



Addressing **global security challenges** in partnership with **defense, security** and **diplomacy communities**





Last year’s National Defense Strategy and National Security Strategy stress that the United States must lead the development of critical and emerging technologies to advance national security and international stability.

Through the Global Security Initiative, Arizona State University is **helping advance transformational capabilities** in key technology areas, from more effective and team-focused AI to new approaches for combating disinformation and misinformation. As technology is only as good as the people who wield it, GSI **creates novel training platforms and tools** to help develop the technically skilled, adaptive workforce needed to meet defense, security and intelligence mission needs. At GSI, our focus is a **more prosperous, secure and resilient world for all.**"

Nadya Bliss

*Executive director,
ASU Global Security Initiative*

How universities can support the National Defense Strategy [↗](#)

01	Tomorrow’s teammates	2
	Redefining how humans and robots work together	4
	Empowering the U.S. Space Force	6
02	Securing the cyber frontier	8
	Creating the future cybersecurity workforce	10
	HARDENing against cyber attacks	12
03	Cutting through the clutter	14
	New faculty boosts mathematical and analytic capacity at NDSI	16
	Countering covert influence in the Indo-Pacific region	18
04	Security problem solving	20
	Critical thinking: imagining defenses to cyberattacks on U.S. infrastructure	22
	Shoring up homeland security	24
05	STEM education for national security	26
	Bringing today’s science to tomorrow’s scientists	28
	Developing AI and machine learning literacy in the military	29
	Hands-on Homeland Security experience for undergrads	30
06	Today’s challenges, tomorrow’s advancements	31
	By the numbers	36

01 Tomorrow's teammates





“
Artificial intelligence, embodied as a robot, a vehicle, or an unembodied agent like ChatGPT, is proliferating and advancing at a rapid pace.

Researchers at the Center for Human, Artificial Intelligence, and Robot Teaming (CHART) are leveraging the science of teaming to determine how we can make this new technology human-centered and best incorporate it into our work, play, education and daily lives.”

Nancy Cooke
Director of CHART

Redefining how humans and robots work together



Take a virtual tour of the GHOST Lab



The GHOST Lab sound installation.

Meet the robots in the CHART Lab.



A tour of the GHOST lab.

The future of space exploration rests on successful partnership between humans and intelligent machines.

Robots are built to accomplish things that would be impossible, dangerous or costly for humans to do. For example, they can survive in space for many years without a return trip and withstand harsh conditions that people cannot, like extreme temperatures or high radiation.

Researchers at a new Arizona State University testbed are helping people, robots and artificial intelligence collaborate more safely and effectively. At ASU's General Human Operation of Systems as Teams (GHOST) Lab, researchers examine people's ability to work with robots and AI in scenarios such as a life-threatening meteor strike on a lunar colony.



YuMi: a robot that can skillfully manipulate objects

[See the robots team up ▶](#)

The Center for Human, Artificial Intelligence, and Robot Teaming (CHART) is a **multidisciplinary center leading the charge to develop methods to assemble the most effective human-synthetic agent teams in support of national security.**

\$13M+
active research portfolio

60+
student and staff
researchers

50+
affiliated faculty

The project is led by Nancy Cooke, director of GSI's Center for Human, Artificial Intelligence, and Robot Teaming (CHART) and professor of human systems engineering at ASU's Polytechnic School. A cognitive psychologist by training, she has spent years working to understand human teamwork and decision-making. She now applies this expertise to human-technology teams, including ones collaborating on space missions.

Her research received funding from the Defense University Research Instrumentation Program, which allowed her to purchase members of a robotic dream team.

First there's Husky, the size of a small dorm refrigerator on wheels, which can explore a two-mile radius under any type of weather or terrain conditions and bring back data. Then there's Fetch, a type of robot that's a hit at Amazon

distribution centers because of its ability to lift heavy objects high in the air and retrieve items off top shelves. YuMi, a stationary robot that's small in stature — about 2 feet tall — has sizable manipulation skills, such as building things out of LEGO. There's also a collection of swarm robots that are ideal for search and rescue missions.

CHART was also awarded an Air Force Office of Scientific Research seedling grant to conduct research at the GHOST Lab associated with Space Force, the space service branch of the U.S. Armed Forces.

Though the scenarios studied by CHART at the GHOST Lab represent what we might see in the future, today it's clear that our AI and robot partners will play a vital role in the exploration of new frontiers beyond the Earth.

Empowering the US Space Force

In June 2022, the U.S. Space Force and Arizona State University signed an agreement making ASU the newest member of the service's University Partnership Program.

GSI's experience with defense research will be instrumental in creating future programs with the USSF.

