



Strategic Thought in Virtual Deterrence and Real Offense: The Computer's Role

by Wanja Eric Naef & Sam Nitzberg

www.iwar.org.uk

& www.iamsam.com / www.NitzbergSecurityAssociates.com

INTRODUCTION

- basics -



Strategy



- Chinese Warrior – Philosophers
- Prisoner's Dilemma Problem
- Mutually Assured Destruction
- Asymmetric Warfare Considerations

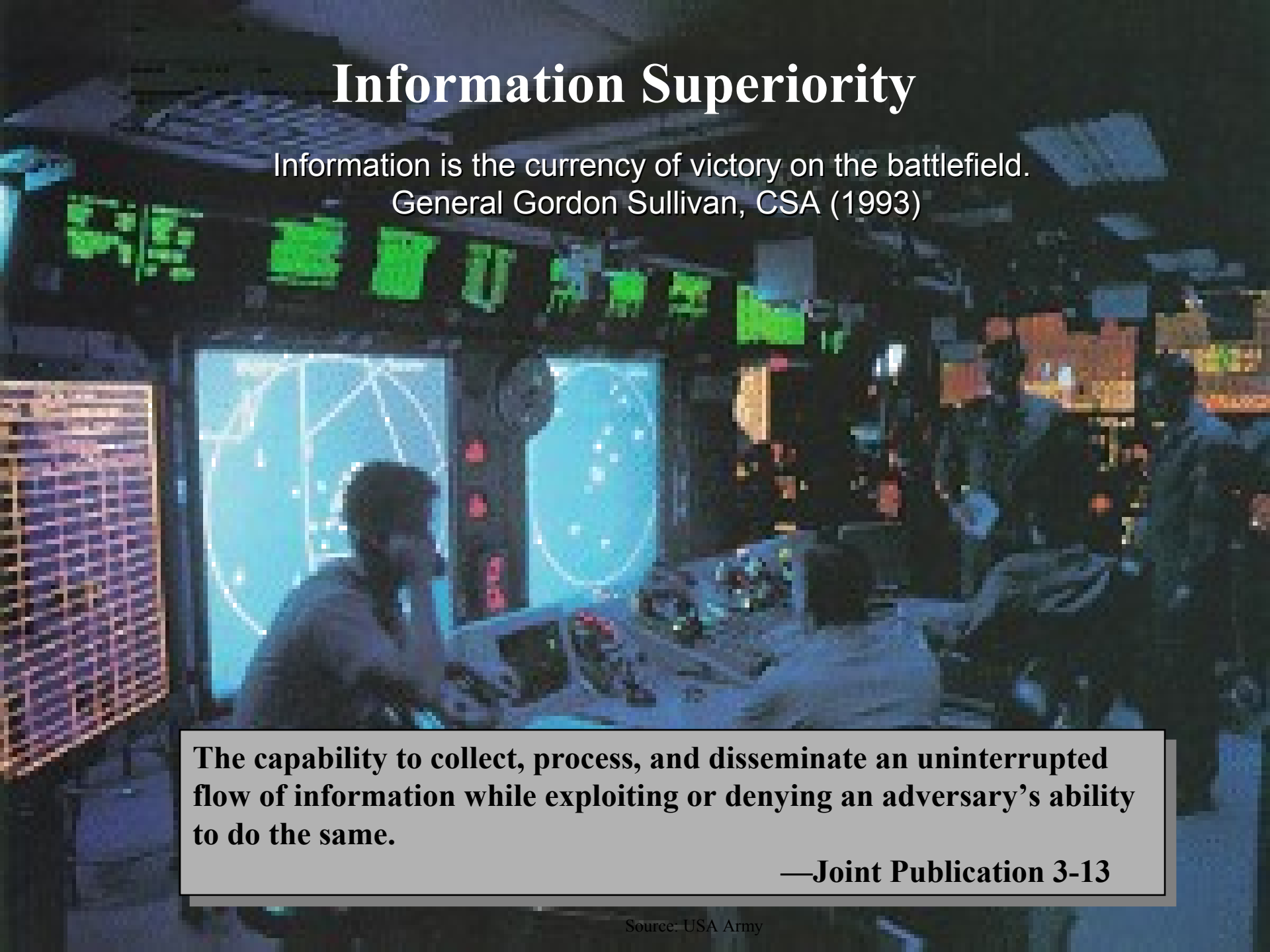
Network Centric Operations

The Real Impact of the Technology



