THE IMPACT OF NUCLEAR WEAPONS SECURITY MEASURES ON BRINKMANSHIP CONFLICT OUTCOMES:

A COMPARATIVE CASE STUDY OF THE PAKISTAN-INDIA BORDER CONFLICT AND U.S.-RUSSIAN TENSIONS OVER THE WAR IN UKRAINE

Senior IS by Cory Horgan
Advisor Dr. Lantis

Overview

1. Literature Review
2. Research Design & Methodology
3. Pakistan-India Case Study
4. US-Russia Case Study
5. Analysis, Theory, & Conclusion

Project Background

- Junior Independent Study Beginnings
  - Nuclear safeguards
- Why nuclear weapons?
- An early focus on **cyber threats** to nuclear weapons security
- Project evolution throughout the process
- Familiarity with deterrence
- Interest in **Nuclear Command, Control, and Communications (NC3)**

1

Literature Review

Deterrence Theory

- Deterrence
- Strategic Stability
- Misperceptions Within Deterrence
- Credibility
- Minimum Deterrence
- Perfect & Rational Deterrence

Inherent System Vulnerability Theory

- Advanced Technology Cognizance
- Inherent System Vulnerability
- Issues with NC3
- The Always/Never Dilemma
- Cyber Challenges

Research Question

Do levels of nuclear security measures influence success or failure in instances of nuclear brinkmanship?

Hypothesis

If countries implement levels of nuclear defense measures with **advanced technology**, then they experience success within instances of nuclear brinkmanship

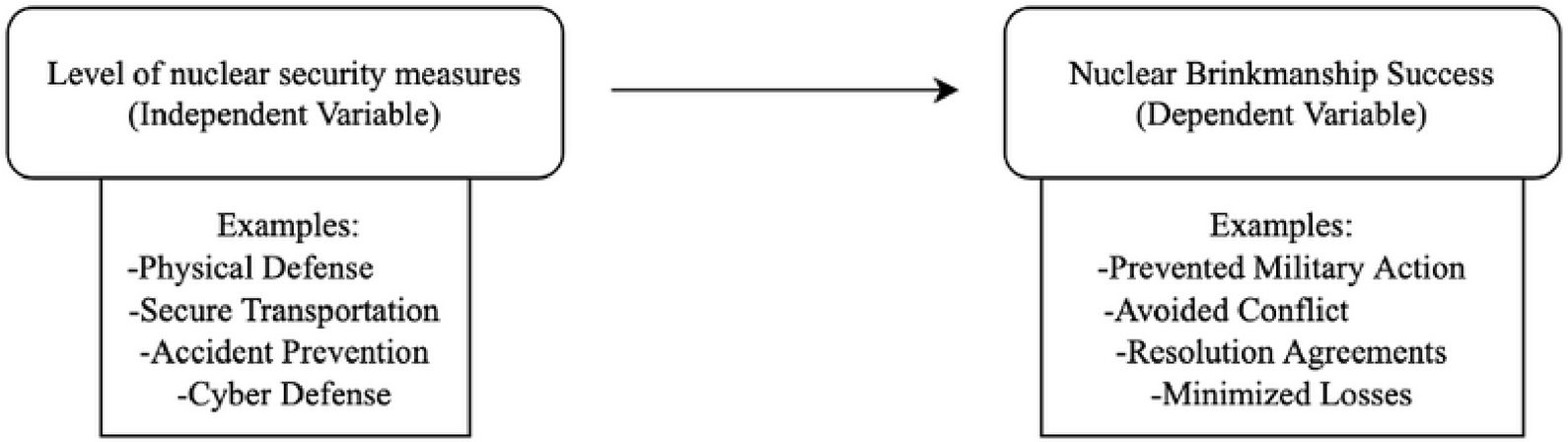
Research Design & Methodlogy

National Nuclear Security Administration

ROSATOM

2

Arrow Diagram & Variables



Methodology, Cases, & Sample IV Coding

- Comparative Case Study Method
- Cases
  - India and Pakistan
    - Kargil War (1999)
    - Line of Control Conflicts
  - The US and Russia
    - Russo-Ukrainian War (2022-)
    - Crimean War (2014) Context

Country X

Nuclear Security Measure	Security Measure is Evidenced by	Security Measure Score
Cyber Security	- NC3 defensibility - Positive control systems - Early warning systems - Data encryption - Hacking prevention	
Permissive Action Links	- Access control safety device - Microprocessor or combination - Ability to permanently disable - Tamper resistance	
Accident Prevention	- Negative control systems - Mitigate human error - Normal accident resilience - Glitch and bug mechanisms - Ready/safe switches - Environmental sensing devices	
Stockpile Stewardship	- Sustainment activities - Modernization efforts - Weapons dismantlement and disposition (WDD) - Production operations - Surveillance	
Secure Transportation	- Use of vehicles - Trailer fleets - Aviation - Reliable communications - Transportation training - Liaison programs	
Physical Defense	- Protection forces - Physical security systems - Information security - Personnel security - Material control - Vulnerability/risk assessments	

3-4

Case Study Setup & Content

All case studies utilized open-source information when assessing nuclear security measures and brinkmanship

01

02

Historical context on conflicts and nuclear weapons programs

Evaluation of the six nuclear security measures for each country

03

04

Evaluation of brinkmanship conflict: which countries experienced success and failure

3-4

Results

Kargil War & LOC Tensions:

- India - Success
- Pakistan - Failure

Russo-Ukrainian War (1st Year):

- United States - Success
- Russia - Failure

Nuclear Security Measure	Security Measure is Evidenced by	Security Measure Score	*Pakistan*	*India*	*US*	*Russia*
Cyber Security	- NC3 defensibility - Positive control systems - Early warning systems - Data encryption - Hacking prevention	20	55	80	60	
Permissive Action Links	- Access control safety device - Microprocessor or combination - Ability to permanently disable - Tamper resistance	30	34	90	70	
Accident Prevention	- Negative control systems - Mitigate human error - Normal accident resilience - Glitch and bug mechanisms - Ready/safe switches - Environmental sensing devices	22	30	90	40	
Stockpile Stewardship	- Sustainment activities - Modernization efforts - Weapons dismantlement and disposition (WDD) - Production operations - Surveillance	50	55	85	95	
Secure Transportation	- Use of vehicles - Trailer fleets - Aviation - Reliable communications - Transportation training - Liaison programs	10	20	100	40	
Physical Defense	- Protection forces - Physical security systems - Information security - Personnel security - Material control - Vulnerability/risk assessments	40	65	100	70	

5

Analysis

1 Security measure scores indicate advanced technology measures tended to be one of the lowest scoring categories. Low cyber security and advanced technology scores may be linked to brinkmanship failure. Legacy technology versus underdevelopment due to recency.

2 Conventional security measures receive more attention and investment. Shared commitment across the physical security and stockpile stewardship categories. Secure transportation consistently experienced low scores.

5

Theory Implications

1 Inherent system vulnerability and broader cyber threats should be investigated further. If the supposed advanced technology neglect is pervasive, countries and scholars must prioritize cyber security theories that address advanced technology threats. Alway/never dilemma is not upheld or solved by continued conventional security investment,

2 Deterrence was insufficient in the Kargil War and the first year of the Russo-Ukrainian War. Deterrence may have wavered, but Kargil was a limited conflict and deterrence began to stabilize at the end of the first year of the Russo-Ukrainian War. Room for strategic stability and to help explain the conflicts.

Conclusion and Ideas

Thank You