Center for Human, Artificial Intelligence, and Robot Teaming (CHART) is conducting research to benefit the Space Force. Ongoing projects include a multidisciplinary space, artificial intelligence and human systems engineering group that is exploring multiteam

systems in space operations. The project makes use of existing unmanned aerial vehicle testbeds and the General Human Operation of Systems as Teams (GHOST) Lab at ASU, as well as a custom radio system with built-in latencies to model distributed space operations of human-machine teams. The project's distributed teams represent NASA Johnson Space Center, the Jet Propulsion Laboratory, the International Space Station as well as orbital and surface-based instruments on Mars and the moon. One goal of the project is to use artificial intelligence to oversee the distributed system and alert NASA if there are communication breakdowns or other issues.



“

ASU is a leader in exploring the universe, from planets to asteroids and from the Milky Way to the most distant galaxies.

We are excited to work with Space Force to continue on this path toward discovery and insight.”

Michael M. Crow
President of ASU

Learn more
about CHART [↗](#)



02 Securing the cyber frontier



“

We are engaging and developing cybersecurity talent, and really instilling a passion for cybersecurity.

At the Center for Cybersecurity and Trusted Foundations (CTF), we have positioned ASU as the place to go, both physically and digitally, to research, develop and learn about cybersecurity.”

Yan Shoshitaishvili
Acting director of CTF

Creating the future cybersecurity workforce

Cyberspace was once a place that seemed far removed from everyday lives — an abstract world or an online realm we logged into.

Fast forward to today and the world lives in cyberspace — from light bulbs and locks in our homes to our cars and cellphones. Just as we need people to maintain the security of the physical spaces where we live, we also need humans to maintain the

security of cyberspace. While cybersecurity is critical to national security, the demand for professionals in the field exceeds the supply. Between 2013 and 2021, the number of unfilled cybersecurity jobs around the world grew 350%, according to Cybersecurity Ventures.

What are the forces in play that are preventing organizations from preparing cyber professionals to fill the gaps?

Filling the cybersecurity expertise gap

“As our society embraces the digital world more and more, we need more cybersecurity professionals. It is difficult to train them because they operate on a much deeper level than what is necessary for a software engineer,” says Yan Shoshitaishvili, acting director of the Center for Cybersecurity and Trusted Foundations (CTF). He is also an assistant professor in the School of Computing and Augmented Intelligence (SCAI) in the Ira A. Fulton Schools of Engineering.

“The problem is that trillions of dollars flow across computers every day, as we have integrated them into every portion of our lives,” says Erik Trickel, a computer science doctoral student in SCAI, and a CTF affiliate. “Whether through ransomware, malware or hacking into servers, companies have to hire people who can also protect themselves. Although the gap continues to grow, I feel that we are taking appropriate steps to stem the tide.”

Expanding the reach of ASU's cybersecurity training

“The faculty at ASU spent a lot of time brainstorming how cybersecurity education should be done at scale, and we came up with this model which the university now provides as an open-source service to the world,” Shoshitaishvili says.

This open-to-the-world platform is pwn.college, preparing the next generation of cybersecurity experts with the moves to thwart cyberattacks.

“Pwn.college comes at it from the hacker's perspective,” says Jamie Winterton, director of strategy at ASU's Global Security Initiative. “To defend networks, it's really essential to know how people think and what they may be doing offensively to your network. It's impossible to do without that hands-on skill. You can play better defense when you know the offense.”



ASU's hands-on approach to cybersecurity education

"We are engaging and developing cybersecurity talent, and really instilling a passion for cybersecurity at the high school level," Shoshitaishvili says. "At the undergraduate level, we have students participating in hacking conventions across the world at events such as DEF CON. We have positioned ASU as the place to go, both physically and digitally, to research, develop and learn about cybersecurity."

Support from the U.S. Department of Defense allowed CTF to develop the practice-based cybersecurity education platform that teaches the world critical security concepts. By learning these concepts, students gain a strong foundation in cybersecurity.

The Center for Cybersecurity and Trusted Foundations (CTF) focuses on the **cybersecurity pipeline, providing opportunities for learners across ages and skill levels.**

\$40 million+
received in award obligations

50+
published research papers

30+
affiliated faculty



HARDENing against cyber attacks

Hackers frequently search computing systems for design features that can inadvertently allow unauthorized access or operation.

Often unrelated and harmless on their own, such features can be abused by attackers and unwittingly add up to an unexpected or emergent execution engine able to run attackers' exploits.

Defending against such attacks and identifying these flaws before they're exploited is a priority of the Defense Advanced Research Projects Agency, and researchers with GSI's Center for Cybersecurity and Trusted Foundations (CTF) have been enlisted to help.

