ASU Global Security Initiative
Arizona State University

2020 Year in review

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

globalsecurity.asu.edu

“Today’s security challenges are borderless, complex and often driven by technologies that offer immense benefits to society while also expanding the threat landscape. Any successful effort at addressing security issues like the spread of disinformation, protecting our critical infrastructure or securing federal networks requires teams of leading experts working together across disciplines. The Global Security Initiative is ASU’s hub for this, creating interdisciplinary teams of experts to conduct mission-driven research and programming aimed at addressing the global security challenges of today and the future.”

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 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.

$34M+ in research expenditures in FY 2020 (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, 6 years, 2016–2021

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

#1 in the U.S. for transdisciplinary science research expenditures
National Science Foundation HERD Survey 2019

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 year 2020 was full of challenges and hardships. More than ever, we saw a clear demonstration of the value of scientific research to society. It took less than a year after the start of a global pandemic that has taken millions of lives for a vaccine to be developed, a remarkable scientific accomplishment that offers the world some hope that the situation will improve in the near future. This is what can happen when resources and attention are focused on big challenges.

And there are plenty of challenges. COVID-19 is still claiming thousands of lives each day, but we also need to be preparing for the next pandemic and developing better early-warning systems. Misinformation and disinformation — accelerated and amplified via social media platforms and the political environment — are wreaking havoc on the institutions critical to democracy and civil society and resulting in acts of physical violence. The SolarWinds hack demonstrated just how vulnerable our cyber networks are, and the attempt to poison a Florida town's water supply by hacking into the water treatment system is a clear example of why we must significantly increase our efforts to protect critical infrastructure, both at the federal and local levels.

These are all daunting issues, but there are reasons for optimism. Advances in scientific research are drastically improving our ability to anticipate, prepare for, respond to, and mitigate the negative consequences of these and other threats. This is what ASU's Global Security Initiative does; we leverage the talent and resources of the most innovative university in the nation to drive responses to the world's most complex security challenges. We do this by thinking beyond solely disciplinary responses and developing more holistic approaches centered on research, education and engagement with decision-makers and the broader public.

Disinformation is a security challenge ripe for this approach, and GSI has been bringing an interdisciplinary group of experts together for years to understand how and why false information spreads, how to identify it early and how to slow its spread before it causes too much damage. These efforts have led to the recent launch of GSI's Center on Narrative, Disinformation and Strategic Influence, which fuses social sciences and humanities with state-of-the-art computer science to develop tools to combat disinformation campaigns and better understand the information environment.

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

Sincerely,

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

Tackling complex problems

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

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.

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.

Security and defense workforce development:

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.

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.

Visualization and analytics:

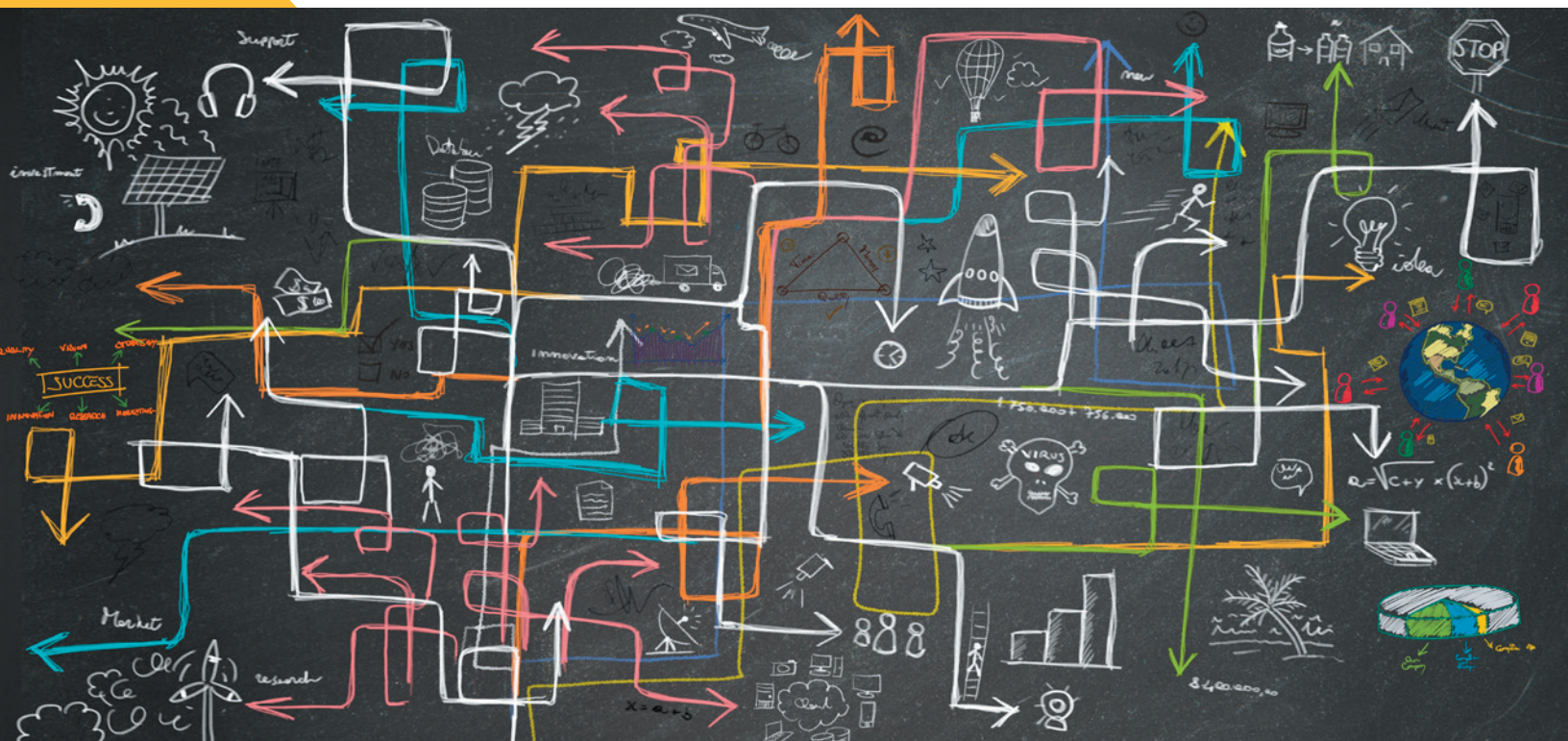
Creating tools that clarify and effectively communicate key information, enabling decision-makers to better plan for and respond to changing events, while making judgments that are credible, salient and legitimate.

Center on Narrative, Disinformation and Strategic Influence

The tumult of 2020 put into stark relief civil society's dependence on credible information for maintaining stability. Widespread misinformation about public health measures hampered unified, collective action to mitigate the effects of COVID-19; severe political polarization was exacerbated by disinformation campaigns designed to dismay audiences, distort situations and distract from actual malfeasance. These campaigns also erode faith that anything is knowable and true — a boon to autocrats and a threat to democratic values. Building on a robust portfolio of existing projects, GSI has established a new center to engage with the complex nature of influence and disinformation.

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 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.



Scott Ruston in discussion with student in 2019

"The power of deceptive memes and falsified videos to influence and polarize is partly determined by unique aspects of human cognition, understanding and identity. We need an interdisciplinary approach that fuses humanities, social science and computer science to defend against disinformation and malign influence."

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

Capabilities:

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

Project highlights:

- **Detecting and tracking adversarial framing**
  Developing the ability to automatically detect adversarial framing — when parties hostile to U.S. interest frame events in the media to justify support for future actions — as it occurs and studying how that framing transitions from known propaganda to nonpropaganda sources.

- **Analyzing disinformation and propaganda tactics**
  Providing policymakers with a fuller understanding of the adversarial communication landscape in Latvia, Sweden and the United Kingdom. The team identified adversarial framing around contentious issues, trained a machine classifier to detect such framing at scale, revealed shifts in messaging strategies and analyzed antidemocracy narratives.

- **Semantic information defender**
  As part of a larger team performing on a Defense Advanced Research Projects Agency program, NDSI is helping develop a system that detects, characterizes and attributes misinformation and disinformation — whether image, video, audio or text. NDSI provides content and narrative analysis, media industry expertise, text detection and characterization methods, and a large dataset of known disinformation and manipulated media objects to the project.

Center for Cybersecurity and Digital Forensics

The Center for Cybersecurity and Digital Forensics (CDF) works closely with industry and government to produce high-impact and practical solutions to real-world cybersecurity challenges. CDF has partnered with leading technology companies including PayPal, Samsung, Google, Microsoft and IBM, and has a broad portfolio of government-sponsored research.

