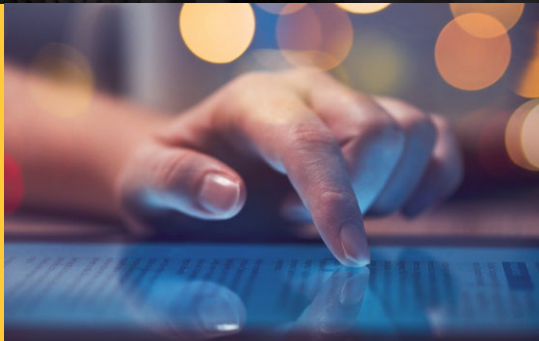


**Addressing global security challenges
in partnership with defense, security and
diplomacy communities**





As society's most important functions — like health care, national and economic security, and political discourse — become increasingly interconnected, it is crucial that our systems are trustworthy and serve the needs of our nation. ASU's Global Security Initiative is a leader in anticipating and addressing complex security challenges through research and education. At ASU, we are striving for a world in which we are safe and secure online; within which augmented intelligence and robotics systems work for the betterment of humanity; and in which we can be confident in the integrity and accuracy of the information we are consuming. ASU could not have a better team leading the charge to create a safe, prosperous and equitable tech-enabled world.”

Sally C. Morton, executive vice president, ASU Knowledge Enterprise

About the Global Security Initiative

GSI's vision is a security and intelligence landscape transformed through interdisciplinary research, education and discovery, in which defense, development and diplomacy operate collaboratively to drive positive outcomes for complex global challenges.



Mission

Catalyze and support Department of Defense, Department of Homeland Security and intelligence community activity across the university. Perform landscape development and provide intellectual leadership for complex global security challenges.

#3 in the nation for DARPA Young Faculty Awards

130+ affiliated faculty

\$30M+ in research expenditures in FY 2021
(funding sources: government, industry and foundations)

About Arizona State University

ASU charter

ASU is a comprehensive public research university, measured not by whom we exclude, but rather by whom we include and how they succeed; advancing research and discovery of public value; and assuming fundamental responsibility for the economic, social, cultural and overall health of the communities it serves.

#1 in the U.S. for innovation
(ASU ahead of Stanford and MIT)

U.S. News & World Report,
7 years, 2016–2022

#1 in the U.S. for transdisciplinary
science research expenditures

National Science Foundation
HERD Survey 2020

#6 in the U.S. for total research
expenditures among universities
without a medical school

National Science Foundation
HERD Survey 2020

Exceptional people. Impactful ideas. Powerful relationships.



Letter from the executive director

The United States is facing a trust deficit, and it is exacerbating pressing national security challenges. Public trust in the institutions that inform us, that craft and execute policy, that drive economic development, and that foster collective action continues to fall, and with it our ability to agree on baseline facts and to come together to tackle big challenges. The consequences are clear — prolonged pandemics, increasingly polarized politics, insufficient efforts to stem a changing climate.

The technological shifts of the last two decades — and the tendency to prioritize capability over security in technological development — have contributed to these challenges. They have changed how we consume and share information, increased the ability of geopolitical rivals to sow confusion and spread disinformation at very little cost, led to a bustling black market for buying and selling personal information, and created an entirely new illegal business sector around ransomware. As a result, people are no longer sure what is worthy of their confidence.

GSI is addressing a component of this trust deficit by re-envisioning how humans interact with technology to improve security. This is a core focus of GSI and a thread that ties all of the research, education and engagement efforts described on the following pages together. The goal is to affect systemwide change in which the inner workings of technology are transparent to its users, including strengths and limitations, and in which newly developed technologies leverage human cognitive strengths to improve performance, defenses and resiliency to attacks.

In the Center for Human, Artificial Intelligence, and Robot Teaming, this is illustrated in efforts to identify how AI-enabled technology can most effectively partner with and complement human strengths. In the Center for Accelerating Operational Efficiency, researchers are designing new tools to help sift through the mounds of data available to decision-makers today to make more informed and timely homeland security decisions. In the Center on Narrative, Disinformation and Strategic Influence, multidisciplinary teams are fusing social science research with computer science expertise to better understand the human and technological factors that shape today's information environment.

With a focus on this type of systemic change, GSI merged its cybersecurity research unit and cybersecurity education unit into a new center — the Center for Cybersecurity and Trusted Foundations. This new center will approach the nation's various cybersecurity challenges holistically, closely coupling its large-scale advanced research portfolio with novel educational tools to help people develop increasingly sophisticated understanding of and engagement with cybersecurity topics.

If you would like to learn more about the Center for Cybersecurity and Trusted Foundations, or any of GSI's other efforts in research, education or engagement, please contact us at gsi@asu.edu.

