and coordinated demonstration efforts further help align technical requirements and operational doctrines across partners. This reinforces U.S. interests, as investment in domestic and allied supply chains ensures the availability resilience, and trustworthiness of these critical technologies and their components. Similarly, given the various dual-purpose applications of ISAC technologies, supporting both defense-oriented transitions and commercial pathways maximizes impact and provides multiple routes for tech adoption. Both academic institutions and small businesses struggle to navigate federal acquisition systems. Simplifying contract vehicles and facilitating partnerships with larger integrators can broaden participation and foster innovation from non-traditional players in this sector.

It is important that ISAC use cases be aligned with national defense and/or strategic priorities. Tying ISAC to top-tier defense priorities will secure institutional support and accelerate allocation and resourcing decisions. As seen in Figure 5, ISAC's capability to manage multiple, competing demands in complex and evolving landscapes make it a strategic multiplier for future conflict scenarios. As such, ISAC should directly support high-priority operations, including resilient space systems, long-range precision fires, and nuclear command and control.

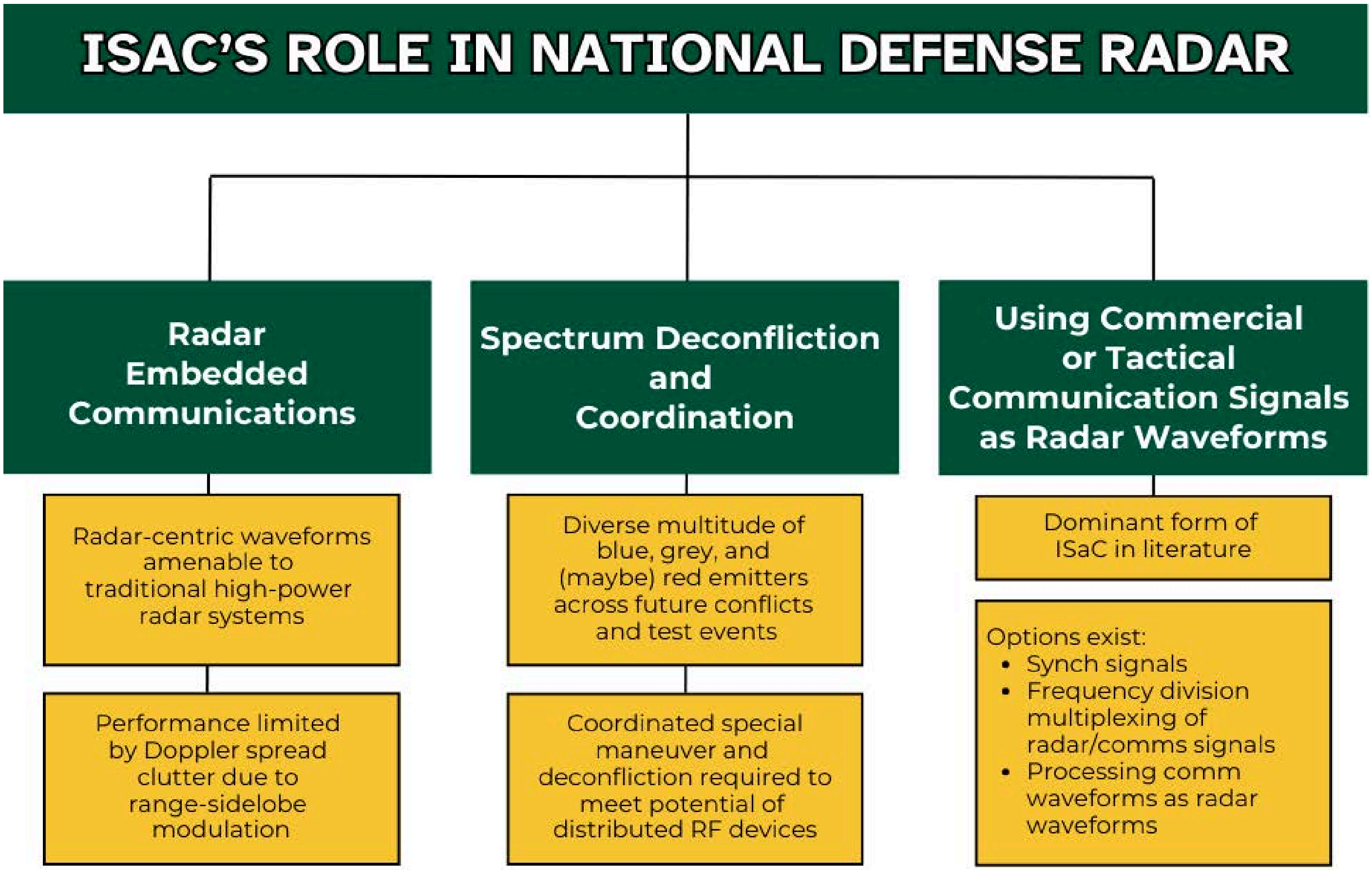


Figure 5: ISAC's Role in National Defense Radar
ISAC capabilities have the potential to be a strategic force multiplier across our national defense portfolio, but especially in radar applications. (@2025 Dr. Justin Metcalf)

Furthermore, workforce development and sustainably building out the talent pipeline is critical to the continued success of ISAC technologies. These systems sit at the intersection of multiple disciplines. Few individuals currently possess the interdisciplinary knowledge required to innovate in this space. Building a specialized talent pipeline ensures that new graduates and researchers can bridge these fields and push the boundaries of what ISAC systems can do. Additionally, without a strong domestic talent base, the U.S. risks reliance on foreign experts or vendors for core sensing and communication capabilities—an unacceptable vulnerability for technologies with military, intelligence, and infrastructure implications. A self-sufficient workforce is essential for secure, sovereign ISAC development. Federal programs should support hands-on learning opportunities and immersive research experiences for students, cross-training between academia and industry.

RECOMMENDATIONS

It remains uncertain whether the U.S. military has developed the capability to create tactics, techniques, and procedures (TTPs) for potential future operations involving adversaries equipped with ISAC.

