Science and Technology

Department of Homeland Security
Science & Technology Directorate

TECHNOLOGY CENTERS RESEARCH AGENDA

TABLE OF CONTENTS

INTRODUCTION

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Technology Centers (Tech Centers) conduct basic and applied research into emerging and future science and technology to ensure science and technology advancements can be harnessed for cutting-edge solutions to DHS operational challenges. In general, our research looks to build knowledge and understanding of:

- Evolving S&T Threats, Hazards & Risks – characterizing the misuses of science and technology, as well as the consequences and intervention and/or countermeasure options
- Current & Emerging Technologies, Scientific Advancements – new science and technology applications, potential technology vulnerabilities, and security measures for use in homeland security operations

Our research is driven by strategic and long-term needs of the Department and Homeland Security Enterprise (HSE) and provides an avenue for S&T to be forward-leaning, looking five to ten years out to understand and anticipate what science-based or technology-related issues may impact the Department in the future and ideally avoid technology surprise and reduce overall risk to the Department.

S&T Tech Centers' research priorities are designed to leverage science and technology advancements to enable key Departmental missions, including the priority mission advancements articulated by Homeland Security Secretary Alejandro Mayorkas in 2022[1]:

- Combat all forms of terrorism and targeted violence
- Increase cybersecurity of our nation's networks and critical infrastructure, including election infrastructure
- Secure our borders and modernize ports of entry
- Build a fair, orderly, and humane immigration system
- Ready the nation to respond to and recover from disasters and combat the climate crisis
- Combat human trafficking, labor exploitation, and child exploitation

[1] Priorities | Homeland Security (dhs.gov)

INTRODUCTION

STRATEGIC INTENT

Given the speed at which technology is evolving, coupled with the convergence of technologies where advances in some emerging technologies can have significant impacts on others, our ability to foresight[2] and monitor emerging technologies from the perspective of the Department is critical to reducing future risks.

The Tech Centers' research portfolio is inherently rooted in the principles of evidence building and scientific integrity. Our goal is to identify and fill critical data and information gaps and to drive innovation and continuous learning so DHS can keep pace with the evolving threat landscape.[3] Responding to the nation's most pressing challenges and executing the Department's core missions requires using the best science and evidence available that are based on facts resulting from rigorous and systematic analysis. These charges are established through "The Foundations for Evidence-Based Policymaking Act of 2018"[4] (Evidence Act) and reflect the mission and values of S&T. Ensuring scientific integrity[5,6] is also critical to all aspects of the Tech Centers' work to guarantee the research and science we produce is objective, clear, unbiased, transparent, reproducible, and accurately represented. Strict adherence to professional values and practices will ensure robust science and lead to trust and confidence in our research.

[2] Foresighting explores the confluence of societal, technological, environmental, economic, political issues with science and technology innovations to inform what solutions or what type of solution options are most viable. Foresighting deepens the understanding of the driving forces behind this confluence, identifies gaps in knowledge; suggests areas of new research required to better understand driving forces, builds consensus among a range of stakeholders about the issues and how to tackle them, identifies and makes explicit some of the difficult policy choices and tradeoffs in the future, creates a new strategy that is resilient because it is adaptable to changing external conditions, and mobilizes stakeholders to action.

[3] Evidence is broadly defined as information that aids in the generation of a conclusion through foundational fact finding, synthesizing the existing body of knowledge, evaluating current or emerging practices, approaches or interventions, filling knowledge and data gaps, and bridging the nexus between research and policy and best position S&T to support the Department. The Government Accountability Office describes evidence building "as a cycle of activities that can help decision makers obtain the evidence they need to address policy questions or identify the questions they should address."

[4] Foundations for Evidence-Based Policy Making Act of 2018 was signed into law in January 2019. The law incorporates many of the recommendations of the U.S. Commission on Evidence-Based Policymaking (2017) to improve the use of evidence and data to generate policies and inform programs in the federal government.

[5] National Science and Technology Council. 2022. "Protecting the Integrity of Government in Science." https://www.whitehouse.gov/wp-content/uploads/2022/01/01-22-Protecting_the_Integrity_of_Government_Science.pdf

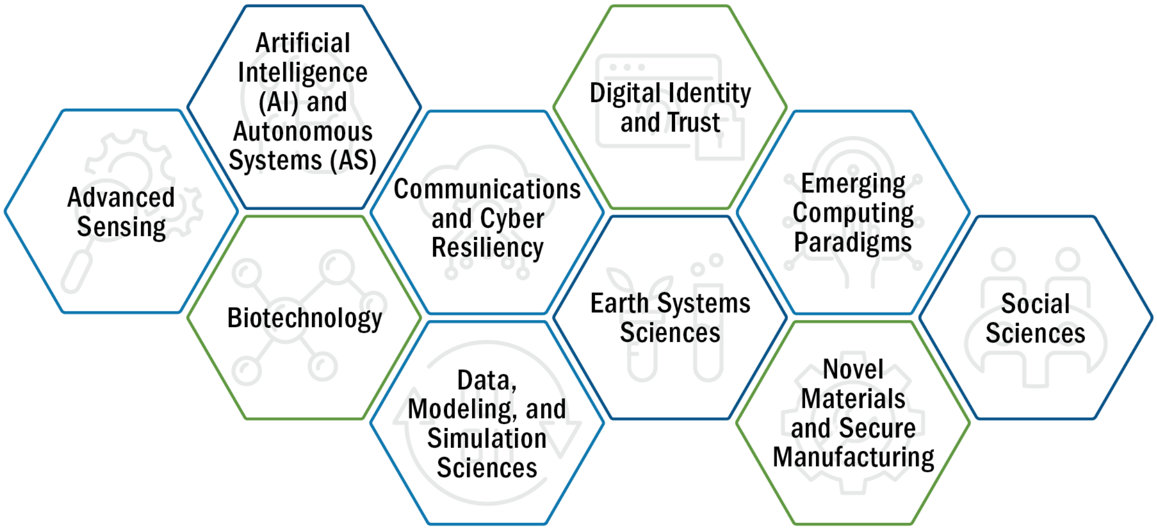
[6] Department of Homeland Security. 2012. "DHS Directive 026-07: Scientific Integrity." https://www.dhs.gov/xlibrary/assets/foia/dhs-directive-026-07-scientific-integrity.pdf

INTRODUCTION

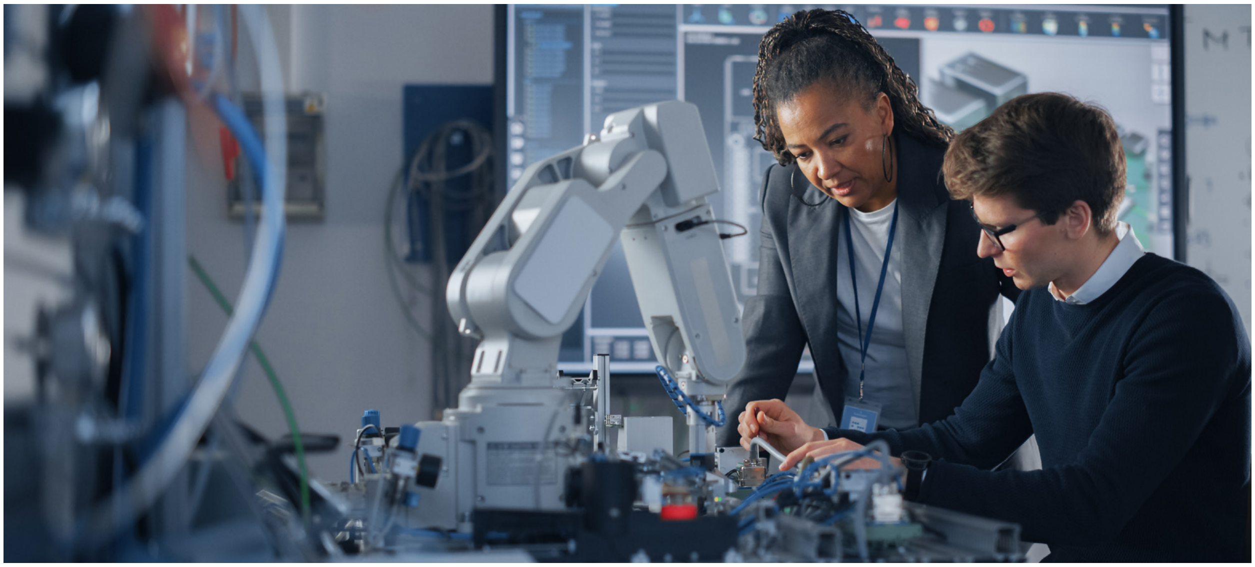
S&T TECH CENTERS RESEARCH PRIORITIES

S&T Tech Centers' Research Agenda is intended to provide the strategic framework against which we align and focus our research portfolio, and it communicates our priorities and objectives over the next three years. This Research Agenda identifies the most critical and impactful advances and developments in science and technology from the perspective of where the emerging technology and science trends are headed and their potential impact or implications to the Department.