Sincerely,

A handwritten signature in black ink, appearing to read 'Nadya T. Bliss', written in a fluid, cursive style.

Nadya T. Bliss, PhD
Executive director, Global Security Initiative

Our expertise

The Global Security Initiative leverages the world-class expertise of more than 130 ASU faculty members, who collaborate with GSI leadership, research professors and research scientists to produce solutions, technologies, decision-making tools and novel approaches to address critical security challenges.

Explore our key focus areas:

Cybersecurity 6

Forging powerful new capabilities in cyber reasoning systems through human-machine symbiosis and building the next generation of cybersecurity talent — from deep technical experts to savvy organizational thinkers to cyber-intelligent policy architects.

Narrative, disinformation and strategic influence 8

Combating the use of misinformation and disinformation by malicious actors, and creating systems and tools to help organizations and decision-makers better understand how information is being used by allies and adversaries alike in pursuit of strategic goals and geopolitical influence.

Visualization and analytics 10

Creating tools that clarify and effectively communicate key information, enabling decision-makers to better plan for and respond to changing events, while making judgments that are credible, salient and legitimate.

Human, AI and robot teaming 12

Identifying how best to work with synthetic agents, cultivating effective, ethical teams of humans, artificial intelligence and robots that work together in support of national security, based on lessons from team science and swarm robotics.

Expanding the STEM talent pipeline for national security 14

GSI is arming lifelong learners at all levels — from primary school students to working professionals — with the technical, critical thinking and problem-solving skills necessary to be digitally literate citizens and to thrive in the rapidly shifting technological sector.



Cybersecurity

From data breaches to ransomware groups shutting down national pipelines, there are near-daily headlines about cybersecurity attacks. To help address the long-term cybersecurity challenges facing the nation and the world, GSI has combined two units — the Center for Cybersecurity and Digital Forensics, and the Cybersecurity Education Consortium — into a single organization that will aim to keep users and their data safe by building up and fortifying the fundamental building blocks of security — technology, process and workforce.

The Center for Cybersecurity and Trusted Foundations (CTF) does this by closely coupling the center's large-scale research portfolio with novel, hands-on educational platforms for a pipeline of learners at varying levels of sophistication, alongside entrepreneurial efforts to ensure new cybersecurity techniques are able to transition from the lab into use.

Capabilities:

- Binary exploitation.
- Reverse engineering.
- Machine learning.
- Web/mobile security.
- Dark web market behaviors.
- Competitive hacking.
- Workforce development.
- Cyber education.

Project highlights:

▪ Student research opportunities

CTF is engaging the next generation of the nation's technical workforce, providing hands-on research experience with government and industry on complex challenges. Alongside professors and software engineers, students are gaining advanced skills to continue leading the world in technological development. Through CTF's \$30 million research portfolio, students have the opportunity to develop expertise in binary analysis, automated vulnerability detection, machine learning and social engineering, among other topics.

▪ DEF CON Capture the Flag

CTF concluded its fourth and final year hosting the world's most prestigious ethical hacking competition, DEF CON Capture the Flag. Since 2018, more than 3,000 teams worldwide have participated in 176 innovative cybersecurity challenges developed by CTF professors, graduate students and collaborators. Across the four years, participants clocked 276 hours of active game time by exploring topics such as binary exploitation, machine learning and cryptography. This offered a real-world test of skills that industry, governments and others need to defend against the rising tide of cyberattacks.

"By educating and training a workforce that knows how to be proactive and reactive, we will foster a society that has stronger security built into its structure. Anticipating vulnerabilities before they're exploited by an adversary means that we can problem solve before it becomes a problem."

Adam Doupé, director, Center for Cybersecurity and Trusted Foundations

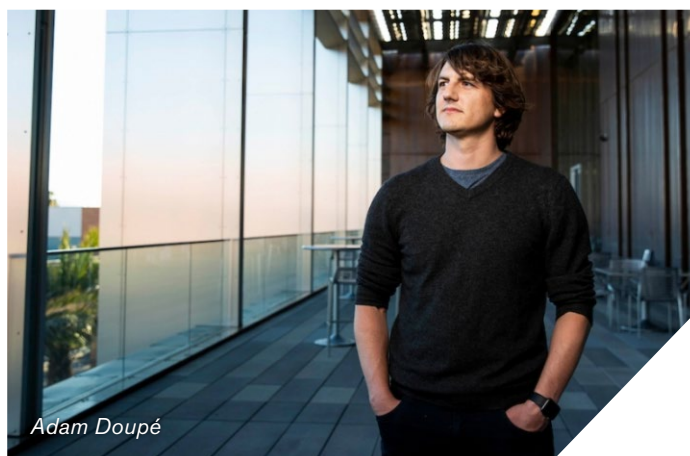


▪ Protecting online retailers

CTF studied how social engineering is used to defraud online retailers through the systemic abuse of return policy loopholes. The research team found that this scam is easy to scale and poses a notable threat to companies, and suggested possible ways to mitigate the threat and protect the retailers. This in-depth study was conducted in collaboration with leading technology companies PayPal and Samsung, as well as partner universities. The team presented their paper "Having Your Cake and Eating It: An Analysis of Concession-Abuse-as-a-Service" at the USENIX Security Symposium.

