Drones, Digits and Dollar$; Intelligence Analytics in the Age of Cyber

University of Alabama at Birmingham
John Grimes
Director of Intelligence Analytics

July 31, 2012
Undertake Information Assurance-based research, development, and outreach to help ensure a safer, more productive world.


Offer practical computer science and justice science research, scholarship, services, and products that enhance the integrity of the global cyber-infrastructure while educating the next-generation of cyber professionals.

Targeted end state?

Is Information Assurance Enough?
Developed from Interdisciplinary Partnership begun in 2006 between UAB Departments of Computer and Information Sciences and Justice Sciences

2011-2012: Interdisciplinary, campus-wide research center

- Basic and applied research
- Workforce training and development
- Service to the community

Key Center Pillars

- Cybercrime
- Forensic Science (including “wet” and “digital” forensics)
- Health Informatics
- **Intelligence Analytics**
- Information Systems and Assurance
- Education, Training and Work Force Development/Placement
Cybercrime/Digital Forensics

- UAB Spam Data Mine supports investigations for many organizations

Logos of companies and organizations including Facebook, Microsoft, UPS, Bank of America, NASA, FDIC, BBVA, Regions, Google, LinkedIn, Twitter, NACHA, Internal Revenue Service, Yahoo, and Alabama Bureau of Investigation.
UAB undergraduate & graduate students are highly sought after by both industry and government organizations, with many placed in cyber security positions with top companies like e-Bay, Microsoft, PayPal, Google, and with the FBI, the State Department, the CIA, and other government organizations.

Student Internships include:

UAB has placed students in a number of local, state, and federal agencies:

**Federal Agencies:**
- Naval Criminal Investigation Service (NCIS)
- U.S. Postal Inspectors
- U.S. Probation
- Secret Service
- U.S. Marshall’s Service
- F.B.I.
- U.S. Army
- Federal Defenders, Middle District of Alabama

**State and Local Agencies:**
- Jefferson County Sheriff’s Department
- Cullman Police Department
- Birmingham Police Department
- Hoover Police Department
- UAB Police
- Homewood Police
- Cullman Police Department
- Birmingham Police Department
- Hoover Police Department
- Adamsville Police
- Homewood Police
- Shelby County Sheriff’s Department
- Alabama Department of Public Safety
- Alabama Bureau of Investigation
Class 5-92
One Shot - One Kill
Seminal Premise Supporting the Value of Adaptive Application of Intelligence Community Analytical Methodologies:

The Intelligence Community does not make decisions for the Customer/Client/Commander/Decision Maker but empowers them to achieve decision-advantage over adversaries by enhancing clients’:

1. Understanding of contextual factors in the decision making environment;

2. Anticipating and war gaming first, second, third order, etc., effects of courses of action under consideration (thus shaping one’s informed destiny - vice becoming victimized by it); and

3. Avoiding the unforeseeable and oftentimes unfortunate cascading consequences resulting from decision making in a vacuum of analyzed relevant information.

“Why, you might ask?”
Operational Cyber Security (Information Assurance) resides at the confluence.
Imagine the potential for order of magnitude advancement to Cyber Knowledge Dominance providing true Decision Advantage via Cyber Intelligence Integration!
Demonstrative IC Analytic Tool for Threat & Consequence Mitigation

Critical Action Model as Supported by IC Methodologies
CIA|JFR Traditional Key R&D Areas

- Information Assurance
- Classic Forensics
- Digital Forensics
- Cloud Security
- Small/Mobile Device Security
- Health Informatics
- Image Analysis
- Natural Language Processing
- Big Data/CIS Research
The Threat Mosaic and Metrics

Adversary “Net Assessment”

Psychology
- Intent
- Region of Most Likely Behaviors

Culture
- Values & Beliefs

Organizations & Institutions
- Capabilities

Opportunity
- Pol-Mil-Econ, Social, Location, Timing

Behavioral Preference/Choice (ECOA)
R&D: An Evolving New IC Model for RoE; (The “Lighter Footprint” Approach)

Critical Response Model as Supported by Intelligence Analytics
Penetrates the guards, gates and guns (ASIS-like) purely kinetic defense-in-depth “feel good” strategies…

Reduces if not eliminates cognitive empathy for victims...

Feeds and fuels emotional appetite for situational dominance and empowerment...

Inspires gambling against the odds and false beliefs of
- Anonymity…
- Indestructibility…

**Is Information Assurance Enough?**
Penetrates the guards, gates and guns (*Parens Patriae*-like) purely kinetic defense-in-depth “feel good” strategies…

- Reduces if not eliminates cognitive empathy for victims...

