Nuclear Command and Control in the 21st Century

Maintaining Surety in Outer Space and Cyberspace

Jared Dunnmon

Stanford University

July 25, 2018

BRIEF OVERVIEW OF NUCLEAR COMMAND, CONTROL, AND COMMUNICATION (NC3)

- LINKS NUCLEAR FORCES TO PRESIDENTIAL AUTHORITY
- SPACE-BORNE AND TERRESTRIAL EARLY WARNING
- FACILITIES TO INTERPRET EARLY WARNING INFORMATION
- TERRESTRIAL AND AIRBORNE COMMAND AND CONTROL POSTS
- COMMUNICATIONS INFRASTRUCTURE: SATELLITE, RF, AND LAND-LINE

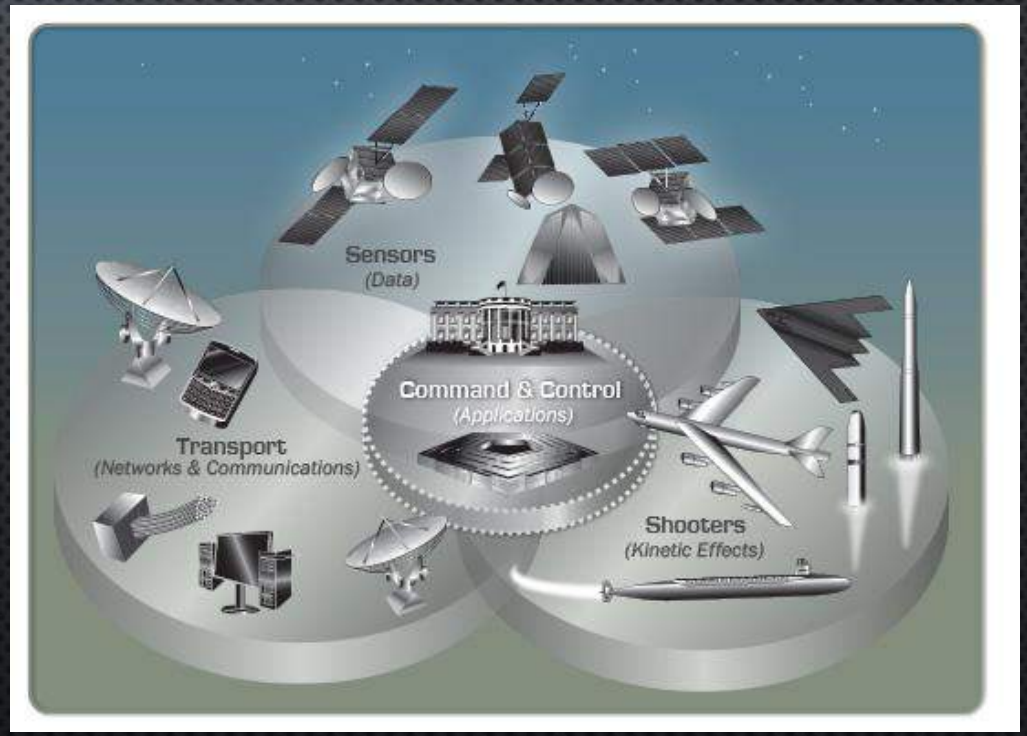


Image: Nuclear Matters Handbook, 2016

CHALLENGES FOR 21ST CENTURY NC3

"ASSURED AND RELIABLE NC3 IS CRITICAL TO THE CREDIBILITY OF OUR NUCLEAR DETERRENT. THE AGING NC3 SYSTEM CONTINUES TO MEET ITS INTENDED PURPOSE, BUT RISK TO MISSION SUCCESS IS INCREASING. OUR CHALLENGES INCLUDE OPERATING AGING LEGACY SYSTEMS AND ADDRESSING RISKS ASSOCIATED WITH TODAY'S DIGITAL SECURITY ENVIRONMENT."