▪ High school research internships

CTF launched its first summer high school research internship program with five high school students from across the country. They were partnered with graduate student mentors for eight weeks of virtual collaborative research, and each team developed a project that was presented to the center at the end of the summer. Topics included scams in decentralized finance, analyzing hosting provider responses to phishing reports and synchronizing reverse engineering results across binary analysis platforms. The center will be hosting its second high school research internship in summer 2022.



Adam Doupé



Narrative, disinformation and strategic influence

A cascade of recent events has highlighted our dependence on credible information for maintaining social stability. Widespread misinformation hampered a unified, collective action to mitigate the effects of the novel coronavirus. Trust in media, government and other essential functions of democracy are at or near an all-time low. Influence and disinformation campaigns designed to distort the truth, dismay audiences and distract from actual malfeasance have exacerbated political polarization. These surreptitious campaigns also erode faith that anything is knowable and true — a boon to autocrats and a threat to democratic values around the world.

The Center on Narrative, Disinformation and Strategic Influence (NDSI) conducts timely, critical research that fuses the humanities and social sciences with state-of-the-art computer science and modeling in order to develop better insights into how information influences human behavior and geopolitics. The center's approach to research on the information environment acknowledges its complexity, and ultimately, its humanity, to counter and overcome malicious actors and support healthy, resilient, democratic societies.

The center provides evidence-based, mission-relevant insights and tools, benefiting national defense and other stakeholders and their efforts to safeguard the United States, its allies and democratic principles.

Capabilities:

- Narrative analysis.
- Information and influence operations signal detection and analysis.
- Media literacy.
- Disinformation detection.

Project highlights:

▪ **Understanding covert influence**

NDSI is partnering with the Center for Strategic Communication; the School of Historical, Philosophical and Religious Studies; and in-country experts to understand covert influence in the Indo-Pacific region. The project fuses narrative theory and analysis with social-cyber forensics to map the information environment in question and to track online influence. This project aims to understand the covert influence campaigns conducted by nation-state actors, their appeal and their calls to action. So far the team has identified suspected coordinated YouTube campaigns, using traditional narrative analysis as well as color-theory-based detection that identifies the consistent and persistent use of the same or similar b-roll. The team has also tracked messaging and rumors surrounding Sinovac, the Chinese COVID-19 vaccine, and the Maritime Silk Road. This project is funded by the Department of Defense through its premiere social science grant program, Minerva.

▪ **Semantic Information Defender**

The project aims to develop a suite of automated capabilities to detect, attribute and characterize

manipulated media on the internet. The incorporation of narrative and professional media researchers takes this project beyond the technical to better understand the human and business side of the information and media environments to build these detection, attribution and characterization algorithms for real-world employment. NDSI, along with researchers from the Walter Cronkite School of Journalism and Mass Communication and the School of Computing and Augmented Intelligence, is in its second year of supporting a seven-university effort to identify “deep-fake” material. This grant is sponsored by the Defense Advanced Research Projects Agency under the Semantic Forensics program.

▪ **Detecting and tracking adversarial framing**

The team has been developing a technical capability to detect issue framing in varied media sources, distill those frames into an “information operations signal” that can be graphed over time, and correlate that signal and those frames with events in the real world. They are in their final year of an Office of Naval Research-funded effort to detect and track adversarial nation-state framing in mainstream and social media. The center, along with researchers from the School of Computing and Augmented Intelligence, are co-investigators with Steve Corman of the Center for Strategic Communication. This effort improves understanding and prediction of “gray-zone” and hybrid warfare operations, and adversarial preparation of the battlefield to justify and develop support for future hostile actions. The project also seeks to understand how propaganda transitions from known propaganda sources to non-propaganda media.



Scott Ruston in discussion with student

“The future of democratic societies will be shaped by how we approach challenges in the information environment. The power of stories and images on public health, national and international security, and democracy itself, cannot be understated. It’s more important than ever that we step up to the challenge with an interdisciplinary team that can harness the humanities, the social sciences, and technological advancements, particularly within computer science, and fuse them to develop holistic understandings of malign influence and disinformation, and support societal resilience to these malicious actors.”