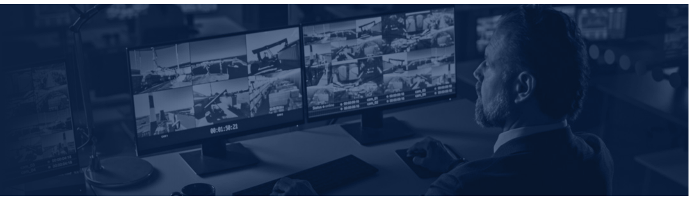
Our Overarching Research Priority Areas Are:



- Advanced Sensing
- Artificial Intelligence (AI) and Autonomous Systems (AS)
- Biotechnology
- Communications and Cyber Resiliency
- Data, Modeling, and Simulation Sciences
- Digital Identity and Trust
- Earth Systems Sciences
- Emerging Computing Paradigms
- Novel Materials and Secure Manufacturing
- Social Sciences



ADVANCED SENSING



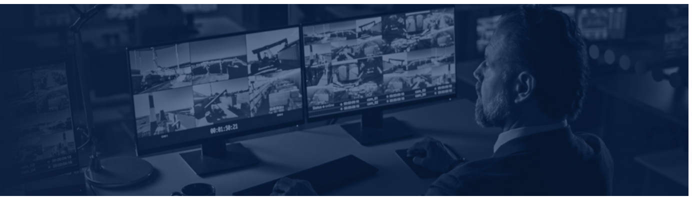
Sensors are vital to almost every mission of DHS. The ability to identify manmade and natural threats and maintain situational awareness during both daily operations and during catastrophic incidents is critical to protecting the homeland. The variety of threats and hazards that we look to detect is broad, and the types of sensors required to detect those threats and hazards are complex and can span several emerging technology areas. From tracking and identifying the movement of goods and people across borders and in maritime environments; monitoring the environment for wildfires, floods and other natural and manmade disasters; and securing buildings, aircraft, and other venues from malicious actors, the DHS mission space is ripe with needs and opportunities for advanced sensing capabilities.

MISSION IMPACTS:

Enhance threat sensing and detection capabilities across multitude of threats and DHS operational environments

As the science and technology landscape continues to evolve and converge, DHS also encounters new challenges that we must address. Such challenges include the need to detect counterfeit microelectronics or to counter new types and nefarious uses of unmanned aerial systems. Research and development (R&D) into advanced sensor technologies may allow us to address those challenges. Emerging technology areas that show promise for advanced sensor capability are quantum sensors and nanotechnology. Quantum sensors are predicted to be many more times sensitive than current systems, supporting the development of magnetic, acoustic and gravity sensors with increased capabilities; low-power, high-sensitivity airborne and space-based sensors; remote sensing; precision timing, etc. These sensors may allow us to alleviate our reliance on potentially vulnerable position, navigation, and timing systems. They may also enhance our ability to sense in more remote environments that are too dangerous to have officers and operators physically in, as well as increase the resiliency of our communications systems. Advances in nanotechnology that reduce the size, weight, power consumption, and cost of sensors could make it possible to deploy sensor networks over large areas in urban or remote environments and better integrate sensors in environments with limited space, such as checkpoints.

ADVANCED SENSING



Advanced Sensing Focus Areas and Technical Objectives

Focus Area 1. Signature Exploitation and Detection – We aim to understand how emerging sensor technologies and existing detection capabilities can be applied in new ways to detect, track, and identify objects, threats, hazards, physical, and cyber conditions.

- **Technical Objective 1:** Identify advancements in sensor technology to detect materials of interest such as chemical, biological and agriculture agents, explosive materials, contraband, as well as monitor environmental conditions for fire and flood.

- **Technical Objective 2:** Identify and evaluate signatures and capabilities not currently being exploited by DHS to understand their potential uses in homeland security applications. Examples include medical, safety, and environmental monitoring where innovation of sensor development is driven by commercial use.

- **Technical Objective 3:** Identify cutting-edge advancements and capabilities for transformative improvements in robustness and suitability of sensing technology within DHS's operational environments, such as remote and maritime environments that require low-power consumption, portability, and resistance to environmental conditions such as extreme temperatures, salt, and humidity.

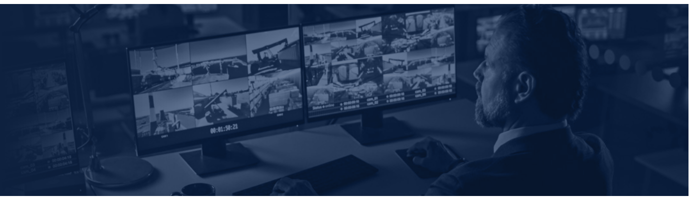
Focus Area 2: Sensor Integration – As novel sensors become available for use, S&T must develop appropriate sensor system architectures, integrate multiple sensors, and evaluate novel sensor effectiveness.

- **Technical Objective 1:** Assess new sensor integration concepts and approaches to understand their potential impact to DHS missions and to enable DHS to remain agile enough to incorporate new technologies as they are developed while maintaining high standards of operational efficiency and readiness.

- **Technical Objective 2:** Understand how to maintain high cybersecurity standards in integrated sensor environments to forecast possible technology advances and threats with an impact on deployed sensors. This will be vital to maintaining the security and effectiveness of current and future integrated sensor environments.

- **Technical Objective 3:** Create novel sensor integration methods, architectures, and interfaces to better leverage new and emerging technologies such as edge computing and advanced analytics, the internet of things, quantum computing, 6G communications, human-machine teaming, immersive visualization, and other advances. These new technologies may provide opportunities to integrate and advance sensor capabilities and address challenges in DHS systems and operations, while maintaining awareness of possible security implications.

ADVANCED SENSING



Focus Area 3: Emerging Sensing Technologies – S&T aims to collaborate with leading researchers and innovators in quantum sensing and nanotechnology to support initial transitions of early development into successful prototypes of novel tools for DHS missions and use cases.

- **Technical Objective 1:** Develop a framework for benchmarking quantum sensing capabilities to enable assessment and analysis of capabilities for DHS missions and use cases.
- **Technical Objective 2:** Identify and test promising quantum technology prototypes relevant to DHS and critical infrastructure missions (such as high-stability inertial sensors for unmanned aircraft systems, or UAS, missions in urban canyons or low-cost atomic clocks for critical infrastructure timing applications).
- **Technical Objective 3:** Track nanotechnology sensor advances that are applicable to DHS use cases. Examples include nanofluidics, nanomaterials, nanoelectronics and other aspects of nanotechnology that could impact sensing threats of interest in DHS environments.

ARTIFICIAL INTELLIGENCE (AI) AND AUTONOMOUS SYSTEMS (AS)

Both the “U.S. Department of Homeland Security Artificial Intelligence Strategy”[7] and the “S&T Artificial Intelligence and Machine Learning Strategic Plan”[8] refer to “Artificial Intelligence” as:

“...automated, machine-based technologies with at least some capacity for self-governance that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.”

Artificial Intelligence (AI) is the most prevalent topic across multiple strategic drivers for R&D within S&T and has the potential both to significantly impact the Department across many missions and to spawn new inventions and additional advances in numerous other domains (e.g., autonomous systems[9], intelligent sensors, etc.).

MISSION IMPACTS:
Transform screening capabilities at ports of entry; defend against advanced AI/AS attacks on critical infrastructure

As AI and AS become mainstream, it is critical that we understand the landscape, the evolution of the various aspects of the technology, the supporting science, and the needs of the Department. Key areas of AI R&D include computer vision for applications such as surveillance and screening systems and biometrics, and natural language processing for applications such as law enforcement and immigration services. Key use cases for AS include transportation (automotive, aerospace, maritime, and rail), utilities (water and wastewater, oil and gas, electric power, and telecommunications), facility operations (security, energy management, environmental control, and safety). Importantly, and as recognized by the North Atlantic Treaty Organization (NATO)[10], “The need for new algorithmic approaches and a better understanding of human-machine teaming has probably never been stronger.” It is imperative that operators in the homeland security enterprise are comfortable/ engaged with the capabilities possible from these technology advances. As these capabilities quickly evolve, we must look ahead in this space, understand capabilities, identify, and push through limitations to meet Departmental needs and anticipate potential threats.

Advances in and accessibility to AI also come with the potential for new and increased threats when capabilities are use with bad intent. “Adversarial AI”[11] is one of the risks/threats at the forefront of the AI research community. Because

[7] Department of Homeland Security. “Artificial Intelligence Strategy.” 2020. https://www.dhs.gov/sites/default/files/publications/dhs_ai_strategy.pdf

[8] Department of Homeland Security Science and Technology Directorate. “S&T Artificial Intelligence and Machine Learning Strategic Plan.” 2021. https://www.dhs.gov/sites/default/files/publications/21_0730_st_ai_ml_strategic_plan_2021.pdf

[9] AI is typically embedded in either analytic process or some kind of (semi or fully) autonomous system process. In semi or fully autonomous systems, AI receives input (e.g., through sensors), produces an output internal to the system (decision), and then acts on that output (action) to affect the external world state. It is well understood that to achieve full autonomy capable of operating in any kind of non-trivial environment, an autonomous system, particularly fully autonomous, will require AI in both the sensing and deciding cycles.

[10] Reding, D.F. and Eaton, J. NATO Science & Technology Organization. 2020. Science & Technology Trends 2020-2040 – Exploring the S&T Edge. p. 54. https://www.sto.nato.int/publications/Management%20Reports/2020_TTR_Public_release_final.pdf

[11] “Adversarial AI” can also be referred to as Adversarial AI Attacks, AI-Based Attacks, AI Adversarial Attacks, Adversarial Attacks in Age of AI, Adversarial Attacks on Machine Learning, Adversarial Attacks on Neural Networks, Adversarial Attacks, etc.

security of AI is a relatively immature sub-discipline, there is some range of interpretation in exactly what space the term covers. For S&T purposes, we define Adversarial AI as the spaces represented in green and blue, as shown in Figure 3.[12] As AI becomes more prevalent in IT, threat actors are finding new ways to use AI to deny, degrade, and disrupt missions (e.g., improved social engineering, deepfakes, improved way of hiding malware, etc.). These attacks can include data poisoning, reverse engineering machine learning data sets, among others attack vectors. The design of attacks can focus on attacks executed in both digital and non-digital spaces, such as electromagnetic spectrum. The point at which an AI-based attack can be detected/thwarted through cyber defenders and the point at which AI-expertise is required to detect, identify, and thwart AI-based attacks remains an open question. Figure 4[13] provides a useful visualization for appreciating the overlap between the two. DHS must understand, not only the underlying technology, but also how to organize and prepare to defend against these types of attacks.

