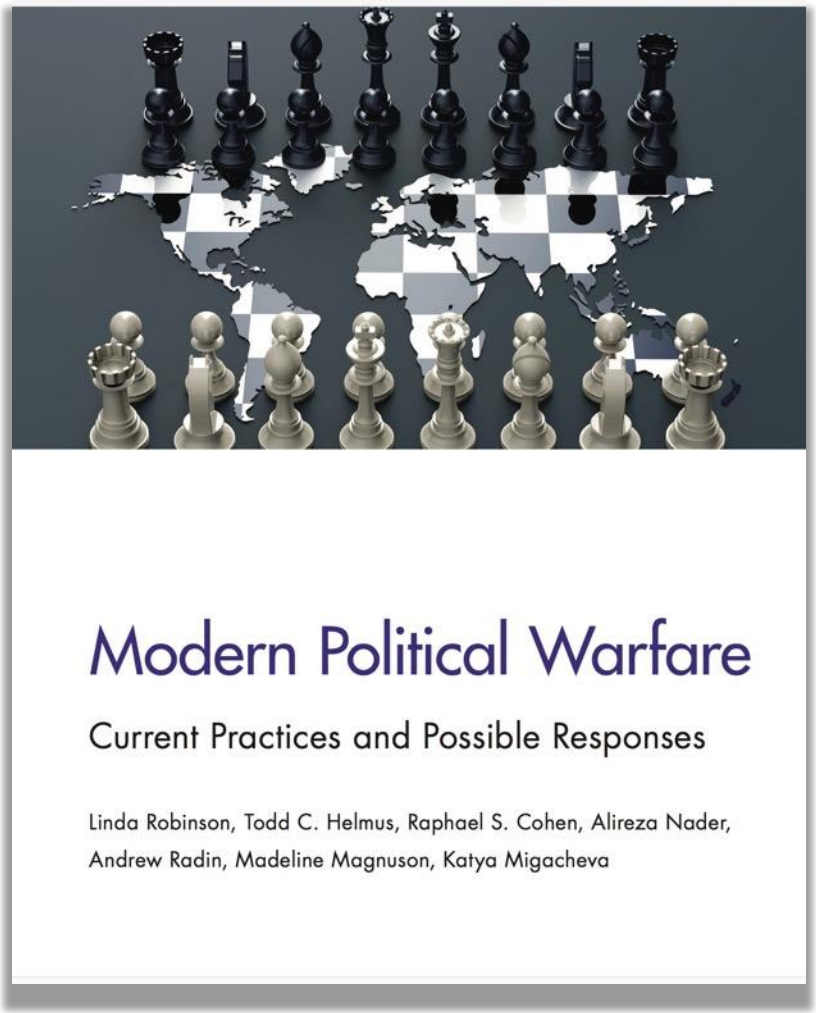

# Modern Political Warfare: Current Practices, Possible Responses

Linda Robinson

RAND Senior Researcher and Author

# Project Overview




- Definitions
- Cold War Experience
- Contemporary Practice: Russia, Iran, ISIS
- Attributes of Current Modern Political Warfare
- Difficulties of Warning
- Response Requirements
  - DoD and Interagency