Armed with a \$3.7 million award, CTF researchers are working on automatically identifying and fixing emergent execution behaviors in software systems as part of DARPA's Hardening Development Toolchains Against Emergent Execution Engines (HARDEN) program. The principal investigator on the project is CTF Director Adam Doupé, an associate professor in the School of Computing and Augmented Intelligence.

**Learn more
about CTF** [↗](#)



“

With so much of our lives taking place online, cybersecurity is everyone’s concern.”

Sally C. Morton
Executive vice president of Knowledge Enterprise at ASU

The CTF team aims to create a common language that describes a system’s capabilities that are relevant to emergent execution behaviors. Using this language, along with automated reasoning techniques, the goal is to identify these design issues so that they can be addressed and neutralized, securing the system for its intended use.

The exploitable design features in computing systems offer considerable advantages to cyber attacks, presenting a pressing concern.

“HARDEN aims to deny these advantages, by combining ethical hackers’ growing understanding of how attackers turn parts of modern computing systems against the whole with the pioneering formal methods and automated software analysis developed with DARPA’s support,” says Sergey Bratus, HARDEN program manager in DARPA’s Information Innovation Office.

03 Cutting through the clutter

A futuristic digital landscape with a man in a suit standing on a glowing path, surrounded by floating windows of various images and data. The background is dark blue with glowing particles and lines. The man is seen from behind, looking at a large window showing a woman and a man working at a computer. Other windows show various scenes like a person on a horse, a person on a boat, and a person on a train. A yellow line starts from the bottom left and curves towards the center.



“

I describe disinformation as primarily a human problem, but one with a substantial technological dimension.

At the Center on Narrative, Disinformation and Strategic Influence (NDSI), we think it is really important that we consider the insights of social scientists and humanities scholars, both of whom have different theories and methods about how to understand the human condition.”

Scott Ruston
Director of NDSI

New faculty boosts mathematical and analytic capacity at NDSI

GSI's Center on Narrative, Disinformation and Strategic Influence (NDSI) conducts **interdisciplinary research that develops tools and insights for decision-makers, policymakers, civil society groups and communities** in order to support holistic defenses against information-related threats to global democracy and the rules-based order.

\$7 million+
in grants awarded or executed since 2018

25+
faculty and research partners across nine ASU schools

One of the biggest problems facing our society today is disinformation, according to Joshua Garland.

Garland joined ASU in 2022 as an associate research professor in GSI's Center on Narrative, Disinformation and Strategic Influence (NDSI), determined to make an impact on the issue.

"We're excited to have Joshua Garland join our growing team," says Scott Ruston, director of the center. "His expertise significantly increases the in-house technical and analytic 'horsepower' of the center as we devise interdisciplinary research programs to better understand the information environment."

Garland came to ASU from the Santa Fe Institute, where he held an Applied Complexity Fellowship. He works to bridge the gap between math theory — which is based on "perfect" conditions — and the messy data of the real world's complex systems, like climate, belief dynamics or the human heart.

"ASU is a place where there's a lot of really interesting people to work with and a lot of interesting research



to do. The agenda at the Global Security Initiative and the Center on Narrative, Disinformation and Strategic Influence in particular was compelling and aligned perfectly with my research interests,” Garland says.

Garland’s proven expertise in complexity and complex systems is an important addition to GSI’s efforts to address the types of interwoven and often mutually reinforcing security issues we see today, like the spread of disinformation, climate change and the public’s deteriorating trust in institutions. In addition to his appointment at GSI, Garland is a faculty member in the School of Complex Adaptive Systems.

His research is centered on discovering effective ways to combat social polarization as well as false narratives. A return to civil discourse, he argues, protects democracy.

“Counterspeech is one of the most promising avenues for fighting disinformation,” Garland says.

Counterspeech is a strategy that uses citizen-generated responses to counter hateful, toxic or dangerous speech or disinformation.

Sometimes people who post and help spread misinformation online do so unintentionally. Garland is interested in finding the best way to engage with such people without bullying or polarizing the conversation more.

“How do we make someone who has been misinformed feel heard, not just censor them, and bring them back to a place where we can talk about the issue?” he asks.



Countering covert influence in the Indo-Pacific region

The use of mis- and disinformation among competing nation states is a strategy as old as nation states themselves, with accounts of influence campaigns stretching back to ancient Rome.

New media in the 21st century has allowed nation state actors to supercharge such campaigns, resulting in sometimes adverse effects on sovereignty and political stability.

