“Back to the Future”

John P. Casciano
Senior VP and Group Manager
Enterprise Security Solutions
August 7, 2003

SAIC
An Employee-Owned Company

What We'll Discuss

- The changing face of the threats and vulnerabilities that face us
- A look at Nebraska, Omaha, and Offutt Air Force Base and their roles in the Information Age
- The need for "synergy" in the virtual environment of the Information Age

Threats and Vulnerabilities

- The International Political System is Changing
- Cold War
  - Superpower Competition
  - Bi-Polar Environment
  - Competing Economic and Ideological Systems
  - Deterrence
- Today
  - One Superpower: how relevant?
  - Multi-player Environment
  - Competing Ways of Life; economic basis
  - Deterrence probably Irrelevant

Threats and Vulnerabilities

- "First, Second and Third Waves"
  - Agrarian
  - Industrial
  - Information
- Differing means and centers of gravity for each
  - First: Land and Food
  - Second: People and the Means of Production
  - Third: Information and the Economy that it enables
- Inevitable overlap
- The people at this conference are key players
  - Whether we like it or not!

Threats

- Outsiders and Insiders
  - Mischief and Embarrassment
  - Threat to Enterprises
- Nation-states
  - Offense, Defense, and Exploitation
  - Military and Intelligence Services
- Groups with a “mission” or “cause”
  - Low cost of entry
  - Advantage with the offense
  - Foreign and Domestic

Vulnerabilities

- Well-known problems – Inadequate solutions
- Time to Market versus Security
- Return on Investment considerations
- People – Process –Technology balance
- The Virtuality of the Global Enterprise
- The “proper” role of government?

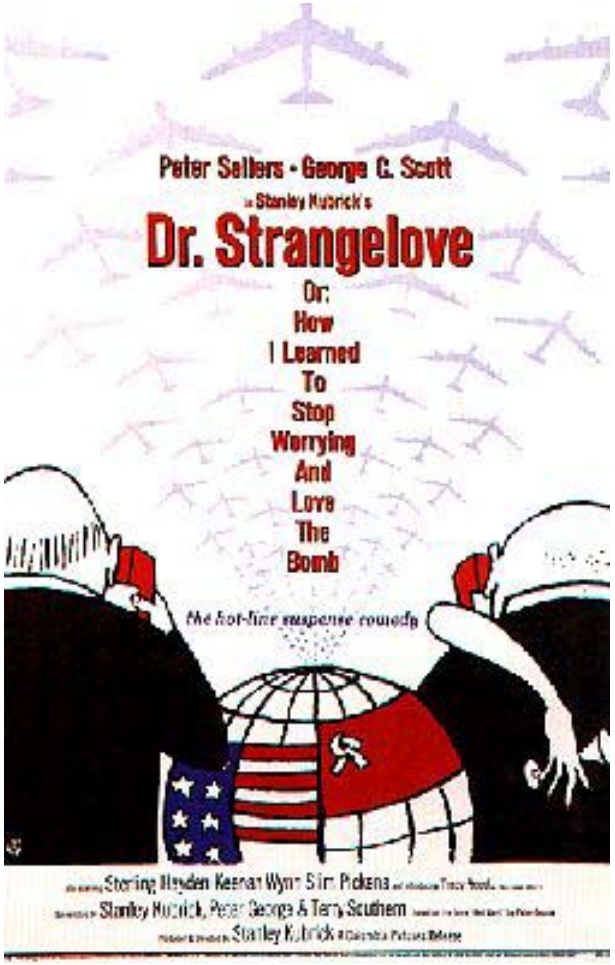
Threats and Vulnerabilities

"Seeing through a glass darkly"

- Military
- Government
- Private Sector

Nebraska, Omaha, and Offutt


HEADQUARTERS STRATEGIC AIR COMMAND
Peace
IS OUR
PROFESSION


Peter Sellers • George C. Scott
in Stanley Kubrick's
Dr. Strangelove
Or:
How
I Learned
To
Stop
Worrying
And
Love
The
Bomb
the hot-line suspense comedy
Stanley Kubrick, Peter George & Terry Southern
Stanley Kubrick


STRANGELOVE
OR:
HOW I
LEARNED
TO STOP
WORRYING
AND
LOVE THE
BOMB


THE RED PHONE...
HIS MISTRESS...HER RIVAL...
HURLING HIM TO THE EDGE OF SPACE... FREEZING HER LOVE ON THE EDGE OF TIME!!
ROCK HUDSON
A GATHERING OF EAGLES
Eastman COLOR
ROD TAYLOR · MARY PEACH · BARRY SULLIVAN