https://www.rand.org/pubs/research_reports/RR1772.html

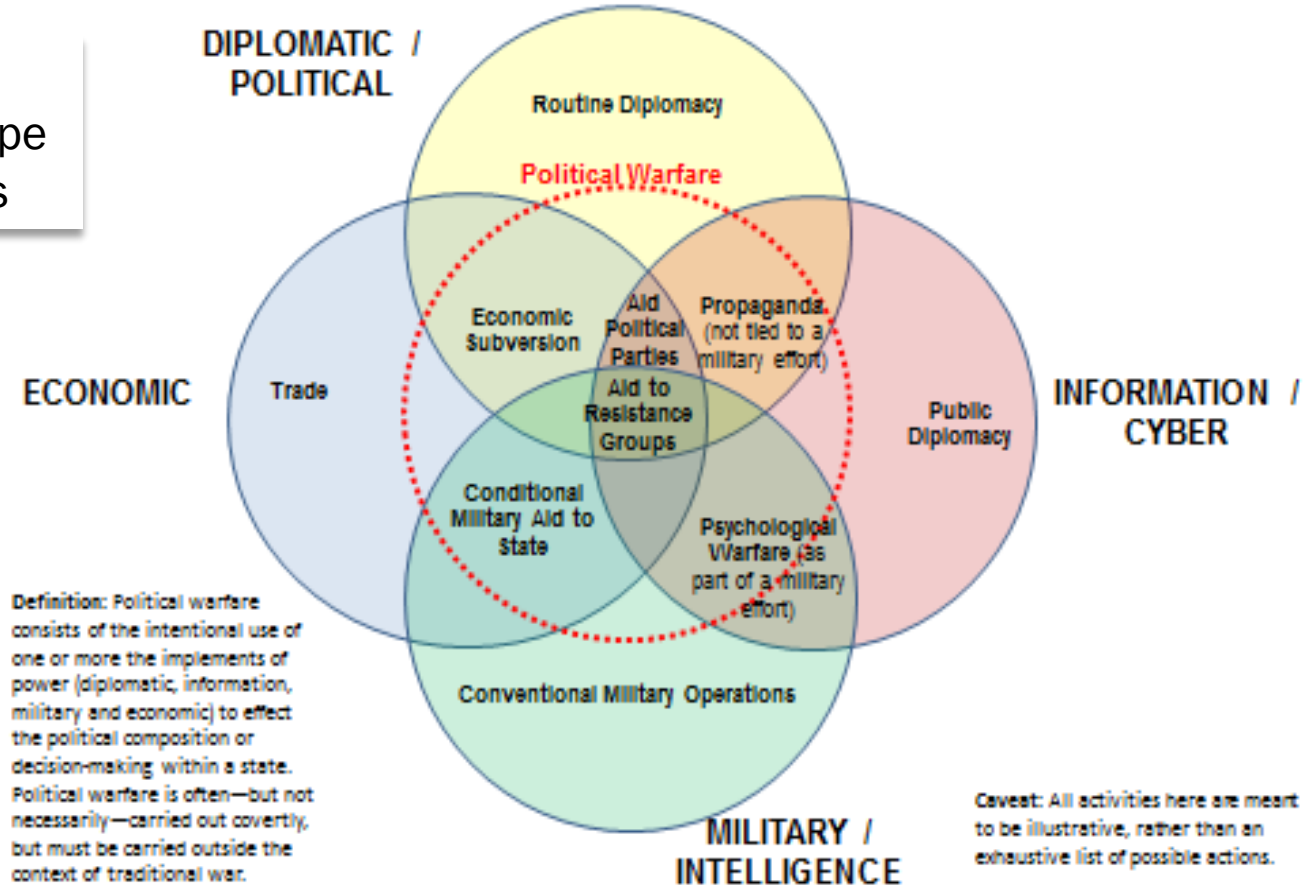
# Kennan’s definition of political warfare

The employment of all the means at a nation's command, short of war, to achieve its national objectives.

