ASU Global Security Initiative

Arizona State University

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

globalsecurity.asu.edu

"The Global Security Initiative is on the leading edge of ASU's comprehensive, interdisciplinary approach to designing enduring solutions for security challenges that impact citizens around the world."

Sethuraman Panchanathan, executive vice president of Knowledge Enterprise and chief research and innovation officer at ASU

About the Global Security Initiative

GSI's vision is a security and intelligence landscape transformed through interdisciplinary research 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 "wicked problems" in global security.

$27.5 million+ in research expenditures in FY 2019 (funding sources: government, industry and foundations)

#3 in the nation for total DARPA Young Faculty Awards

150+ affiliated faculty

About Arizona State University

ASU Charter

ASU is a comprehensive public research university, measured not by whom it excludes, but by whom it includes 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, 5 years, 2016–2020

#3 in student Fulbright awards among public universities
U.S. Department of State

#3 in the U.S. for transdisciplinary science research expenditures
National Science Foundation HERD Survey 2017

One of the fastest-growing research universities in the U.S., with more than $100 million in research expenditures

Top 10 in global patent rankings
National Academy of Inventors and the Intellectual Property Owners Association

A "Best for Vets" school
Military Times, 2019

Exceptional people. Impactful ideas. Powerful relationships.

Letter from the executive director

The democratization and globalization of technology — the widespread access to and adoption of the types of advanced technologies that were once reserved for governments or large organizations — is perhaps the defining societal shift of the last 20 years.

In terms of security, this shift has produced mixed results. It has provided national security policymakers with exponentially more information and data on current and potential threats, but has also created entirely new threat surfaces and arenas for geopolitical rivalries to play out. It has led to the creation of some of the largest companies in the world, and to a robust black market for cybercriminals trafficking in stolen personal data. It has helped improve productivity and gross economic output, yet serves as a gateway for bad actors and adversarial nations to wreak havoc, sow discord and cause large-scale economic disruption.

Governments, companies and people the world over are grappling with the consequences of this transformation. With the global race for the next generation of artificial intelligence, quantum computing, 5G networks, offensive and defensive cyber capabilities, and other advanced technology in full throttle, the opportunities and threats associated with technological advancement are only gaining urgency and becoming more decisive in determining geopolitical power and personal safety.

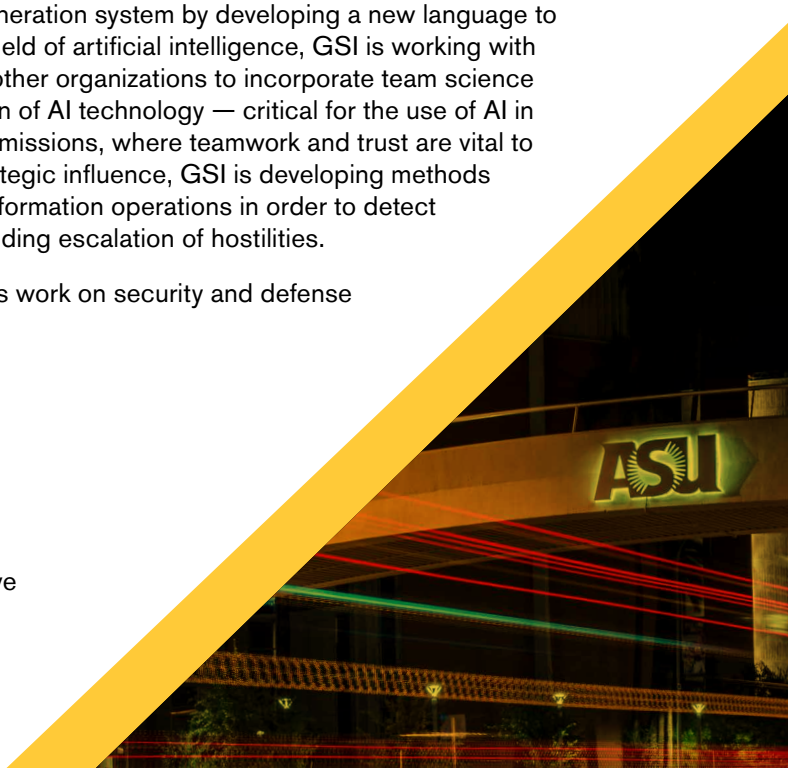
ASU's Global Security Initiative is tackling this grand challenge, leveraging ASU's expertise, creativity, size and culture of innovation to help steer the direction of technological advancement, foster a public capable of thriving in a rapidly evolving world, and build human-centric tools and systems that prioritize security *alongside* capabilities.

