



USING SPACE CAMP MODEL FOR NEXT GENERATION SECURITY TRAINING



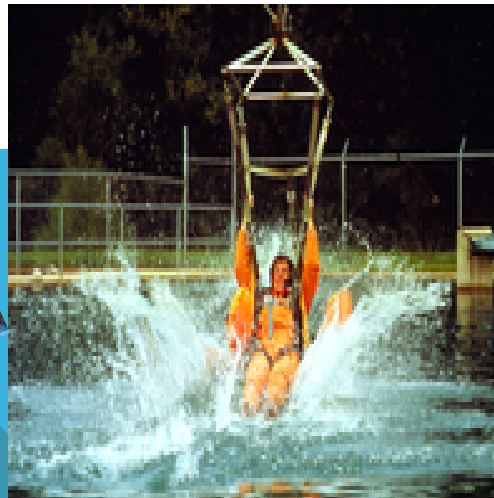
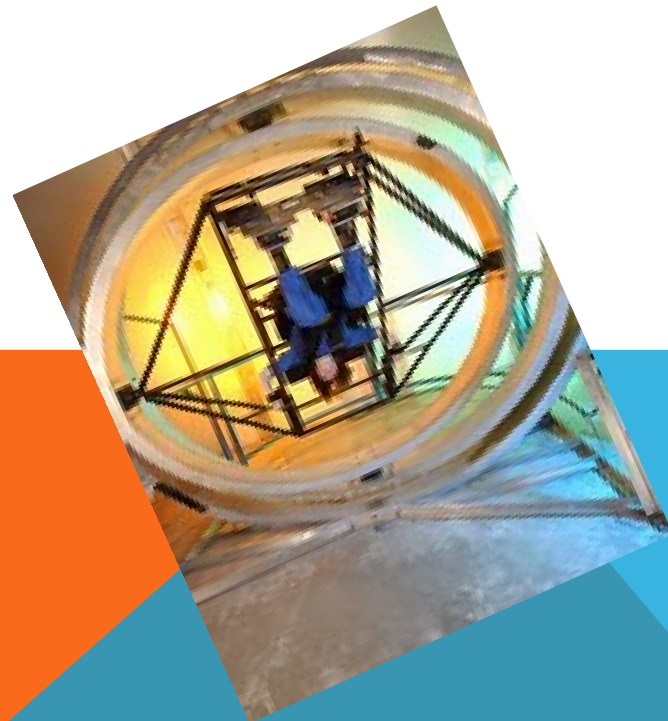
OR

“HARRY POTTER MEETS HOMELAND SECURITY”

HACKERS ON PLANET EARTH CONFERENCE

JULY 13, 2012

NEW YORK CITY



SECURITY INTELLIGENCE LAB® AND SI-7° ACADEMY®

SECURITY INTELLIGENCE TO THE 7TH DEGREE



***...THE PUZZLING
ART AND SCIENCE OF SECURITY***

THE SITUATION

“There are about 1,000 security people in the U.S. who have the specialized security skills to operate at world-class levels in cyberspace

– we need 10,000 to 30,000.”

Jim Gosler, director of the CIA's Clandestine Information Technology Office.

WHY

Hackers attack computers **2,244 times a day** as a result of weak user names and passwords. (Uni. of Maryland)

Median **cost of an attack per year: \$3.8 million** (“The First annual Cost of Cyber Crime Study” sponsored by ArcSight)

Among the 2,807 publically disclosed data breaches worldwide in the past five years, the cost to victim firms as well as those whose information was exposed = **\$139 billion!** (“The Leaking Vault” by Digital Forensics Association)

"Every major company in the United States has already been penetrated by **China**. My greatest fear is that, rather than having a cyber-Pearl Harbor event, we will instead have this death of a thousand cuts.” (Richard Clarke, a former cybersecurity and cyberterrorism advisor for the White House.)

Cyber attacks on critical infrastructure in the US have rocketed over the past three years, according to a new report from the Industrial Control Systems Cyber Emergency Response Team. ICS-CERT, which is part of the Department of Homeland Security, received just **nine** incident reports in 2009, but that number leapt to **41** in 2010 and **198** in 2011.

IT'S A DIGITAL WORLD

- Social Media, like Facebook, Google+, Linked-In, texts, Twitter, Gmail, email providers, other
- Critical Infrastructure: water, power, gas, food supply, airports/airlines, other
- Financial Information: banks, credit and debit cards, on-line banking, etc.
- The Pentagon.
- The Justice Department and other government offices.
- Intellectual Property...yours, mine, everyone's
- Academic Institutions.
- Corporations, businesses.
- Hospitals.
- Emergency management.