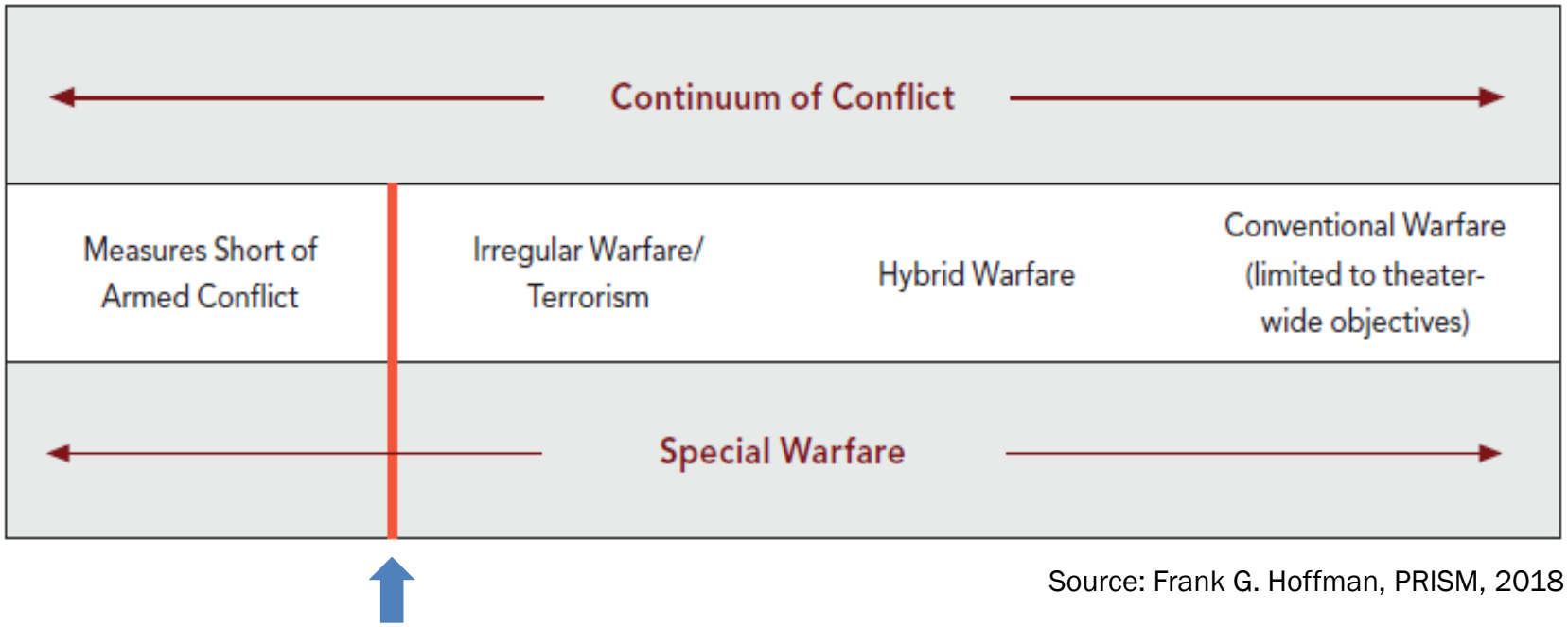
Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures ... and "white" propaganda to such covert operations as clandestine support of "friendly" foreign elements, "black" psychological warfare and even encouragement of underground resistance in hostile states. *- May 1948*