Faced with evolving threats and adaptive attackers, the center is keeping the future in mind and training the next generation of cybersecurity professionals. The center takes a hands-on approach to education, which includes encouraging students to participate in capture-the-flag competitions, collegiate cyber challenges, and industry-sponsored events to sharpen their skills.

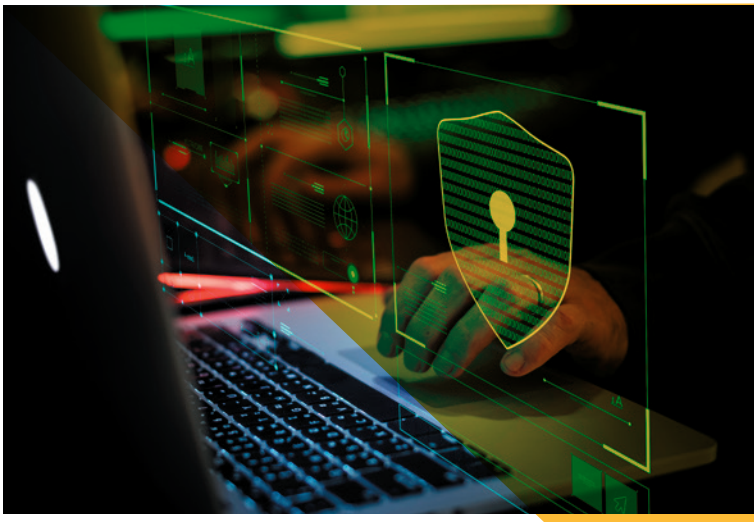
CDF is designated a National Center of Academic Excellence in cyber defense and research by a joint National Security Agency and U.S. Department of Homeland Security program.

"Businesses are essentially unable to hire enough professionals with the level of cybersecurity expertise that is needed. We must address this gap to train students so they can perform at the level needed by the government and industry to defend our systems. We're fighting a very smart adversary who has a lot of motivation to break into our systems."

Adam Doupé, acting director, Center for Cybersecurity and Digital Forensics

Capabilities:

- Binary exploitation
- Reverse engineering
- Machine learning
- Web/mobile security
- Dark web market behaviors
- Competitive hacking



Project highlights:

- In collaboration with PayPal, CDF led pioneering research that explored the full life cycle of phishing attacks. From the launch of a phishing campaign to an account being compromised, researchers tracked nearly 4.8 million victims over a one year period. This groundbreaking research captured valuable data about the success rates of phishing, and helped develop a framework for measuring victim traffic and protecting accounts.

- CDF is developing new automated methods for "understanding" the machine-readable form of software, reversing the translation process, and generating human-readable source code as part of the Defense Advanced Research Projects Agency's Assured Micropatching (AMP) Program. The code can then be repaired, retranslated, and integrated back into the deployed software. The goal of AMP is to develop a system that can rapidly repair mission-critical software in a targeted manner while minimizing potential side effects without original source code.

- CDF orchestrates DEF CON's annual Capture the Flag competition, widely recognized as the 'Olympics' of ethical hacking featuring top hacking teams from around the world. The 2020 tournament began in the spring with over 1,300 teams participating, and concluded with 16 teams competing in the finals in August. The finals lasted approximately 36 hours, with teams competing on topics like binary exploitation, machine learning and cryptography.

- CDF developed and deployed pwn.college, a first-stage education platform that targets emerging members of the cybersecurity community by providing scaffolded learning opportunities to build knowledge and experience. Modules include training on program misuse, shellcode, sandboxing, binary reverse engineering, memory corruption, exploitation and other topics. While the platform is aimed at a higher education demographic, it is open to a global audience at no cost. Visit pwn.college for more information.

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 (CAOE) is one of these centers.

Led by ASU, CAOE develops and applies advanced analytical tools and technologies to enhance planning, information sharing and real-time decision-making in homeland security operations.


2019 Capstone TSA

Capabilities:

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


Ross Maciejewski with students at CIDSE in 2018

Project highlights:

- **Pivoting to respond to a pandemic**
  When the spread of COVID-19 turned into a pandemic in March 2020, the CAOE quickly pivoted some existing research efforts to address anticipated pandemic-related challenges. For example, the center shifted the focus of an ongoing project on natural disaster preparedness to address expected supply chain challenges around medical equipment and vaccines.