Information Superiority

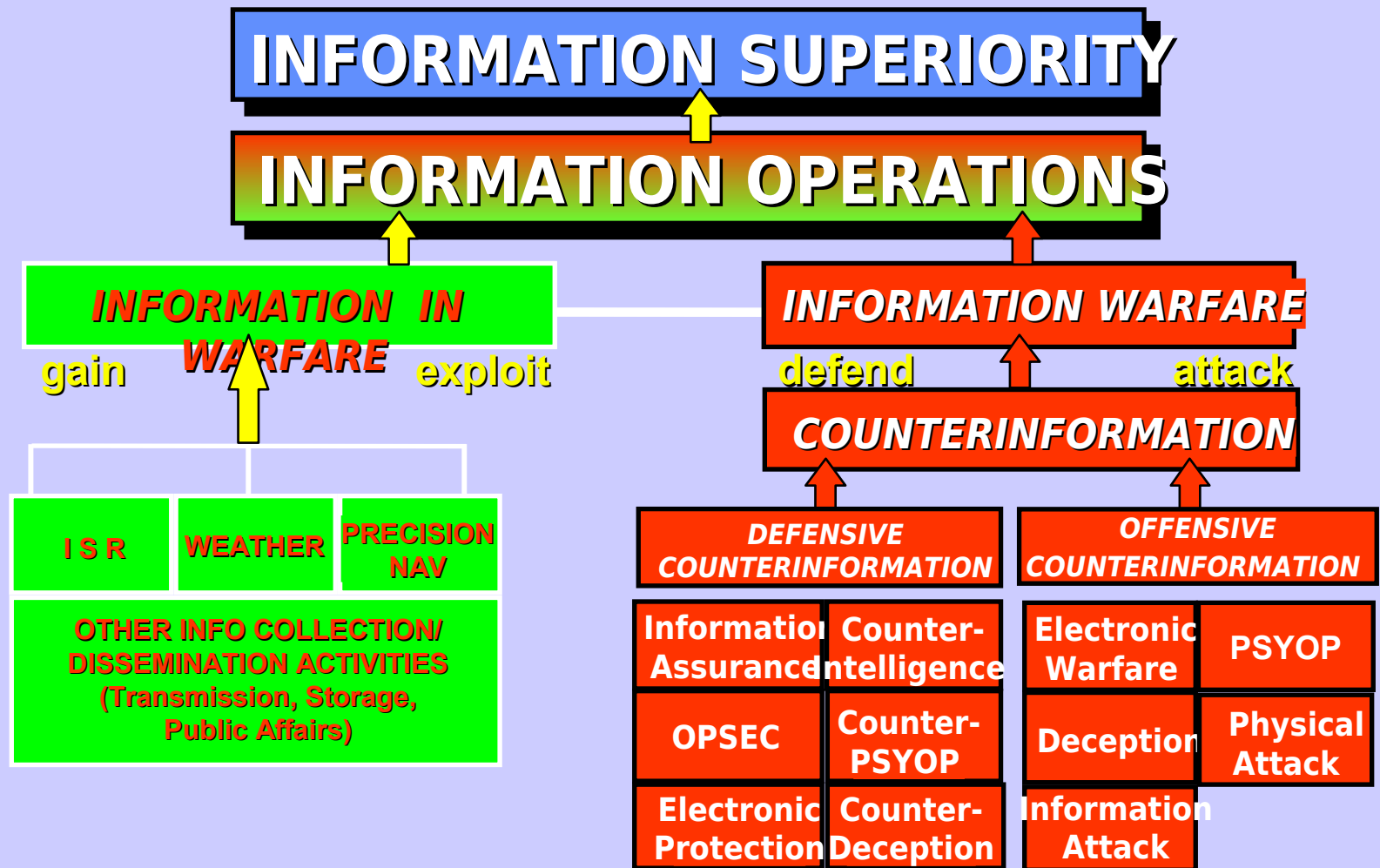
Information is the currency of victory on the battlefield.
General Gordon Sullivan, CSA (1993)

A person is seen from the side, sitting at a desk in a dimly lit room filled with computer monitors. The monitors display various tactical maps and data, with some showing green and red overlays. The person is looking intently at the screens. The room appears to be a control room or a command center.