# Kennan's definition of political warfare continued

Political warfare scope conditions



# Continuum of Conflict

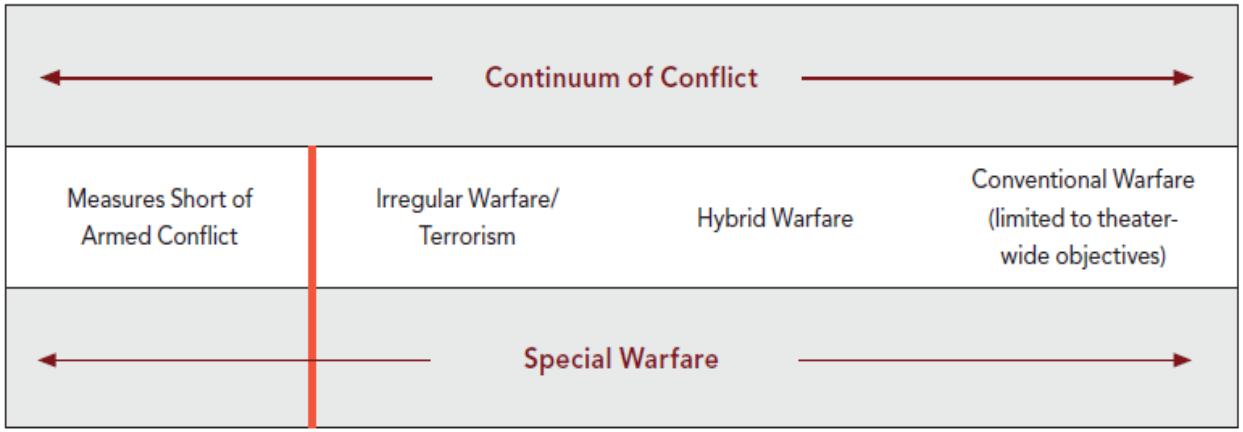


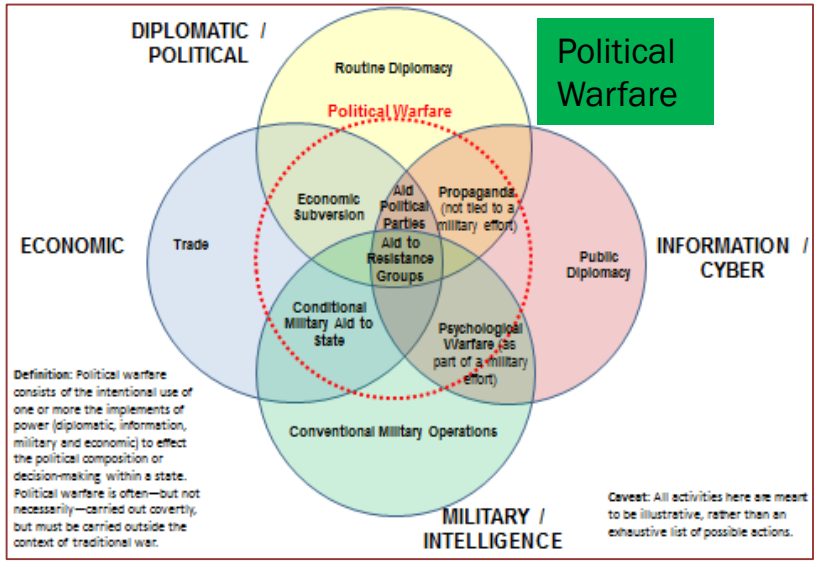

Source: Frank G. Hoffman, PRISM, 2018

- Alternative terms in use include Hybrid Warfare (NATO version), Gray Zone
  - All exclude Conventional (i.e. WWII-type) Warfare

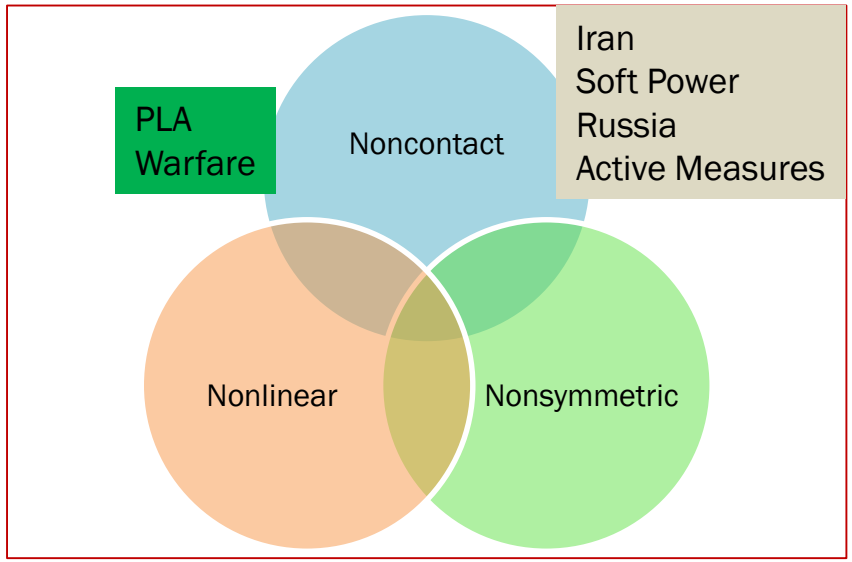
- Hoffman's continuum seeks definitional clarity based on **use, degree, type of violence**
  - However, warning and response may be delayed if violence is the tripwire
  - American "way of warfare" focuses on WWII conventional use of violence – adversaries do not
  - "Little green men" occupied Crimea w/ no shots fired; referendum achieved goal

# The WWII Mental Model Based on Physical Violence Inhibits Our Thinking




Political Warfare



# Modern Political Warfare: Study Approach

- **Examination focus:** nonmilitary activities and noncombat military activities
- **Relevant Cold War experience**
- **Case study method:**
  - Doctrine, theory
  - Operational approach, tactics
  - DIME framework for activity analysis
    - Diplomatic/political
    - Informational/cyber,
    - Military/intelligence
    - Economic/financial

# The Russia Case

Russia views its activities as defensive in reaction to US democracy promotion, NATO expansion

Strategic culture and Soviet history favor indirect action, active measures

Extensive shaping, propaganda, compatriot policy, followed by opportunistic intervention (Estonia, Ukraine)

Bronze Soldier 2007: Denial of service attacks avoided attribution

Russian “New Gen Warfare” innovations include massive troll farms, media penetration, Night Wolves, Orthodox church, energy dependence, economic sanctions