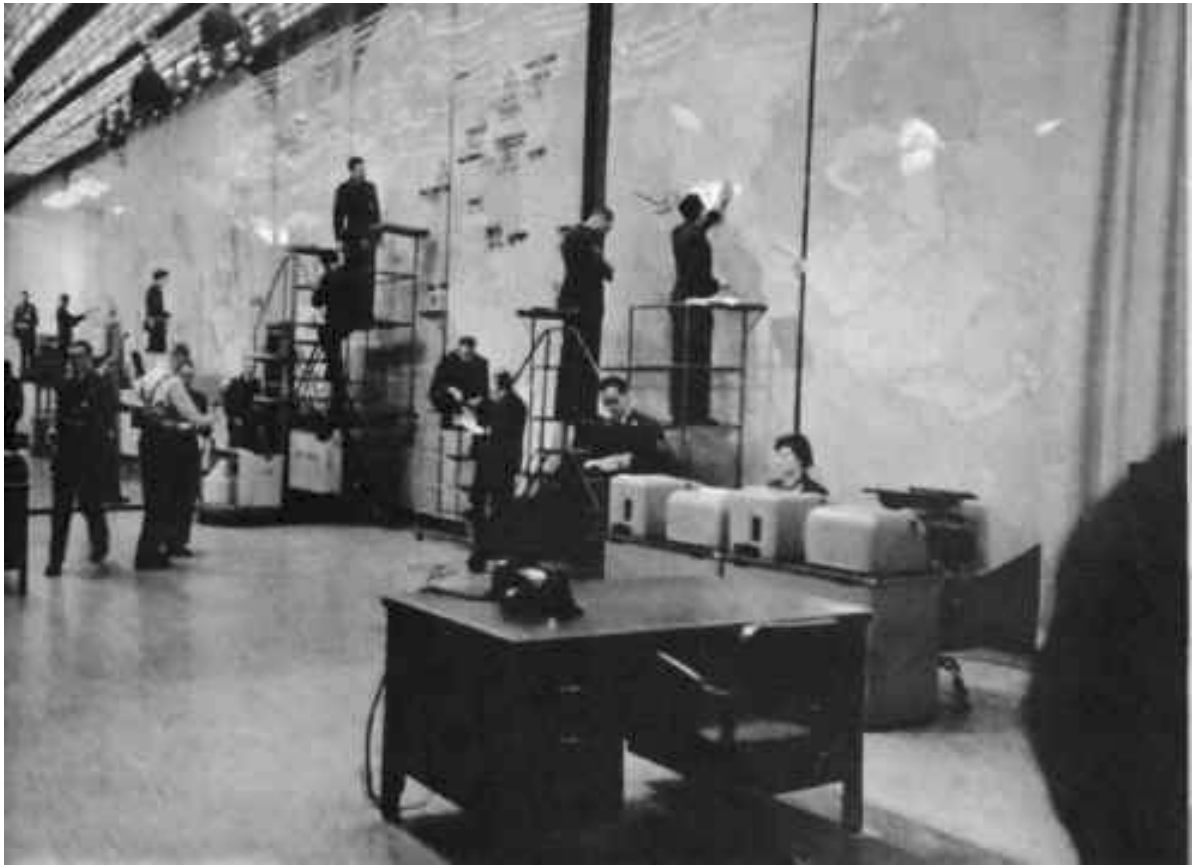

Bombs Away!
U. S.
AIR FORCE

Nebraska, Omaha, and Offutt

- Central Role during Cold War
  - Location
  - Infrastructure
  - Local Support
- Global Capabilities
  - Strategic Weapons
  - Intelligence, Surveillance and Reconnaissance
  - Command and Control
  - Communications
- A culture and an approach
  - Worldwide perspective
  - Understanding of “synergy”
  - Jointness

But It Didn't Just Happen!

- Followed a typical American approach
  - More weapons than targets
  - Cottage Industries
  - Disassociated planning
  - Waste and inefficiency
  - Politics
- Eventually, we found our way
  - SAC: 1946
  - Joint Strategic Target Planning Staff: 1961
  - Joint Strategic Connectivity Staff: 1980
- A steady evolution to figure it out



The Historical Analogy

- Nebraska, Omaha, and Offutt once again called to address 21st Century/Information Age/Third Wave threats and vulnerabilities
- United States Strategic Command: 1992
  - A culture and an approach
    - Worldwide perspective
    - Understanding of "synergy"
    - Jointness
- New Missions: 2002
  - Computer Network Operations (CNO)
  - Information Operations
- Gain, Exploit, Defend, Attack