The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

—Joint Publication 3-13

IO Framework



Information Operations

Physical Attack/Info Attack



Deception, PSYOP, EW



Command, Control, Communications & Computers



Intelligence, Surveillance and Reconnaissance



Assurance (OPSEC, INFOSEC, COMPUSEC, COMSEC, EMSEC)



Position/Navigation, Weather, PA, Transmission/Storage



Peace

Crisis

Conflict

Restoration

Peace

JUST - WAR CRITERIA

(JUS AD BELLUM):

- **JUST CAUSE**
- **COMPETENT AUTHORITY**
- **RIGHT INTENTION**
- **FORMAL DECLARATION**
- **LAST RESORT**
- **REASONABLE HOPE OF SUCCESS**
- **PROPORTIONALITY**

MORALITY IN WAR: (JUS IN BELLO)

- **PROPORTIONALITY**
- **SAFEGUARDING NONCOMBATANTS**
- **CONDUCT IN ACCORDANCE WITH
INTERNATIONAL AGREEMENTS**

KEY LEADERSHIP RESPONSIBILITIES

- **ACCOMPLISH MISSION: FIGHT AND WIN**
- **RESPONSIBILITIES TO SOLDIERS: LOOK AFTER THEIR NEEDS**
- **PROTECT INNOCENT CIVILIANS**

FROM THE JUST-WAR TRADITION

- **EDUCATE AND TRAIN SOLDIERS IN THE LAWS OF WAR**
- **ENFORCE THE RULES OF WAR**
- **LIMIT CIVILIAN CASUALTIES**

Issues



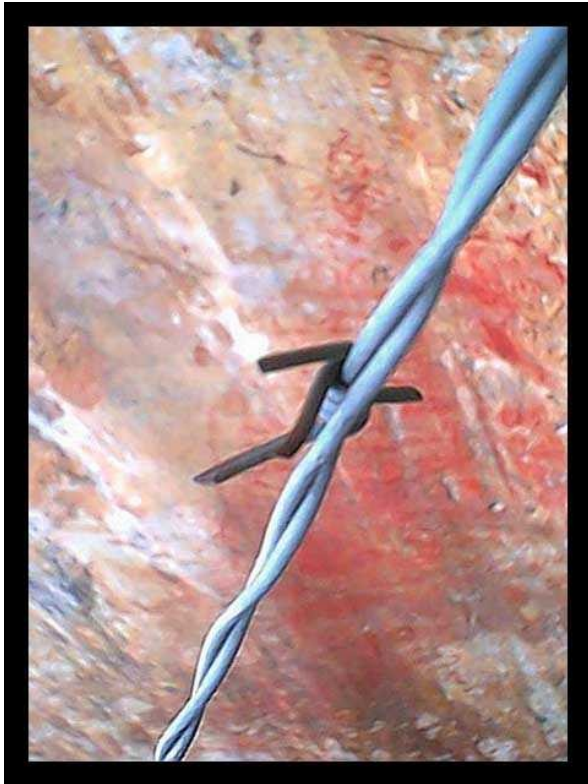
(From Columbia Pictures)

- 1) Are traditional or contemporary notions of strategy sufficient to understand information operations and warfare?
- 2) How do you analyze (in strategic terms) asymmetric threats – the notion of the lone individual being “disproportionately powerful,” should he choose to act?

VIRTUAL DETERRENCE



What is virtual deterrence, and how is it different from “defense”



Not firewalls

Fear factor



Alertness Fatigue



What do we do about this? Can
this apply to governments or
military bodies?

Retaliation

Retaliation as a nation-state, a virtual counterattack is only one means ...

Conventional
Non-conventional





General Background Issues

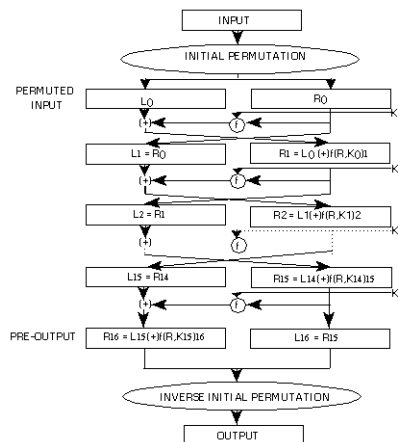


- Dual-Use technologies.
- Asymmetric warfare threat – agreements with whom? “Rogue” individual or cells ?
- Dr. Strangelove – one deterrent factor – new arms race? Cyber Warfare Disarmament

-----BEGIN SIGNATURE-----

IQB1AwUBMVSIA5QYCuMfgNYjAQFAKgL/
ZkBfbcNEsbthba4BlrcnjqabcKgNv+a5kr4537y8RCd+RHm
75yYh5xxA1ojELwNhnb7cltrp2V7LIOnAelws4S87UX80cL
BtBcN6AACf11qymC2h+Rb2j5SSU+rmXWru+=QFMx

-----END SIGNATURE-----



Issues



(From Columbia Pictures)

1) Will anyone be so scared of retaliation that computer-based information attacks won't work? Is "Virtual Deterrence" deterrence ?

