U.S. Department of Defense Information Assurance

Colonel Gene Tyler
Director, Defense-wide Information Assurance Program
Office of the Assistant Secretary of Defense,
Networks and Information Integration
Gene.Tyler@osd.mil
703-602-9988

Information Assurance (IA)

- IA (U.S. Definition)

  Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities.

  Protect - Provides for the availability, integrity, authenticity, confidentiality, and non-repudiation of information or transactions

  Detect - Provides for the ability to detect efforts to disrupt and deny services

  React - Provides for reconstitution of information and services in case of a successful disruption or denial

Definitions

- **Availability** - Information and information systems are available when needed to support mission critical, mission support, and administrative purposes.
- **Integrity** - Data is unchanged from its source--has not been accidentally or maliciously altered.
- **Authentication** - Data, and their originators, are authentic, and that a recipient is eligible to receive specific categories of information
- **Non-Repudiation** - Strong and substantial evidence of an information exchange or transaction.
- **Confidentiality** - Information can be read only by authorized entities e.g. encryption

Information Assurance – Emphasis Starts at the Top

SECDEF’s Transformational Goals*:

- First, to defend the U.S. homeland and other bases of operations, and defeat nuclear, biological and chemical weapons and their means of delivery;
- Second, to deny enemies sanctuary—depriving them of the ability to run or hide—anytime, anywhere.
- Third, to project and sustain forces in distant theaters in the face of access denial threats;
- Fourth, to conduct effective operations in space;
- Fifth, to conduct effective information operations; and,
- Sixth, to leverage information technology to give our joint forces a common operational picture.

> ***“….Protect our information networks from attack”...***
>
> ***...Use information technology to link up different kinds of US forces so that they can in fact fight jointly...”***

*** From Secretary Rumfeld’s speech to the National Defense University 21 Jan 2002**

Information Assurance – Senior Leadership Emphasis

Our ability to leverage the power of information will be key to our success in the 21st Century. I am committed to:

- **Make information *available* on a network that people depend on *and trust***

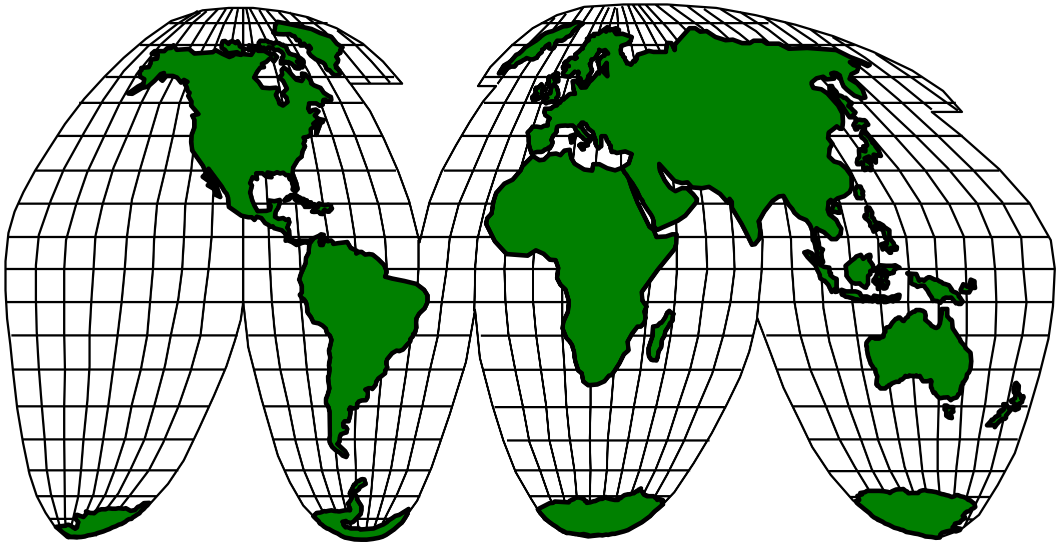
- **Populate the network with new, dynamic sources of information to defeat the enemy**

- ***Deny the enemy information advantages* and exploit weakness to support Network Centric Warfare and the transformation of DoD business processes.**

John P. Stenbit
ASD(NII)