Net effects can be division, confusion, paralysis rather than outright win – “frozen conflicts”

# Russia Uses Whole Spectrum of State Power, Drawing on Range of Actors

- Extensive reach and capabilities, but important limits in resources and capabilities

- *Diplomatic and proxies*: 1) MFA, Rossotrudnichestvo; 2) Russkiy Mir foundation; 3) Biker gangs; 4) friendly political parties

- *Informational:* Russian propaganda establishment very influential among Russian speakers, less popular in West but ubiquitous
  - Rossiya Segodnya/ Sputnik (Official state organization)
  - RT (state funded)

- *Cyber:* Intelligence services in part draw on private capabilities

- *Intelligence:* Four competing agencies with differing resources, capabilities, geographic reach based in part of Soviet legacy

- *Military:* Improving Airborne, Spetsnaz, and other elite light infantry; use of intimidation via snap exercises, presence and harassing patrols

- *Economic:* Russia has energy exports and major investments, but economic statecraft may in some cases have economic, not political motives

# The Iran Case: Not just Great Power Competition

Iran “soft power” uses cultural, political, religious influence w/ Shia, pan-Arab, pan-Islamic audiences

Religious tactics include funding of junior clerics and mass pilgrimages

Robust aid to allies and political parties

Economic leverage through energy

Financial and cyber tools are well developed

IRGC Quds Force creates, sustains proxies who become political forces, create own proxies

# Key Attributes of Modern Political Warfare

Employs diverse (DIMEFIL) elements of power

Relies heavily on unattributed forces and means

Information arena is an increasingly important battleground

- Success is often determined by perception rather than outright victory

Information warfare works in various ways

- e.g.: amplifying, obfuscating, sometimes persuading

Cyber tools accelerate, compound effects

Economic leverage and coercion are increasingly preferred tools

Exploits shared ethnic or religious bonds, as well as social divisions

Extends rather than replaces traditional conflict

- Can achieve aims at lower cost

Non-state actors conduct political warfare with unprecedented ability

# Difficulties of Detection

Multifaceted form of warfare relies on ambiguity and deception

Detection is difficult, attribution more so

**Warning**

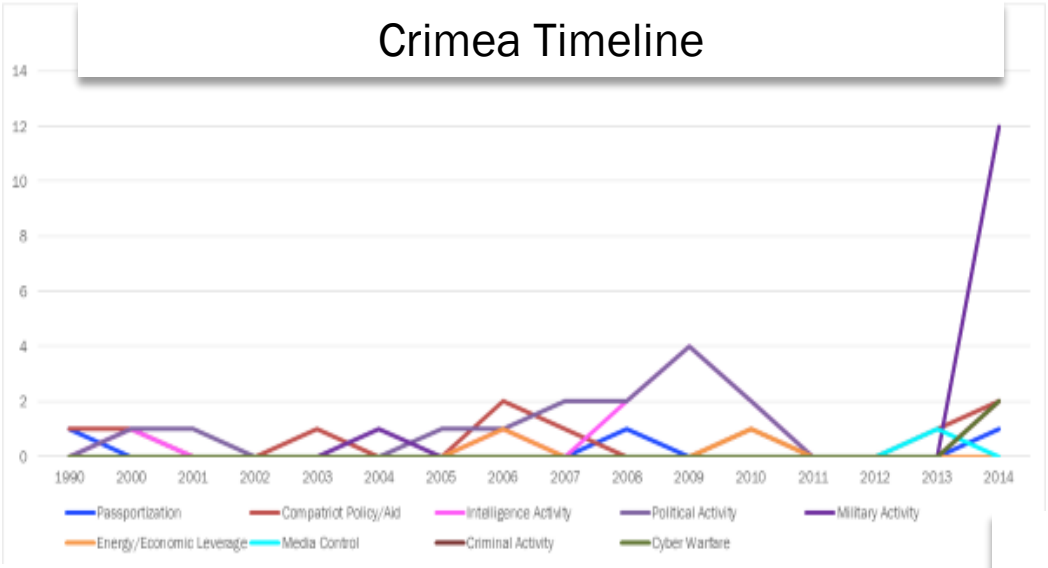
Even when once activity and authorship is established, what constitutes a significant threat?