2) What about attacks intended to subtly damage the integrity of key systems? Here, the premise may be that the origin of a successful attack might never be discovered.

3) To what extent can networks truly be protected? Given the above, is there a real point to even trying?

Most critical infrastructure is not in government's hands (85%) – Howard Schmidt

REAL OFFENSE



Clausewitz



Virtual and Real Center of Gravity in Information Operations

What are centers of Gravity in Information Operations?

Military
Economic
Political

...

Information Processors
Command and Control Military Centers
COMMS
Power Plants
Bourses / Stock Exchanges
Sensors

OODA LOOP

Observe:

- See the battlespace
- Maintain mobile battlespace view
- Universal access to battlespace view

Orient:

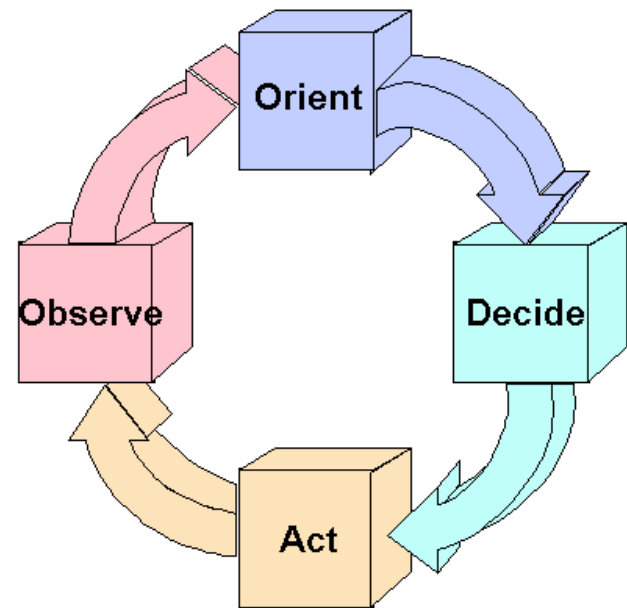
- Tailor view of the battlespace
- Comprehend the battlespace view

Decide:

- Decide what is important and what may require action
- Determine action required to rectify undesirable situation

Act:

- Immediate access to assets to rectify undesirable situation
- Feedback on actions and inactions taken



Machines don't fight wars. Terrain doesn't fight wars. Humans fight wars. You must get into the mind of humans. That's where the battles are won.

-Col John Boyd

Computer Network Operations

- Computer Network Exploitations (CNE)
- Computer Network Attack (CNA)
- Computer Network Defense (CND)