Together with in-country experts, researchers at GSI's Center on Narrative, Disinformation and Strategic Influence (NDSI) are working to understand foreign covert influence in the Philippines, Indonesia and

Malaysia. Funded by the Department of Defense through its premiere social science grant program, the Minerva Research Initiative, the project fuses narrative theory and analysis with social-cyber forensics. Led by NDSI Director Scott Ruston, researchers are working to map the information environment in the region, track online influence and understand nation-state generated influence campaigns, their appeal and their calls to action.

In 2022, the team identified suspected coordinated campaigns on YouTube using traditional narrative analysis as well as color-theory based detection that identifies the consistent and persistent use of the same or similar imagery. Disinformation campaign networks on video sharing platforms can be difficult to uncover,



but this technique helps researchers identify potential members of a network through reused propaganda imagery.

The team has also tracked messaging and rumors surrounding the Chinese COVID-19 vaccine Sinovac and the Maritime Silk Road – both key topics in which state-sponsored actors hope to gain influence in the region.

This research is filling the critical capability and knowledge gap the United States faces with regard to adversaries' engagement in "informationized" warfare, and is establishing a broad model for effective analysis of strategic influence in Asia-Pacific, Europe and other regions.

**Learn more
about NDSI** [!\[\]\(e2376d476d06eb31946dc01a69a4403a_img.jpg\)](#)

04 Security problem solving





“
**The Center for
Accelerating
Operational
Efficiency gives
researchers the
opportunity to
engage directly
with homeland
security agencies
such as TSA, CBP
and CISA.**

Our researchers at CAO E create real-world solutions that can be used to provide DHS with dynamic information and predictive tools that can be used to improve homeland security today.”

Ross Maciejewski
Director of CAO E



Critical thinking: imagining defenses to cyberattacks on U.S. infrastructure

In March 2022, the Cybersecurity and Infrastructure Security Agency sounded an alarm: U.S. infrastructure may be vulnerable to Russian cyberattacks.

Threats to our critical infrastructure are nothing new — natural disasters, human-inflicted harm and accidents have challenged our infrastructure countless times. But the continual advancement of new technologies and their integration into infrastructure presents new avenues of attack we must prepare to face.

In an effort to help the United States thwart potential cyberattacks, the Center for Accelerating Operational Efficiency (CAOE), led by GSI, collaborated with the Department of Homeland Security's Science and Technology Directorate in May 2022.

Convening subject matter experts (SMEs) and students from four other university-led DHS Centers of Excellence, CAOE held a hackathon to identify real-life scenarios and develop actionable solutions to current and emerging infrastructure risks and threats.

“As a Center of Excellence, one of our primary missions is to provide cutting-edge educational opportunities to our students, and to encourage them to apply what they learn in the classroom to current events and issues that are impacting homeland security,” says CAOE Director Ross Maciejewski. “In order to do this, we’ve created and implemented a number of programs, one of which is our collaborative annual hackathon, which started in 2019.”

The hackathon oriented around three central problem statements: strategies for detecting, preventing and mitigating a hacked autonomous vehicle, identifying illegal activity on open-source networks while protecting critical infrastructure, and the prevention, detection and response to attacks on digital components of



infrastructure. Hackathon teams planned, developed and presented solutions to each problem statement.

The event drew 73 undergraduate and graduate students from each of the five participating Centers of Excellence and their affiliated universities.

“Each year, our participating students and SMEs continue to level-up in terms of the information that they share with each other, and the one-of-a-kind solutions that they propose to very real and current issues,” says CAOE Education and Workforce Director Anthony Kuhn. “We look to continue this trend and ensure that our future events continue to be better and better.”

The Center for Accelerating Operational Efficiency (CAOE), led by Arizona State University, develops and applies **advanced analytical tools and technologies to enhance planning, information sharing and real-time decision-making in homeland security operations.**

\$16 million+
total research expenditures

150+
students

100+
affiliated research faculty from
50 institutions



Shoring up homeland security

The mission of the Department of Homeland Security is as multifaceted as it is formidable:

Securing the nation's borders and ports of entry, protecting against and responding to natural and man-made disasters, and ensuring economic success and prosperity.

In 2022, Center for Accelerating Operational Efficiency (CAOE) made strides to deliver much needed tools and strategies that better equip the Department of Homeland Security's operational planning, information exchange and decision-making ability.

From storm surge to virus surge

In the aftermath of a hurricane, supply chains may be in disarray, hospitals overcrowded and first responders overworked. Similar problems were observed all over the world during the height of COVID-19.

Recognizing the overlap, a CAOE team used several years of research and development of tools for hurricane response and preparedness and applied it to pandemic response. Working with the University of Texas at Austin, the team created a vaccine access and antiviral logistics

model and in 2022, completed a two-year project. From May 2020 to March 2022, CAOE deployed a staged alert system for COVID-19 in Austin that weighed the city's health care capacity while minimizing closures. The tool used daily COVID-19 hospital admissions to toggle between mitigation stages.