The Historical Analogy

- Following a typical American approach
  - More weapons than targets
  - Cottage Industries
  - Disassociated planning
  - Waste and inefficiency
  - Politics
- Eventually, we will find our way
- Admiral Ellis, General Goslin
  - Right People
  - Right Place
  - Right Time
- But this is only part of the equation

CyberSecurity Since 9-11

- Generally, more focus on physical effects of terrorism
  - Protection
  - Recovery
  - Reconstitution
- Government re-emphasis of CyberSecurity
  - GAO, OMB, and Congressional prodding
- Commercial sector treading water
  - Greatly impacted by economic slowdown
  - A search for converged physical and cyber solutions
- The Patriot Act … new/evolving powers
- **Role of the Department of Homeland Security**
  - Evolution of the "National Strategy"
  - Federal outreach … consensus building

Why Haven't Things Gotten Better Since 9-11?

- We are learning more about cyber threats and vulnerabilities
  - BUT, the "bar" keeps rising
- CyberSecurity is still not a priority for the "masses"
- Impacts are not understood, and potential threat is not believed … high "geek" factor
- Responsibility and accountability are diffuse
- Nothing really bad has happened yet--no deaths from a cyber attack
- CyberSecurity does not compete well for budget if the tradeoff is functionality

The National Strategy to Secure Cyber Space

- Thoughtful, well-conceived *consensus* document … but that's OK!
- A "Living Document"
  - Work in Progress
  - Sound familiar?
- CyberSecurity is not unlike other problems we have faced
  - "Bubbling up out of the Primordial Soup"
- Federal Government appears to be stepping up
  - Leadership and dollars
- State/Local will continue to have cash challenges
  - Need Federal help
- Civil/Industry Partnership will be a tedious, evolutionary process
  - Trust issues affect information sharing … Industry – Government and within Industries
  - Effect of Laws

Overview: The National Strategy to Secure Cyber Space

- A Case for Action: Threats and Vulnerabilities
- National Policy and Guiding Principles
- Highlights
  - Home User and Small Business
  - Large Enterprises
  - Critical Sectors
    - Federal
    - State and Local
    - Higher Education
    - Private Sector
  - National Priorities
  - Global
- Recommendations

The National Strategy to Secure Cyber Space: Threats and Vulnerabilities

- Recap of the "who," the "what," and the "what's possibly next"
- Themes
  - Increasing numbers, sophistication, severity, and cost
  - Economy is dependent on Cyber Space
    - A case for corporate investment?
  - A "Digital Disaster" a day … cascading effects
  - An ounce of prevention will reduce risks
  - It can be worse in the future
  - Need public-private partnership
  - Everyone must help secure Cyber Space
    - People, process, technology