Scott Ruston, director, Center on Narrative, Disinformation and Strategic Influence



Visualization and analytics

The research, systems and technology developed at the Center for Accelerating Operational Efficiency (CAOE) provide homeland security agencies with real-time information, predictive tools for resource and response planning, and systems that increase the odds of resolving security problems.

The CAO E is a Department of Homeland Security Center of Excellence, one of an extended consortium of universities conducting groundbreaking research to address homeland security challenges. Led by ASU, CAO E develops and applies advanced analytical tools and technologies to enhance planning, information sharing and real-time decision-making in homeland security operations.

Capabilities:

- Data analytics.
- Operations research and systems analysis.
- Economic analysis.
- Homeland security risk sciences.

Project highlights:

- **Predicting cross-border migration patterns**
Human migratory decisions are the result of a complex range of interacting factors, including economic, social and environmental vulnerabilities. Advancing our understanding of why, how and where migration occurs across U.S. borders will help guide both U.S. government border operations and U.S. social-economic policies with countries experiencing surges in migration into the country. The CAOIE is applying machine learning techniques to better understand the drivers of migration in order to inform future policy decisions.

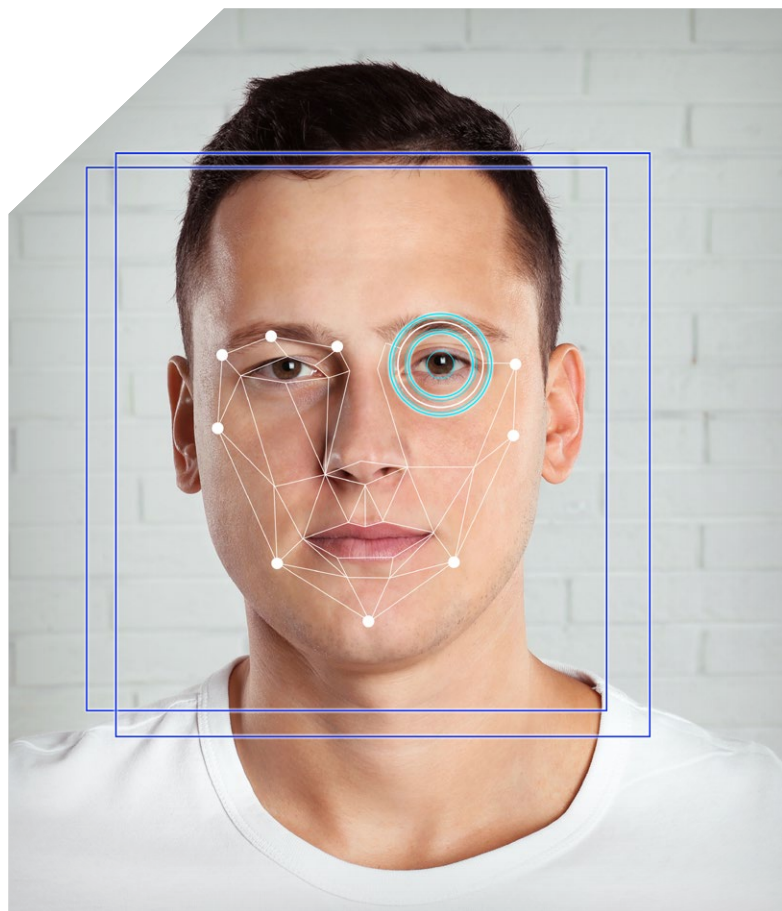


VIDEO:
[Predicting Migration Patterns](#)

- **Expanding airport security working with diverse faculty**
The CAOIE is developing new analytical tools to help planners in the Transportation Security Administration (TSA) maximize efficiency in the passenger check-in processes while simultaneously improving safety and the passenger's experience, with the goal of developing new guidelines for the optimal setup of airport security points under different passenger arrival rate scenarios. A portion of this research project is being conducted as a follow on to the Summer Research Teams Program, an effort by DHS to increase and enhance scientific leadership at Minority Serving Institutions.

▪ Trust in AI-enabled decision support systems

As increasingly autonomous systems enabled by artificial intelligence (AI) are deployed in real-world scenarios, it is critical to understand how trustworthy those systems — and by extension the decisions they make — really are. The CAOIE is testing and validating current instruments used in evaluating the trustworthiness of AI-enabled decision systems that could be used for security tasks like traveler identification. Examples of the technologies being evaluated include facial recognition and natural language processing tools.



"Homeland security challenges are particular in the sense that they tend to appear deceptively simple but in reality they are very complex. What we are trying to do is understand which parameters play more of a role in driving migration and how migration patterns can be manifested."

