Information Infrastructure: Cyberspace, Outer Space, and the U.S.-China Security Relationship

Jon R. Lindsay

University of California Institute on Global Conflict and Cooperation

jrlindsay@ucsd.edu

Jiakun Jack Zhang

University of California, San Diego

jjz007@ucsd.edu

This research is supported by Office of Naval Research Grant N00014-14-1-0071 and the Department of Defense Minerva Research Initiative

Cross Domain Deterrence and China

- Cross Domain Deterrence (CDD) extends classical deterrence by investigating how threats in one domain can be countered by unlike capabilities in another
- Domains: land, air, sea, space, and cyber
- Pentagon interest motivated by the rise of China's A2/AD capabilities
- China's A2/AD arsenal includes naval, missile, and air force modernizations with particular emphasis on space and cyber systems to extend command and control and deny it to an adversary
- This paper investigates the role of cyber and space domains in a potential conflict against China

Space and cyber war

- “The next Pearl Harbor could very well be a cyber-attack”

  – Leon Panetta, Secretary of Defense

- “Space is foundational capability for all military operations, yet we don’t really plan for anything but success…the heavens aren’t the ‘peaceful sanctuary’ they once were”

  – William Shelton, Air Force Space Command

- “Theoretically speaking, it is impossible for an operating information system to completely protect itself from enemy’s infiltration”

  – *The Science of Campaigns*

Outline

- Theory becomes vital in the absence of precedent
- We apply theories of interdependence to the space and cyber domains
- 1) Information infrastructure: space and cyber systems derive value from their ability to gather, transmit, and process information
- 2) Military-technical logic of vulnerability: Asymmetry, offense dominance, instability
- 3) Political-economic logic of restraint: Opportunity costs, credible signals, transforming preferences
- "Looking at today's cyber domain, interdependence and vulnerability are twin facts that are likely to persist" (Nye 2013)

Information Infrastructure

- Space and cyber systems involve very different technologies but serve the same political-economic purpose
- Not valuable in and of itself, they are not low-cost alternatives to traditional power projection
- Space and cyber capabilities are information infrastructure, they are institutions as well as technology
- Their value stem from their control relationship to other activity
- Their vulnerability is predicated on networked systems, therefore mutually constituted and cross-domain in nature
- Force multipliers in traditional domains, which in turn support political objectives

Military-Technical
Logic of Vulnerability

- Existing security literature has focused on vulnerability (Mulvenon 2009, Blasko 2011, Pollpeter 2012, Kello 2013, Junio 2013, Gompert and Libicki 2014)
- Asymmetric attack – vulnerability of control systems
- Offense dominance – offense easier than defense
- Crisis instability – ‘use it or lose it’
- Tactical and operational levels, space and cyber systems can be destabilizing