CAOE continues to explore other uses of the research including: applying wastewater monitoring to the staged alert system, and agent-based models to predict disease spread with various levels of mitigation measures as well as to quantify and mitigate disruptions to the food supply chain by accounting for worker absences.



**Learn more
about CAOE** [↗](#)

Privacy a 'PET' project

In an age when our personal data is more valuable than ever, privacy is priceless.

Privacy-enhancing technologies, or PETs, promise to control the sharing and use of sensitive information while minimizing the risk of unauthorized access. Examples include communication anonymizers, synthetic data generators and data encryptors. PETs have been under development for years, but are slowly integrated into operational use.

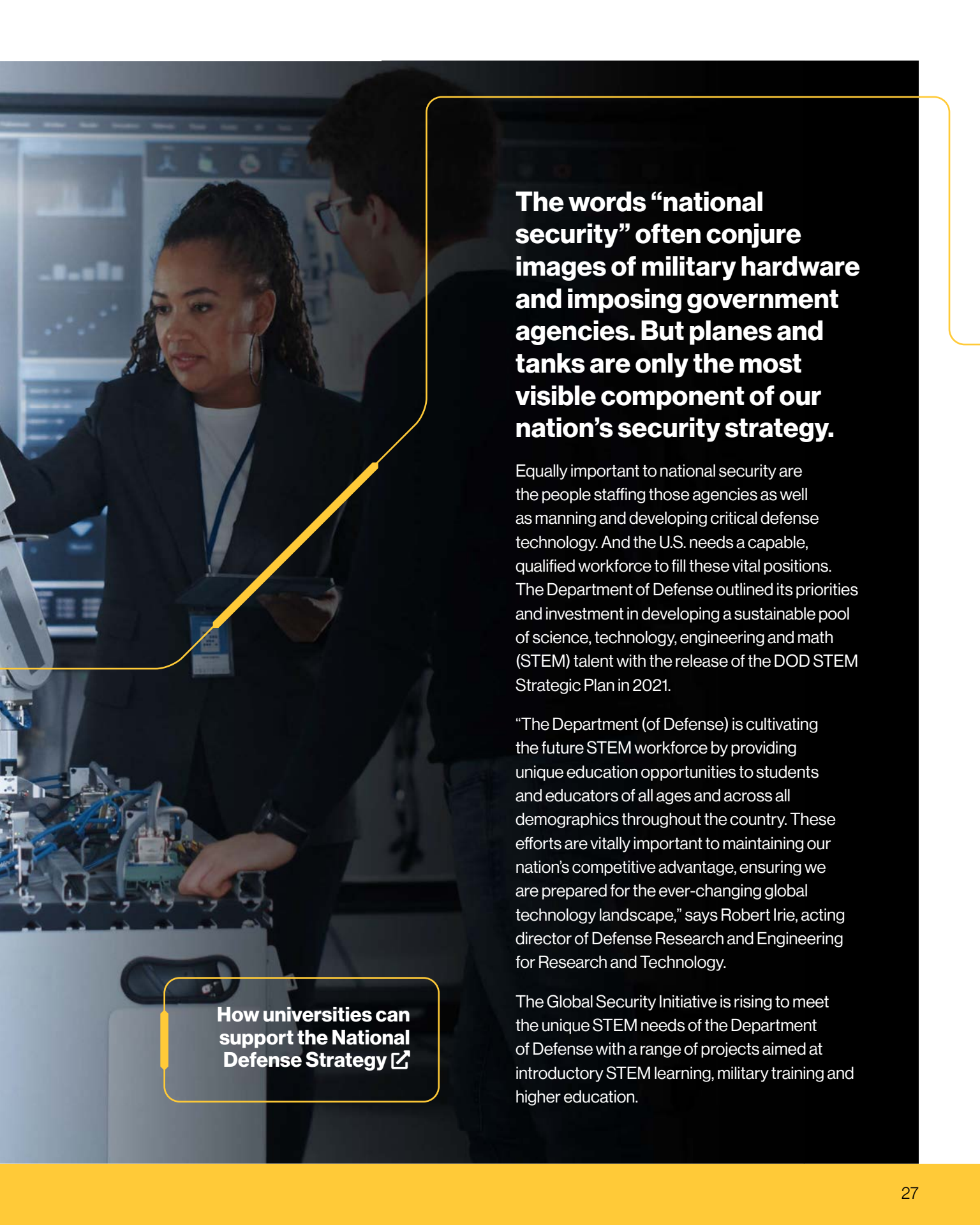
In June 2022, CAOE hosted a daylong workshop with the DHS Privacy Office, convening DHS stakeholders and academics to review real-life case studies related to

PETs. They reviewed pressing needs, such as methods to protect social security numbers and other private information, as well as ways to enhance biometric cybersecurity. Twelve white papers were presented, showcasing new and emerging technologies that could address the needs of DHS and its component agencies.