Anthony Stefanidis, professor of computer science, College of William and Mary



Human, AI and robot teaming

Advances in artificial intelligence and robotics are producing machines that can work alongside humans as teammates. In order to recognize AI's full potential, we must understand how to engineer technology that most effectively teams with humans.

Based on lessons from the science of teamwork, the Center for Human, Artificial Intelligence, and Robot Teaming (CHART) is developing and deploying technologies, tools and best practices to ensure these unconventional teammates complement each other to successfully complete missions. The center develops capabilities, conducts experiments and measures outcomes through human-machine teaming testbeds.

Capabilities:

- Distributed team training with virtual teammates.
- Search and rescue missions.
- Teaming in space operations.
- Collaborative planning.
- Driverless vehicles and human drivers.

Project highlights:

▪ **GHOST Lab**

CHART completed construction on a new lab that functions as both a scientific testbed and an art installation. The General Human Operation of Systems as Teams (GHOST) Lab leverages the capabilities of its Fetch, Husky and YuMi robots, as well as Stacker and TurtleBot3 Burger swarm robots, to gauge humans' trust in and ability to work with robot teammates with various levels of autonomy. The lab also seeks to inspire meditation on historical and philosophical issues surrounding robots, while simultaneously encouraging contemplation about the future of human/robot collaboration.

▪ **Virtual testbeds to mimic real-world scenarios**

Multiple CHART projects for sponsors such as the Defense Advanced Research Projects Agency, Army Research Laboratory and Air Force Office of Scientific Research have been conducting experiments to evaluate and enhance teaming between humans, artificial intelligence (AI) and robots. Researchers worked with human participants in these dynamic environments to collect data, with

goals that include developing a more helpful, socially intelligent AI, and increasing understanding of trust and situational awareness in human/AI/robot teams.

▪ **Improving cybersecurity by understanding the human behind the attack**

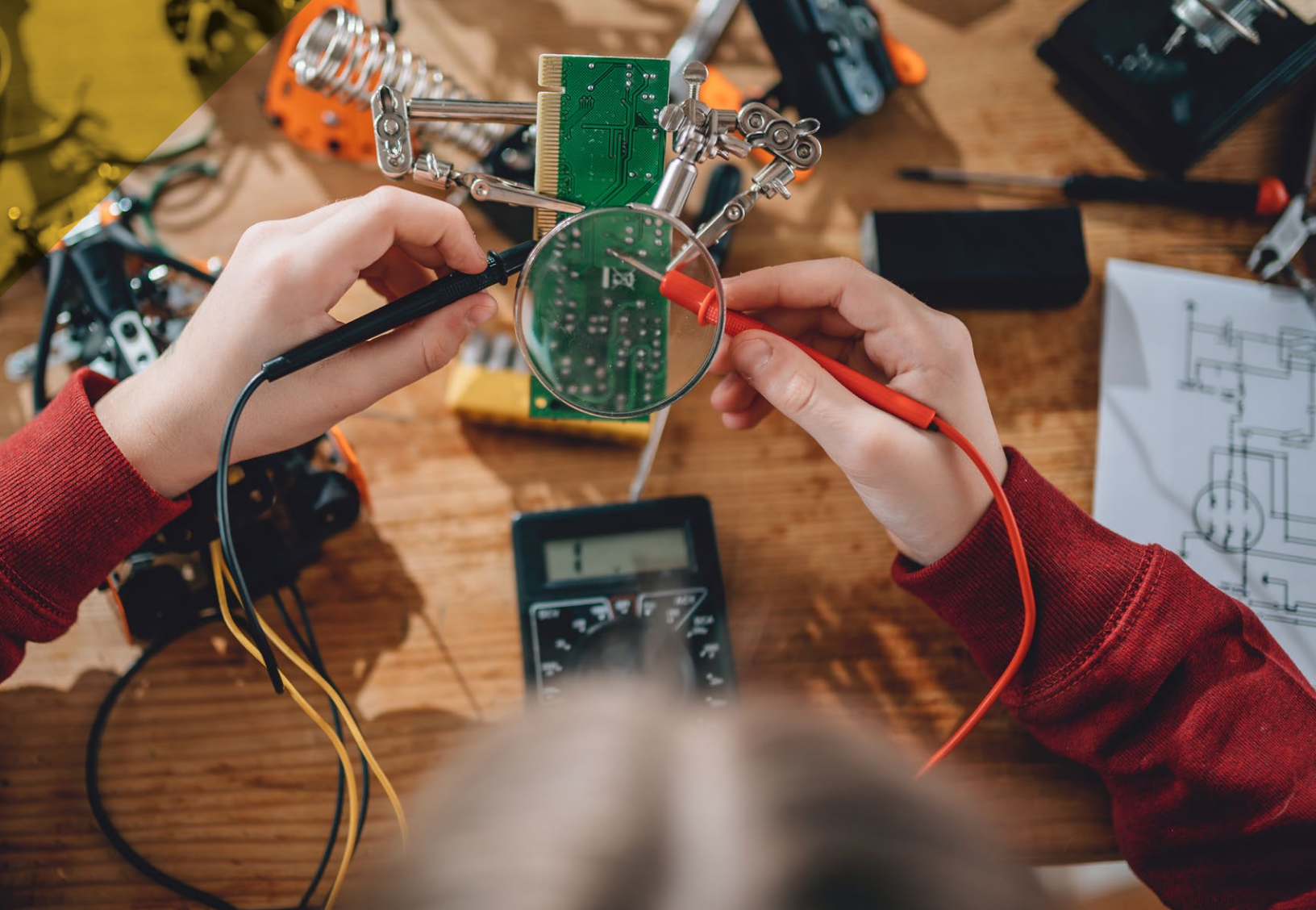
CHART researchers are learning and testing how to make malicious hackers' interactions with cyber systems more difficult and more prone to error, thereby improving cyber defense and making it more likely that the hacker is found and stopped before damage is done. The Oppositional Human Factors project is using human factors methods to better understand how malicious hackers think and to identify ways to bias their decisions so they are more likely to be caught. This is important because all technologies have inherent weaknesses and, eventually, malicious actors can learn how to exploit them.