- Feeds and fuels emotional appetite for situational dominance and empowerment...

- Inspires gambling against the odds and false beliefs of
  - Anonymity…
  - Indestructibility…
  - Addiction denial…

*Is Information Assurance Enough?*
MISTAKES

It could be that the purpose of your life is only to serve as a warning to others.
By Dana Priest and Barton Gellman
The Washington Post

Deep inside the forbidden zone at the U.S.-occupied Bagram air base in Afghanistan, around the corner from the detention center and beyond the segregated clandestine military units, sits a cluster of metal shipping containers protected by a triple layer of concertina wire.

The containers hold the most valuable prizes in the war on terrorism — captured al-Qaeda operatives and Taliban commanders.

Some who refuse to cooperate inside this secret CIA interrogation center are sometimes kept standing or kneeling for hours, in black hoods or spray-painted goggles, according to intelligence specialists familiar with CIA interrogation methods.

Those who cooperate are rewarded with creature comforts. Some who do not cooperate are turned over — “rendered,” in official parlance — to foreign intelligence services whose practice of torture has been documented.

U.S. officials have said little publicly about the captives, and virtually nothing about interrogation methods. But interviews with several former intelligence officials and 10 current U.S. national security officials provide insight into how the U.S. government is prosecuting this part of the war.

The picture that emerges is of a brass-knuckled quest for information, often in concert with allies of dubious human rights reputation, in which the traditional lines between right and wrong, legal and inhumane, are evolving and blurred.

While the U.S. government publicly denounces the use of torture, each of the current national security officials interviewed for this article defended the use of violence against captives as just and necessary. They expressed confidence that the American public would back their view. The CIA, which has primary responsibility for interrogations, declined to comment.

The off-limits patch of ground at Bagram is one of a number of secret detention centers overseas where U.S. due process does not apply, according to several U.S. and European national security officials, where the CIA undertakes or manages the interrogation of suspected terrorists.

U.S. officials oversee most of the interrogations, especially those of the most senior captives.

In some cases, CIA officers question captives through interpreters. Sometimes, female officers conduct interrogations, a psychologically jarring experience for men from a Muslim culture.

According to U.S. officials, nearly 3,000 suspected al-Qaeda members and their supporters have been detained worldwide since Sept. 11, 2001. Some officials estimated that fewer than 100 captives have been rendered to third countries, the officials said.

At a Sept. 26 joint hearing of the House and Senate intelligence committees, Cofrer Black, then head of the CIA Counterterrorist Center, spoke cryptically about the agency's new forms of "operational flexibility" in dealing with suspected terrorists.

"This is a very highly classified area, but I have to say that all you need to know: There was a before 9/11, and there was an after 9/11," Black said.

"After 9/11, the gloves come off."

U.S. National Security Council spokesman Sean McCormack declined to comment last week on CIA or intelligence-related matters. But, he said: "The United States is treating enemy combatants in U.S. government control, wherever held, humanely and in a manner consistent with the principles of the Third Geneva Convention of 1949."

The convention outlined the standards for treatment of prisoners of war. Suspected terrorists in CIA hands have not been accorded POW status.
In Summary…

Intelligence Analytics’ Bottom Line:

Center’s Value Added Mission to the Decision Maker:

1. Provide *Fusion* of all relevant information *without* compromise of *Sources* and *Methods*;

2. Through application of *analytical capabilities* that the *Center* is uniquely positioned to (1) *assemble*, (2) *task-organize* and (3) *leverage* by virtue of its placement & access to University research assets and resources; and

3. That answers a critical *information gap* or need as *perceived* by the *Customer/Client/Commander/Decision Maker* thus providing them, progressively, *information assurance, knowledge dominance* and ultimately *decision-advantage* over their adversaries in the successful accomplishment of goals, objectives and/or mission.
John W. Grimes, JD
Director of Intelligence Analytics & Assistant Professor
Department of Justice Sciences &
Center for Information Assurance and Joint Forensics
Research*
* National Security Agency & Department of Homeland Security
credentialed National Center of Academic Excellence in Information
Assurance Research (CAE-R)

210 University Boulevard Office Building
1201 University Boulevard
Birmingham, AL 35294

205.934.8509 (campus)
205.329.9112 (bb)

jwgrimes@uab.edu

http://blog.al.com/businessnews/2012/04/on_the_record_john_grimes_inte.html
http://thecenter.uab.edu/