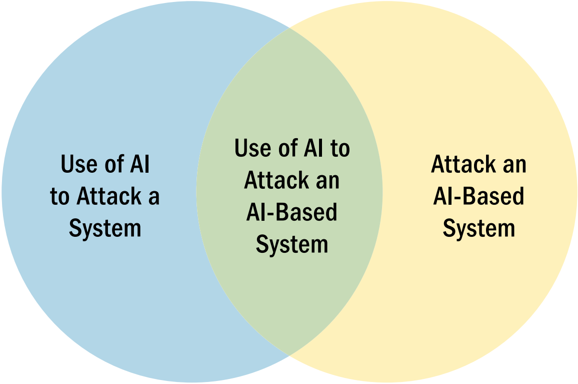

Use of AI to Attack a System
Use of AI to Attack an AI-Based System
Attack an AI-Based System

Figure 3. Adversarial AI. Described as the Use of AI to Attack an AI-based System

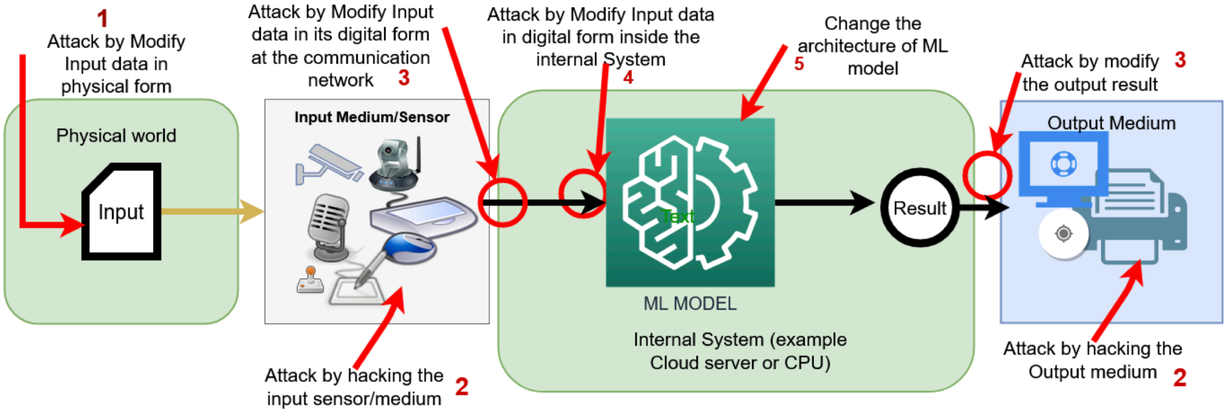

1
Attack by Modify Input data in physical form
Attack by Modify Input data in its digital form at the communication network
3
Attack by Modify Input data in digital form inside the internal System
4
Change the architecture of ML model
5
Attack by modify the output result
3
Physical world
Input
Input Medium/Sensor
Text
ML MODEL
Result
Output Medium
Internal System (example Cloud server or CPU)
Attack by hacking the input sensor/medium
2
Attack by hacking the Output medium
2

Figure 4. Generalized Adversarial Attach Points on Machine Learning Model

[12] We assume that "Attack" can be either design or execute or both, and that AI Attacks can be directed at non-digital infrastructure.

[13] Borrowed from Gupta, K.D. and Dasgupta, D. (2021). "Who is Responsible for Adversarial Defense?", Proceedings of the 38th International Conference on Machine Learning PMLR 39, 2021.

ARTIFICIAL INTELLIGENCE (AI) AND AUTONOMOUS SYSTEMS (AS)

Artificial Intelligence and Autonomous Systems Focus Areas and Technical Objectives:

Focus Area 1: Trustworthy AI/AS – DHS needs to be able to assess the performance of AI/AS for potential operational use in order to maintain the integrity of DHS missions and to ensure the appropriate systems are employed. In general, this focus area aims to:

- Effectively assess the performance of AI/AS systems against technical and mission metrics.
- Provide operators making critical decisions an appropriate level of trust and confidence in the AI/AS system.
- Inspire trust in the general public towards AI/AS systems deployed by DHS.

- **Technical Objective 1:** Understand when explainability[14] is important in AI applications and assess the effectiveness of explainability in DHS missions that depend on AI.
- **Technical Objective 2:** Assess and advance AI/AS robustness[14] to ensure the reliability of AI implementations in the DHS mission spaces.

Focus Area 2: Adversarial AI – Across all the layers in the communications and tech stacks (data, software, hardware, networks, and communications), we must guard against sophisticated adversaries employing AI attacks.

- **Technical Objective 1:** Identify, characterize, and classify known adversarial attacks, both in the academic community and in the intelligence community, to increase understanding an awareness across the broader DHS and federal interagency community.
- **Technical Objective 2:** Understand the effectiveness of attacks against digital and non-digital infrastructure (e.g., physical devices and electromagnetic spectrum) and their potential impacts to HSE missions.
- **Technical Objective 3:** Understand what will be required to deter, protect against, detect, and respond to adversarial AI attacks against digital and non-digital assets in zero trust architecture environments including traditional information technologies, operational technologies, and electromagnetic spectrum.

[14] Because AI is a relatively immature discipline, terms like "explainability" or "robustness" are terms of art and subject to interpretation. "Explainability" generally addresses the extent to which human users can comprehend the results of an AI/AS. "Robustness" generally addresses the degree to which the AI/AS is stable despite noisy data or perturbations in the data.

ARTIFICIAL INTELLIGENCE (AI) AND AUTONOMOUS SYSTEMS (AS)

Focus Area 3: Advanced Applications of AI/AS for Unique DHS Missions – This focus area aims to advance AI/AS capabilities in various subfields (such as computer visioning, natural language processing, predictive modeling, etc.) to drive application of AI/AS across specific DHS missions and needs (e.g., biometric capabilities, media, and analytics for mis/dis/mal information, digital forensics, etc.).

- **Technical Objective 1:** Understand how humans and AI/AS can most effectively collaborate to successfully carry out homeland security missions. Investigate human supervision and interaction with AI/AS to optimize human-machine systems and performance in DHS's operational settings.
- **Technical Objective 2:** Identify and develop use cases based on DHS missions that will benefit from application of AI/AS, considering AI/AS sub-components such as:
  - Natural language processing and generation and machine translation, including transformer architectures, social listening, automated strategic communication, and media and analytics.
  - Anomaly detection in events, images, texts, video, speech, and other sources.
- **Technical Objective 3:** Identify challenges in operationalizing AI within DHS. (Examples include embedding AI components in real time, feedback situations including deep reinforcement learning, secure AI edge applications including distributed sensors, and actuators and computation.)
- **Technical Objective 4:** Assess the efficacy of adopting high-end AI chips for homeland security big computing use cases.

BIOTECHNOLOGY

Biotechnology is generally defined as the integration of the life sciences and engineering with the goal of harnessing the power of biological molecules, cells, and/or even whole organisms for industrial, commercial, or other purposes. More specifically, biotechnology comprises genetic, metabolic, tissue, and microbial community engineering, biopharmaceutical development, catalysis, bioleaching and bioremediation, selective plant and animal breeding, and other applications. Scientists have many biotechnological tools at their disposal, including: polymerase chain reaction (PCR), nucleotide (e.g., DNA) synthesizers and sequencers, DNA-cutting and pasting enzymes, genome editors, bioinformatics databases and analytics, cloning and gene delivery vectors, bioreactors, cell-based assays, genetically tractable molecular chasses, antibodies, nanoparticles, and a vast array of other proteins that can perform specific functions including chemical sensing and transformation.

MISSION IMPACTS:
Detect and defend against new biothreats and new pathways for bio and agroterrorism

Global research activity in biotechnology is intense and driven largely by its applications to public health, agriculture, other industrial products (e.g., biofuels), manufacturing, and the demands of basic science; however, biotechnological tools are inherently dual-use and have been recognized as "critical and emerging technologies" by the National Science and Technology Council (NSTC)[15]. DHS must therefore fully understand their associated risks and opportunities.

To counter the threats of bioterrorism, DHS must address issues such as the misappropriation of biotechnological tools by state or non-state actors for offensive use, how DHS can deter or prevent attempts by state or non-state actors to misappropriate biotechnological tools for offensive use, and whether DHS can harvest any biotechnological tools to augment the defensive posture of the United States. Close and continuous evaluation and research into these issues will enable DHS to make sound tactical and strategic decisions and inform policy, strategy, and investments to ensure that the United States not only continues to lead the innovation in biotechnology but does so with a full understanding and preemptive mitigation of foreseeable downside risks—thus enhancing public safety.

[15] National Science and Technology Council. "Critical and Emerging Technologies List Update" 2022. https://www.whitehouse.gov/ostp/news-updates/2022/02/07/technologies-for-american-innovation-and-national-security

BIOTECHNOLOGY

Biotechnology Focus Areas and Technical Objectives:

Focus Area 1: Worldwide Developments in Biotechnology – DHS must continuously monitor worldwide developments in biotechnology—and the life sciences more broadly—to fully understand new opportunities for U.S. adversaries to misappropriate those developments for offensive use and to enable the United States to harvest them for defensive use.

- **Technical Objective 1:** Identify topics and trends in biotechnological research and assess how new research results could expand and/or impact an actor's options along a potential biological attack pathway to prevent technological surprise.
- **Technical Objective 2:** Identify approaches to counter emerging material threats.
- **Technical Objective 3:** Identify and harvest emerging opportunities to bolster the bio-defensive posture of the United States.

Focus Area 2: Existing and Emerging Biological Agent Detection – DHS must support homeland resiliency by developing capabilities that can quickly detect and identify any potentially hazardous materials in environmental aerosol samples.