Nancy Cooke with students

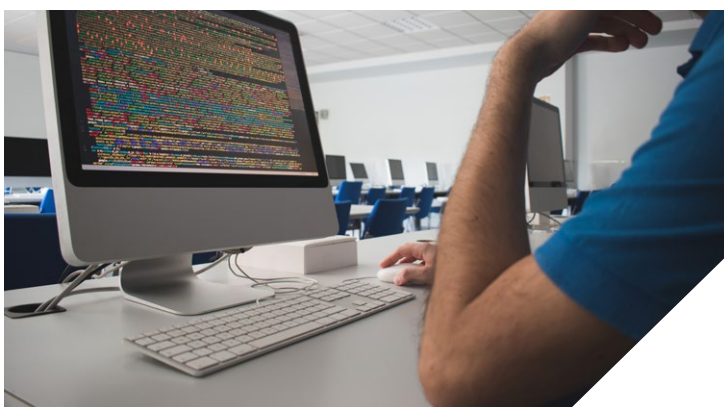
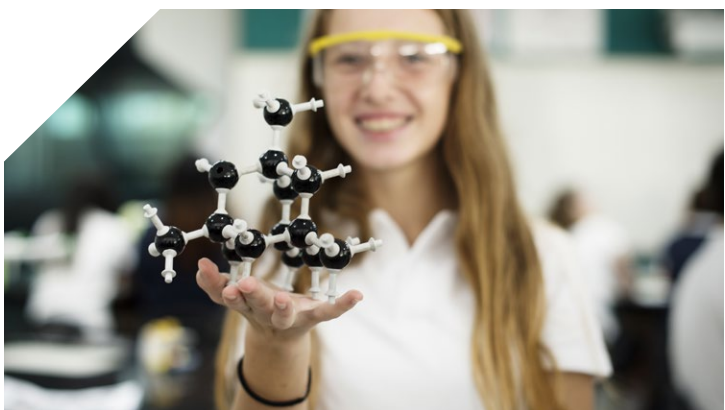
"We believe that mechanisms for teaming with AI can draw from what we know about human-animal teams such as those in the military with working dogs and the Navy's marine mammal programs. Along these lines, AI should be viewed as a different species, with capabilities different from and complementary to those of humans."

Nancy Cooke, director, Center for Human, Artificial Intelligence, and Robot Teaming



Expanding the STEM talent pipeline for national security

The U.S. Department of Defense is the nation's largest employer of scientists and engineers, but routinely has trouble filling these important national security positions due to lack of qualified applicants. GSI seeks to expand the pipeline of science, technology, engineering and math (STEM) talent interested in defense and security careers by providing novel educational experiences to learners — from primary school students to professionals seeking to develop new skill sets.



Project highlights:

▪ **Free biotech education for high school students**

ASU is helping introduce inquiry-based biotechnology education to more than 300 Arizona students, at no cost to them or their schools, and will expose some of the students to federally funded research at biotechnology laboratories. ASU is partnering with 10 Arizona secondary schools and Oak Ridge National Laboratory on this effort, part of the National Defense Education Program.

