Russian Security State
GOVT-5519 / IPOL-3519 / REES-5519
Lecture 22. Information and Cyber Warfare

Yuri M. Zhukov
Associate Professor
Georgetown University

November 19, 2024

Today's objectives

1. *Take stock*: how has Russia leveraged "nonmilitary means" of war?
2. *Discuss*: how effective Russia's use of information operations has been
3. *Consider*: how cyber operations have (not) affected battlefield events

Generations of war (Russian taxonomy)

1. Pre-12th Century
   a) cold steel (spears, arrows)
   b) line & column tactics
2. 12th - 18th Century
   a) gunpowder
   b) smoothbore firearms, artillery
   c) fortifications, siege tactics
3. 18th - 19th Century
   a) rifled weapons
   b) dispersed formations
4. 19th - 20th Century
   a) internal combustion engine
   b) mobile armored warfare
   c) air power
5. Mid-20th Century
   a) nuclear weapons
6. Late 20th, early 21st Centuries
   a) long-range precision strike
   b) multi-domain (e.g. nonmilitary)

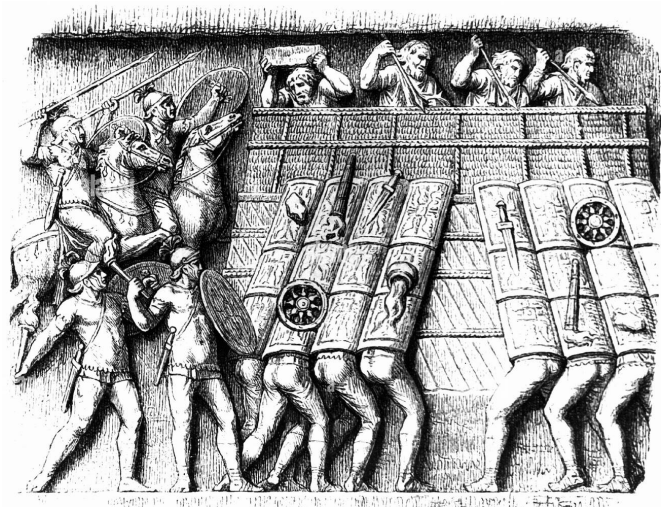

Figure 1: Testudo then

Figure 2: Testudo now

Non-military means

1. Role in Russian military strategy
   a) includes political, economic, informational, spiritual, cyber measures
   b) employed in peacetime & wartime as part of Active Defense concept
2. Cold War origins
   a) in communist camp:
      - discredit "apostates" (e.g. Tito)
      - construct negative image of West
   b) in West:
      - expose social problems (e.g. civil rights, homelessness, poverty)
      - undermine trust in state, elites
   c) in non-aligned countries:
      - support anti-colonial movements
      - offer education, scholarships (e.g. Patrice Lumumba University)
3. What's different now?
   a) info ops more targeted, less costly

Figure 3: Anti-Tito

Figure 4: Anti-lynching

Non-Military Instruments of Power

Overview

Non-military means: actors involved

	Russian State Actors	Russian Private Actors	Local Partners
Political	foreign ministry, IC (FSB, GRU, SVR)	NGOs, think tanks (e.g. IDC)	political parties (e.g. AfD, FN)
Economic	state enterprises (e.g. Gazprom), IC	private enterprises (e.g. RosUkrEnergo)	MNCs (e.g. Exxon), banks, state utilities
Spiritual	Moscow Patriarchate, IC	nationalist media (e.g. Tsargrad)	ROCOR, OCA, UOC-MP
Information	state media (e.g. RT, Sputnik), IC	troll farms (e.g. IRA), milbloggers	journalists, activists, NSAs (e.g. WikiLeaks)
Cyber	IC (e.g. "Fancy Bear", "Cozy Bear")	contractors, hackers co-opted into service	anti-Western hacktivists

Categories of non-military actions

1. Overt actions
   a) public and directly attributable to RF (e.g. diplomacy, media broadcasts)
   b) (usually) not illegal
   c) no effort to conceal state involvement
2. Covert actions
   a) secret and (usually) illegal actions (e.g. cyber attacks, bribery)
   b) extensive effort to conceal involvement
3. Denied actions
   a) covert actions that are either discovered, or too big to conceal (e.g. support for DNR/LNR)
   b) official denial, despite public evidence

Figure 5: alt.facts

Figure 6: Vote JC

Types of information operations

1. Plant novel messaging
   a) goal: create new narrative
   b) approach:
      - message "seeded" on Russian state media or proxy source
      - message becomes "unmoored" from original Russian source
      - message circulates organically
2. Amplify existing messaging
   a) goal: reinforce existing narrative that aligns with Russian interests
   b) approach:
      - publicize, "re-up" message already in circulation
3. Flood the zone
   a) goal: confuse, exhaust
   b) approach:
      - seed, amplify multiple (mutually contradictory) messages

Figure 7: Don't

Discussion

Russian information operations often seem uncoordinated, decentralized.