- **Technical Objective 1:** Continuously assess machine learning-enabled analytic methods for DNA/RNA sequencing, proteomics/protein sequencing, spectroscopy, mass spectrometry, and other computational approaches that can be used to identify biological and biochemical hazards.
- **Technical Objective 2:** Develop computational capabilities to quickly identify and tentatively characterize any potential nucleotide-based (i.e., DNA/RNA) biological hazard. This includes further development of models of gene function and organization and deep learning to identify patterns within genomes.
- **Technical Objective 3:** Identify approaches and capabilities for high-sensitivity and high-specificity real-time identification of components of environmental aerosol samples.

COMMUNICATIONS AND CYBER RESILIENCY

Operational assurance in an increasingly digitally integrated environment requires resiliency across data, software, hardware, and communications networks. DHS operations are often conducted in challenging, congested, and contested environments across cyber and electromagnetic domains. While technologies continue to evolve independently in both domains, it will be critical to integrate multi-domain solutions that are able to prevent, detect, and respond to threats holistically at speed and scale to secure operations across the homeland security enterprise.

MISSION IMPACTS:
Enhance resiliency to cyberattacks & communication disruptions; enable 24/7 interoperable emergency communications

DHS is the national lead for protecting and enhancing the security and resilience of the nation's civilian cyber and communications systems and critical infrastructure. Furthermore, DHS relies on and employs a broad set of communications and computing technologies to accomplish its many missions to include securing our digital and physical borders, protecting the transportation system, responding to natural disasters and emergencies, and safeguarding our financial systems. As part of this mission, it is essential to assess and counter evolving cybersecurity threats that may materialize as malicious activity and cybercrime. In addition, law enforcement will need increasingly sophisticated cyber tools to prevent, identify, investigate, disrupt, and dismantle criminal enterprises that are increasingly reliant on digital technologies.

The need for and importance of cybersecurity is well recognized by the government and industry. Recent events such as SolarWinds[16] and the Colonial Pipeline[17] attacks highlight the need for continued investments and advancements in this domain, as the threats remain persistent and evolving as technologies and capabilities continue to advance. Under the DHS 2020 – 2024 Strategic Plan,[18] Goal 3 is to "Secure Cyberspace and Critical Infrastructure" with objectives focused on securing federal civilian networks, assessing and countering evolving cybersecurity risks, and combating cybercrime. Executive Order (EO) 14028 "Improving the Nation's Cybersecurity"[19] further outlines specific areas of focus for bold changes and investments to protect the nation from malicious cyber actors while recognizing that government and industry must work hand in hand to foster a more secure cyberspace. The EO states *"...that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security."*[20]

[16] Cybersecurity and Infrastructure Security Agency. "Emergency Directive 21-01 - Mitigate SolarWinds Orion Code Compromise." 2020. https://www.cisa.gov/emergency-directive-21-01

[17] Congressional Research Service. "Colonial Pipeline: The DarkSide Strikes." 2021. https://crsreports.congress.gov/product/pdf/IN/IN11667

[18] Department of Homeland Security. "The DHS Strategic Plan – Fiscal Years 2020-2024." 2019. p. 26-35. https://www.dhs.gov/publication/department-homeland-securitys-strategic-plan-fiscal-years-2020-2024

[19] Executive Office of the President. "E.O. 14028 – Improving the Nation's Cybersecurity." 2021. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[20] Executive Office of the President. "E.O. 14028 – Improving the Nation's Cybersecurity." 2021. p. 26633 https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

COMMUNICATIONS AND CYBER RESILIENCY

Cybersecurity is not a stand-alone field, nor is it limited to traditional IT applications. As more and more digital capabilities are realized and interconnected, cybersecurity plays a role in ensuring those technologies, such as AI, IoT and other sensors, space-based applications, and countless more, are securely leveraged and protected against things like ransomware attacks.[21] As the EO states, *"the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced."*[22] As new, digitally based technologies evolve, cybersecurity plays a key role in reducing or eliminating potential new exposures and vulnerabilities.

While AI will give us unprecedented ability to protect against, detect, and respond to cybersecurity threats at a greater scale, so too will this technology be used to generate and deploy new and novel attacks at speeds and sophistication levels unseen in today's networks. Furthermore, increasingly robust communications capabilities will enable more effective information sharing and collaboration between humans and technologies but will also provide an expanded attack surface for adversaries to detect and affect the resilience of our operations.

Increasing assurance of the data, as well as the software and hardware that store and process that data, is only part of the solution. For humans and machines to make effective use of the data for automated decision-making and action-taking, it is essential to increase the resilience of the wired and wireless communications networks that are used to share data between these technology systems. Similar to cybersecurity, communications is also a well-documented area of continued need and importance for the HSE.[23, 24, 25] The communications ecosystem includes both terrestrial (e.g., narrowband, broadband, High Frequency (HF), undersea, aerial) and non-terrestrial (e.g., celestial, space) solutions. Advanced communication networks are a key element of tomorrow's digital infrastructure and are an enabler of technology such as AI, internet of things (IoT), and augmented reality/virtual reality (AR/VR). The promises of advances in technologies such as 5G/XG and the proliferation of low Earth orbit satellite constellations (LEO) are anticipated to be revolutionary. 5G is expected to facilitate fundamentally new classes of applications, from real-time remote operations and enhanced situational awareness, to self-driving cars, smart buildings, AR, and more.

[21] As stated in Reding, D. F. and J. Eaton's 2020 NATO Science & Technology Trends 2020-2040 - Exploring the S&T Edge, "Cyber-attacks against BLUE (commercial or military) space control centres open up additional areas of vulnerability and the possibility of ransomware."

[22] Executive Office of the President. "E.O. 14028 – Improving the Nation's Cybersecurity." 2021. p. 26633 https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[23] The Office of Science and Technology Policy FY22 Research Priorities calls out advanced communications networks and encourages investment in "the development of applications that leverage 5G and advanced networks that incorporate security and privacy as fundamental values" as well as the application of AI/ML to communications and cybersecurity with the goal of secure and trusted applications.

[24] The Cybersecurity and Infrastructure Security Agency's National Emergency Communications Plan, the nation's strategic plan to strengthen and enhance emergency communications capabilities, includes national strategic objectives centered around building resilient and secure emergency communications systems to reduce cybersecurity threats and vulnerabilities.

[25] The U.S. Coast Guard's (USCG) first line of effort in the 2019 Arctic Strategic Outlook is to "Enhance Capability to Operate Effectively in a Dynamic Arctic" and the sub-objective "Close the Critical Communications Gap in the Arctic" is one of three sub-objectives through which the USCG seeks to operate effectively, maintain maritime domain awareness, and share information across a harsh and unforgiving environment.

COMMUNICATIONS AND CYBER RESILIENCY

Quantum-based technology is another area that provides both threats and opportunities in terms of resilience of our computer and communications networks for the future. The race for quantum supremacy is spawning research investments by nation-states as well as industry and pushing the science and technology forward at a pace not seen before.[26,27] With these technical advances, however, come emerging threats as well. The Administration's FY22 R&D budget priorities[28] highlight Quantum Information Science (QIS) as one of its top five research priorities to "enable next-generation quantum devices, and expansion of efforts exploring and piloting uses of quantum technology to help support agency missions." The field of QIS and its applications is broad but offers significant technical advances in speed, precision, or functionality[29] primarily applied in areas such as cryptography, computation, sensing and imaging, communications and materials.[30]

Within the quantum computing domain, the most well-known and immediate concern is the ability of a quantum computer to crack current encryption schemes used today. Although the timelines on when such a quantum computer will be achieved are varied, the cybersecurity impacts are significant and will likely affect sensitive data that is being generated now and in the near future.[31] Informed planning can help the Department protect its equities, and thus, staying abreast of developments is critical in order to help advise and inform the Department as it develops guidance.

Additionally, quantum-based communications and networking offers the ability to maintain secure communications worldwide and eavesdropping detection, but again these capabilities are likely 10 years[32] or more away. However, nearer term applications of quantum technologies such as Rydberg atom sensing can provide opportunities to increase the resilience of communications systems in congested and contested electromagnetic environments.

[26] Office of the Deputy Assistant Secretary of the Army (Research & Technology). 2019. Emerging Science and Technology Trends: A Synthesis of Leading Forecasts. https://apps.dtic.mil/dtic/tr/fulltext/u2/1078879.pdf

[27] China has invested heavily in quantum computing, spending upwards of $10B on the country's National Laboratory for Quantum Information Sciences. Is China leading the quantum computing race? - Tech Wire Asia

[28] Office of Science and Technology Policy. "Fiscal Year (FY) 2022 Administration Research and Development Budget Priorities and Cross-cutting Actions." 2020. P.4. <https://www.whitehouse.gov/wp-content/uploads/2020/08/M-20-29.pdf>

[29] National Quantum Coordination Office. 2021. About QIS. About - National Quantum Initiative.

[30] Reding, D. F. and J. Eaton. Brussels: NATO Science & Technology Organization. "Science & Technology Trends 2020-2040 - Exploring the S&T Edge." 2020.

[31] i.e. technical developments that can impact timelines and capabilities such as qubit capabilities, cold quantum, quantum storage, quantum networks, error rates, etc.

[32] Reding, D. F. and J. Eaton. Brussels: NATO Science & Technology Organization. "Science & Technology Trends 2020-2040 - Exploring the S&T Edge." 2020.

COMMUNICATIONS AND CYBER RESILIENCY

Communications and Cyber Resiliency Focus Areas and Technical Objectives:

Focus Area 1: Data-centric Security – This focus area aims to increase the reliability and employability of data for homeland security missions.