▪ **Vets4Tech**

Working closely with the Pat Tillman Veterans Center and other ASU units, GSI spearheaded an internship and employment program aimed at placing ASU students with military backgrounds in national laboratories. ASU is currently partnering with Lawrence Livermore National Laboratory on this pilot project and plans to expand its scope in the coming year.

▪ **A primer on working with artificial intelligence**

A professor in ASU's School of Computing and Augmented Intelligence developed and delivered a primer course on artificial intelligence, machine learning and data science for warrant officers in the U.S. Army Intelligence Center of Excellence (USAICoE). The seminar's curriculum is a collaborative effort with the USAICoE and the Army Research Laboratory, and was delivered on two separate occasions at the U.S. Army's Fort Huachuca.

▪ **Introducing cybersecurity concepts into the classroom**

In partnership with the Center for the Future of Arizona, GSI provided Arizona teachers and students with free access to the U.S. Cyber Range. By practicing cybersecurity skills firsthand in a safe virtual environment, students learn important lessons on what cyber criminals look for and how to protect themselves online. More than 440 high school students have participated in this effort.

GSI is leading the conversation by **engaging the public**, **decision-makers** and **guiding experts** in discussions on key security issues.



Highlights:

- **The role of computing in addressing climate change**

Bliss co-authored a Computing Community Consortium (CCC) whitepaper, “Computing Research for the Climate Crisis,” to highlight the role of computing research in addressing climate change-induced challenges. The whitepaper outlines potential approaches to six key areas of impact — energy, environmental justice, transportation, infrastructure, agriculture, and environmental monitoring and forecasting.



- **Bulletin of the Atomic Scientists' panel on the future of AI**

In April, GSI Executive Director Nadya Bliss moderated a Bulletin of the Atomic Scientists' panel on the National Security Commission on Artificial Intelligence's Final Report and how AI can negatively amplify existing threats while simultaneously offering a path forward to international stability, if used wisely. The panel featured Professor Missy Cummings of Duke University and Microsoft Chief Scientific Officer Eric Horvitz.

- **Harnessing the computational and social sciences to solve critical societal problems**

Bliss served on a steering committee of the 2020 NSF CISE-SBE Roundtable and the following report on Harnessing the Computational and Social Sciences to Solve Critical Societal Problems. Key themes that emerged from the roundtable included the need for more and better data, the need for partnerships, the need to create and sustain multidisciplinary teams, and the need to orient research around sociotechnical problems. The steering committee was co-chaired by Elizabeth Mynatt and Duncan Watts, and also included Alondra Nelson, Willie Pearson and Rob Rutenbar.

- **Revitalizing trust in institutions**

The Center on Narrative, Disinformation and Strategic Influence (NDSI) Center Director Scott Ruston helped the public recognize misinformation and disinformation and sought to foster trust in the judiciary by serving on the Arizona Supreme Court's task force on disinformation. The task force researched the problem of disinformation relative to the status of the judiciary in Arizona, and made recommendations for mitigating the effects of disinformation, including increased civic engagement and educational programming, as well as a playbook for responding to disinformation.

- **Students collaborate to solve homeland security challenges**

In March, the Center for Accelerating Operational Efficiency (CAOE) led a design challenge for teams of students from ASU and the University of Nevada, Las Vegas on hardening soft targets. During this three-day event, students worked directly with experts from the Department of Homeland Security and the Phoenix Police Department, as well as industry leaders and members of academia who participated as mentors and judges, with each team working on one of three challenges: protecting the perimeter of a marathon from vehicle ramming; designing city infrastructure to prevent vehicle ramming attacks; or ensuring that municipalities' water systems are protected from cyberattacks.



Looking ahead

- **Coupling advanced research with hands-on learning experiences**

ASU's new Center for Cybersecurity and Trusted Foundations aims to holistically address the long-term cybersecurity challenges facing the nation by building up and fortifying the fundamental building blocks of security — technology, process and workforce. CTF will leverage its \$30 million research portfolio and novel educational platforms to generate interest in and excitement about cybersecurity as a career and to provide skills-building opportunities for learners at all levels.