Information Security & Global Networks

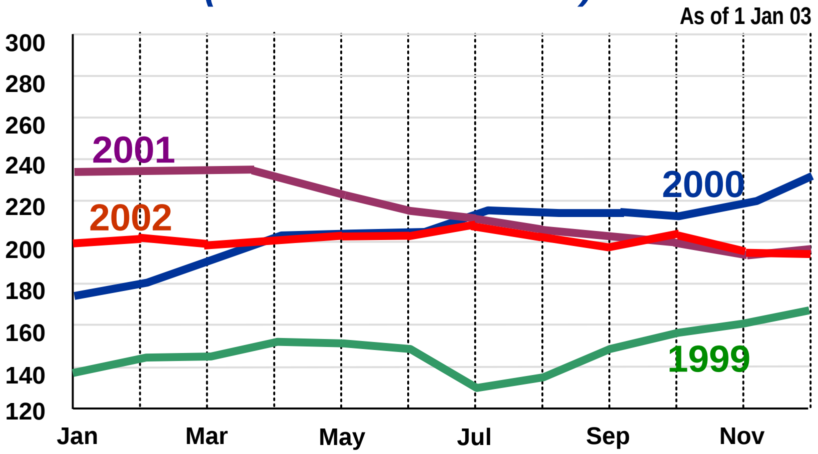
- Global Economy
- Global Information Environment
- Electronic Security Must Be Global
- U.S. Cannot “Solve” Problem Unilaterally
- International Cooperation Required



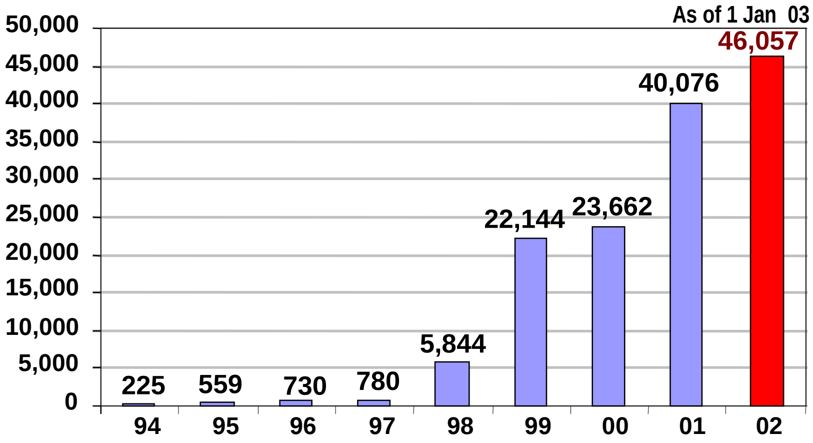
Think Global!

Malicious Activity Continues to Climb

Virus Growth Per Month
(Internet - "Wild List")

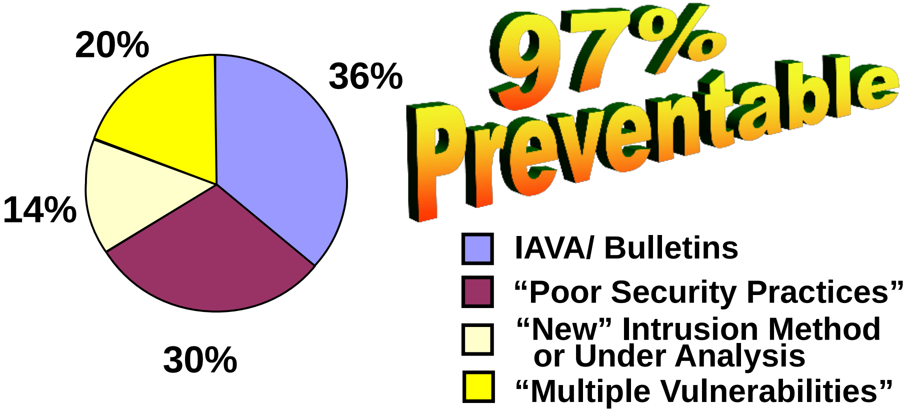


Detected "Events"



> *"Information Networks must be controlled, protected, and managed as effectively as weapon systems"*
>
> *Lt Gen Harry D. Raduege, DISA Director*

Unauthorized DoD Intrusions
(314 Category 1 & 2 Intrusions as of 1 Jan 03)