Many activities' effects accumulate slowly over time

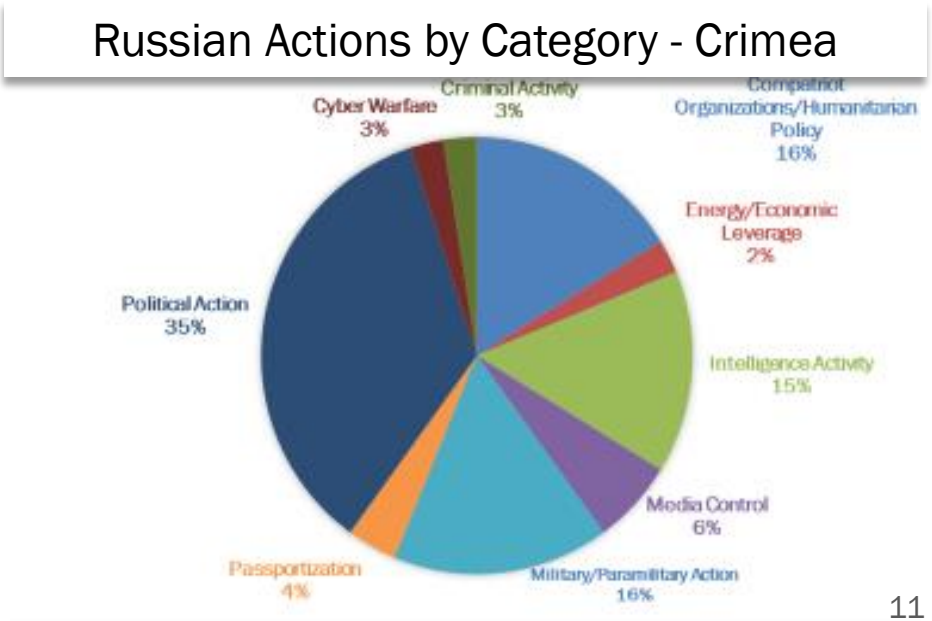
No single activity may seem threatening

Coup de grace may be sudden and opportunistic

# RAND Analytic System (ACTIV) tracks adversary activity and country vulnerability

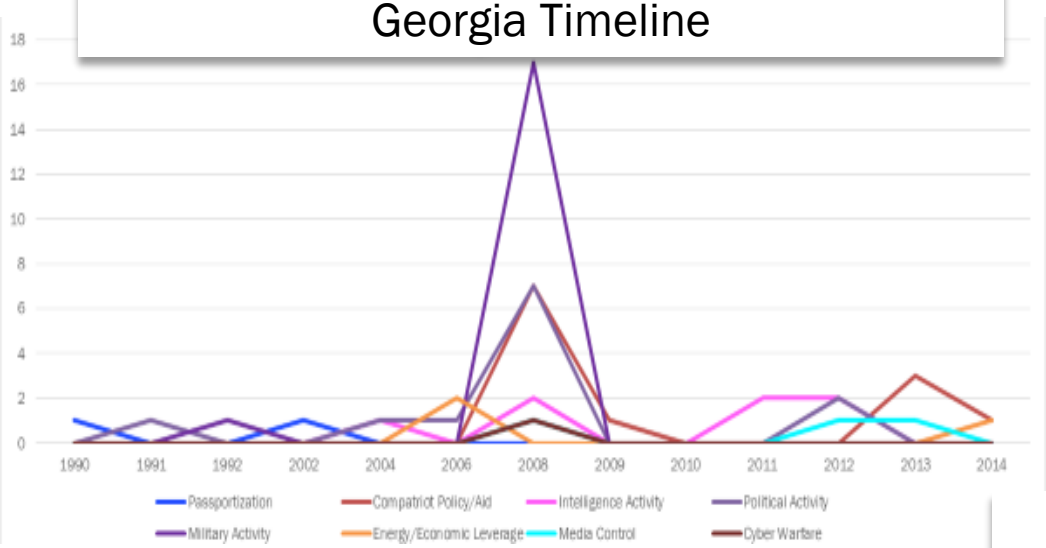



Illustration



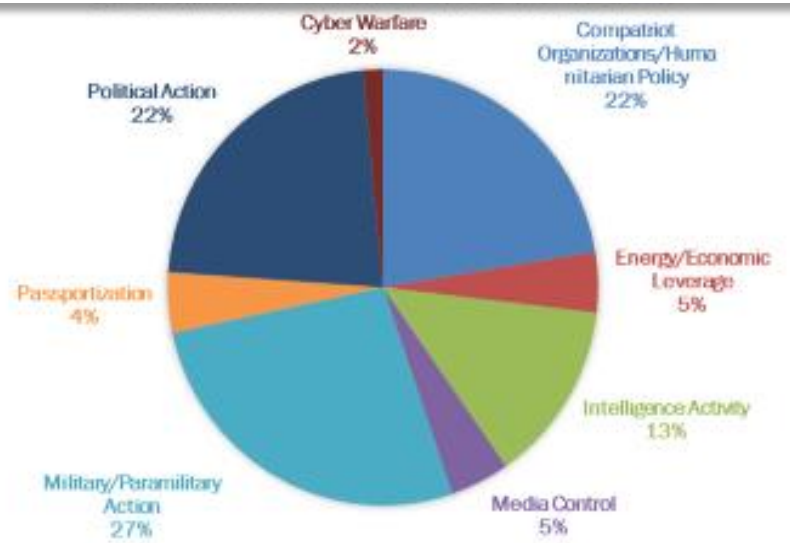
# RAND Analytic System (ACTIV) tracks adversary activity and country vulnerability

Georgia Timeline




Illustration

Russian Actions by Category - Georgia



# Response 1: Recognition as a form of warfare

**Increase prioritization**

US national security strategy historically prioritizes conventional and nuclear threats as most dangerous contingencies

**Be aware that political warfare is the most likely contingency**

- Cheaper to execute
- Can achieve aims if no response
- Appears to be increasing

**Seek multilateral response by governments**

- NATO declared Article 5 applies to Hybrid Warfare
- Provide support to states under attack

# Response 2: Strategy and Architecture

**Proactive Strategy Required**

Promote and Defend Rules-Based International Order

Promote and Defend Shared Interests and Values

**Architecture for Integrated Response**

Lead Coordinator required

- Kennan proposed State Department as lead
- Country expertise, diplomatic tools
- Oversee support to states under attack

**Government and Society**

- Total Defense (Nordic, Baltic models)
- Citizen roles span informational, cyber and local watch/defense

**Requirements and Capability Gaps**

- Presidential directive required to designate lead agency
- Funding increase and organizational reform
- Personnel, training and interagency requirements

# Response 3: Ways and Means

**Detect, Defend and Deter**

Audit vulnerabilities and increase resilience

**Respond**

- Effective Statecraft: Revive, revise and use cold war era toolkit
  - Expose and attribute informational and cyber attacks; levy financial sanctions; vet foreign direct investments; require intrusive inspections of technology (5G), assert freedom of movement, bolster allies through assistance, posture, exercises,