The National Strategy to Secure Cyber Space: National Policy

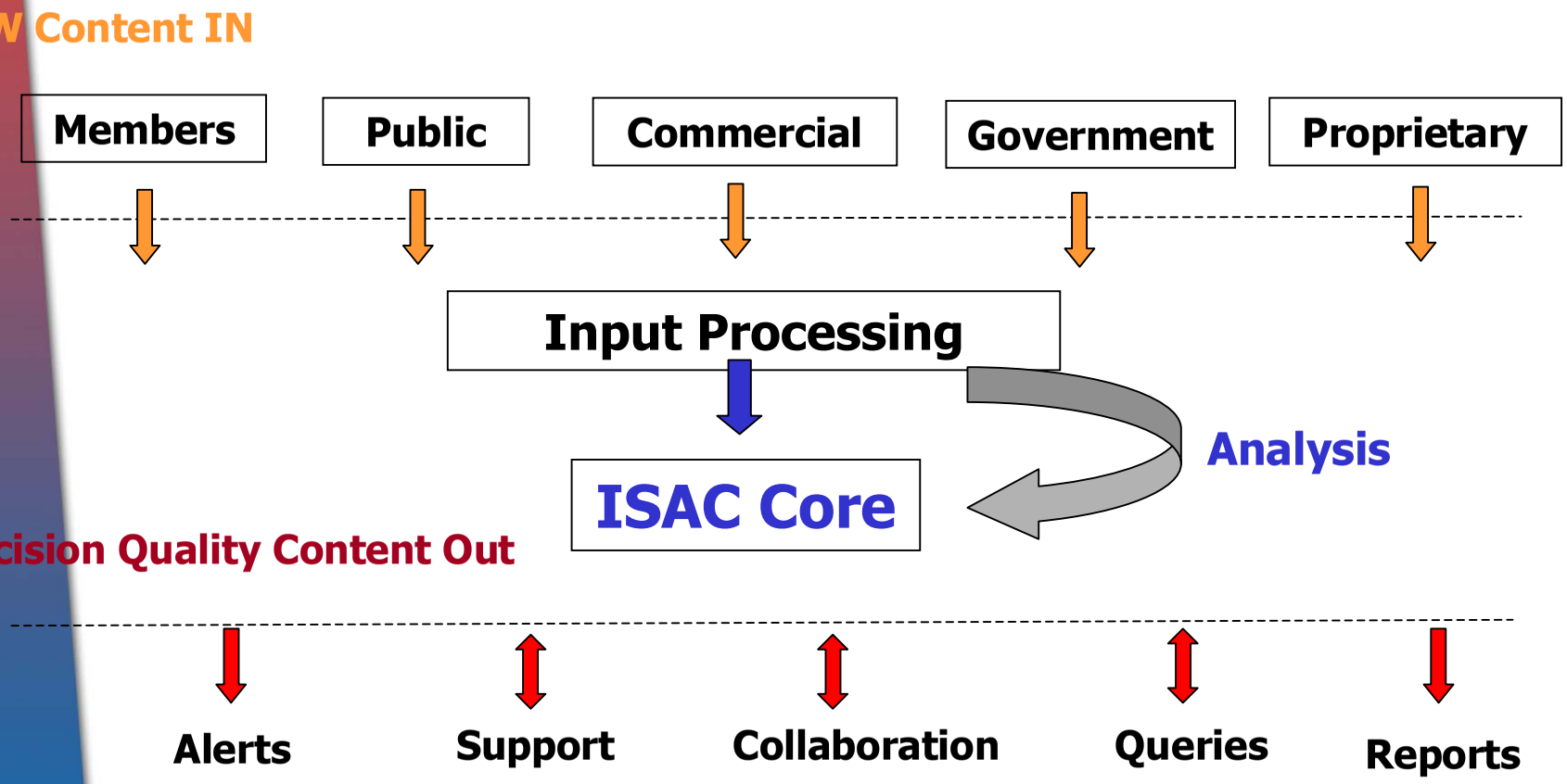
- The Federal government will perform key HLS and national security missions, and ensure the public health and safety
- State and Local governments will maintain order and deliver essential public services
- The Private Sector will ensure the orderly functioning of the economy and the delivery of essential infrastructure services

The National Strategy to Secure Cyber Space: Guiding Principles

- Embrace Public-Private Partnerships
- Avoid Regulation
- Safeguard Civil Liberties and Privacy
- Coordinate with Congress
- Cooperate with State and Local Governments
- Secure the parts of Cyber Space to achieve security of the whole
- Rapidly evolve security measures to stay ahead of changing technology/vulnerabilities
  - Can the “Defense” stay ahead of the “Offense?”
- Use the acquisition power of the federal government to prod industry on security

Some ISAC Examples

Information Sharing and Analysis (ISAC) Framework



Recent Events and Current Threats

- Slammer
  - Fastest spreading worm to date
  - Damage without malicious payload
  - 6 month old vulnerability
  - Implications...
- Bugbear B
- Lots of “Noise” in the last few weeks
- Heightened Terror Alert
- War with Iraq
  - State- and terrorist-sponsored cyber-attacks?
  - “Virtual Coalitions” of those opposed?
  - Individuals?

Prudent Steps for Security Managers to Take

- Place and keep on CEO agenda
- Reaffirm authorities and responsibilities
- Reinforce CyberSecurity Policies … all employees
- Check for known vulnerabilities
- Triage and implement patches
- Keep IDS and Antivirus applications current
- Review/update emergency and recovery plans
- Identify and plan for “calling in the Reserves”
- War-game and exercise defensive capabilities
- Monitor cyber and other intelligence sources
- Check “comms”

In Summary

- No alarms … but, conceivable multiple-attack scenarios against U.S. critical infrastructures--commercial and government targets:
  - Physical and cyber attacks combined and sequenced for maximum impacts
    - Human--public health/emergency services
    - Economic--threats to jobs and globalization
- Continuity of government operations - and our economic health - at risk if information infrastructures degrade seriously or fail:
  - The events on 9/11 revealed the extent that the U.S. depends on government at all levels for reassurance and support
  - Government services closest to people often have most vulnerable information infrastructures
  - Ability to make effective response, project U.S. forces, and support law enforcement could be jeopardized
  - Potential for loss or misuse of critical government resources

Challenges

- Coping with the "Third Wave"
  - National Security = Economic Security + Way of Life
  - Privacy Issues
- Tying the pieces together: Private – Public Partnership
  - Military
  - Civil: Federal, State, Local
  - Private Sector
- Time as the enemy
  - Awareness
  - Money: Public Funding
  - Commitment

Questions/Comments?