"I will be encouraging the participants in the workshop to share these case studies with their networks to continue the collaborative process between the researchers and DHS participants," said former DHS Chief Privacy Officer Lynn Parker Dupree following the workshop.

A woman with short blonde hair and glasses, wearing a blue and white plaid shirt, is working in a laboratory or industrial setting. She is focused on a white robotic arm that is part of a larger piece of equipment. The background is filled with various cables and equipment, suggesting a complex technical environment. The overall lighting is dim, with some highlights from the equipment and a computer monitor in the background.

05 STEM education for national security



The words “national security” often conjure images of military hardware and imposing government agencies. But planes and tanks are only the most visible component of our nation’s security strategy.

Equally important to national security are the people staffing those agencies as well as manning and developing critical defense technology. And the U.S. needs a capable, qualified workforce to fill these vital positions. The Department of Defense outlined its priorities and investment in developing a sustainable pool of science, technology, engineering and math (STEM) talent with the release of the DOD STEM Strategic Plan in 2021.

“The Department (of Defense) is cultivating the future STEM workforce by providing unique education opportunities to students and educators of all ages and across all demographics throughout the country. These efforts are vitally important to maintaining our nation’s competitive advantage, ensuring we are prepared for the ever-changing global technology landscape,” says Robert Irie, acting director of Defense Research and Engineering for Research and Technology.

The Global Security Initiative is rising to meet the unique STEM needs of the Department of Defense with a range of projects aimed at introductory STEM learning, military training and higher education.

How universities can support the National Defense Strategy [↗](#)



Bringing today's science to tomorrow's scientists

From rising bread and domesticated dogs to penicillin and rubber, humans have a long history of shaping our world through biotechnology — using biological systems and organisms to improve or create desired products.

With genetically modified crops and new vaccine techniques, biotechnology continues to play a large role today — which is why it is so important to introduce this subject to the next generation of scientists and decision-makers.

Armed with a \$1.4 million National Defense Education Program grant from the U.S. Department of Defense, researchers at Arizona State University and local teachers are doing just that with the BioSense Network. To apply for the grant, project lead Abhishek Singharoy worked with GSI's dedicated proposal team to navigate the DOD's unique application process and craft a competitive proposal.

"The team works with you toward making sure that your milestones are met, so the principal investigator can focus on their part," says Singharoy, an assistant professor in the School of Molecular Sciences. "They essentially guide us through the entire process."

Singharoy developed the backbone of BioSense in his spare time. Visual Molecular Dynamics, or VMD, is a program that taps into ASU's computing power to give students interactive simulations of molecular processes, unlocking the world of biotechnology in classrooms across Arizona.

Over the course of the three-year program, the BioSense Network team will develop six curriculum modules, as well as the technology platform to support the VMD software and training for teachers — all of which will come at zero cost to schools. Each module will have two versions: one for high school and one for middle school.

Singharoy notes that biotechnology is ripe for developing foundational technologies that people can apply to many types of problems — including those related to national security. Exploring the latest science developments now will also help tomorrow's leaders make more informed choices. Additionally, biotechnology classes ask students to solve problems and make decisions in unique ways.

"We're trying to build a decision-making science mind, and that's a skillset that comes in handy when you're making decisions pertaining to national defense," Singharoy says.



Developing AI and machine learning literacy in the military

Any veteran or active duty service member will tell you that training is ongoing. As new technologies make their way onto the battlefield, soldiers need to stay up to date to remain resilient and capable.

In response to this need, the Global Security Initiative helped create artificial intelligence and machine learning training to incorporate into the Warrant Officer Advanced Course at Fort Huachuca, Arizona. The training was developed in collaboration with the U.S. Army Intelligence Center of Excellence (USAICoE) and the Army Research Laboratory and serves as a primer for military intelligence Soldiers on artificial intelligence, machine learning and data science.

“As new technologies like AI are developed and implemented, it’s important that we include the perspectives of multiple stakeholders to make sure our approaches are relevant and solve real-world problems,” says Jamie Winterton, GSI’s senior director of strategy. “Engaging with the Chief Warrant Officers gave us great

insights into how we can effectively teach AI and machine learning to new audiences, and how we can build new AI systems to solve Army problems.

