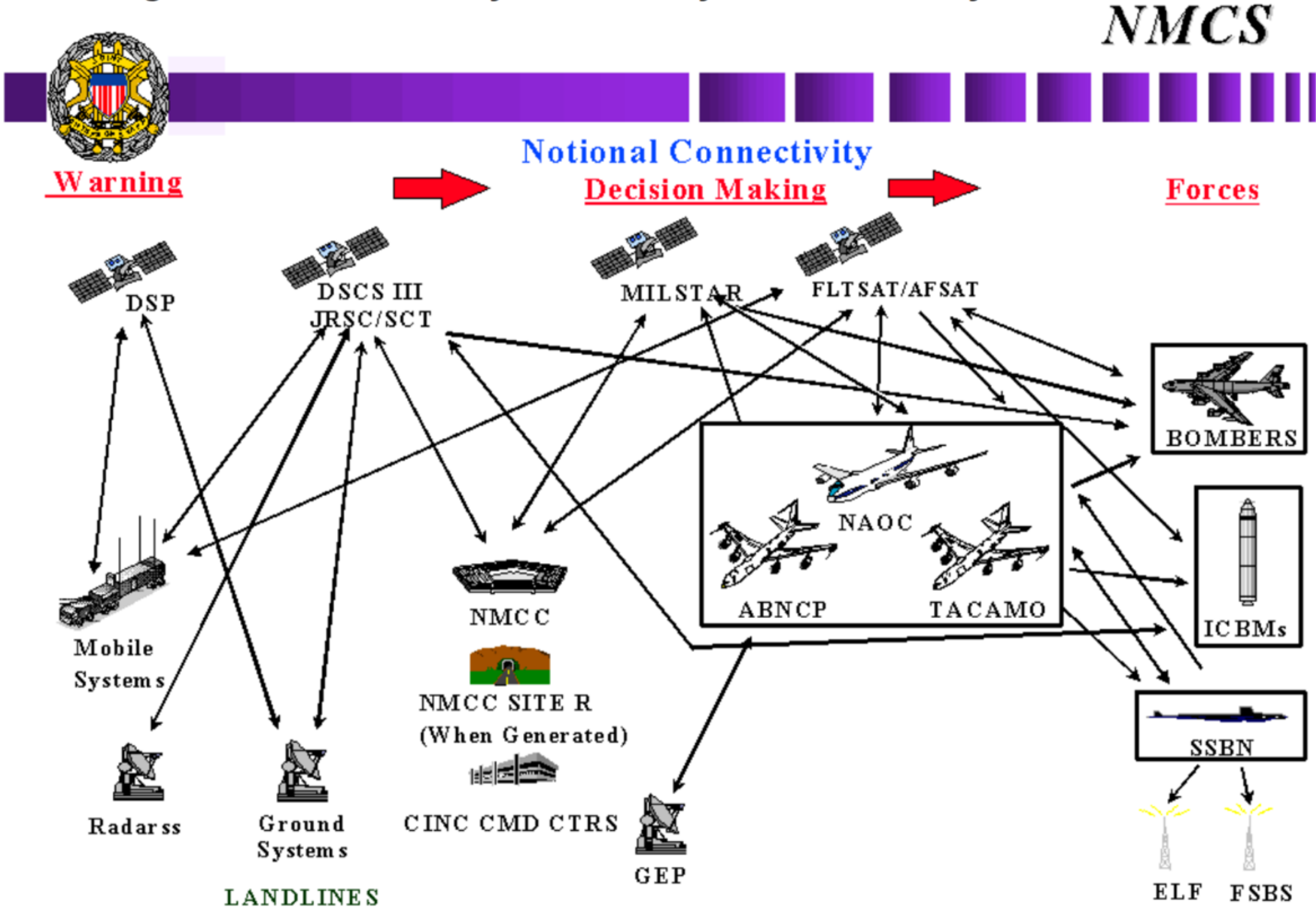# Why we need to tamper-proof our society

Data manipulation poses a more systemic threat than theft or disruption

- Risks

  - Command and Control Systems

  - Military Logistics

  - Financial systems

  - Political institutions

- Mitigation

The New York Times

A Powerful Russian Weapon:
The Spread of False Stories

Risk: Command & Control Systems

Figure 2. National Military Command System Connectivity to the Forces

NMCS

Notional Connectivity

Warning → Decision Making → Forces

DSP

DSCS III
JRSC/SCT

MILSTAR

FLTSAT/AFSAT

BOMBERS

NAOC

ABNCP   TACAMO

ICBMs

Mobile
Systems

NMCC

NMCC SITE R
(When Generated)

SSBN

Radars

Ground
Systems

CINC CMD CTRS

GEP

ELF   FSBS

LANDLINES

Source: "National Command & Control: The National Military Command System (NMCS)," October 2001, at [http://www.afcea.org/education/briefs/lublinoct2001.ppt].

Risk: Command & Control Systems

Indian Command & Control
Operations Center

Pakistani Command & Control
Operations Center

Risk: Military Logistics

- 90% of military logistics is coordinated via non-military systems

US Military Fuel Tanker Being
Unloaded from Commercial Ship

Risk: Financial Systems

- Integrity of NASDAQ OMX data was a major concern in early 2011

NASDAQ Transaction Systems

Risk: Political Institutions

- Research is pretty convincing that manipulation of select systems is plausible

THE FRIDAY COVER

How to Hack an Election in 7 Minutes

With Russia already meddling in 2016, a ragtag group of obsessive tech experts is warning that stealing the ultimate prize—victory on Nov. 8—would be child's play.

By BEN WOFFORD | August 05, 2016

TLP: AMBER

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

18 August 2016

Alert Number
T-LD1004-TT

WE NEED YOUR HELP!
If you find any of these indicators on your networks, or

In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been released TLP: AMBER: The information in this product is only for members of their own organization and those with DIRECT NEED TO KNOW. This information is NOT to be forwarded on beyond NEED TO KNOW recipients.

Targeting Activity Against State Board of Election Systems

Mitigation: Tech Considerations

Focus on ensuring integrity of critical systems

- Assume credentials will be compromised

- Assume air gaping won't completely mitigate risks

- Immutable data stores

- Distributed ledgers

Mitigation: Policy Questions

How do we incentivize greater investments in integrity-guaranteeing solutions?

How do we deter manipulation of critical systems?

Discussion: How do we make ourselves a harder target?

From a Russian discussion forum…