Currently, some theoretical approaches are being explored within academic circles and commercial research laboratories. The research community must be pressed to move beyond the theoretical to the applied in a test environment. For instance, commercial research has shown a drone flying near a building can be hidden by the RF reflections from the building. Without knowing how advanced the adversary's capabilities are (or self-testing) it is unknown how close the drone needs to be to to fly undetected. Additionally, as the U.S. moves to deploy ISAC in the future, the adversary will already be a decade ahead in developing their TTPs to defeat our systems.

To spur meaningful advancement in ISAC technologies and strengthen national defense, the government must embrace a dual-pronged approach to closing the gap: First, it must actively and intentionally facilitate collaboration across academia, industry, and government. A common theme from the workshop is that dual-use interests should be prioritized. By creating value for incentivizing commercial investment. Second, it must shift from its traditional research paradigm, adopting an iterative approach that embraces rapid prototyping and does not shy away from failure. It can promote parallel innovation through multiple avenues, including:

- Supporting the development of large-scale testbeds and open ISAC ecosystem incubators to test the limits and feasibility of ISAC technologies.
- Integrating research programs including those focusing on novel technology and novel extensions of existing technology.
- Developing and sharing of less-restricted use cases to encourage broader collaboration.
- Intentionally developing and aligning the talent pipeline, including the integration of students across levels into projects.
- Establishing an alignment between the commercial telecommunications industry, academia and the DoD/IC research ecosystem which seeks to create a balance between security restrictions and academic innovation.
- Convergence Accelerator Track: Launching an ISAC-focused track in the NSF Convergence Accelerator Program. This would fund large, multi-year consortia of industry, universities, and government labs to develop prototypes (e.g., integrated transceiver hardware or field-test campaigns) (Convergence Accelerator | NSF - National Science Foundation).

A pair of USAF F-16s.

- Partnership Grants: Using the NSF Technologies, Innovation, and Partnership (TIP) Directorate's flexible partnership awards to support joint projects. For example, solicit proposals for university–industry partnerships on specific ISAC challenges (spectrum sharing algorithms, security protocols, etc.).