Literally every aspect of our lives is recorded or controlled in a digital format.



WHAT'S AT RISK

...***EVERYTHING***



THE **FBI** LACKS RESOURCES

The Department of Justice Inspector General found that more than one-third of 36 elite cyber-investigators in 10 of its 56 bureaus “reported that they **lacked the networking and counterintelligence expertise** to investigate national security [computer] intrusion cases.”

UTICA, N.Y. (WKTV) - U.S. Senator Charles Schumer says a new report shows that **over a third of FBI agents are under-qualified to fight the growing threats of cyber-crime and online terrorism** and is urging FBI Director Robert Mueller to train FBI agents.



GOVERNMENT ACTION

On 23 June 2009, the Secretary of Defense directed the Commander of U.S. Strategic Command (USSTRATCOM) to establish USCYBERCOM.



The command is located in Fort Meade, Maryland
USCYBERCOM centralizes command of cyberspace operations,
organizes existing cyber resources and synchronizes defense of
U.S. military networks

BUT...EFFORTS ARE UNCOORDINATED

DHS and the National Security Agency (NSA) jointly sponsor the Centers for Academic Excellence, a consortium of universities that focus on advanced information security education. While participation in the program has snowballed, **federal funding for scholarships has not kept pace.**

One of the most important steps policymakers can take is **to nourish the education and training of a new crop of security experts.**




ACADEMIC SOLUTIONS

Universities are offering degrees in Cyber Security, but training is slow and is often diluted by other academic subjects.

According to Richard Marshall, the director of global cyber security management at the Department of Homeland Security, the flow of cyber security experts **graduating from the nation's universities** with advanced degrees remains **anemic**.

"...we are going to fail if we don't invest more money, time, attention and rewards to educate the workforce," Marshall said. "That's our legacy-to-be."



COMPETITIONS & CAMPS

U.S. Cyber Challenge launched a nation-wide talent search in 2011. Cybersecurity camps were conducted in California, New York, and Delaware. The goal is 35 camps in 32 states in 2012.

In addition, cyber talent will be identified from 3 competitions:

1. **DC3 DIGITAL FORENSICS CHALLENGE**, tasks faced by a cyber crime analyst
2. **NETWARS**, a virtual network game
3. **CYBER PATRIOTS DEFENSE**, an Air Force sponsored competition in schools around the nation



ALSO...

CyberCIEGE™

...an innovative video game and tool to teach computer and network security concepts

Sponsored by the US Navy, the Naval Education and Training Command, the Office of Naval Research, the Biometrics Task Force, the Office of the Secretary of Defense, and the National Science Foundation.

Hacker U™

... a subsidiary of the ethical hacking firm, Parameter Security™ and an EC-Council Accredited Training Center (ATC), dedicated to IT professionals and non-IT professionals who desire training to stop malicious hackers.



WE NEED...

...More than Games

...More than Workshops

...More than University Classroom Courses

...More than Adult Certification Programs by Professional Organizations

WE NEED A DIFFERENT KIND OF TRAINING: **IMMERSIVE**

AND DIFFERENT TRAINEES: **BRIGHT, MOTIVATED, YOUNG PEOPLE**



MARC W. TOBIAS, PHYSICAL SECURITY EXPERT, SAYS:

“What is wrong with the U.S. intelligence community is that it doesn’t have any kids and consequently **lacks imagination.**”

He thinks the answer to the nation’s intelligence problems is a **specialized academy** for students featuring a curriculum of extensive lessons in a kind-of ‘modified spycraft.’

“I call it Harry Potter meets Homeland Security,” Tobias said, envisioning an espionage Academy where cyber wizards and lock professionals teach the basics security to their talented protégés.

Kids would be immersed in a technology environment that inspires, motivates, and excites them to vertical thinking and creative problem solving.



A SPACE CAMP OF CYBER SECURITY



SECURITY INTELLIGENCE LAB & SI-7 ACACEMY

Mission:

To deliver a continuum of timely, world-class **immersive** education, training, and research in physical and cyber security.

Why:

To fill the need for a highly educated, technically advanced, creative, physical & cyber security work force.



WHO IS INVOLVED IN THIS PROJECT

...the world's most distinguished security professionals and experts who understand the modus operandi of predatory hackers, both physical and cyber, and stay on the cusp of ever-evolving, imaginative criminal techniques and technology.