1. Is there an advantage to an uncoordinated information campaign?
2. Which of these considerations are more/less important for IO?
   a) resilience / continuity of effort
   b) plausible deniability
   c) message discipline
   d) synchronization of effort
   e) economy of effort (avoiding redundancy, duplicate effort)
3. How does this square with tradition of centralized C2 in Russia?
4. Would more centralized C2 make Russian IO more deterrable?

Effectiveness of Russian Information Operations

How do we know if info ops are effective?

1. Observational data
   a) compare opinions/actions of people exposed to more vs. less messaging
   b) difficulties:
      - isolating effect of Russian messaging from all other content
      - people self-select into exposure groups (e.g. InfoWars vs. CNN)
   c) hard to establish causal inference
2. Experimental data
   a) randomly expose study subjects to message vs. placebo
   b) advantage:
      - no self-selection
      - causal effect identifiable
   c) disadvantage:
      - external validity (lab ≠ real life)

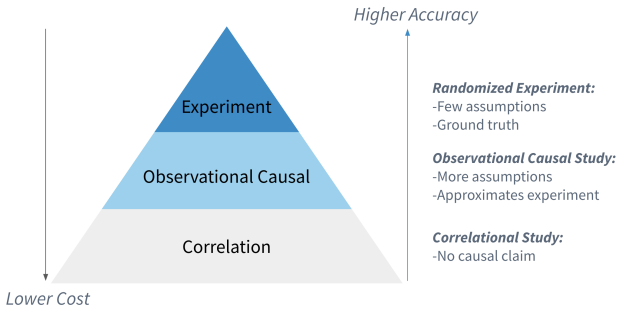

Figure 8: Truth pyramid

What do the data say?

1. Evidence is mixed
   a) little/no evidence that Russian IO affects attitudes or behavior in West (Eady et al 2023)
   b) strong evidence that Russian IO affects domestic public opinion (Krishnarajan and Tolstrup 2023)
2. What might explain this disparity?
   - ☐ more competition for audience attention in West
   - ☐ volume of messaging too low
   - ☐ "ceiling effect" due to audience micro-targeting (messages sent to hyper-partisans, not persuadables)
   - ☐ audience not receptive or resistant to messaging
   - ☐ Russian involvement too overt

Figure 9: Not easy

Cyber Warfare

Varieties of malicious cyber activity

1. Cyber espionage
   a) objectives:
      - passively collect information
      - discover system vulnerabilities
2. Cyber crime
   a) objectives:
      - raise revenue by weaponizing information discovered in #1
3. Cyber propaganda
   a) objective:
      - influence elite, public opinion
      - undermine support for policy
4. Cyber disruption
   a) objective:
      - sabotage opponents' ability to operate in physical, electronic domains (e.g. DDoS attacks)

Figure 10: Info is power

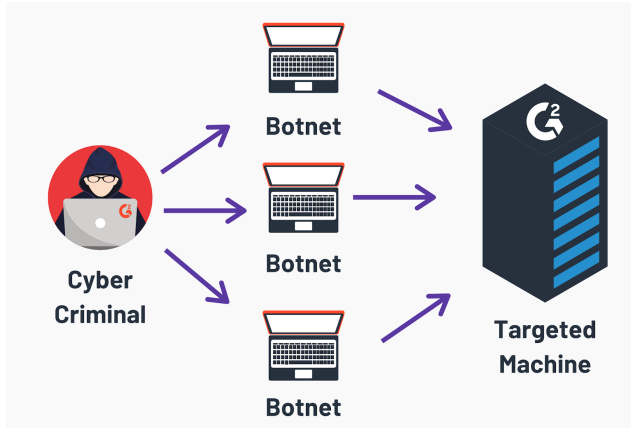

Figure 11: DDoS

Examples of malicious cyber activity

1. Cyber propaganda
   a) Sony Pictures hack 2014
   b) "Cyber Caliphate" 2015
   c) DNC email leak 2016
   d) BlueLeaks 2020
2. Cyber disruption
   a) USSR pipeline 1982
   b) Estonia mass DDoS 2007
   c) Iran Stuxnet 2010
   d) Ukraine 2014-
      - power grid 2015
      - "NotPetya" 2017
      - hacking of CCTV cameras
      - artillery mobile app