In cybersecurity, GSI is advancing state-of-the-art fundamental analysis algorithms in order to address vulnerabilities. Progress this year included significantly increasing the robustness of a next-generation Automatic Exploit Generation system by developing a new language to reason about attacker capabilities. In the field of artificial intelligence, GSI is working with the Department of Defense, industry and other organizations to incorporate team science into the development of the next generation of AI technology — critical for the use of AI in battlefield scenarios and national security missions, where teamwork and trust are vital to successful outcomes. In narrative and strategic influence, GSI is developing methods that collect and code data on adversary information operations in order to detect shifts in tactics that may indicate an impending escalation of hostilities.

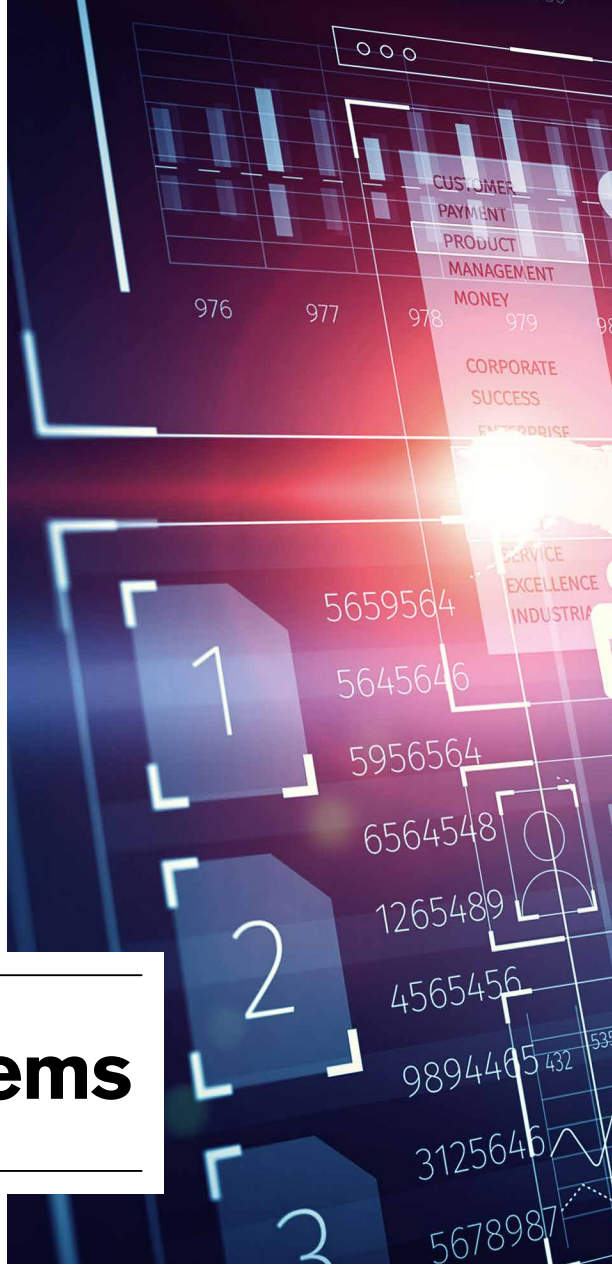
If you would like to learn more about ASU's work on security and defense issues, please contact us at gsi@asu.edu.

