Cyber Persistence and National Security

Dr. Michael P. Fischerkeller – Institute for Defense Analyses
mfischer@ida.org

Outline

- Strategic environments and the central questions
- How US cyber operations/campaigns can support deterrence strategies
- How cyber operations/campaigns and other cyber actions can undermine deterrence strategies
- Closing comments

Strategic Environments and the Central Questions

Mixed-security Environment

- Nuclear
  - Security rests in the mind of your adversary (deterrence)
- Conventional
  - Security rests in aligning your strategy to the prevailing offense-defense condition (offense or defense advantage)
- Cyber
  - Security rests in initiative persistence, which manifests primarily as continuous, exploitative cyber *fait accompli* campaigns whose effects are short of threats and uses of force

- Questions:
  - How can US exploitative cyber campaigning support the efficacy of US deterrence strategies?
  - How can cyber campaigns/operations and other cyber actions undermine the efficacy of US deterrence strategies?

How US Cyber Campaigning can Provide Support to Deterrence Strategies

- **Day after day**, the Department will **strengthen *integrated deterrence*** and gain advantage against competitors' most consequential coercive and exploitative, non-coercive actions that fall below perceived thresholds for US military action by ***campaigning*** *in and through cyberspace.* *(modified from 2022 NDS to include emphases in 2023 NCS)*
- In support of *Integrated Deterrence*, exploitative cyber campaigning can:*
  - *Limit, frustrate, and disrupt competitor activities that seriously affect US interests, especially those carried out in the gray zone*
  - *Oppose acute forms of coercion*
  - *Improve baseline understanding of the operating environment*
  - *Improve position (set conditions in one's favor)*
  - *Shape perceptions, including sowing doubt*
  - *Complicate competitors' military preparations*

* These bullets should not be considered exhaustive or mutually exclusive.

How Cyber Operations/Campaigns could Undermine Deterrence Strategies

- Adversary exploitative cyber campaigning could
  - Alter the international distribution of power.
  - Alter the actual or perceived local balance of power.
  - Alter resolve by eroding social or alliance cohesion.
- "Winning too much" in and through such campaigning could encourage an opponent to resort to arms to redress losses.
- Targeting nuclear command, control, and communications through such campaigning in competition and militarized crisis could
  - Remove "assured" from "assured second strike," and
  - Undermine nuclear strategic stability *and* global geostrategic stability.
- Novel, independent cyber operations in a crisis could
  - Introduce uncertainties, thereby increasing the likelihood of miscalculation which, in turn, increases the potential for accidental or inadvertent escalation into armed conflict.

Closing Comments

- Exploitative cyber campaigning contributes to national security in two ways:
  - By independently generating or inhibiting strategic outcomes
  - By supporting other security strategies, e.g., integrated deterrence.
- The strategic value of cyber capabilities primarily derives from continuous, exploitative campaigning short of threat or use of force.
- Campaigning in competition establishes the strategic value of cyber capabilities in competition, crisis, and armed conflict.

Backups

From the 2022 National Defense Strategy …

- The Department will advance our priorities through integrated deterrence, campaigning, and actions that build enduring advantage. ***Integrated deterrence*** entails working seamlessly across warfighting domains, theaters, the spectrum of conflict, all instruments of U.S. national power, and our network of alliances and partnerships.
- **Day after day**, the Department will **strengthen deterrence** and gain advantage against competitors' most consequential coercive measures by ***campaigning*** - the conduct and sequencing of logically-linked military initiatives aimed at advancing well-defined, strategy-aligned priorities over time.
- Gray-zone activities: Competitors now commonly seek adverse changes in the status quo using gray zone methods – ***coercive*** approaches that may <u>fall below perceived thresholds for US military action</u> and across areas of responsibility of difference part of USG.
- ***Deterrence or a variant is mentioned 91 times; coercion or a variant is mentioned 20 times.***

IDA

From the 2023 National Cybersecurity Strategy …

- **Cybersecurity is essential to** the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communication, and our **national defense**.
    - These represent national sources of power and instruments of national power that are being subject to **adversary *exploitative* cyber actions** that fall below perceived thresholds for US military action.
- Technologies have been misused to: steal data and intellectual property; distribute disinformation; disrupt critical infrastructure; proliferate online harassment, exploitation, and abuse; enable criminals and foster violent extremism; and threaten peace and stability.
- Pillar II: Enhance collaboration around disrupting and dismantling threat actors.
    - Disruption ***campaigns*** must be sustained and executed at scale.
- ***Deterrence or a variant is not mentioned at all; Coercion or a variant is mentioned once.***