Figure 12: Cyber Caliphate

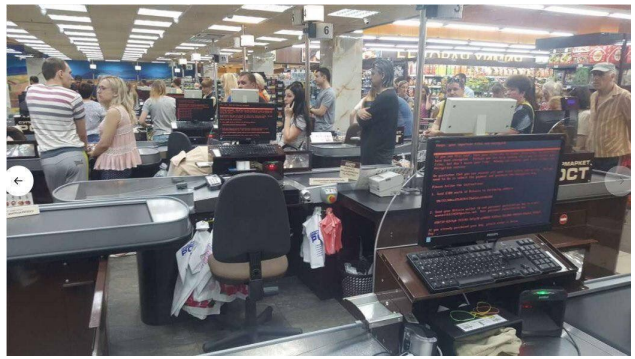

Figure 13: NotPetya

Effectiveness of cyber warfare

How big of a threat is cyber warfare?

Alarmist view

1. Offensive advantage
   a) can strike targets at great strategic, operational depth
   b) ability to quickly disrupt opponent's C4I
2. Low cost to attacker
   a) operators not in harm's way
3. Element of surprise
   a) target initially unaware of own vulnerabilities ("zero day" attacks)
4. Challenges of attribution
   a) attackers cover own tracks
   b) can be hard to establish origin of attack with high confidence

Cyber is "top threat to U.S." (DNI, 2015)

Figure 14: Threat matrix

How big of a threat is cyber warfare?

Skeptical view

1. Costs to target are also limited
   a) disruptions are mostly temporary
2. Depreciation after first use
   a) no more surprise after "zero day" (software patches, updates)
3. Hard to synchronize with kinetic ops
   a) malicious code takes time to write, effectively deploy
   b) hard to launch attacks on tactically-relevant timeline
4. Commitment problems
   a) targets may see compliance as unnecessary or insufficient to stop attacks (due to misattribution, limited damage, quick recovery)

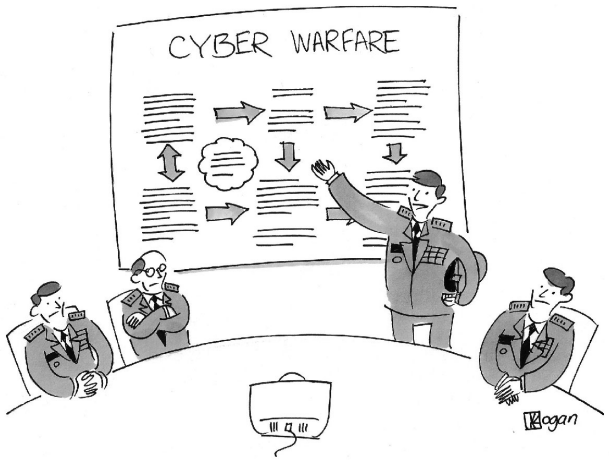

Figure 15: Best laid plans

Case study: Ukraine, 2014-2016

Can cyber attacks shape battlefield events?
Evidence from War in Donbas

1. Cyber attacks
   a) 1,841 cyber attacks (2013-2016)
      - DDoS detected by Arbor Networks
      - attacks claimed on social media (Facebook, VKontakte, Twitter)
      - websites/blogs of non-state actors
      - Ukrainian, Russian media sources
   b) interviews cybersecurity experts
2. Kinetic operations
   a) 29,289 actions by pro-Russian and Ukrainian govt forces (2014-2016)
      - Ukrainian, Russian media sources
      - event classification via ML
      - weekly & daily time series