- Private Sector: Big tech assume active role, e.g., through adoption of code of conduct on authorship, sponsorship and content

**Defeat**

Mount active resistance to roll back subversion via aid, collective defense, support to resistance

# Response 4: Remedy Gaps in US Information Practices and Capabilities

Strategic-level communications are high-profile and bureaucratically risky, characteristics that militate against speed and initiative.

- Interagency coordination and National Security Council guidance pertaining to message themes remain lacking.

The new Global Engagement Center (GEC), established by presidential executive order and located at the Department of State, focuses on third-party validators or influencers from the bottom up, but has encountered various limitations.

CENTCOM Web Ops and USSOCOM JMWC are efforts to increase agile and effective internet-based information operations

- Unattributed communications may have counterproductive effects that should be anticipated and mitigated.

Robust academic work underway to determine what works best to win in the information space

# Recommendations for Special Operations Forces

Military commanders and the State Department should identify critical information requirements for political warfare threats. The IC should in turn increase collection and analysis dedicated to detecting incipient subversion, coercion, and other emerging threats short of conventional warfare.

DoD and the State Department should support deployment of special operations forces in priority areas deemed vulnerable to political warfare threats as an early and persistent presence to provide assessments and develop timely and viable options for countering measures short of conventional war.

The special operations community should make it a high priority to improve and implement fully resourced, innovative, and collaborative information operations. MISO requires both increased manpower and new media training.

5 additional recommendations to increase SOF/DoD-interagency coordination and mutual support for Title 22 environment

RAND ARROYO CENTER

# Discussion and Questions

Thank You