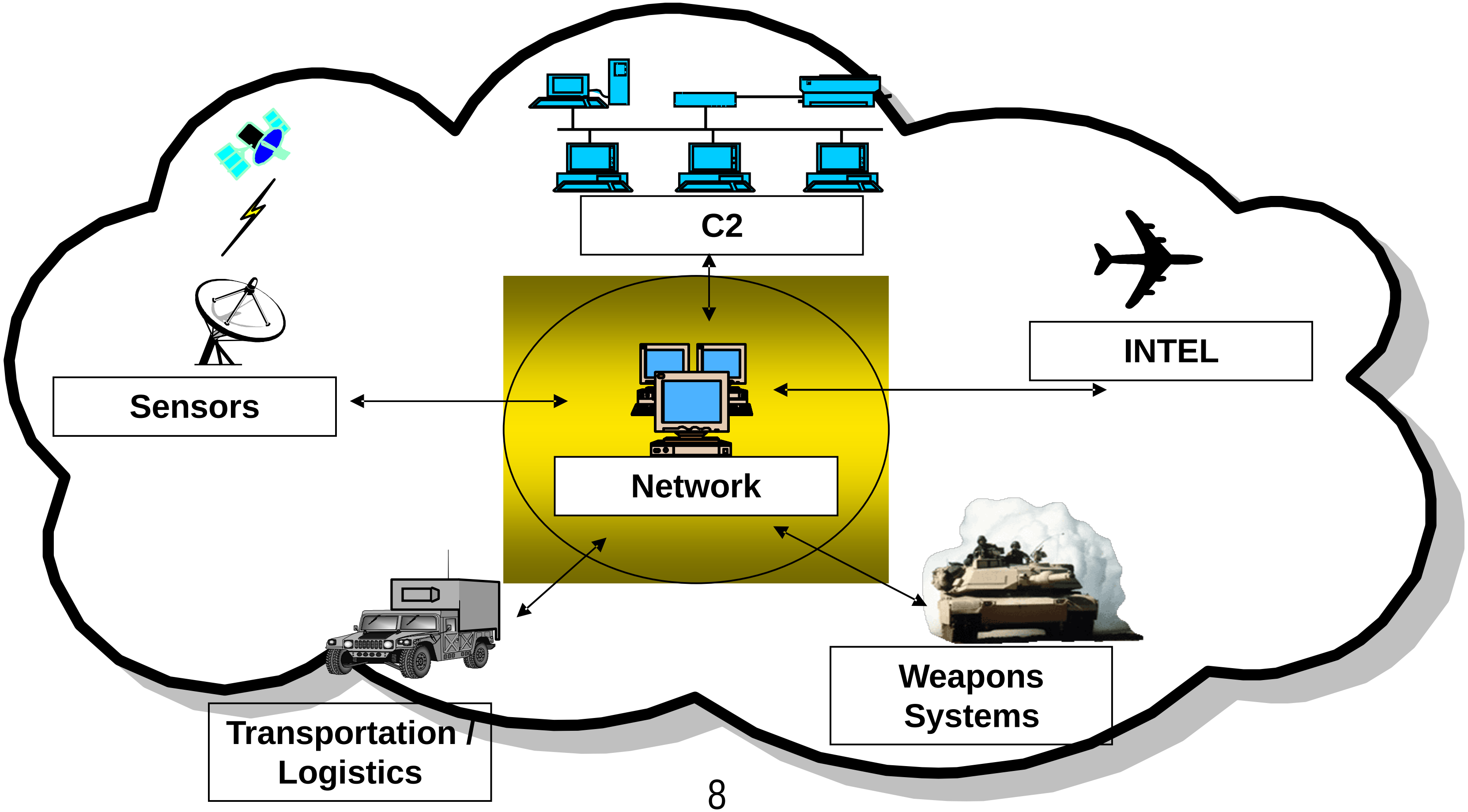


Net-Centric Warfare

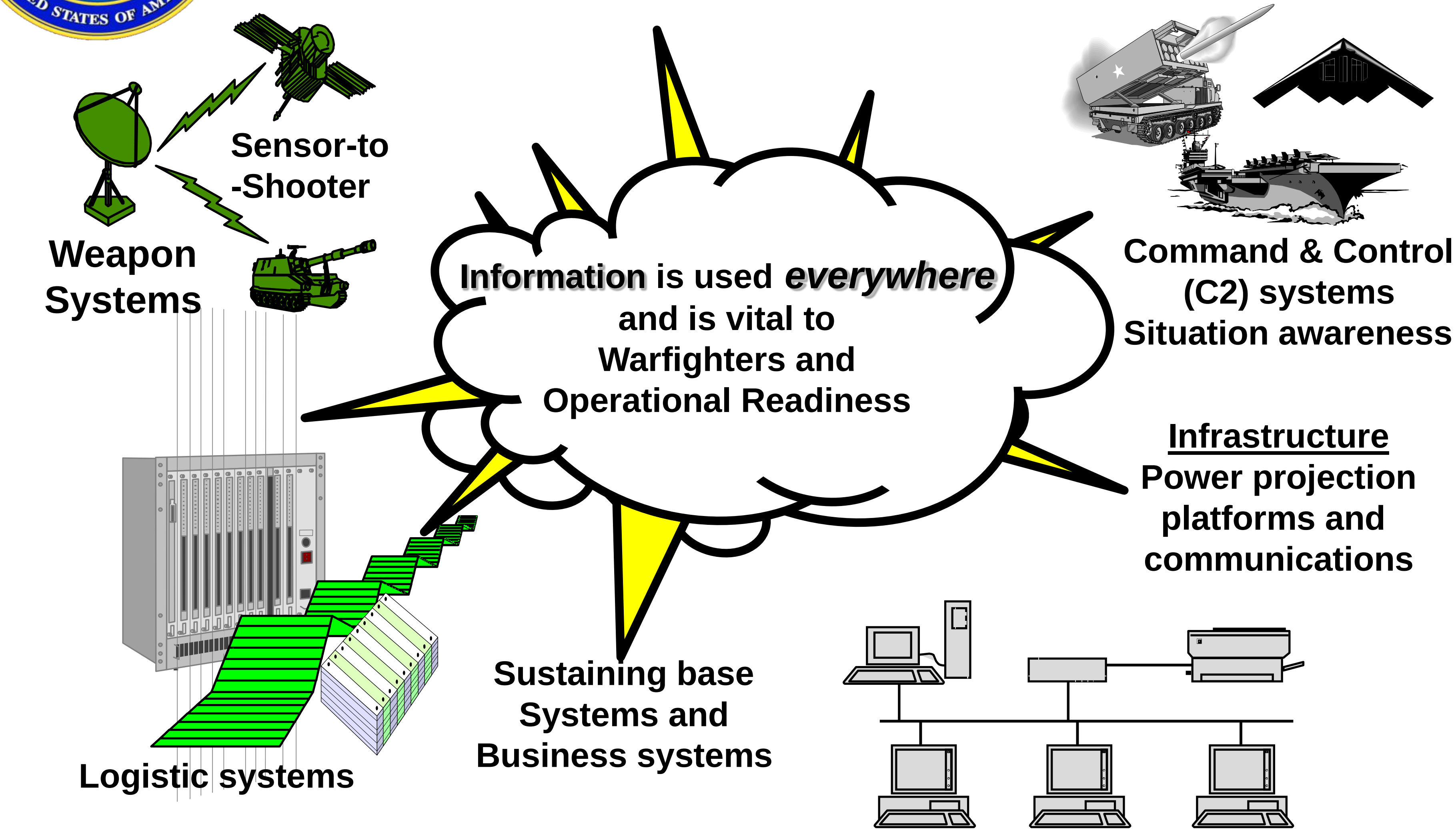
In NCW, the Network is the

center of gravity:

the focus on which all elements of combat power depend



Scope of the IA Mission



Information is used *everywhere* and is vital to Warfighters and Operational Readiness

Weapon Systems

Sensor-to -Shooter

Command & Control (C2) systems
Situation awareness

<u>Infrastructure</u>
Power projection platforms and communications

Sustaining base Systems and Business systems

Logistic systems

The Changing Technology Environment

- PAST
  - dedicated circuits
  - stovepiped systems
  - government developed

    and produced solutions
  - “risk avoidance”
  - limited cooperation with industry
  - government-owned and
  - controlled security mgt infrastructure (SMI)

- PRESENT
  - highly interconnected
  - interdependent
  - commercial technology forms the basis for solutions
  - “risk management”
  - full and open cooperation with industry
  - global interoperable public key-based SMI

- FUTURE
  - genetic algorithms
  - neural networks
  - intelligent agents
  - nano-technologies
  - distributed computing
  - wireless
  - changing architectures, operations, technology all aimed at leveraging the “richness and reach” of the internet
  - where are the boundaries?