C.D. Haney. Statement to Senate Committee on Armed Services, 2014.

INCREASED US RELIANCE ON SPACE-BASED NC3

"THE UNITED STATES IN PARTICULAR IS DEEPLY RELIANT UPON SPACE. WHILE SUCH RELIANCE ENABLES THE UNITED STATES AND OUR ALLIES AND PARTNERS TO UNDERTAKE A RANGE OF OPERATIONS IN SUPPORT OF PEACE AND SECURITY, THIS RELIANCE HAS INCREASINGLY BEEN VIEWED BY POTENTIAL ADVERSARIES AS A VULNERABILITY TO BE EXPLOITED THROUGH THE DEVELOPMENT OF COUNTERSPACE CAPABILITIES."

F. Rose. "Using Diplomacy to Advance the Long-Term Sustainability and Security of the Outer Space Environment," 2016.

NC3 VULNERABILITIES IN OUTER SPACE

- Laser-based systems
- EM jamming
- Physical asat systems
- Space debris
- cyberattack vectors

Image: Wikicommons, 2017

WHAT IS CYBERSPACE?

"AN OPERATIONAL DOMAIN FRAMED BY THE USE OF ELECTRONICS AND THE ELECTROMAGNETIC SPECTRUM TO CREATE, STORE, MODIFY, EXCHANGE, AND EXPLOIT INFORMATION VIA INTERCONNECTED AND INTERNETTED INFORMATION SYSTEMS AND THEIR ASSOCIATED INFRASTRUCTURE."

D. Kuehl. "From Cyberspace to Cyberpower: Defining the Problem," 2009.

NC3 VULNERABILITIES IN CYBERSPACE

- Heterogeneous networked systems create large attack surface
- Documented vulnerabilities
- Insecure supply chains
- Increasing complexity
- Additional reliance on complex software and over-the-air updates
- Cost of proving system security

Image: Motherboard, 2015

Major Classes of Exploitable Flaws

- Hard-coded credentials: undocumented credentials that can authenticate in documented interfaces
- Undocumented protocols: protocols not intended for end users
- Insecure protocols: end-user protocols that pose a security risk
- Backdoors: mechanisms used to access features not intended for end users – not only software!

"A Wake-up Call for SATCOM Security." IOActive, 2014.

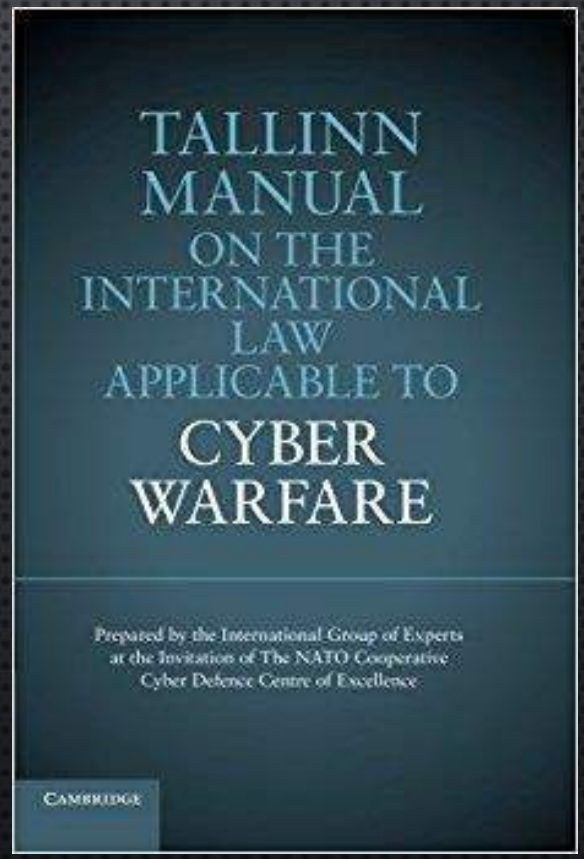
TECHNOLOGICAL TOOLS FOR RISK MITIGATION

- ADVANCED FORENSICS AND NETWORK DEFENSE
- MINIMIZING THE CODE BASE
- SMALL-SCALE LAUNCH + INEXPENSIVE HARDWARE
- DECREASE RELIANCE ON SPACE-BASED NC3