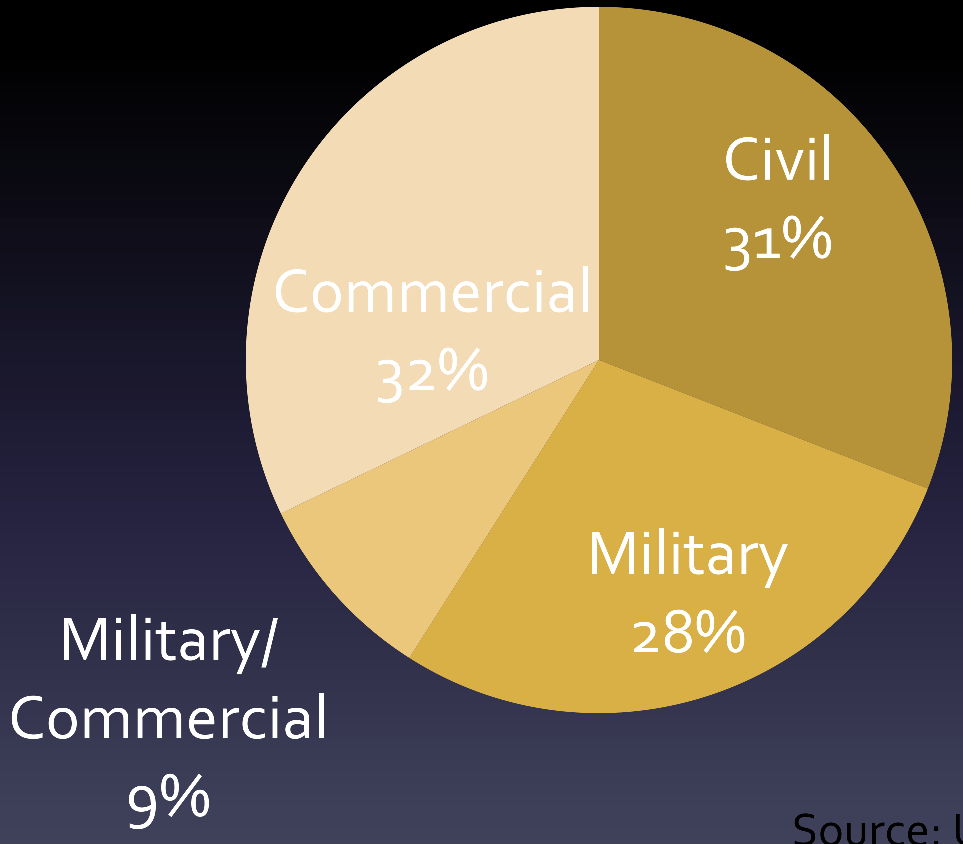
Institutions and Interdependence

- Commerce is a more appropriate analogy
- Exchange based on institutions (common protocols), accept mutual vulnerability, enhance existing capabilities
- Invulnerability in cyber and space come at the expense of advantages in the traditional domains
- This vulnerability creates the dynamics for liberal peace: constrain, inform, transform (Kastner 2009)
- Information infrastructure is built upon cooperation, thus makes room for optimism for future dynamics in cyber and space

Opportunity Costs

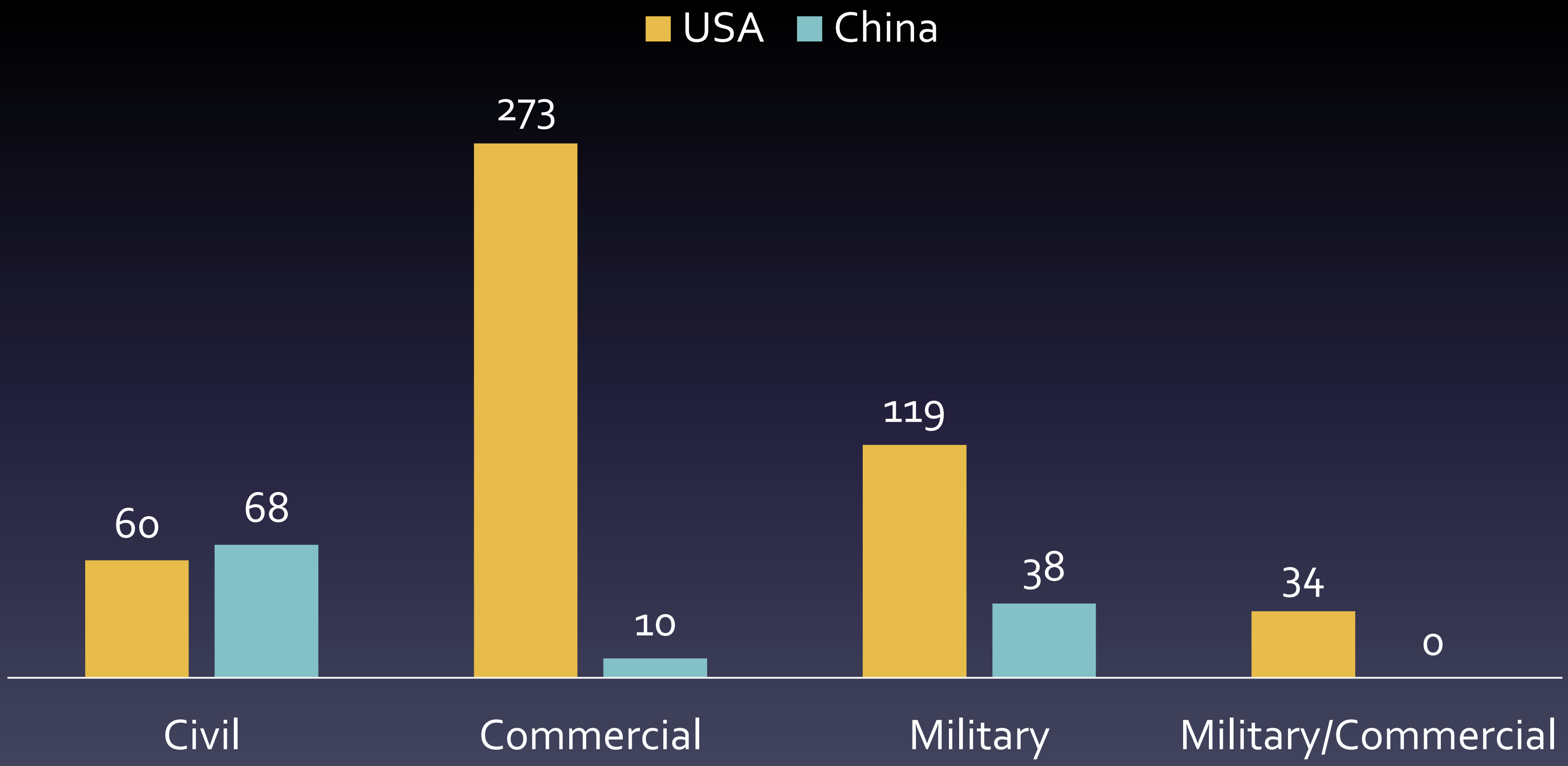
- Information infrastructure is not only useful for C4ISR but also foundational to global capitalism
- Conflict in outer space and cyber space would generate opportunity costs
- Escalations will be constrained by state desire to avoid collateral damage for multi-use infrastructures
- Externalities in space are particularly salient because of the long term impact of space debris