Specifically, from a research perspective, it is the consensus of the workshop that the first task should be to establish academic consortium to develop a unified definition, theory, and standardized performance metrics of and for ISAC.

A foundational challenge in ISAC research is the lack of a clear and consistent definition of what it is and what it includes. Does it entail spectrum monitoring and environmental awareness, or is it strictly target-oriented? What are the key performance indicators that most accurately describe system performance? The first question must be addressed to answer the second, and the second question needs to be answered and standardized to inform system design and guide evaluation. Without this foundation, research and technological progress will be inherently limited. The next iterative task should be developing a unified/standard ISAC system design. Ideally, this should incorporate modular components which can easily be both scaled and/or swapped out as necessary.

These two tasks are critical to establishing sustained, meaningful progress in this field. Once these theories, parameters, and metrics are in place, early research should focus on 1) sensor fusion, specifically multi-modal data fusion algorithms (including exploration of the potential of integrating covariant electromagnetics data inputs from the system), real-time edge-based AI processing, and sensor fusion under adversarial conditions; 2) optimization to ensure signal integrity and reduce interference – both internal and external; and 3) the development of advanced novel, flexible, and power-efficient processing capabilities — such as coarse-scale heterogeneous processors that achieve both flexibility and efficiency by accelerating key, computationally expensive, domain-specific elements within a flexible, dynamically reconfigurable architecture.

OTHER FINDINGS

The potential for ISAC to reap mutual benefits between sensing and communications. For example: radar could be leveraged to improve communication latency. Conversely, communications signaling could be leveraged to improve radar performance.

Dr. Robert Calderbank (Duke University): Optimization of the legacy OFDM waveform for ISAC applications and the development of new waveforms, such as Orthogonal Time Frequency Switching (OTFS), which offers the potential for mutually unbiased sensing and communication.

Dr. Yao Zheng (University of Hawai'i at Manoa) and Dr. Georgios Trichopoulos (Arizona State University): The development of Reconfigurable Intelligent Surface (RIS) technology to enhance both sensing and communication performance in RF environments.

Dr. Nuria Gonzales-Prelcic (University of California San Diego): Expanded research further examination in the role ISAC in a space-air-ground integrated network (SAGIN).

Dr. Brenda Connor (Texas Tech University): The role of ISAC in vertical sector environments and critical infrastructure and the need to standardize meta-data to facilitate ISAC across different applications.

CONCLUSION: ISAC, 6G & BEYOND

As ISAC is expected to become a core feature of 6G networks, the rise of the Open Radio Access Network (O-RAN) will provide a unique platform to bring this vision to life.

O-RAN will introduce openness, modularity, and intelligence to wireless networks by decoupling hardware and software components and enabling standardized open interfaces. These characteristics allow seamless integration of sensing capabilities into the cellular infrastructure. By leveraging the abundant data generated across distributed network elements and exploiting the open interfaces of O-RAN, ISAC systems can support real-time environmental sensing alongside communication. This convergence not only boosts spectrum and hardware efficiency but also enables new, context-aware applications in domains such as intelligent transportation, smart cities, and industrial automation. As 6G aims to facilitate deeply integrated physical and digital worlds, ISAC within the O-RAN framework becomes a critical milestone toward next-generation intelligent wireless networks.

Throughout U.S. history, moments of technological urgency – such as the Space Race, the rise of the Internet, and the global race for 5G and beyond – have galvanized national focus and innovation. The emerging competition over 6G and ISAC represents the next frontier in this lineage of strategic races. This is not just a matter of being a global leader technologically; it is critical to our national security. ISAC will rapidly become essential to preparing our military forces for an increasingly complex and uncertain battle space, as well as for the safeguarding of our homeland against emerging and increasingly nebulous threats. Within the context of evolving defense structures – such as the "Golden Dome", which seeks to unify layered domain awareness through advanced sensors, interceptors, and resilient infrastructure – ISAC represents a foundational enabler. The capability to converge communication and sensing technologies into a single, adaptive framework makes ISAC uniquely suited to address the speed, scale, and ambiguity of modern threats.