- **Technical Objective 1:** Identify and evaluate new and emerging technological applications, such as post-quantum cryptography and homomorphic encryption, to ensure the confidentiality, integrity, and availability of data at rest, in process, and in transit.
- **Technical Objective 2:** Identify and evaluate new resilient machine learning approaches, explainable AI (XAI) and human-machine teaming capabilities, and generative adversarial attack identification and mitigation approaches to increase trustworthiness of advanced data science and analytics.

Focus Area 2: Software and Hardware Assurance – This focus area aims to ensure the resilience of the data, software, and hardware used to execute homeland security mission functions.

- **Technical Objective 1:** Ensure the confidentiality, integrity, and availability of data at rest, in process, and in transit across software and hardware platforms by researching and evaluating new and emerging applications such as post-quantum cryptography and homomorphic encryption.
- **Technical Objective 2:** Ensure advanced computing software and hardware applications are designed to rapidly adapt to the evolving security environment and future technologies. Example applications include but are not limited to sensors and IoT, operational technologies (OT), cyber physical systems (CPS); high performance computers (HPC); microelectronics, edge, cloud, fog, mobile, and quantum computing and civil space systems.
- **Technical Objective 3:** Leverage advances in emerging technologies such as memory-safe programming languages, zero trust architectures; infrastructure as code/pilot light (IaC/PL); augmented, virtual, and cross reality (AR/VR/XR) and adaptive secure-by-design architectures to increase cybersecurity across operations.
- **Technical Objective 4:** Increase assurance across the supply chain and lifecycle of key software and hardware employed in cybersecurity functions and critical infrastructure such as security orchestration and automated response (SOAR), software bill of materials (SBOM), and federated identity, credential, and access management (ICAM).

COMMUNICATIONS AND CYBER RESILIENCY

Focus Area 3: Communications and Network Resiliency – This focus area aims to protect and enhance the networks that transport the voice and data between devices/humans and the interconnected software and hardware systems (e.g., V2X).

- **Technical Objective 1:** Identify and understand new and emerging communications concepts and technologies such as spectrum agility, broadband virtualization, and software defined networking to enable communications resilience in the face of increasingly congested and contested operational environments (spectrum scarcity, intentional interference).
- **Technical Objective 2:** Investigate advanced communications technologies (i.e., 5G/XG mobile networks, optical interlinks across proliferated low-Earth orbit satellite (LEO) networks, and quantum sensing receivers) to identify and assess new risks and potential attack surfaces as well as enable new use cases to dramatically enhance capabilities and create efficiencies for DHS missions.
- **Technical Objective 3:** Create techniques to maintain security and communications in an environment where new complex architectures (everything-as-a-service) present more attack surfaces for adversarial exploitation.
- **Technical Objective 4:** Identify gaps in existing standards that result in non-interoperable, proprietary, or inefficient solutions, to inform and accelerate the development of new standards resulting in improved techniques to test and verify conformance to standards.

DATA, MODELING, AND SIMULATION SCIENCES

We are shifting from a world where data were rare, precious, and expensive to a world where data are ubiquitous, commonplace, and inexpensive. In this data-rich environment, we can leverage data science developments across multiple homeland security missions to find signals, patterns, or structure within high-dimensional, noisy, uncertain input data and simulation sciences conduct experiments to predict different operational outcomes. Figure 5 shows the interconnectedness between the two. Such research has the potential to impact a range of homeland security operations, such as improving phenomenology of crowd models, improving tool sets available in cyber analytics platforms, decreasing time to develop training data annotations in law enforcement missions, improving air interdiction of drug trafficking, adapting training according to the trainee's strengths and weaknesses. In all cases, this requires an improved data ecosystem. This work plays a critical role in informing, evaluating, and advising the Department on the cutting-edge capabilities and envisioning and prototyping use cases that benefit from a best of breed approach as technology drives us to a smart, connected world.

MISSION IMPACTS:
Advance training via virtual reality; enable greater data analytics capabilities across DHS missions

Additionally, both data and simulation sciences are increasingly combined with machine learning approaches.[33] Science-based simulations are increasingly relying on embedded ML models not only to interpret results from massive data outputs but also to steer computations. Science-based models (e.g., provides a more easily communicated and understood digital representation of a system that enables experimentation) are being combined with data-driven models (e.g., finding signals, patterns, or structure within high-dimensional, noisy, uncertain input data) to represent complex systems and phenomena. This recognition of "models" is significant as models are another common component to both data and simulation sciences. As such, this category of the research area also represents modeling areas of importance to DHS that do not fall in classic science-based simulations discussed thus far. These include technologies such as virtualization, game engines, and virtual/augmented reality. Example applications of these modeling technologies include enhanced situational awareness in operations through AR and digital twinning, improvements in training through VR and game engines, and improvements in testing through virtualization and digital twinning.

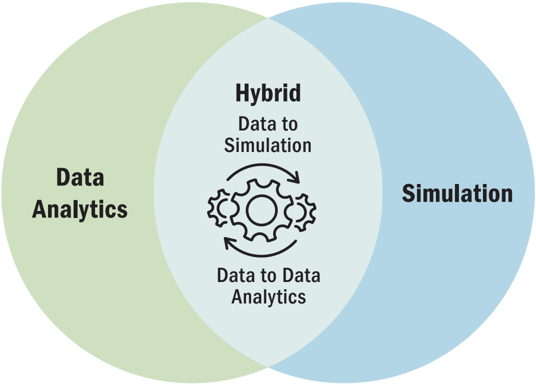


Figure 5. Complementary Nature of Data Analytics and Simulation

[33] As described in Section H. Emerging Computing Paradigms, machine learning is also driving convergence at the hardware level as high-performance computing elements are being introduced into both simulation and data-centric systems to support its application.

DATA, MODELING, AND SIMULATION SCIENCES

Finally, as massive stores and streams of digital data are driving an increasing emphasis on more sophistication at the application level (e.g., on-demand computation, rapid data processing, comparisons between simulations and observations, machine learning, etc.), the importance of an effective data ecosystem is increasingly apparent. It must consist of multiple integrated resources and software services, including resources for managing data, processing data, analyzing data, exploring data, collaborating with data, and sharing data. Data need to be discoverable, accessible, reproducible, secure, trusted, and reusable. Data management and lifecycle policies (e.g., curation, storage, retention and deletion, I/O requirements, etc.) are key concerns. And, in contrast to traditional scientific computing infrastructure, the data ecosystem must place greater emphasis on establishing a workable system for users providing access to systems, managing files, and connecting with data collection instruments.

Data, Modeling, and Simulation Sciences Focus Areas and Technical Objectives:

Focus Area 1: Advance Data Analytics Capabilities – This focus area aims to improve existing data analytics capabilities and invent/adapt new and emerging capabilities for DHS use.

- **Technical Objective 1:** Assess the performance of data science capabilities against DHS use cases involving data, such as survey and scientific data, text, speech, audio, images, video, and live streams, and determine methods to leverage for DHS use.
- **Technical Objective 2:** Identify and adopt emerging data analytics concepts and technologies and characterize their ability to scale to support DHS operations.

DATA, MODELING, AND SIMULATION SCIENCES

Focus Area 2: Advance Modeling and Simulation Capabilities – This focus area aims to improve existing modeling and simulation capabilities and adapt new and emerging capabilities for DHS use.

- **Technical Objective 1:** Identify key classes of models of significant impact to the homeland security enterprise that do not yet have consensus across theoretical underpinnings (e.g., crowd modeling, cyber traffic modeling, etc.) and document the breadth of approaches to enable developers, practitioners, and accreditors across the homeland security enterprise can benefit from this collection.
- **Technical Objective 2:** Assess, leverage, and advance the use of scientific ML (e.g., hybrid algorithms and models for predictive scientific computing, ML-enabled adaptive algorithms, parameter tuning and multiscale surrogate models, etc.) for homeland security applications.

Focus Area 3: Combine Data Analytics and Simulation Capabilities

- **Technical Objective 1:** Experiment with stream processing and in-memory processing techniques for analyzing high-rate, real-world data on a digital twinning application, linking a simulation of a system with the real-world data collected from that system. Example includes maintaining synchronization between a digital twin of the southern border and sensor platforms at the southern border in near real time.
- **Technical Objective 2:** Understand the limitations of learning models from simulated environments and explore how simulation and other apps, such as video games, can collect data that can later be used for experimentation or predictive analytics.
- **Technical Objective 3:** Explore Model-Test-Model paradigms, augmenting test and evaluation with simulation-based capabilities, and develop the automation, analytics and algorithms necessary to update the simulation model with live data collected from the test.

DATA, MODELING, AND SIMULATION SCIENCES

Focus Area 4: Data Ecosystem – This focus area aims to increase knowledge and inform best practices for data ecosystems that serve all modeling communities and enable data analytics, simulation, and AI applications.

- **Technical Objective 1:** Evaluate automated methods to assist in data set maturation (e.g., data annotation mechanisms to characterize data sets, synthetic data generation methods to thicken data sets, automated synchronization of object models across heterogeneous data sets, etc.) to better enable machine learning applications and to find better, faster, cheaper ways of engineering data needed across DHS operations and oversight.
- **Technical Objective 2:** Determine how to characterize infrastructure and tech stacks needed for efficient and secure data collection and data engineering to streamline data-analytics workflow automations to find better, faster, cheaper ways of creating value to the operational community from the data it collects.

DIGITAL IDENTITY AND TRUST

Trust is a key issue for being able to transact electronically with natural persons and non-person entities, such as organizations and machines, across different systems. Ensuring the provenance, confidentiality, integrity, and availability of data is critical to transact with trust and maintain privacy across interconnected services, devices, and users. The proliferation of online services and cloud computing are enabling new operational efficiencies while simultaneously creating novel risks. Digital trust enabled by new capabilities such as digital credentials (e.g., mobile driver licenses) and zero trust architecture are critical to DHS successfully deploying and operating 5G communication systems, critical infrastructure, government services, and many other Department missions.