SECURITY INTELLIGENCE LAB INITIATIVES

Training of Lock Engineers and Others

Services to Corporations

Exploration of Security Issues

Problem Solving and Demo Lab for Lock Companies

Research

Recommendations & Referrals

Certifications

Immersive Training Programs:

SI-7 ACADEMY

Corporate Security Professionals Session

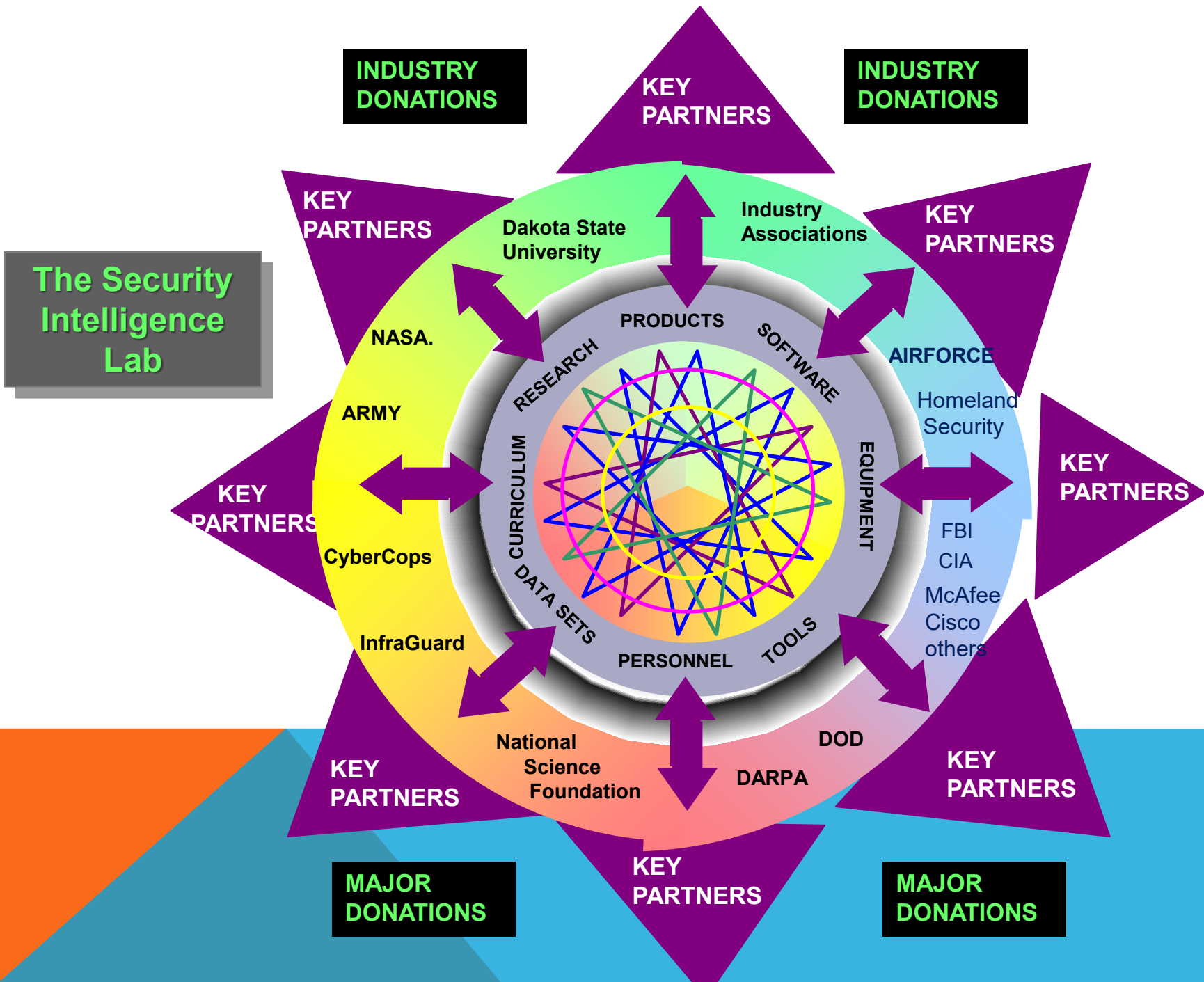
Governmental Security Officers Program

Infrastructure Security Guardians Academy

Citizen Protector Camp

SECURITY INTELLIGENCE LAB





SI-7 ACADEMY®

An immersive training academy for the puzzling art
and science of security

Advanced tools

High level techniques

Vigorous curriculum

...delivered in a challenging, innovative, high tech
environment by the world's most distinguished
security professionals.

...a

“Cyber-Security SPACE CAMP®.”