Figure 16: Cyber

Figure 17: Kinetic

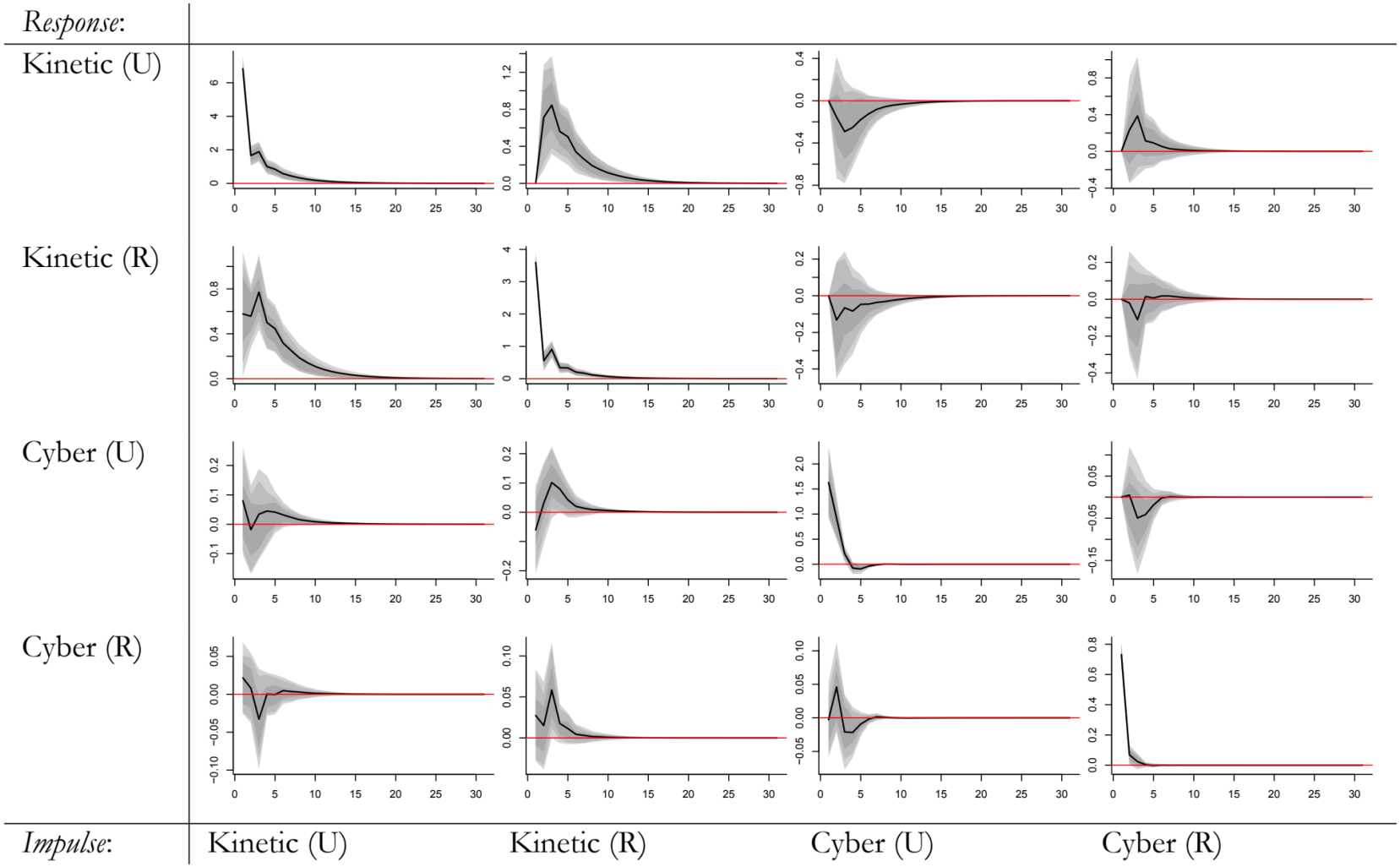

Figure 18: Impulse-response of kinetic, cyber operations in Ukraine

What do the data say?

1. No interdependence b/w kinetic, cyber ops
   a) strong Kinetic (U) $\leftrightarrow$ Kinetic (R) link
   b) but cyber shocks account for $< 1\%$ of variation in kinetic ops
2. Cyber warriors hardly even respond to each other's cyber attacks
   a) no evidence of reciprocity, instant retaliation
3. Cyber domain seems totally disconnected from kinetic domain, and itself

Figure 19: Couch warriors

Explanations

1. Limited resources and capabilities
   a) limited pre-2014 investment in cyber units, capabilities in Ukraine
   b) but this can't explain coercive failure on Russian side
2. Lack of coordination with hackers
   a) SBU initially had limited desire to cooperate with non-state hacktivists
   b) but this not true in Russia
3. No good targets
   a) Ukrainian industrial control systems, critical infrastructure mostly off-line
   b) but power grid attack shows massive disruption is possible
4. Cyber warfare never seriously attempted
   a) Russia hesitant to compromise ongoing cyber-espionage operations
   b) priorities (on both sides): propaganda > disruption

Figure 20: Back to kinetic

NEXT MEETING

Backgrounder: Ukraine (Th, Nov. 21)

- What is a "nation"? Which groups attain "nationhood"? Why?
- What does it mean to "decolonize" the study of Ukraine?