Image: Rocket Lab, 2015; Planet, 2017

POLICY TOOLS: ADAPTING OLD RULES TO NEW DOMAINS

- JURISDICTION: WHAT CAN WE REASONABLY KNOW?
- RESPONSIBILITY: ESPIONAGE VS. ATTACK?
- USE OF FORCE: THIRD PARTIES?
- SELF-DEFENSE: WHAT IS "THE LAST WINDOW"?



SCENARIO: AEHF SATELLITE MALFUNCTION

- MECHANISM?
- CONSEQUENCES?
- AGGRESSOR?
- CYBERATTACK?
- CC3 OR NC3?
- RESPONSE?

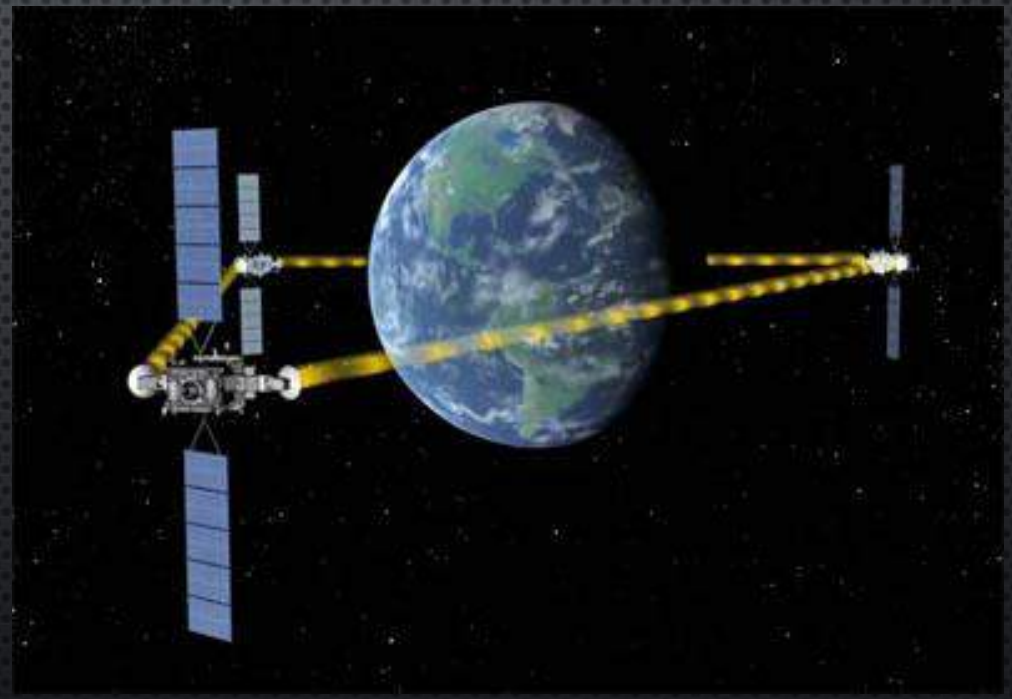


Image: Lockheed Martin, 2010

Concluding Thoughts

1. The credibility of the nuclear deterrent directly relies on our ability to be believably resilient to attempted NC3 disruption – *space-based components are just the tip of the iceberg*

2. NC3 and associated systems will keep getting more complex, and in all likelihood they will be hacked – *more automation is a double-edged sword*

3. The continuation of strategic stability requires the integration of cyber capabilities into the calculus of nuclear deterrence – *this is not easy, it is not inexpensive, and it is not a choice*