MISSION IMPACTS:
Adapt to and assess emerging identity paradigms while maintaining security & privacy

The ability to establish and verify an individual's identity enables the Department to perform risk-based decision making that is tailored to the individual. Such decision making may involve determining whether an individual is eligible to receive specific services or benefits or ascertaining if an individual is a known or suspected threat. For example, as the Transportation Security Administration begins to accept mobile driver's licenses at airport checkpoints and U.S. Customs and Border Protection examines travelers' documents (e.g., passports) through customs checkpoints, we must be able to detect whether those documents are compromised in some way. In addition, as DHS develops and scales different identity verification technologies to meet evolving needs, we must ensure approaches include effective privacy and civil rights and liberties safeguards for U.S. citizens consistent with U.S. laws, regulations, and DHS authorities as they are developed.

The Office of Science and Technology Policy FY22 priorities[34] state that "Departments and agencies should also prioritize R&D aimed at improving data accessibility and security, including fundamental research into efficient privacy and security preserving techniques and building and/or strengthening infrastructure, platforms, and tools that facilitate responsible data use." Advancements in U.S infrastructure and security will also require the development of robust privacy protections and controls. The evolution of privacy enhancing technologies, processing, and correlation necessitate investing in research to conduct thoughtful tradeoffs of risks, performance, and mission needs.

[34] Office of Science & Technology Policy. "Fiscal Year (FY) 2022 Administration Research and Development Budget Priorities and Cross-cutting Actions." 2020. p.9. <https://www.whitehouse.gov/wp-content/uploads/2020/08/M-20-29.pdf>

DIGITAL IDENTITY AND TRUST

Digital Identity and Trust Focus Areas and Technical Objectives:

1. Focus Area 1: Digital Identity – This focus area aims to assess and manage risks associated with new, emerging, and disruptive technologies that may affect DHS's ability to establish and verify identity of entities (natural person, non-person) to strengthen and manage risks across a diverse range of DHS missions.

- **Technical Objective 1:** Organize, characterize, and prioritize risks to in-person and online activities to establish or verify asserted identity and biometric information.
- **Technical Objective 2:** Assess and manage risks and verify the uniqueness, integrity, validity, and provenance of identity and biometric information.
- **Technical Objective 3:** Establish appropriate datasets and assess capabilities to enable experimentation and minimize risks associated with use of personally identifiable information.
- **Technical Objective 4:** Facilitate the development of standards, best practices, test tools, and certification criteria to enable identity issuing authorities and relying parties to implement secure infrastructure and use of trustworthy identity information.

Focus Area 2: Privacy Enhancing Technologies – This focus area aims to understand effective and performant ways to meaningfully exchange data while respecting the confidentially and use of entities information

- **Technical Objective 1:** Develop and assess data anonymization and minimization techniques for effectiveness, performance, and fit for DHS use cases.
- **Technical Objective 2:** Develop methods for evaluating the effectiveness, performance, and fit of privacy enhancing technologies for DHS use cases.
- **Technical Objective 3:** Identify and assess methods for DHS's investigative and protection mission to lawfully investigate bad actors while minimizing access others data.

DIGITAL IDENTITY AND TRUST

Focus Area 3: Trust and Safety – This focus area aims to understand how trust can be gained, lost, and enhanced between entities on digital platforms.

- **Technical Objective 1:** Characterize threats in which bad actors can obfuscate, misattribute, and manipulate their identity.
- **Technical Objective 2:** Characterize threats in which bad actors can access, obfuscate, misattribute, and manipulate their data and communication channels.
- **Technical Objective 3:** Understand the governance and efficacy of emerging technology and trust frameworks, including zero trust architecture, cryptographic agility, omni-channel experiences and service design, and trust and safety of online communities.

EARTH SYSTEMS SCIENCES

Earth Systems Science (ESS) is the transdisciplinary analysis of the structure and functioning of the Earth as an adaptive, integrated system and the interactions between environmental (including geophysical), human, and technological systems. ESS is a recently new field of science, emerging over the last two decades. Its goal is to produce unified sets of concepts and analytical frameworks that can address facets of ongoing global change holistically. Global research in the Earth systems science domain has grown exponentially and is driven largely by the need to better understand how Earth systems are reacting to human, technological, and climate change; consequences for life on Earth; and implications to safety and security with potential influences on emerging risks and threat vectors toward enabling prediction, adaptation, and mitigation of undesirable consequences.

MISSION IMPACTS:

Counter new threats to climate change initiatives, such as exploiting social inequality; enhance critical infrastructure resilience to climate-related disasters

The Biden Administration placed climate change at the top levels of its international and domestic agendas, with a $2 trillion whole-of-government climate plan that will have far-reaching effects on the U.S. economy.[35] The need for investment in Earth systems science to better understand global change is amplified by the 2021 Annual Threat Assessment issued by the Director of National Intelligence, which identifies climate change as a major transnational security threat,[36] as does the National Intelligence Council[37] and Department of Defense.[38]

Disasters from all-hazards and climate change will continue to challenge DHS across a range of missions and frontline operations exacerbating known and unknown risks to public safety and national security. Physical impacts of extreme weather and changing climatic conditions such as environmental degradation will increasingly intersect with human impacts of population growth, economic development, and technological innovation (geo-engineering and digitization). DHS will be affected in the short- and long-term with rising disaster costs and losses, worsening risks

[35] In the January 27, 2021, Executive Order on Tackling the Climate Crisis at Home and Abroad, the President calls for a wide range of unilateral and bilateral measures to ensure the nation fully engages in both a domestic and international response to this crisis. This includes establishing a White House Office of Domestic Climate Policy. <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/27/executive-order-on-tackling-the-climate-crisis-at-home-and-abroad/>

[36] On April 9, 2021, in the 2021 Annual Threat Assessment, the Office of the Director of National Intelligence said, "We assess that the effects of a changing climate and environmental degradation will create a mix of direct and indirect threats, including risks to the economy, heightened political volatility, human displacement, and new venues for geopolitical competition that will play out during the next decade and beyond." p.18. <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf>

[37] On October 21, 2021, in the National Intelligence Estimate on Climate Change, the National Intelligence Council said, "We assess that climate change will increasingly exacerbate risks to U.S. national security interests as the physical impacts increase and geopolitical tensions mount about how to respond to the challenge... Countries are arguing about who should act sooner and competing to control the growing clean energy transition. Intensifying physical effects will exacerbate geopolitical flashpoints, particularly after 2030, and key countries and regions will face increasing risks of instability and need for humanitarian assistance." p.i.
< https://www.dni.gov/files/ODNI/documents/assessments/NIE_Climate_Change_and_National_Security.pdf>

[38] In the Department of Defense's Climate Risk Analysis, published in October 2021, the DoD says, "Climate change is reshaping the geostrategic, operational, and tactical environments with significant implications for U.S. national security and defense. Increasing temperatures; changing precipitation patterns; and more frequent, intense, and unpredictable extreme weather conditions caused by climate change are exacerbating existing risks and creating new security challenges for U.S. interests... To train, fight, and win in this increasingly complex environment, DoD will consider the effects of climate change at every level of the DoD enterprise." p.2.
< https://media.defense.gov/2021/Oct/21/2002877353/-1/-1/0/DOD-CLIMATE-RISK-ANALYSIS-FINAL.PDF>

of environmental degradation, critical infrastructure and supply chain disruptions, civil unrest, and social instability. Adversarial threats from climate terrorism and extremism will continue to emerge as malign actors seek to exploit these risks for advantage and tensions mount with particular effects on the most vulnerable.

In response, DHS issued a strategic framework for addressing the climate crisis and incorporated climate change as a priority in its strategic and long-term planning. DHS also seeks to optimize climate risk management for safety and security and understands the key decisions, data, and information requirements for effective action. DHS must therefore fully understand these associated risks and opportunities through the application of Earth systems science. Close and continuous research into the key areas outlined below will enable DHS to make sound tactical and strategic decisions and inform key policy and investments decisions to enhance U.S. resilience to the impacts of climate change, ensure U.S. leadership in climate adaption, resilience, and sustainability innovation, and best positioned to address emerging security challenges and future risks.

S&T's ongoing efforts in this research area align with the Department's priority mission to prepare the nation to respond to and recover from disasters and combat the climate crisis. We seek to understand the impacts of climate change to DHS missions along the lines of safety and security. Issues that DHS will address include emerging security challenges associated with a changing climate, effects of climate change on DHS missions and operations, and the potential for malign actors to exploit climate risks and/or climate technology innovation.

Earth Systems Sciences Focus Areas and Technical Objectives:

Focus Area 1: Worldwide Developments in Earth System Science and Climate Innovations – DHS must continuously monitor worldwide developments in Earth system science—and climate technologies and innovations more broadly—to fully understand new opportunities for U.S. adversaries to misappropriate those developments for offensive use and to enable the United States to harvest them for strategic use.

- **Technical Objective 1:** Identify topics and trends in Earth systems science (i.e., geoengineering and technology innovations) and assess how new research results could expand and/or impact an actor's options along a potential climate resilience pathway to prevent adversarial surprise.

- **Technical Objective 2:** Identify approaches to counter malign use of emerging climate interventions (i.e., geoengineering) and adversarial threats (i.e., exploit civil grievances and social inequality).

- **Technical Objective 3:** Identify and harvest emerging opportunities to bolster the climate security posture of the United States.

Focus Area 2: Earth System Monitoring and Detection Capabilities – DHS must support homeland resiliency by identifying, leveraging, and developing capabilities that can quickly detect and identify any potential first-, second-, and third-order effects of climate change and extreme weather risks.