SI-7 ACADEMY CURRICULUM

Participants will achieve critical levels of accomplishment through:

Scenario driven course work

Gaming

Competition

Lectures

In a TECHNOLOGY VILLAGE



TECHNOLOGY VILLAGE CAMPUS AND ACTIVITIES

(SAMPLE)

Locktite Tavern

...a virtual space “cave”
...partying inside the security
locks

SCIF Landing

...Sensitive Compartmented
Information Facility
...a very secure environment for
briefings/lectures by top
personnel

CyberTools Street

...place to buy, borrow, barter, or
make tools to solve the security
puzzles

Avatar Café and Chill Lounge

Parallel Talk

...instruction for lock
hackers...social media

Tobias’ Alley (Hogan’s Alley)

Robotic IQ

...cracking robotic crime

WikiCops™ Competition

...recover the evidence, catch the
hacker

Magic inside the keyboard

...3D virtual computer space

FYF Class

PODS ...connecting camps in
or satellite locations

friend...GeoCoding,
GeoCatching, and other

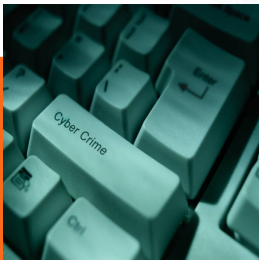
Electron Surfing

Driving ...Cycling-a la Tron and
a Veyron...gaming
across the satellite PODS

Node to Node

hackers ...instruction for cyber

CYBER CRIME



SECURITY SYSTEMS

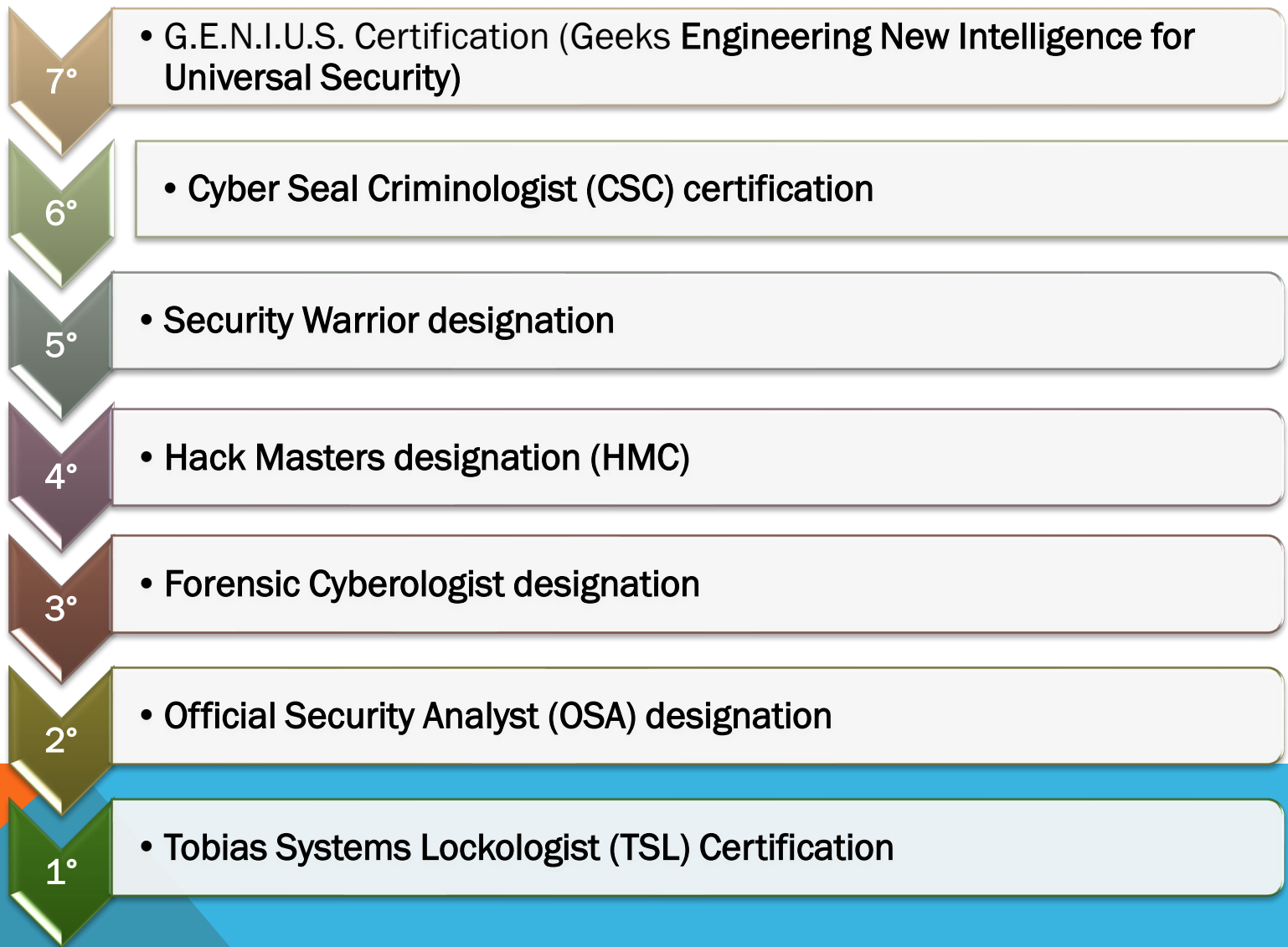


IDENTITY THEFT



LOCKS





PARTICIPANTS

Technology-wise young people with imagination, intelligence, determination, and talent.

And...only those with **sterling ethics** will be admitted.