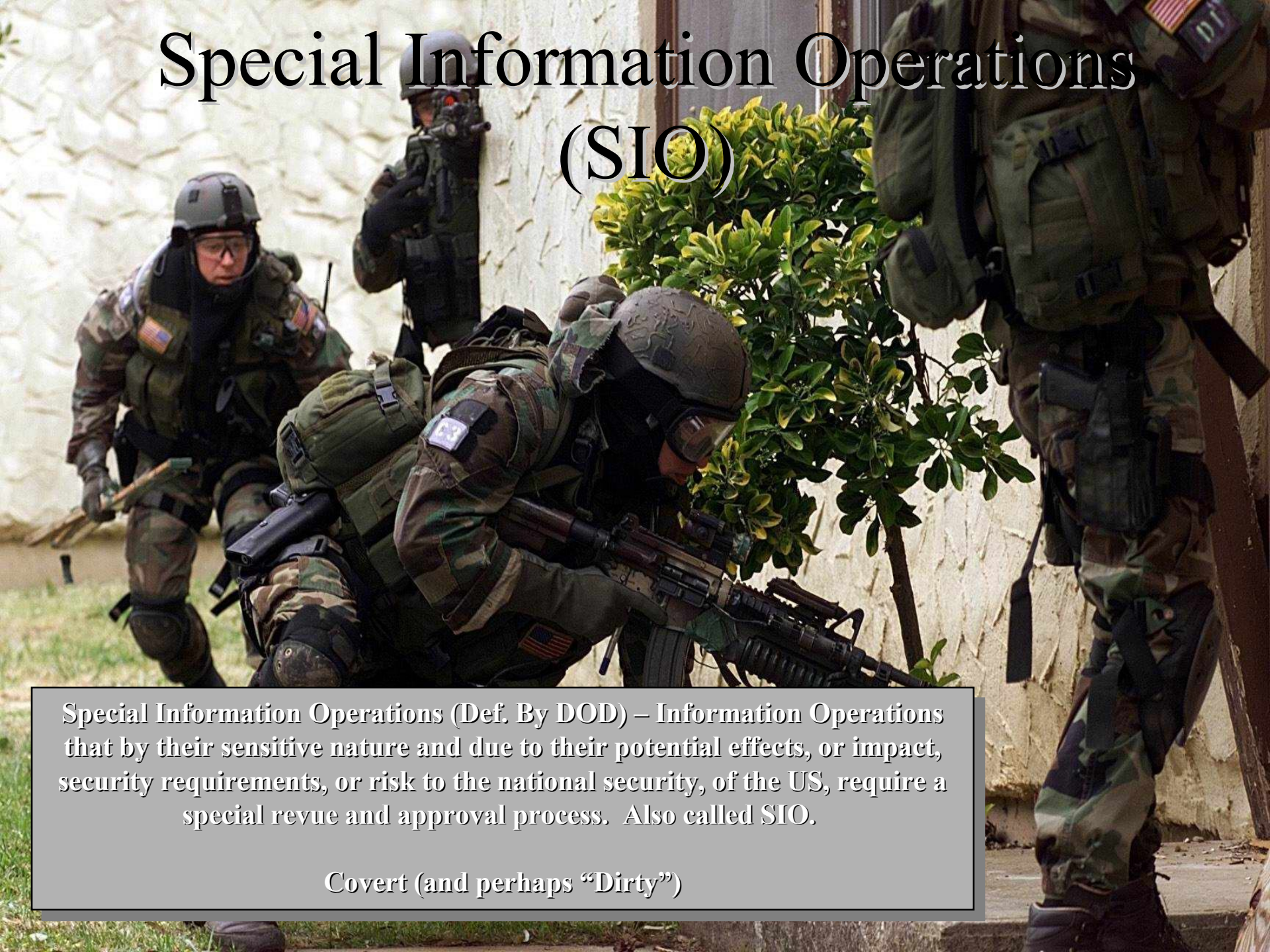


AIR STRATEGY



Air Supremacy VS. Information Supremacy

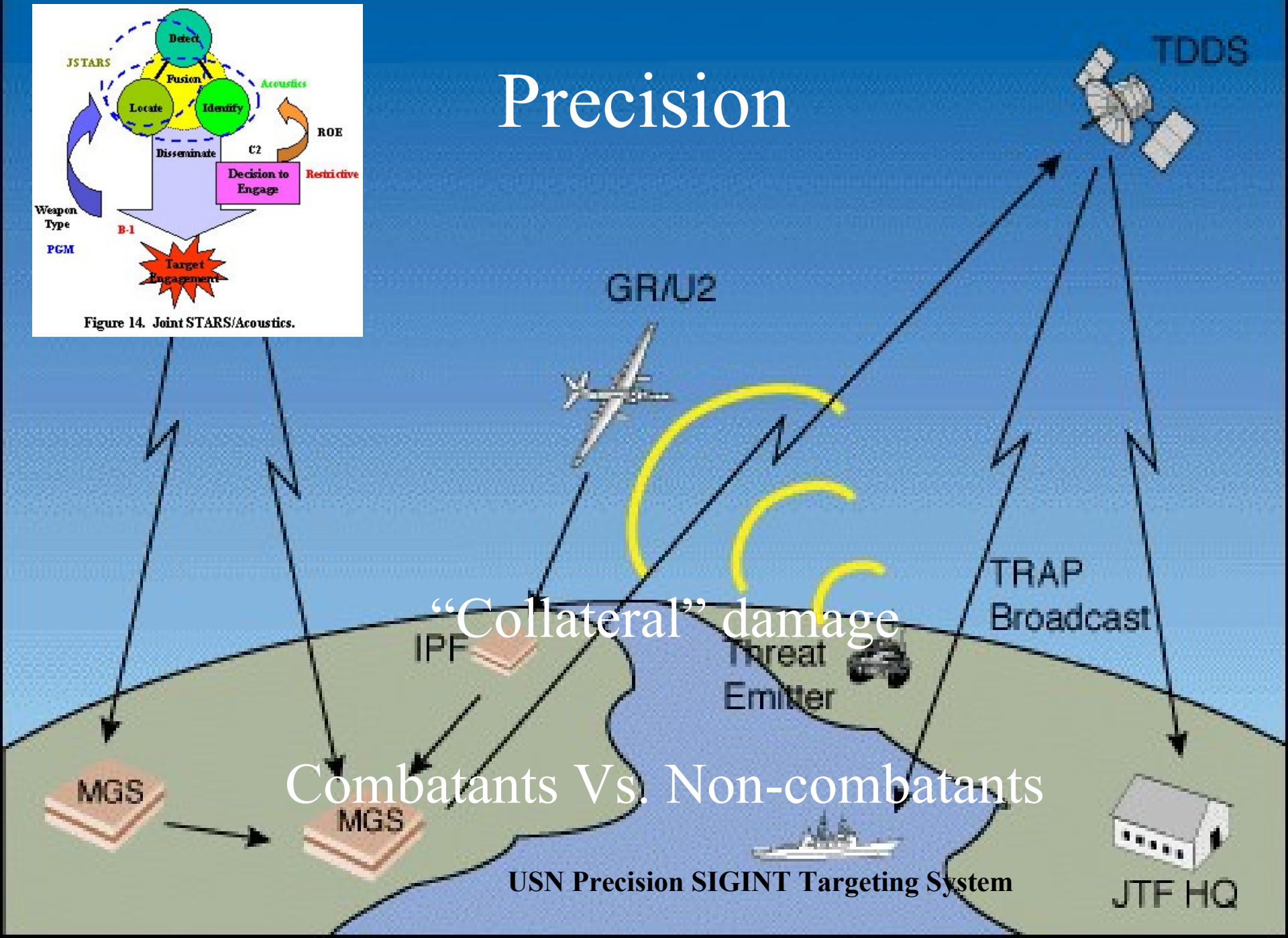
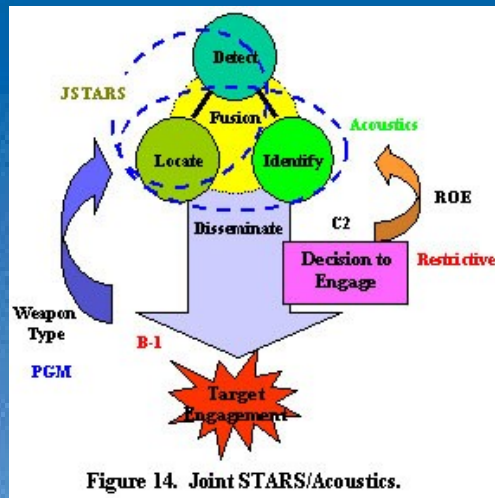
Special Information Operations (SIO)



Special Information Operations (Def. By DOD) – Information Operations that by their sensitive nature and due to their potential effects, or impact, security requirements, or risk to the national security, of the US, require a special review and approval process. Also called SIO.

Covert (and perhaps “Dirty”)

Precision



11:51am up
59 processes:
CPU states: 7
Mem: 94024
Swap: 97980

PID	USER
964	root
409	root
1123	sam
1095	sam
898	sam
1243	root
1	root
2	root
3	root
4	root
5	root
6	root
7	root
8	root
13	root
142	root
302	root
331	root