Sincerely,

Nadya T. Bliss
Executive Director, Global Security Initiative



The Global Security Initiative leverages the world-class expertise of more than 150 ASU faculty members to produce its solutions, technologies and decision-making tools. The faculty, together with GSI leadership and research scientists, work in teams to produce outcomes in the following global security areas:



Tackling complex problems

Cybersecurity:

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:

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.

Military readiness, resilience and recovery:

Protecting military personnel, first responders and civilians from biological threats, as well as helping them recover quickly from injury and illness.

Human, AI and robot teaming:

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.

Visualization and analytics:

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.

Arizona State University has an applied research organization that is capable of conducting classified and midrange-technology-readiness-level (TRL) services for the defense and security industry. Learn more at **asure.asu.edu**.

Center for Cybersecurity and Digital Forensics

The Center for Cybersecurity and Digital Forensics produces high-impact and practical solutions to real-world cybersecurity challenges. Working closely with industry and government, CDF focuses on the development of novel tools and technologies that can be transitioned into practice.

Faced with evolving threats and adaptive attackers, the center is keeping the future in mind and training the next generation of cybersecurity professionals. Our hands-on approach involves competitive capture-the-flag events and other cyber challenges to ensure all students possess the skills and confidence to succeed.

"Software is everywhere, and software has vulnerabilities. Hackers can demonstrate the flaws in systems so we can ultimately make things more secure."

Adam Doupé, associate director
Center for Cybersecurity and
Digital Forensics

Sample projects:

- CDF is developing the next generation of cyber reasoning systems, which can automatically find vulnerabilities, synthesize exploits and create patches of real-world software. With two awards from the Defense Advanced Research Projects Agency totaling over $19 million, the center is developing systems to effectively and quickly address cybersecurity risks by integrating human knowledge with automated cyber reasoning systems. This research will help fill the gaps in the cybersecurity job market, increase the reach of the existing cybersecurity workforce and provide additional safety for companies and individuals.

- Working with PayPal, CDF significantly improved the consumer security ecosystem. They identified critical vulnerabilities in anti-phishing tools and worked with companies such as Google, Microsoft and Mozilla to address the problems they found, improving the safety of online payments.

- CDF — in collaboration with the international hacking group Order of the Overflow — took over leadership and design of the DEF CON Capture the Flag competition, considered to be the Olympics of competitive hacking. In this role, the CDF and the Order of the Overflow design and run the challenges; host international qualification events, in which over 1,200 teams from around the world competed in 2019; and coordinate the main event featuring the best 16 hacking teams in the world, which is located at the DEF CON cybersecurity conference in Las Vegas.

Phishing: a common method of cybercrime in which criminals pose as a legitimate company to steal user credentials (usernames and passwords).

Center for Accelerating Operational Efficiency

The Department of Homeland Security's Centers of Excellence is an extended consortium of universities conducting groundbreaking research to address homeland security challenges. The Center for Accelerating Operational Efficiency is one of these centers.

Led by ASU, CAOE is working with agencies like the Transportation Security Administration and the Cybersecurity and Infrastructure Security Agency to bring cutting-edge technology and academic rigor to bear on operational challenges.

Capabilities:

- Data analytics: real-time rapid response
- Operations research and systems analysis: improving process and decision time
- Economic analysis: understanding the true cost
- Homeland security risk sciences: identifying and prioritizing risk

Project highlights:

- **Detecting and tracking isolated malicious activities**
  Recent airport security breaches, mass shootings at public events and cyberattacks on sensitive data present the challenge of combating diverse, isolated malicious activities or "lone wolf" type of attacks. CAOE is creating technology that will give law enforcement the ability to identify rare signals that indicate probable activities from IMAs.

- **Improving airport checkpoint performance**
  With more than 2.5 million passengers flying each day through U.S. airports, CAOE is working with the TSA to improve airport checkpoint performance through resource allocation decision tools that evaluate passenger demand. Outcomes include reduced average wait time, improved customer service and quicker responses to unplanned events without compromising security.