- **Technical Objective 1:** Continuously assess scientific methods, remote sensing technologies, and other computational approaches (including AI) that can be used to identify, monitor, and track climate change-driven effects (e.g., wildfires, permafrost melt, extreme heat, invasive species, and pathogens).

- **Technical Objective 2:** Advance computational capabilities to quickly identify and tentatively characterize large-scale changes coupled to human-environmental systems. This includes furthering approaches to in situ, aerial, and space-based observation and detection.

- **Technical Objective 3:** Identify opportunities to develop capabilities for high-sensitivity and high-specificity real-time detection and monitoring of climate impacts in harsh operating environments (e.g., Arctic).

Focus Area 3: Disaster Adaptation and Resilience Capabilities – DHS must support homeland resiliency by identifying, leveraging, and developing capabilities for enhanced adaptation to and resilience from disasters.

- **Technical Objective 1:** Continuously assess Earth system science to understand the interplay between geophysical and anthropogenic forcing and model transition waypoint, recognizing a need for adaptive management strategies to address future unknowns.

- **Technical Objective 2:** Advance computational capabilities to optimize climate change investments, translate the benefits into policies and incentives, and measure the effectiveness of these climate interventions.

- **Technical Objective 3:** Develop capabilities to model upsides, downsides, potential barriers and/or, reaction of society or regulators to new public policy or technology solutions for climate change and gamify climate now- and future-casting.

EMERGING COMPUTING PARADIGMS

The Von Neumann architecture implemented on a silicon chip is the engine of the present-day information technology revolution. It is the basis for exploring derivatives, such as parallel and distributed computing, and continues to produce significant capability in the conventional computing space. While the U.S. continues to invest in and advance digital computing, trends suggest that current technology is expected to fall short of meeting requirements of future computing needs. Big data centric applications, like simulation and AI, demand improved performance, and the need for them is growing at the same time as Moore's Law is breaking down in silicon-based computing. Data heavy applications like extreme sensor data streams and embedded Internet of Things (IoT) require low energy consumption and efficiency in computationally intensive algorithms. The needs of these kinds of innovations are increasingly mismatched to current forms of general-purpose chips, which suffer from memory bandwidth due to the physical separation between processing and memory units.

MISSION IMPACTS:
Increase data processing speed for faster, real-time analysis and decision making

There are, however, a number of emerging computing architecture platforms (e.g., quantum, neuromorphic, optical, etc.) on the horizon, better aligned with emerging application needs, that have the potential to significantly accelerate performance, efficiency, cost, while reducing power consumption. These next-generation computing paradigms are deserving of our vigilant attention.

Most AI applications run in a Cloud. The learning phase, for which large datasets are necessary, is done in the Cloud, and inference tasks are performed on the same assets. Given the increasing demand for intelligent devices, such a scheme is not sustainable in the long run. The data centers will not be able to sustain the load and part of that load will need to be allocated to the edge devices themselves. This is the current challenge that research teams are taking on: to enable running inference tasks at the edge, thanks to dedicated hardware accelerators. However, having accelerators dedicated to inference tasks at the edge is only the first step. The future challenge will be to perform the learning phase locally as well. This will require advances in performance, efficiency, cost and power consumption, only envisioned available in next-generation computing architectures and technologies.

EMERGING COMPUTING PARADIGMS

The need to improve current-generation conventional computing paradigms while preparing for next-generation computing paradigms, provides two classes of research activities under the *Emerging Computing Paradigms* topic:

(1) Engineering and architectural analysis of specialized digital computing derivatives (e.g., parallel, distributed, edge, etc.) and special purpose chips (e.g., AI accelerators, graphics processing units, tensor processing units, etc.).

(2) Understanding the likely trajectory of relevant hardware and software technologies in next generation computing paradigms (e.g., quantum, neuromorphic, extreme parallelism, etc.), as well as preparing for experiments with these technologies.

Emerging Computing Paradigms Focus Areas and Technical Objectives:

Focus Area 1: Ubiquitous Computing – This focus area aims to enable tasks with aggressive performance requirements (e.g., simulation, AI, real-time control systems, etc.) to be performed anywhere – in the cloud, locally (on Prem), or at the operational edge. We also aim to understand computing architectures and supercomputing advances that will enable DHS to leverage data for enhanced real-time decision making.

- **Technical Objective 1:** Identify key research challenges for DHS missions using multiple networked devices on multi-cloud, inter-cloud, edge, supercomputing, and visualization of capabilities and multi-modal interfaces.

- **Technical Objective 2:** Identify key research challenges for scaling data-driven applications deployed in a distributed networked environment and that require efficient compute over high loads of streaming data, some of which may belong to different parties.

- **Technical Objective 3:** Understand how DHS use cases centered on “Big Compute” may be further enhanced by next-generation computing capabilities, such as leading-edge industry AI accelerator chip capabilities.

EMERGING COMPUTING PARADIGMS

Focus Area 2: Next-generation Computing Capabilities – This focus area aims to examine developments in post-Moore computing and potential applications for DHS use cases.

- **Technical Objective 1:** Demonstrate a quantum[-inspired] use case on commercial capabilities (e.g., Azure, D-Wave). For example, investigate optimization using quantum computers for DHS specific problems such as simulation, searching, or AI.
- **Technical Objective 2:** Understand the scope and magnitude of long-term threats that may emerge if large-scale quantum computing or neuromorphic computing are fully realized and, in particular, monitor post-quantum encryption advances.
- **Technical Objective 3:** Investigate the state of neuromorphic technology, articulate the challenges and opportunities in major areas of neuromorphic technology (e.g., materials, devices, neuromorphic circuits, neuromorphic algorithms, and applications), and project the potential dual-use capabilities/threats of combining quantum and neuromorphic computing.

NOVEL MATERIALS AND SECURE MANUFACTURING

The future impacts of novel materials and manufacturing are quickly gaining interest in the United States and abroad due to the projected impact of these areas on innovation and the ability to adapt technologies at an accelerated pace. Advanced materials are artificial materials with unique and novel properties of interest, and advanced manufacturing is the use of innovative technologies and methodologies for improved competitiveness in the manufacturing sectors.[39] Advanced manufacturing is comprised of techniques that can produce highly customized products at lower cost, greater efficiency, and less waste, which holds the promise to have broad-reaching impacts to lowering cost and availability of technologies for DHS use. S&T is interested in harnessing the potential of advanced materials that could help drive down cost and improve suitability of these materials for use in DHS operational environments. As advances are discovered, applying these to DHS mission spaces will be vital to providing improved capability to screen, interdict, and protect against threats.

MISSION IMPACTS:
Identify new security concerns from novel materials; develop self-healing materials to increase resilience to disasters

Novel materials and advanced manufacturing capabilities, however, can create new threats, such as 3-D printed weapons and new attack vectors like backdoor entry points in embedded electronics.[40] Other forces, such as limited supply chains can also impact the threat space. The microelectronics or the semiconductor-based integrated circuit safety and supply chain has garnered much national attention in the last decade. This is due to the migration of the manufacturing base from the United States to other countries along with the uptick in malicious actors threatening to cause havoc on U.S. infrastructure. A recent Executive Order 14017 on "America's Supply Chains"[41] assigns DHS the responsibility of building resilient supply chains and securing microelectronics while combatting trafficking in counterfeit, fake, and maliciously affected chips and preventing their entrance into the country.[42]

Novel materials and advanced manufacturing have the potential to reduce cost and provide enhanced capabilities and benefits, such as self-healing materials and 3-D printed critical parts across multiple DHS mission spaces. At the same time, these advances in materials and manufacturing can also pose new threats or attack vectors. A report from the Homeland Security Advisory Council indicates that future advancements in 3-D printing

[39] Reding, D.F. and Eaton, J. NATO Science & Technology Organization. 2020. Science & Technology Trends 2020-2040 – Exploring the S&T Edge. p. 104. <https://www.sto.nato.int/publications/Management%20Reports/2020_TTR_Public_release_final.pdf>

[40] Department of Homeland Security Homeland Security Advisory Council. 2020. "Final Report of the Emerging Technologies Subcommittee: 3D-Printing." <https://www.dhs.gov/sites/default/files/publications/final_report_hsac_emerging_technology_subcommittee_3dprinting_508_compliant.pdf>

[41] Executive Office of the President. 2021. E.O. 14017 – America's Supply Chains. <https://www.federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chains>

[42] U.S. federal statute enacted by the 117th U.S. Congress – <https://democrats-science.house.gov/chipsandscienceact>

NOVEL MATERIALS AND SECURE MANUFACTURING

can pose a threat to the security of the U.S. in the next three to 10 years[43] across multiple different domains such as embedded electronics, safety critical parts, and biological tissue engineering. These advances can pose challenges to DHS mission spaces due to the potential ease of sabotaging critical parts, concealing illicit objects, creating untraceable weapons, spoofing biometrics, etc.

Novel Materials and Secure Manufacturing Focus Areas and Technical Objectives:

Focus Area 1: Novel Materials Applications – This focus area aims to adapt to understand and assess application of novel materials in multiple DHS mission spaces.

- **Technical Objective 1:** Develop use-case scenarios to help further explore the application of novel materials within DHS mission spaces. For example, self-healing materials have multiple, potential applications in the DHS mission space for blast mitigation and recovery, fire, and water resistance, etc.
- **Technical Objective 2:** Identify, track, and assess the development and applicability of "smart" materials for use in homeland security environments to meet the need for cost-effective, multi-use materials. Examples are materials that could be components of wearable sensors to monitor the health and safety of DHS personnel.
- **Technical Objective 3:** Identify areas of security concern and consequences from novel materials to homeland security missions with a focus on strategic hazards and threat vectors, such as easier dispersion of threats such as a chemical, biological, radiological, nuclear, and explosive, or CBRNE, agent.

Focus Area 2: Advanced Manufacturing Security and Threats – As manufacturing technologies evolve, we must understand the security impacts to both supply chains and the goods that are used by the American people, as well as the potential ways these processes can be misused.