The seminar features a lecture by Chitta Baral, professor in the School of Computing and Augmented Intelligence in the Ira A. Fulton Schools of Engineering and a GSI affiliate. After the lecture, students separated into small practical exercise groups where they worked with data scientists to develop a presentation on an intelligence function that could benefit from artificial intelligence and machine learning.

“Our adversaries are certainly focused on implementing AI in their military,” says Chief Warrant Officer 3 Jonathan Berry, a student from the Utah National Guard’s 142nd Military Intelligence Battalion. “So in order to stay relevant in future conflicts, AI certainly does need to be implemented.”



Hands-on Homeland Security experience for undergrads

Classroom instruction and testing is an important — though incomplete — part of learning. At the end of the day, there's no substitute for experience.

Keeping with that adage, the Center for Accelerating Operational Efficiency (CAOE), led by GSI, hosts an annual hands-on research experience that gives students an opportunity to apply data analytics to real-world scenarios. As a Department of Homeland Security Center of Excellence, CAOE uses actual operational challenges faced by the Transportation Security Administration to inform the content of the

CAOE Summer Experience Quantitative Analytics, or SEQAL. A four-week program, SEQAL began in 2019 — paused due to COVID in 2020 — and returned as a virtual experience in 2021.

In 2022, SEQAL selected 21 students from nine academic partners after a competitive application process. From its inception, SEQAL has placed a focus on minority serving institutions, and 2022 was no different, as six of the nine universities were designated MSIs: Norfolk State University, Tennessee State University, University of Texas Rio Grande Valley,



**Learn more about
STEM education for
national security** [↗](#)

University of Nevada Las Vegas, Universidad de Puerto Rico and Jackson State University.

SEQAL includes both team assignments and lectures on statistics and decision analysis from ASU faculty. Topic areas include: problem solving simulations and data analytics, data visualization and deceptive data, stochastic simulation models and deterministic operations research.

The experience culminates in a design challenge in which students developed and tested a hypothesis on

improving the airport experience. Their plans for data acquisition and analysis were then presented to a panel of judges led by Mohamad Mirghahari, former senior advisor to the chief of staff for the Transportation Security Administration.

Feedback from students on the experience is consistently positive, with many highlighting the importance of applying their classroom knowledge to real-world problems, and the benefit such experience could have on career prospects.



06 Today's challenges, tomorrow's advancements



Today's security challenges often spur tomorrow's scientific advancements. Through service on national committees and boards to interfacing with policymakers, GSI engages in national conversations on the future of critical defense challenges, from securing the microelectronics supply chain to planning for the security impacts of climate change.

Executive Director Nadya Bliss unpacks how ASU is helping realize a positive vision for technology's impact on national security.



National security issues to consider with **microelectronics**

Microelectronics underpin the interconnected, online world we inhabit today. These components are not only integral to our smart devices and appliances, but crucial to military operations and economic sectors like health care.

If any of those were compromised, Nadya Bliss says, the consequences would also impact national security.

“Think of the U.S. Department of Defense’s computer systems, communications systems, transportation systems — they all rely on microelectronic devices to function properly,” says Bliss.

In their final report, the National Security Commission on Artificial Intelligence noted the need to develop a resilient microchip and semiconductor supply chain in the U.S. in order to stay ahead in the geopolitical technology arena.

“Increasing the design and fabrication of these technologies in the U.S. would address a major national security vulnerability — that an adversarial nation could tamper with the technology at some point in the supply chain,” Bliss says.

Though America’s share of the global semiconductor production has fallen from 37% in 1990 to just 12% today, new multibillion dollar manufacturing facilities from Intel and Taiwan Semiconductor Manufacturing Company are under construction in Arizona. As the U.S. works to bring more of this vital industry stateside, ASU and GSI are poised to supply a skilled workforce and cutting-edge research resources.



Climate change isn't just an environmental problem

Both the Department of Defense and the U.S. Intelligence Community recently highlighted the threat climate change poses to national security. At the direction of Congress, the Office of the Director of National Intelligence and the National Academies of Sciences, Engineering, and Medicine have entered into a partnership to establish a Climate Security Roundtable.

The roundtable is composed of experts to provide perspectives and analysis to help the Climate Security Advisory Council leverage the technical expertise and capabilities outside the federal government and

better inform national security assessments. Among the appointees is Nadya Bliss, who finds promise in both the Climate Security Roundtable and ASU's role in it.

"It's really important to take a hopeful perspective, knowing there are ways to move forward that are positive," she says. "I think the National Academies brings the level of rigor, professionalism, expertise and convening power that is needed for this kind of problem. ASU has committed to tangibly improving the world in many dimensions. And anticipating and mitigating national security risks is one of them."