Nuova



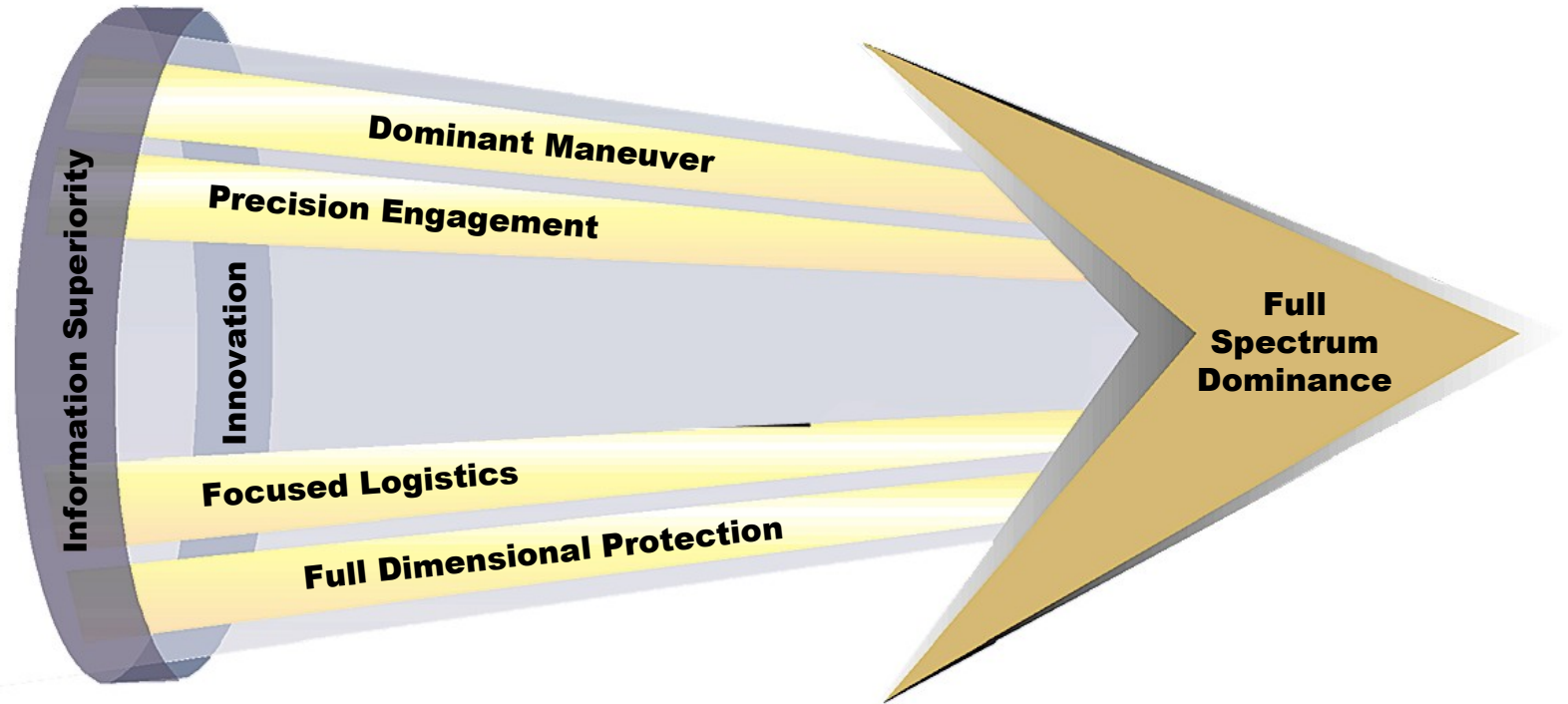
‘War is Unlawful’



Laws of War: (UN Charter –
Reluctance to declare war –
Article 2, Section 4 “All
members shall refrain in their
international relations from
the threat of or use of force
against the territorial integrity
or independence of any state)



Joint Vision 2020



Dedicated individuals and innovative organizations transforming the joint force for the 21st Century to achieve **full spectrum dominance** :

- persuasive in peace
- decisive in war
- preeminent in any form of conflict

Issues



(From Columbia Pictures)

1) Is Information Supremacy a smaller component of a grander vision of [electronic] warfare?

Can Information Supremacy be achieved without bombs, electronic warfare, and air assaults ?

CONCLUSION



Thought-provoking – not FUD



In order to protect nation, one must consider this, because enemies will consider it.

Any government not to consider this would not be very wise.