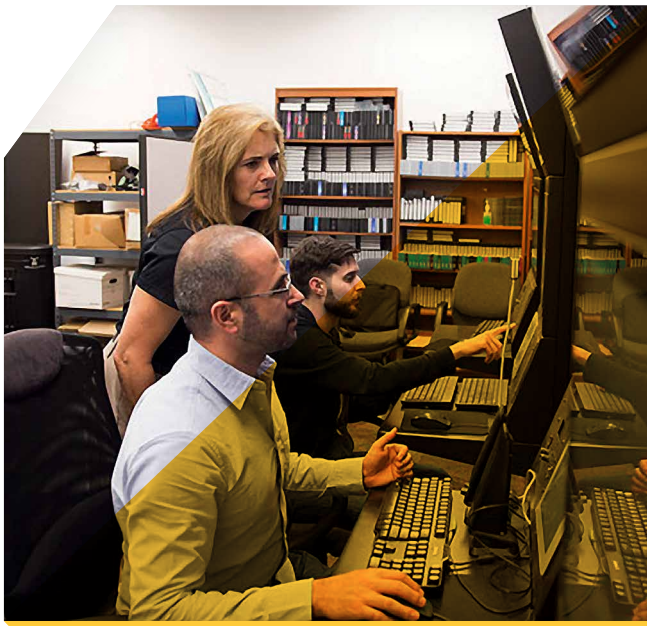
"We will do everything in our power to secure our national transportation systems. We will be proactive, becoming the tip of the spear with new initiatives and technologies. Our partnership with CAOE and ASU provides innovative and high-level support to help accomplish that goal."

Scott Thaxton, acting federal security director, Transportation Security Administration

Center for Human, Artificial Intelligence, 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 is focusing on the system by developing and deploying technologies, tools and best practices to ensure these unconventional teammates complement each other and successfully complete missions.



Project highlights:

- Comparing the effectiveness of human-only teams vs. teams that include a synthetic teammate powered by artificial intelligence. Using simulated environments, GSI is identifying any shortcomings that stem from the inclusion of synthetic teammates.
- Improving the teaming of humans and unmanned vehicles for future combat vehicles by developing a taxonomy of possible interactions that can be associated with interaction methods and metrics.
- Developing methods for programming self-driving cars to make decisions and behave with moral integrity, necessary for building public trust in the new technology.

"We take a lot of measures of what we call team process. How do they interact, how do they communicate, how do they coordinate? All of those things are relevant for trying to understand how to make teams better. We don't want to ask people to interact better with robots. We want robots to interact better with the people."

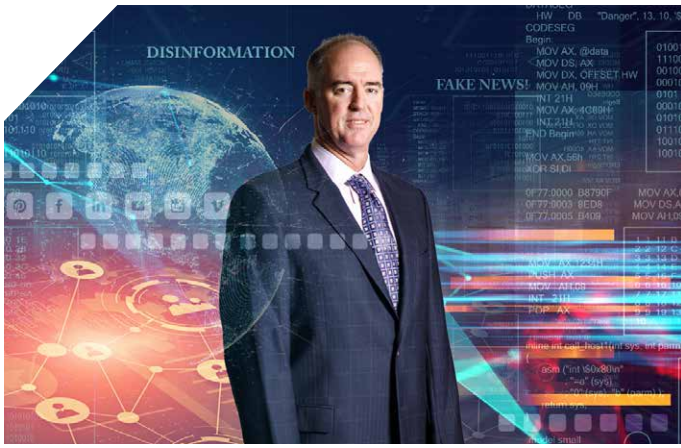
Nancy Cooke, Director
Center for Human, Artificial Intelligence, and Robot Teaming

Narrative, disinformation and strategic influence

Information warfare campaigns use propaganda and disinformation to assault political will, manipulate public opinion and erode sociopolitical institutions, thereby weakening democracies. GSI researchers are designing methods and building tools to identify and combat malicious information operations before they gain traction and cause harm.