- **Technical Objective 1:** Assess the threats, potential unintended consequences, and impact of 3-D printing on security and DHS missions. Three-dimensional printing has advanced to a stage where objects can be printed directly from a wide variety of materials, including materials used for explosives, making it more complex to fully characterize the integrity of, or discern them from commodity products.
- **Technical Objective 2:** Identify approaches to detect, mitigate and prevent the threat of semiconductor-based integrated circuit safety and the supply chain. The continuous emergence of new vulnerabilities in microelectronics design, fabrication, test, and lifecycle necessitates innovative research into technologies that will efficiently detect these vulnerabilities, provide end-to-end lifecycle assurance and authentication, and improve supply chain resiliency.

[43] Department of Homeland Security Homeland Security Advisory Council. 2020. "Final Report of the Emerging Technologies Subcommittee: 3D-Printing." p. 11. <https://www.dhs.gov/sites/default/files/publications/final_report_hsac_emerging_technology_subcommittee_3d-printing_508_compliant.pdf>

SOCIAL SCIENCES

Developing a scientific understanding of how individuals, small groups, and organizations affect threats, prevention, deterrence, resilience, security, and recovery activities related to the homeland security mission is a massive but vitally important undertaking. Social sciences focus on the root causes of behavior at individual, organizational, and institutional levels and represent numerous fields including sociology, economics, psychology, criminology, or political science to name a few. Many of the challenges faced by DHS are not easily or appropriately solved by technology, or, at least not discoverable by the implementation of technology. Social sciences share an analytic focus on the behavior, attitudes, beliefs, and practices of people and their organizations, communities, and institutions. Social scientists employ the scientific method using mixed research approaches based on systematic use of evidence to enable better understanding of the motivations, actions, and potential risks or threats posed by individuals, institutional or group actors. Finally, by examining past successes and failures of DHS mission related programs, policies, actions, or decisions, social and behavioral scientists can systematically determine what led to these results and how they can be replicated, avoided, or improved.

MISSION IMPACTS:
Gain understanding of motivations behind human-based threats; enable the acceptance of new technologies into DHS missions

Social sciences are important to DHS – we must understand the nature of threats and risks, as well as how the Department's responses to these threats and risks can be most effective. In this area, combatting terrorism, human trafficking, child exploitation, and targeted violence, and helping to build a fair, orderly, and humane immigration system, are among the Department's priority missions and an integral part of S&T Tech Centers' work in social sciences.

To enable mission success, we must build knowledge and deepen our understanding of the unique human, social, societal, and behavioral drivers of these unique crimes, risks, and threats. To uncover the nature, causes, and correlation of these issues also enhances DHS mission capabilities and leads to more informed and successful methods, processes, policies, etc. to combat and prevent crimes and threats to the United States.

Additionally, understanding individual and organizational decisions that explain responses to these threats is equally important. Whether technologies are accepted and adopted by public workforces is critical for successful integration of technology into our missions and those of other federal, state, and local government organizations. Private industry has used behavioral economics, particularly in manufacturing, to study this problem for many years, but no body of knowledge has previously attempted to address this problem in the public sector. Finally, measuring the effectiveness of mitigating threats through systematic evaluation and evidence is vital to the future success of DHS responses and activities.

Understanding and mapping the causes and consequences of social structures and processes is critical, as is understanding the continuously evolving social landscapes and their implications on DHS missions. Using these insights to produce the

knowledge and tools necessary will enable the Department to help manage risk, find remedies for ills, and prepare for change in future. These challenges not only necessitate complex, interdisciplinary efforts, but they also require the specialized techniques and knowledge that social sciences bring to bear on issues of this scale.

Additionally, as technical, societal, and geopolitical landscapes continue to evolve and reshape our world, understanding the human reactions/responses/aspects and the social and societal implications of these changes will enable us to be better prepared and provide evidence to inform policy and strategy decision-makers on a host of issues whether it is for our workforce, the integration of technology advances in our missions, or the responses to new or emerging threats.

Social Sciences Focus Areas and Technical Objectives:

Focus Area 1: Motivations and Drivers – This focus area aims to increase our understanding of the underlying motivations and drivers of specific human-centric DHS missions and produce the knowledge, fundamental understanding, and tools necessary to manage risk, find remedies for ills, and prepare for change in the future of DHS missions.

- **Technical Objective 1:** Analyze, describe, and explain continuously evolving human-centric threat landscapes and their implications on DHS missions, and map the causes and consequences of social structures and processes. Homeland security challenges require specialized techniques and knowledge such as knowledge on “ultra-rare” events where occurrences are too low to employ traditional statistical techniques as applied to strategic communication or terrorism events.

- **Technical Objective 2:** Uncover and explain the motivations underpinning key DHS mission areas and solutions. Human behavior and social phenomena are central to DHS missions such as terrorism and targeted violence, human trafficking, cybersecurity incidents, or illegal immigration.

- **Technical Objective 3:** Investigate and develop new social science methods, data, and analysis techniques that allow DHS to describe and examine mission area problems consistently, quantitatively, and objectively. This allows DHS to systematically address problems, determine cause and effect, and understand emerging themes and threats in detail while creating conditions for future scientific inquiry and growth of a broader homeland security corpus of knowledge that is transparent and based in empirical data.

SOCIAL SCIENCES

Focus Area 2: Changing Behavioral and Social Implications – This focus area aims to improve our awareness and understanding of how changes in the technology landscape (particularly as science and technology continues to evolve) impact social interactions, behaviors, and threat vectors.

- **Technical Objective 1:** Describe the digital landscape of environments/ platforms of social engagement, to include evolving technologies and ecosystems around social media, metaverse / gamification / immersive technologies.
- **Technical Objective 2:** Identify and analyze how potential changes in human behavior and the confluence of social change across physical and cyber space (i.e., changes in human behavior when one is online, online in a group, anonymous, etc.) may exacerbate existing and create new threat vectors, as well as the potential impacts to DHS missions.
- **Technical Objective 3:** Ascertain the differences in early warning signs/ indicators given these environments/platforms and social interfaces and identify DHS capabilities to address current and emerging threats and risks.

Focus Area 3: Technology Acceptance and Limitations – This focus area aims to advance the acceptance of new technologies into DHS missions.

- **Technical Objective 1:** Understand why and how the public, organizations, and workforces, including government programs, accept or reject new technology.
- **Technical Objective 2:** Identify ways humans best utilize new technologies, including how they interact with digital interfaces, and create methods for incorporating lessons learned into DHS operations.

APPENDIX A: PRIORITIES AND FOCUS AREAS

Advanced Sensing

- Signature Exploitation and Detection
- Sensor Integration
- Emerging Sensing Technologies

Artificial Intelligence (AI) & Autonomous Systems (AS)

- Trustworthy AI/AS
- Adversarial AI
- Advanced Applications of AI/AS

Biotechnology

- Worldwide Developments in Biotechnology
- Existing and Emerging Biological Agent Detection

Communications & Cyber Resiliency

- Data-Centric Security
- Software and Hardware Assurance
- Communications and Network Resiliency

Data, Modeling, and Simulation Sciences

- Advanced Data Analytics Capabilities
- Advanced Modeling and Simulation Capabilities
- Combined Data Analytics and Simulation Capabilities
- Data Ecosystem

APPENDIX A: PRIORITIES AND FOCUS AREAS

Digital Identity & Trust

- Digital Identity
- Privacy Enhancing Technologies
- Trust and Safety

Earth Systems Sciences

- Worldwide Developments in Earth System Science and Climate Innovations
- Earth System Monitoring and Detection Capabilities
- Disaster Adaptation and Resilience Capabilities

Emerging Computing Paradigms

- Ubiquitous Computing
- Next-Generation Computing Capabilities

Novel Materials & Secure Manufacturing

- Novel Materials Applications
- Advanced Manufacturing Security and Threats

Social Sciences

- Motivations and Drivers
- Changing Behavior and Social Implications
- Technology Acceptance & Limitations

APPENDIX B: ACRONYM LIST

5G = Fifth-generation Technology
6G = Sixth-generation Technology
AI = Artificial Intelligence
AR = Augmented Reality
AS = Autonomous Systems
CBP = Customs and Border Protection
CBRNE = Chemical, Biological, Radiological, Nuclear and Explosives
CHIPS Act = Creating Helpful Incentives to Produce Semiconductors for America Act
CPS = Cyber Physical Systems
C-UAS = Counter-Unmanned Aircraft System
DHS = Department of Homeland Security
DL = Deep Learning
DNA = Deoxyribonucleic Acid
EO = Executive Order
ESS = Earth Systems Science
HF = High Frequency
HPC = High Performance Computing
HSE = Homeland Security Enterprise
IaC/PL = Infrastructure as Code/Pilot Light
ICAM = Identity, Credential, and Access Management
I/O = Input-output Requirements
IoT = Internet of Things
ML = Machine Learning
NATO = North Atlantic Treaty Organization
OMB = Office of Management and Budget
OSTP = Office of Science and Technology Policy
OT = Operational Technologies
PCR = Polymerase Chain Reaction
PLEO = Proliferated Low Earth Orbit Satellite
QIS = Quantum Information Science
R&D = Research and Development
RNA = Ribonucleic Acid
S&T = Science and Technology Directorate
SBOM = Software Bill of Materials
SME = Subject Matter Expert
SOAR = Security Orchestration and Automated Response
TCD = Technology Centers Division
TRL = Technology Readiness Level
TSA = Transportation Security Administration
UAS = Unmanned Aircraft System
VR = Virtual Reality
V2X = Vehicle-to-Everything
XAI = Explainable Artificial Intelligence
XG = Next-Generation Technologies: 6G, 7G, etc.
XR = Cross Reality