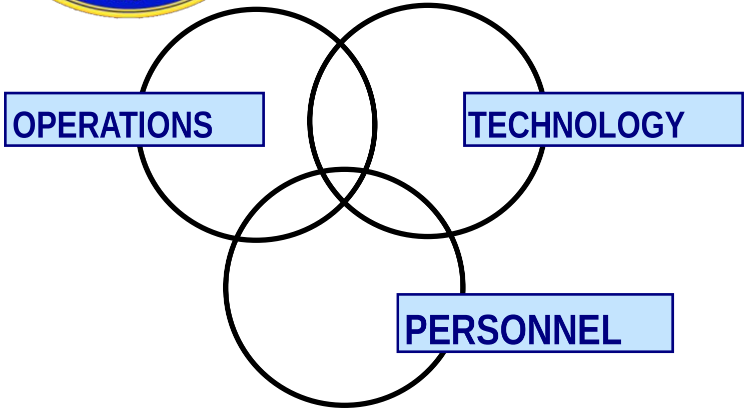
We cannot afford to “stay the course”

IA Mission and Strategy

IA Mission: Assure DoD's Information, Information Systems and Information Infrastructure and Support DoD's Transformation to Network and Data Centric Operations and Warfare

Goals	Protect Information	Defend Systems & Networks	Provide Situational Awareness / IA C2	Transform and Enable IA Capabilities	Create an IA Empowered Workforce
Objectives	Promulgate IA Architecture	Establish GiG Network Defense Architecture & To Be Baseline	Establish timely Intelligence and I&W information to enterprise SA	Ensure IA is integrated & sustained in all programs throughout the lifecycle	Standardize baseline certifications
	Define Protection Criteria for Netcentric Opns	Develop & Enforce CND Policies	Create SA Visualization capabilities	Improve strategic decision making	Provide trained/skilled personnel
	Develop & Deploy Protection Capabilities	Evaluate & Deploy CND Tools and Capabilities	Coordinate IA ops & decisions	Expedite dynamic IA capabilities through innovation	Enhance IA skill levels
	Transform SMI	Establish vertical & horizontal defense mechanisms w/I CND RAF	Harmonize NETOPS, IO, CNA, CND relationships	Enable Information sharing & collaboration	Infuse IA into other disciplines

The DoD IA Strategy



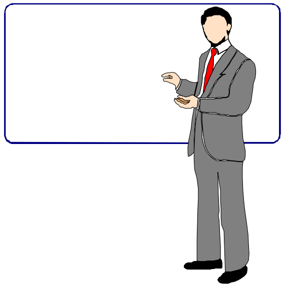
No Single Solution!

- Solution requires a multidimensional approach
  - Trained and disciplined personnel
  - Improved operations (including updated policies)
  - Innovations in technology
- Solutions must address importance of Information Technology in elements of the Critical Infrastructure, for example, Power, Transportation, other

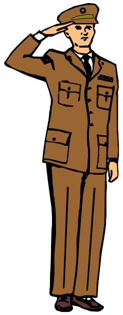
I WANT YOU
for INFORMATION
ASSURANCE

BACKUP

Personnel



- Cyber security training and awareness
  - Platform Training
  - Computer Based Training (CBT)
  - Video
- Certification of information system operators, administrators, and maintainers



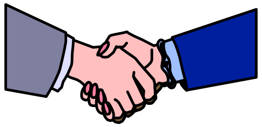
- Career field management - focus on retention
- Partnership with industry for cooperative internships
- National InfoSec Education & Training Program
- Academic Centers Of Excellence (36 today)

Operations

- Integrated Information Assurance Policy
- Information Assurance Vulnerability Alert (IAVA) Process
  - Positive Control
- Service and Agency Computer Emergency Response Teams
- Joint Task Force - Computer Network Operations (JTF-CNO)
  - Coordination within the Department of Defense, and with other government departments and agencies
- Continuous Vulnerability Analysis and Assessment Program
- Exercises to test protection, detection, and response capabilities

Technology

- Full spectrum Information Assurance solutions
  - Layered Information Assurance strategy (Defense-in-Depth)
  - Deployment of intrusion detection technology
  - Strategic partnership with industry
    - Security-enabled commercial products
    - Open security framework
  - National Information Assurance Partnership (NIAP)
    - Common Criteria evaluations



- Global, <u>interoperable</u> Security Management Infrastructure
- R&D for *highly assured* products and systems
- R&D for real-time monitoring, data collection, analysis, and visualization

IA Strategy and Defense-in-Depth (DiD) Interface

Defense-in-Depth: Establishes our defenses in place and gives DoD a basic defensive framework

IA Strategy: Takes concepts of DiD and brings the warfighter into the IA arena