Project highlight:

- **Identifying areas that are prone to conflict before violence starts**
  GSI is developing methods for identifying changes in adversary information tactics that might presage an elevation from competition to conflict. GSI and the Center for Strategic Communication are collaborating with Lockheed Martin's Advanced Technology Lab to identify changes in strategic framing in media that could signal impending instability and conflict.



"More than simply detecting adversarial bots, we are interested in understanding the entirety of information manipulation, from the information pathways to malicious actors to how stories are told to influence individuals, communities and nations."

Scott Ruston, GSI research scientist

01 **COLLECT** texts from propaganda outlets

02 **CODE** examples of adversarial framing

03 **TRAIN** a machine classifier to recognize adversarial framing in a large corpus of texts from vulnerable regions

04 **DETECT** shifts over time that would indicate change in targeting or tactics

Looking ahead

- **Building the workforce America needs**
  The rapid advancement of new technologies has had a tremendous impact on America's workforce, and employers are now seeking employees committed to being lifelong learners. GSI will establish a workforce development effort aimed at preparing the next generation of workers and up-skilling the current generation, both on technical skills for nontechnical employees, and management and leadership skills for technical professionals.

  ASU co-hosted the National Initiative for Cybersecurity Education conference in November 2019, along with Florida International University and New America. GSI led ASU's involvement in the conference, titled "Reimagining the Future of the Cybersecurity Workforce: Adapting to a Changing Landscape."

- **An interdisciplinary team to combat an urgent threat**
  GSI will ramp up efforts to identify and combat disinformation campaigns, bringing together experienced journalists from ASU's Walter Cronkite School of Journalism and Mass Communication, computer scientists from the Fulton Schools of Engineering, and GSI experts in narrative and strategic framing, among others.

- **The next generation of artificial intelligence**
  A current limitation of artificial intelligence is the technology's lack of social intelligence, which inhibits its ability to effectively team with human counterparts. In the coming year, ASU will team with Aptima to create and apply the Social Intelligence Manipulation and Measurement Laboratory, a virtual testbed for replicable evaluations of AI social intelligence.

Leading the conversation

GSI leadership and researchers engage the public in discussions of key security issues through a wide variety of venues, from appearances in national media outlets like the Washington Post and CNN to organizing high-level discussions of critical security needs.

Highlights:

- **"Code 8.7: Using Computational Science and AI to End Modern Slavery"**
  GSI helped organize a conference at the United Nations that brought the computational research and artificial intelligence communities together with those working to combat modern slavery and human trafficking. "Code 8.7: Using Computational Science and AI to End Modern Slavery" featured discussions on vulnerability mapping, using technology to find hidden populations and developing a research pipeline aimed at combatting modern slavery.

- **Future Warfare Conference at the Australian Defense Force Academy**
  GSI Executive Director Nadya Bliss was a featured speaker at the conference, presenting on "The Democratization of Technology: Opportunities and Threats." The event featured military and academic leaders from Australia, the U.S. and the U.K.

- **The Future of National Security Research at ASU**
  GSI convened leaders on national security issues from across the university to learn about the university's capabilities, spur collaboration and set the stage for increased security research at ASU. Topics discussed included emerging research trends in national security, autonomy, cybersecurity and combatting disinformation.

- **Informing policymakers on the importance of U.S. leadership in research and development**
  GSI Executive Director Nadya Bliss served on a panel at a Capitol Hill event on the need for increased federal funding for science and technology research and development. The panel centered on the release of a "Task Force on American Innovation" report highlighting America's declining leadership in research and technology. Other panelists included Eric Fanning, former secretary of the Army and current president and CEO of the Aerospace Industries Association; John Neuffer, president and CEO of the Semiconductor Industry Association; and Michael McQuade, vice president for research at Carnegie Mellon University.

"GSI prioritizes security and defense mission needs, and a big part of that is ensuring the research, tools and ideas generated at GSI can be transitioned to the end user, whether they be in government or industry. We understand the need for workable solutions."

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.
©2020 Arizona Board of Regents. All rights reserved.

Global Security Initiative is a unit of ASU Knowledge Enterprise.