SI-7º ACADEMY INSTRUCTORS

Award-Winning, certified security professionals

Security Leaders

Instructors with real-world experience in the field

Individuals/peers from major computer network and system manufacturers, NCIS, USSS, DARPA, INTEL Community, Interpol, FBI, National Security Labs, security companies, Homeland Security, University professors, “White Hat,” hackers,” criminal investigators, and other high level professionals.



WHY ATTEND SI-7 ACADEMY?

To develop “ethical hacking” skills and become a highly sought after security professional.



FACTS ABOUT SI-7 ACADEMY

- uses next generation technology
- held in an extraordinary, futuristic, immersive environment
- location: Dakota State University, Madison, SD
 - one of 30 NSA designated Universities of Academic Excellence for Cyber Security
 - one of 4 universities chosen for CyberOps

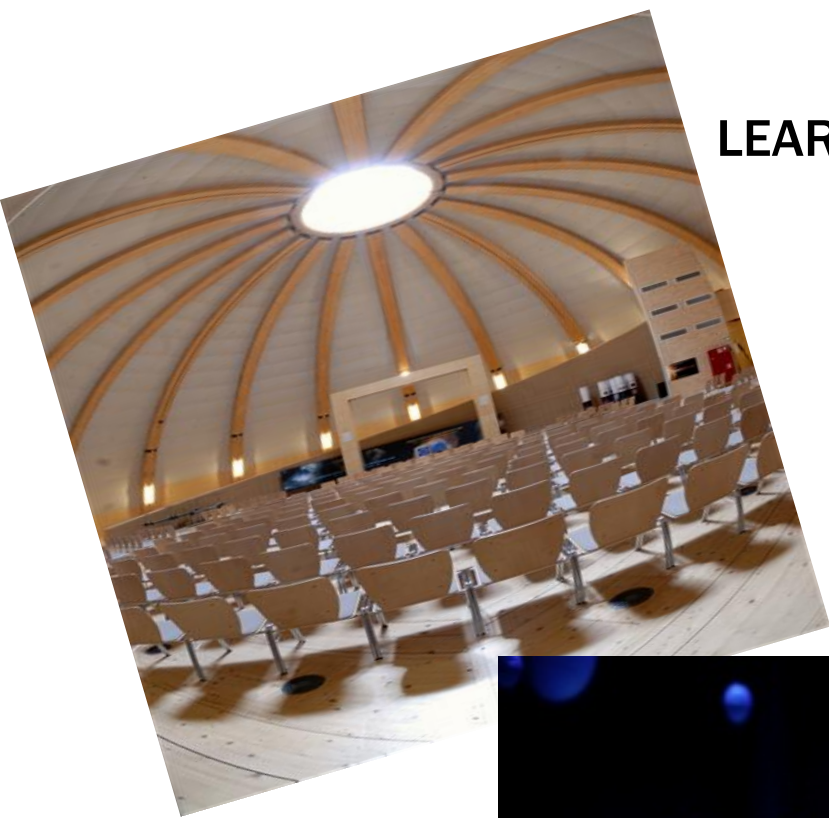


A MONOLITHIC DOME IN A CORNFIELD





LEARNING SPACES



DAKOTA STATE UNIVERSITY CAMPUS



POTENTIAL SATELLITE SITES



ANYWHERE IN THE WORLD

WHAT WE NEED FROM YOU

CREATIVE SUPPORT

PARTNERSHIP OPPORTUNITIES

INFRASTRUCTURE/FACILITIES

FUNDING RESOURCES

ADDITIONAL CONTACTS

FEEDBACK

YOUR IDEAS



CONTACT INFORMATION

Marc Weber Tobias

mwtobias@security.org

Tommie R. Blackwell

tnonnie7@yahoo.com or tommie@creativecynergy.com

Kevin Mason

wmd000wmd@gmail.com