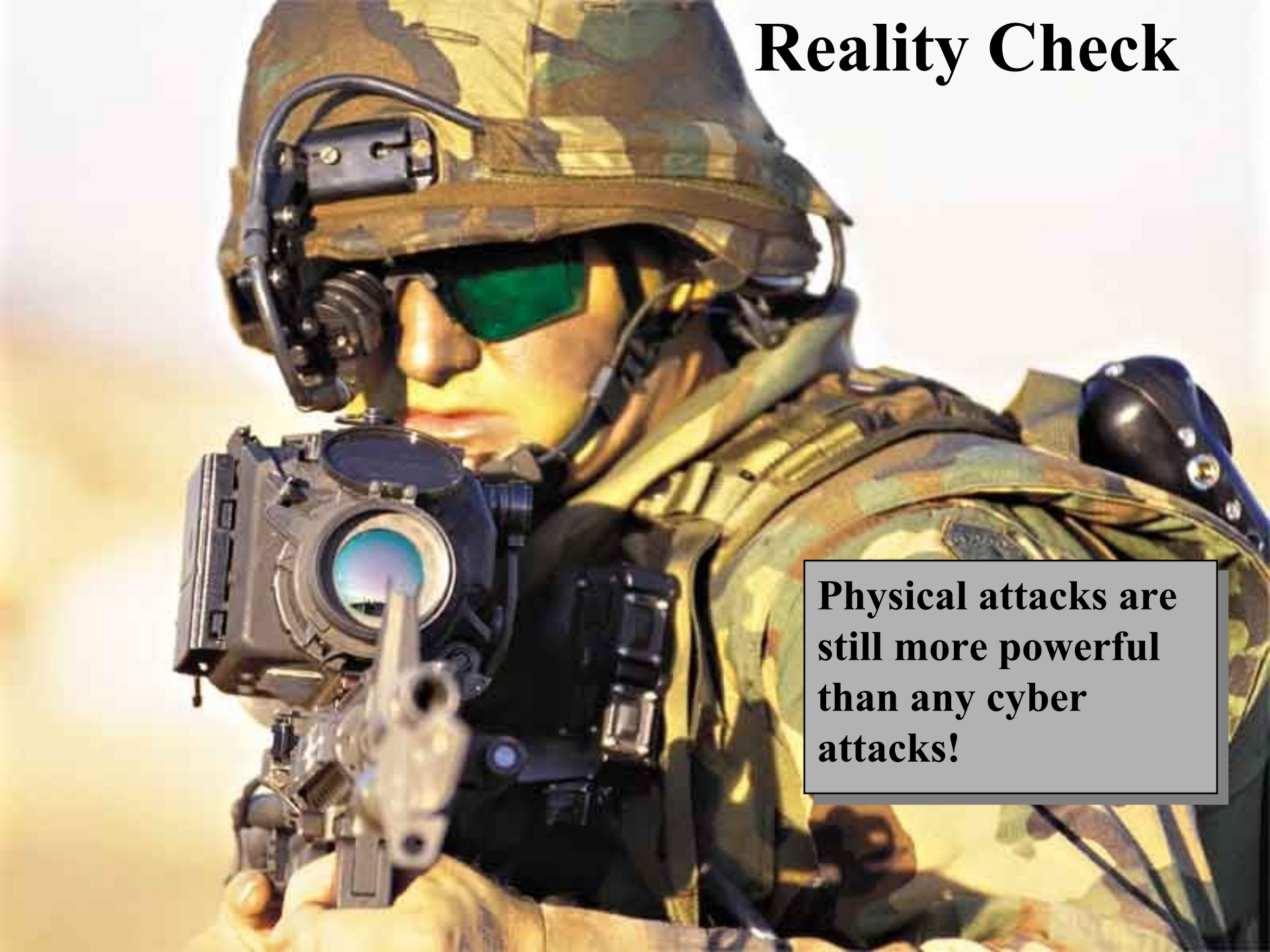
Doctrine is not fully understood, nor realized. Consider history of air doctrine.

Online message center for this subject.

<http://www.iwar.org.uk/h2k2.htm>

... any form of warfare, must be underpinned by a real understanding of the enemy. Understanding of one's ability to implement IO, likewise is key. Sun Tzu already stressed this

Reality Check

A close-up, low-angle shot of a soldier in full combat gear. The soldier is wearing a camouflage helmet with various attachments, including a night vision device and a communication system. They are wearing green-tinted goggles and a tactical vest. The soldier is holding an assault rifle with a scope, aiming it directly at the viewer. The background is a bright, hazy outdoor environment.

**Physical attacks are
still more powerful
than any cyber
attacks!**

What we can do ?

- **Separate Life-Critical, Mission-Critical, and Infrastructure – Critical components from less critical systems**
- **Software Development and Ethics :**
Build systems well and carefully, as ‘with great powers come great responsibilities’
- **Information Assurance Education**
- **Don’t cause unnecessary harm in conflict.**

INFORMATION WARFARE

BEFORE COMPUTERS

For Slides & Discussion List
Go to
www.iwar.org.uk/h2k2.htm

Thank You!



INFORMATION SECURITY CONSULTING
WWW.NITZBERGSECURITYASSOCIATES.COM

Sam Nitzberg's web site
WWW.IAMSAM.COM

IWS

The Information Warfare Site

working for the protection of cyberspace