- **The Procurement Innovation Lab (PIL)**
  PIL is a DHS initiative designed for experimenting with new techniques for increasing efficiency and implementing best practices in the procurement process and lowering entry barriers to encourage new, nontraditional contractors to compete. A CAOE project is developing an objectively derived procurement performance metric structure that can be used to measure how well PIL is advancing the acquisition process at DHS and making recommendations on potential improvements.

- **Dynamic workforce management at network screening facilities**
  The development of new workforce management tools are critical for the Transportation Security Administration (TSA) as it faces multiple challenges like airport space constraints and an increasing number of security threats. Researchers at CAOE are developing new analytical tools to assist TSA planners in responding to these and other demands, with the goals of maximizing efficiency, increasing safety and improving the passenger experience.

"The center has always focused on projects that directly contribute to the operational mission of the Department of Homeland Security. When DHS's tactical priorities shift and they are faced with responding to a crisis, we adjust as well."

Ross Maciejewski, director, Center for Accelerating Operational Efficiency

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 (CHART) 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.

Nancy Cooke with students in 2018

Capabilities:

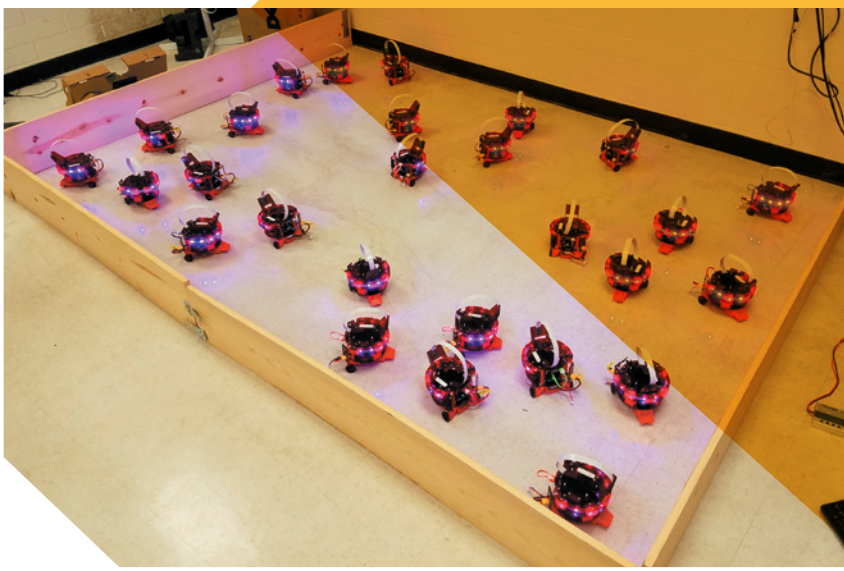
- Distributed team training with virtual teammates
- Search and rescue missions
- Teaming in space operations
- Collaborative planning
- Driverless vehicles and human drivers

Project highlights:

- **Artificial social intelligence for assisted teams**
  Collaborating with over 200 top AI and cognitive science researchers from industry and academia with the goal of producing AI with the social intelligence to team more effectively with humans, as part of a Defense Advanced Research Projects Agency program.

- **Space challenge**
  Determining how AI can be used to most effectively and safely support multiteam systems in space by monitoring system performance under variable latency and bandwidth issues in communications to identify anomalies.

- **Team effectiveness**
  Developing models and metrics of team effectiveness in future military vehicle crews that include humans and AI working together, by exploring factors that impact team effectiveness within a military reconnaissance scenario.



"We take teaming seriously at CHART and do research to learn how to best assemble, develop and assess teams made up of humans, AI and robots. By using synthetic task environments and the Wizard of Oz paradigm (in which a human emulates AI) we can answer these questions that lead to effective human-AI-robot teams. Too often people are asked to adapt to the intelligent machines. Instead, intelligent machines should adapt to people."

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

Cybersecurity Education Consortium

The Cybersecurity Education Consortium (CEC) partners with schools, educators and the broader cybersecurity community to ensure students are prepared to lead and be changemakers in the cybersecurity workforce.

The Consortium serves as a hub for ASU students to find information about cybersecurity education and events, educators at all levels to network and find student-centered solutions for curriculum and courseware, and industry partners to connect with ASU and the educational community.