How a trilateral security pact could lead to more effective international collaborations on **technology development**

AUKUS, a trilateral security partnership between Australia, the United Kingdom and the United States, holds great potential for national security research and development.

In an essay for Security & Defence PLuS, Nadya Bliss charted a course for how AUKUS could alter the international research and development landscape and provide a blueprint for allied collaboration on advanced technology in critical national security areas.

“With innovative structures and targeted incentives aimed at overcoming traditional obstacles, AUKUS could demonstrate how joint efforts to develop advanced national security capabilities in areas like cybersecurity, artificial intelligence, quantum computing, and others can not only work, but create better technologies and systems on an accelerated timeline,” Bliss wrote.

Bliss highlights artificial intelligence as a “field of fields,” a dual-use technology that underpins advances in the other areas — creating greater capabilities, but also greater threats.

“Global leadership in AI will be highly influential in determining global leadership in other technological areas,” wrote Bliss.

Bliss outlined a three-pronged strategy that could supercharge this approach: continued investment in the research ecosystem by allied nations, the creation of new joint initiatives that leverage unique alliance strengths and the foundation of an AUKUS lab to accelerate the transition and deployment of new technologies.

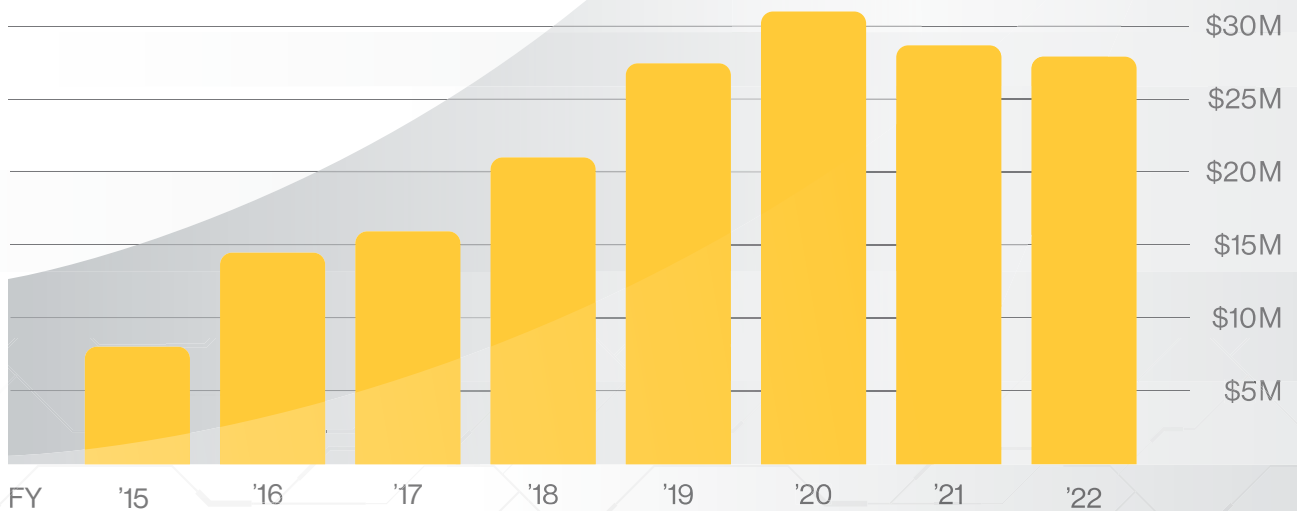
“The creation of AUKUS opens up an opportunity to marry the strengths of three global leaders in research and development,” wrote Bliss. “With some creativity and sustained political support, AUKUS could leverage both member nation and alliance strengths to create something far more impactful than the sum of its individual parts. It could create a blueprint for advancing democratic security interests far beyond the Indo-Pacific region and to the rest of the world.”

By the numbers

GSI both **leads and catalyzes defense and security research** across Arizona State University. Our research expenditures have more than tripled over the last eight years.

\$175M+

total expenditures
since 2015



In fiscal year 2022, GSI worked with more than 140 faculty affiliates across ASU to generate:

\$28M+

total research **expenditures**

78

active sponsored **awards**

65

proposals submitted


ASU Global Security Initiative
Arizona State University

Sign up for the GSI newsletter 



Follow us

 @asu_gsi

 asu-global-security-initiative

 ASU Global Security Initiative

globalsecurity.asu.edu

Global Security Initiative is a unit of ASU Knowledge Enterprise.
Produced by ASU Knowledge Enterprise. ©2023 Arizona Board of Regents.
All rights reserved. GSI year in review 3/2023.