Breakdown of Satellites by Type



Source: UCS Satellite Database

Comparative Breakdown of Satellites of the USA and China



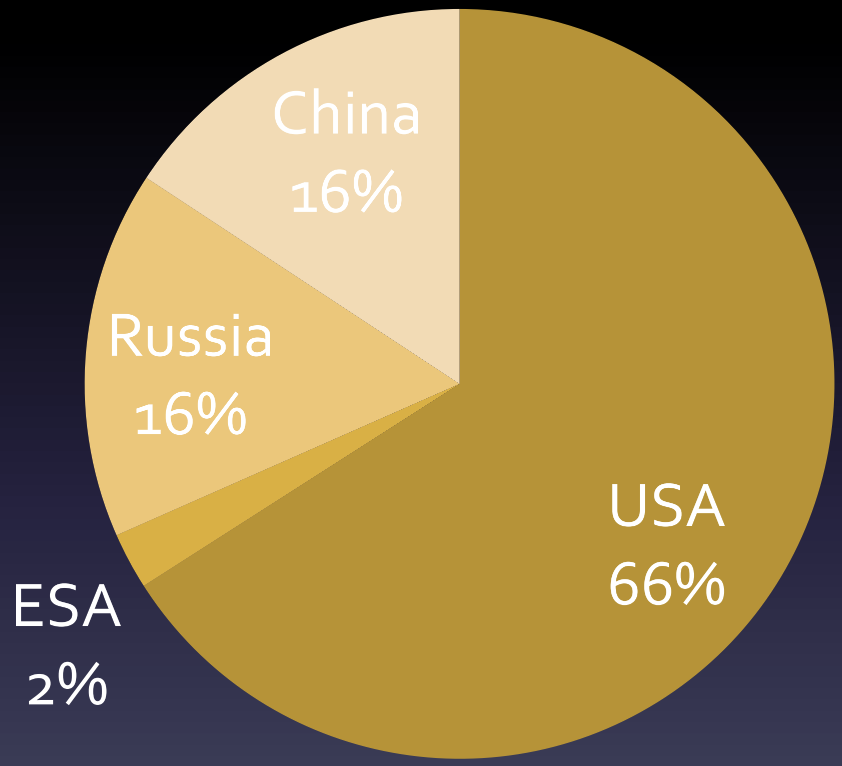
Credible Signals

- Cyber and space assets help detect costly signals (ex. Mobilization) made in other domains, helping reduce bargaining failure over uncertainty about capabilities
- Robust and reliable C4ISR allows states to differentiate signals from cheap talk and prevents inadvertent escalation
- Live and let live dynamic in US and USSR space race (ex. Outer Space Treaty)
- Serious attempt to degrade C4ISR or C2 would be interpreted as a very strong signal of hostile intention (equal to nuclear war)
- This danger should lead to restraint and caution rather than escalation

Transformed Preferences

- Preferences of decision makers are not fixed and cooperation can be socialized
- More likely in space and cyber than traditional domains because they are already highly institutionalization
- The development of norms and rules for cyber and space governance are prominent in policy writing
- Lawfare more likely than warfare: “It is necessary to proactively participate in the formulation of outer space laws, and strive to establish the laws that are advantageous to us, and disadvantageous to the enemy” – *Course of Study of Space Operations*

Breakdown of Satellites by Nationality



Source: UCS Satellite Database

Through a Glass, Half Full

- Room for optimism in U.S.-China relations in new domains
- China is developing increasing space and cyber capabilities, but this is not necessarily a threat to stability
- Interdependencies do not eliminate competition, friction will persist but prevent high intensity escalation is no more likely
- Important not to conflate low intensity friction with high intensity conflict

Conclusion

- Weigh in the policy debate on space and cyber to present the case for optimism
- Introduce the logic of interdependence to another realm
- Interdependence both enables and constrains the military utility of information infrastructure
- At tactical and operational levels, space and cyber systems can be destabilizing
- Viewed as institutions, the political economic incentives for restraint also exist
- Importance of norms and conventions

Thank you