Project highlights:

- **CyberDay4Girls**
  The CEC partnered with IBM to host a CyberDay4Girls event, bringing more than 200 middle school girls to ASU to learn the basics of blockchain, cryptography and the internet of things. Attendees also heard from a panel of women in the field of cybersecurity who discussed their own professional journeys.

- **Providing lesson plans to teachers**
  The CEC developed a middle school cybersecurity curriculum grounded in the Arizona computer science state standards to fill an educational gap in many Arizona schools, helping to introduce students to core cybersecurity concepts before they enter high school. The curriculum is available to anyone for free on the CEC's website.

- **A virtual cyber range for Arizona students**
  As a pilot project in collaboration with the Center for the Future of Arizona, the CEC is providing 15 teachers and more than 400 students in Arizona with free access to the U.S. Cyber Range. With the chance to practice cybersecurity skills firsthand in a safe virtual environment, students learn important lessons on what cyber criminals look for and how to protect themselves online.

2019 CyberDay4Girls event

"Our students are really enjoying the cybersecurity simulations. This is something that they did not have access to prior to our partnership with CEC, and they are very excited about."

Barbara Coakley, director, MET Professional Academy

Leading the conversation

GSI frequently engages the public, decision-makers and leading experts in discussions on key security issues.

Nadya Bliss and Jamie Winterton in 2019

Highlights:

- **Two GSI leaders named to Information Science and Technology Study Group**
  The Defense Advanced Research Projects Agency named Executive Director Nadya Bliss and Director of the Center for Human, AI, and Robot Teaming Nancy Cooke to the Information Science and Technology Study Group (ISAT). The group brings 30 of the brightest scientists and engineers together to identify new areas of development in computer and communication technologies and to recommend future research directions.

- **GSI's director of strategy a member of Washington Post's Cybersecurity 202 Network**
  Jamie Winterton is a member of the group of high-level digital security experts from across government, the private sector and security research community. She has commented on topics such as government efforts to establish an encryption backdoor and the responsibility of companies to disclose data breaches.

- **Showcasing the latest science**
  Two GSI centers host regular speaker series featuring leading domain experts discussing the most recent advances in science and technology. The Center on Human, AI, and Robot Teaming has covered topics such as trust in automation, autonomous vehicles and engineering human performance in the age of AI. The Center for Accelerating Operational Efficiency has discussed subjects such as misinformation, deep fakes and biometrics. These sessions are open to join remotely, and audiences are encouraged to contribute to the conversation and discussion points.

- **Security vs. capability: lessons for the future of cybersecurity**
  Executive Director Nadya Bliss served as a featured presenter as part of the National Academy of Engineering Grand Challenges for Engineering Speaker Series. Bliss discussed the historical context that led to the creation of today's information technology ecosystem, why capability was consistently prioritized over security and how to move forward with a reinvigorated security mindset.

- **Detecting, combating and identifying disinformation and misinformation**
  Executive Director Nadya Bliss moderated and organized a scientific session at a 2020 annual meeting on detecting, combating and identifying disinformation and misinformation. The session featured experts from the Office of the Director of National Intelligence, ASU, the University of Washington, and New York University.

Looking ahead

- **Improving our ability to recognize and resist disinformation**
  GSI will expand the capacity of its newest center, the Center on Narrative, Disinformation, and Strategic Influence, to address societally impactful topics such as “deep fakes,” media literacy and the critical role of narrative theory in identifying and combating disinformation.

- **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 will ramp up efforts to expand the DOD’s pipeline of science, technology, engineering and math (STEM) talent by providing students from preschool through college with increasingly sophisticated learning materials to inspire sustained interest in STEM topics and increase awareness of defense and security career pathways in STEM.

young STEM students building robots in 2019

- **Launching a global security and technology speaker series**
  GSI will launch a new speaker series focused on the intersection of global security and technology, aimed at providing an Arizona audience access to leading thinkers on security and defense issues. Speakers will include defense and national security officials, leading technologists, journalists, academics and others driving the agenda around technological development for defense and security purposes.

“When we design novel technologies, security can often be an afterthought. As our reliance on online platforms and interconnected systems grows, the threat landscape grows with it. We need to prioritize security alongside development of capabilities. This is fundamental to the national security mission and is a major focus of the Global Security Initiative.”

Nadya Bliss, executive director, 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.
©2021 Arizona Board of Regents. All rights reserved.

Global Security Initiative is a unit of ASU Knowledge Enterprise.