- **Supporting ASU's New Economy Initiative**

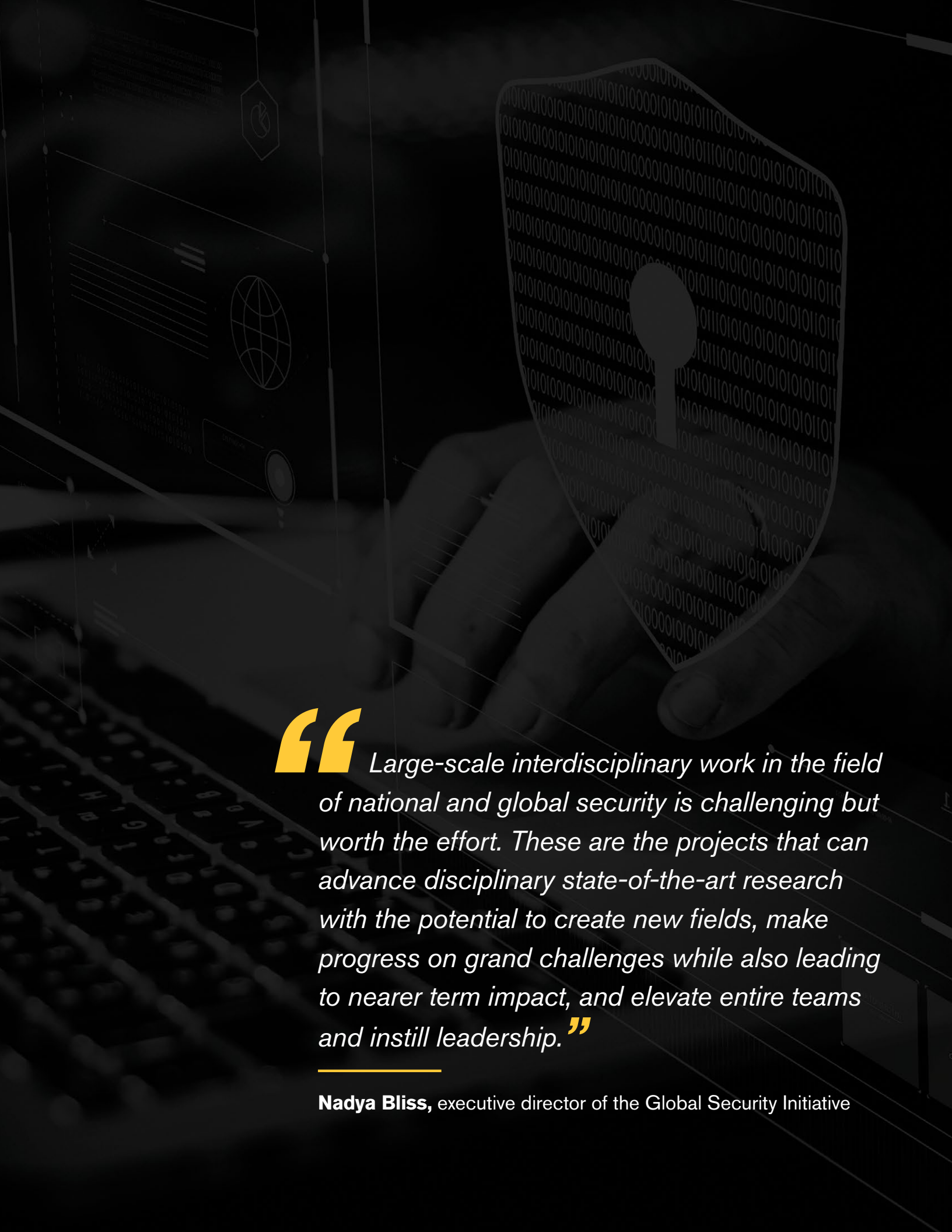
The New Economy Initiative is a forward-thinking investment by the state of Arizona that leverages the breadth and depth of ASU's knowledge and expertise to improve Arizona's competitiveness in the sectors that matter most for 21st century industrial growth. ASU is supporting the New Economy Initiative by partnering with industry to understand emerging technological and market needs and by providing education, producing skilled workers and supporting innovation to drive sustained economic growth. GSI will contribute to this effort in the areas of cybersecurity, artificial intelligence, automation and robotics, big data and more.



- **Addressing security challenges of climate change**

The U.S. Department of Defense is prioritizing the national security risks of climate change in its strategic planning process, to ensure the department can continue to operate under changing climate conditions. GSI will identify key research areas in which ASU can contribute to the DOD's understanding of climate change and its potential effects on national security issues.





“ Large-scale interdisciplinary work in the field of national and global security is challenging but worth the effort. These are the projects that can advance disciplinary state-of-the-art research with the potential to create new fields, make progress on grand challenges while also leading to nearer term impact, and elevate entire teams and instill leadership.”

Nadya Bliss, executive director of the Global Security Initiative



access | excellence | impact

Global Security Initiative

PO Box 875604
Tempe, AZ 85287
Phone: 480-727-8598

Find out how you can partner with
GSI at globalsecurity.asu.edu.

Produced by ASU Knowledge Enterprise.
©2022 Arizona Board of Regents. All rights reserved.
GSI YIR Brochure - 03/2022

Global Security Initiative is a unit of ASU Knowledge Enterprise.