We urge institutions such as the Department of Defense and the National Science Foundation to consider the potential, and importance, of ISAC not in isolation, but as a critical component of America's broader strategic posture. The findings and recommendations presented in this report are intended to support that vision – and to contribute meaningfully to the next era of our country's technological leadership.

ACKNOWLEDGEMENTS

This research would not have been possible without the dedication and support of numerous individuals. We are especially grateful to the faculty from George Mason University's College of Engineering and Computing and the Rapid Prototyping Research Center, whose time and expertise helped shape the two-day workshop that preceded this report. We also thank Jordan Mason, Program Manager of the Northern Virginia Node at the Commonwealth Cyber Initiative, and Brian Mark, Interim Chair of the Electrical and Computer Engineering Department, whose leadership and dedication were vital to the successful completion of this report. We are also thankful to George Mason University's Vice President for Research, Innovation, and Economic Impact Andre Marshall for his guidance and encouragement.

The organization of and the data collection during the preceding two-day event was made possible through the efforts of PhD student Megan Herceg from the Institute for Digital Innovation, Communications Director Pamela Shepherd, and the valuable support of several graduate students whose contributions were critical to the project's execution.

We extend our sincere appreciation to the individuals and universities listed on the following page for their significant contributions. In particular, we would like to thank Sheryl M. Genco (Ericsson Advanced Technologies), Jamil N. Jaffer (George Mason University), Robert Justice (FT-Innovations), Diane Rinaldo (Open RAN Policy Coalition), Robert S. Spalding III (SEMPRE), and Steve Vogelsang (Nokia Federal Division) for their insights and engagement, which have substantially enriched the quality and impact of this research.

We also thank the U.S. Army, Navy, Air Force, Marine Corps, and Coast Guard for the photos used throughout this report.

Lastly, we are deeply thankful to the Office of the Under Secretary of Defense for Research and Engineering, FutureG Office, and the National Science Foundation for their foresight and interest in this study.

CONTRIBUTORS

Christopher F. Barnes
Associate Professor, Electrical and Computer Engineering
Georgia Tech

Daniel W. Bliss
Professor, Electrical, Computer, and Energy Engineering
Arizona State University

Joe Bricio
Research Faculty
George Mason University

Robert Calderbank
Professor of Computer Science, Electrical Engineering, and Mathematics and Director of the Information Initiative
Duke University

Sarah Campbell
Associate Vice President, Research for Defense and Security Initiatives
George Mason University

Brenda Connor
Professor of Practice and Senior Technical Managing Director of the Critical Infrastructure Security Institute
Texas Tech University

Long Jiao
Assistant Professor, Computer and Information Science
University of Massachusetts Dartmouth

Changzhi Li
Professor and Whitacre Endowed Chair in Electrical and Computer Engineering
Texas Tech University

Husheng Li
Professor, Aeronautics and Astronautics and Electrical and Computer Engineering
Purdue University

Lingjia Liu
Professor, Electrical Engineering and Computing
Virginia Tech

Victor M. Lubecke
Professor, Electrical Engineering
University of Hawai'i at Manoa

Brian Mark
Professor, Electrical and Computer Engineering
George Mason University

CONTRIBUTORS

Andre W. Marshall
Vice President, for Research, Innovation, and Economic Impact
George Mason University

Justin Garth Metcalf
Associate Professor, Computer Engineering
University of Oklahoma

Parth Pathak
Associate Professor, Computer Science
George Mason University

Nuria González Prelcic
Professor, Electrical and Computer Engineering
University of California San Diego

Jeffrey Reed
Professor of Electrical and Computer Engineering
Virginia Tech

Georgios Trichopoulos
Associate Professor, Electrical, Computer, and Energy Engineering
Arizona State University

Zhengdao Wang
Professor, Cybersecurity Engineering
George Mason University

Duminda Wijesekera
Professor, Cyber Security Engineering and Computer Science
George Mason University

Moe Z. Win
Robert R. Taylor Professor
Massachusetts Institute of Technology

Huacheng Zeng
Assistant Professor, Computer Science and Engineering
Michigan State University

Kai Zeng
Professor, Electrical and Computer Engineering
George Mason University

Yao Zheng
Associate Professor, Electrical and Computer Engineering
University of Hawai'i at Manoa