Strategic Studies Discipline and Cyber Innovation in Military Affairs – State of The Field

International security experts are preoccupied today with describing, explaining, conceptualizing and predicting cyber strategic behavior. Scholars are working to reduce social and technical uncertainties associated with cyber operations.

This talk reflects on the main conceptual debates tendencies in the cyber realm in several strategic communities around the world.

Apply classical strategic and military terminology, adjust the existing terminology and invent new terms to describe an unprecedented phenomenon.

*Strategic Studies Discipline, Cyber Capabilities and Evolution of Warfare: A Theoretical Overview*

This talk examines core academic debates dealing with the impact of cyber capabilities on the character of warfare. Specifically, it reflects on the four main questions posed by the strategic studies discipline in this regard today: (1) whether cyber capabilities herald change or continuity in the nature of warfare, and thus constitute a revolution or an evolution in military affairs? (2) How does cyber capabilities impact the offense-defense (resilience) balance and which form of strategic activity do they favor? (3) What is the nature of deterrence and coercion in the cyber realm? (4) Whether cyber-warfare is a stand-alone domain of military activity or a component of other domains? Various strategic communities around the world conceptualize these questions and strategize about cyber interactions differently. This talk will touch upon this competition of learning in the cyber realm and will highlight several unique characteristics of the Russian approach to these issues.

This talk examines concepts and notions about the impact of cyber capabilities on the character of warfare that have been circulating in Russian strategic and expert community during the last decade. The talk situates Russian approach in the comparative context of the global cyber competition of learning, reflects on the intellectual sources of Russian thinking about information (cyber) warfare, and highlights several unique traits of the Russian approach – “holism,” “hybridity,” and “permanency.”

**The title and about myself.**

**Basic Assumptions**

* Cyber – one of the main contemporary mil innovations. Definition of the RMA.
* Current moment – a la 20s-30s & 40s-50s Situation similar to early RMAs. We are in a similar situation to the 20’- 30’ (mechanization of warfare) or the 40’-50’ (nuclearisation of warfare).
* Arms Race and Competition of learning among various strategic communities.
* Many unanswered academic-conceptual and critical national security questions on how to relate oneself to cyberspace.
* Classical strategic thought is restudied, deconstructed and applied in the new context.
* Practitioners and theoreticians of strategy develop new knowledge
* When the new innovation is introduced, SS theoreticians try to conceptualize it and describe its major characteristics. The growth of the arsenals and practice outpaces conceptualization. Practitioners outsource questions to theoreticians.
* Very common in the US and EU, in general and now. In Israel less common but also gathers momentum in the last years (less in the cyber realm).
* Our common goal: to evaluate the impact of cyber capabilities on strategy. Joint learning process. No consensus yet on the main questions and how main terms apply to this phenomenon. I will register for you the state of the field and will reflect on main questions and debates.

Contents

Disclaimer 1: work in progress for Aluf Baidatz in Mabal Research Center

Disclaimer 2: pls let me present and then learn from your Q, remarks and observations.

**Is Cyber a Separate Domain and another RMA?**

* What’s RMA and Why its Important – Force Build-Up, CONOP, OrgStr, Budget.
* Is cyber a 5th domain of warfare or a factor operating in the traditional four? If, it is a separate domain, then it’s an RMA.
* Definition: Digital Abuse / Cyber warfare enablers: cyber crime, cyber espionage, hacktivism. Cyber warfare: Computer Network Exploitation/Attack on ICS (industrial control systems) a la Stuxnet.
* **The RMA thesis proponents** holds that:
* IT enabling digital disruption and physical destruction herald new form of warfare – the Cyber RMA.
* Before, it is part of EW. The discontinuity. When whole world becomes WWW based in the 1990s, it turns into the human domain and then warfare domain.
* A la Strategic Bombing /Nuclear concept. One can generate strategic effects and achieve political goal bypassing actual conventional battlefield. Imposing once will on the opponent without conquering his territory, producing mass destruction, without making one shot.
* Devastating cyber strike breaks enemy's will and capability to wage conventional warfare.
* Thus, cyber is strategic substitute, rather than operational complement to conventional military.
* Cyber capabilities (CNA/E) change the character of war:
* precise & tailored effects that a conventional attack cannot.
* reduce the importance of fighting in traditional domains
* no specific physical space and time for waging the war.
* Expand the range of strategic opportunities to harm significantly in between war and peace, without resort to traditional violence (New type of social-economic disturbance – ex. weeks of gov. paralysis in Estonia; paralyzing gov communications in Georgia)
* Power projection: Obliterates the traditional differences between local and distant conflicts.
* Supporting evidence: organizations are emerging and, traditional forms of warfare become obsolete. It is moving in the direction of the RMA.
* RMA proponents: **Cyber as discontinuity – the 5th Domain of Warfare**

Cyber RMA thesis: more influential among practitioners, than among the theoreticians of strategic studies.

* **The RMA thesis opponents**
* Prolongation of the IT-RMA
* Further refinery of the EW against C4ISR and its extension of NCW and EBO.
* Truly devastating cyber attacks will be extremely difficult to execute outside 4 traditional domains.
* Devastating cyber weapon is impossible because collateral damage will quickly reach the attacker.
* To early to judge. No real cyber war between two militaries. So far no dramatic effects (even Stuxnet).
* RMA opponents: **Cyber as continuity – extension of the of the 4 traditional Domains**
* Less useful if Isolated and divorced from other domains.

**What is the Offense – Defense Balance in Cyber Domain?**

* Each and every new military innovation shapes the offense-defense balance.
* **Offense Dominant Environment**
* Technically, it is impossible to block all attacks – computer has to accept incoming connections. Internet designed for easy connections.
* Analogy with the nuclear first**-**strike – no credible defense.
* (Speed)Offense initiates, Defense catches up slower. No counter-measure until the attack takes place. Antivirus is based on the databases of existing malware. Attacker can vary signatures and vectors of attack quicker than defender can detect and close them. Takes time to develop a countermeasure.
* (Cost) Attacker should succeed only once. Defender should succeed every-time against every attack. Defense is thus more expensive – more to cover. Attacker chooses the place and time
* Certain capabilities may be produced on-line. Offensive Botnet Armies are easier to mobilize. Defensive forces divided between public and private sector.
* Defense fragmentation: lack of total cooperation of private and public sector, which enables access from multiple undefended vectors.
* Vulnerability: users prefer convenience over security.
* Bottom line**:** the Cyber attack will always get through. (a la strategic bomber)
* **Alternative view of Offense-Defense**
* Complexity of weaponization makes cyber offense (CNA a la Stuxnet aimed at physical destruction) less easy, and defense more feasible.
* Offense dominant for criminals, espionage and hacktivists, but not for soldiers (not for the warfare).
* Damage produced by Stuxnet was quickly repaired.
* Lack of massive strategic cyber-warfare a la Stuxnet – possible evidence of the superiority of defense. Questionable effectiveness of offence.
* Lowering defense costs: on-line open source community can work for the Defense (Stuxnet investigation case).
* Defenders can:
* build in redundancy and robustness of the systems
* make environment difficult and unfamiliar for attacker to address.
* use deception and confuse attackers
* traps that reveal attackers identity

**Is Deterrence Possible in Cyber Domain?**

* D Definition and its Two forms: Denial and Punishment
* D in Cyber: convincing an actor by threat to not opt for cyber attack.
* Widespread thesis: Deterrence is ineffective in cyberspace, compared to nuclear or conventional realms. Why?
* *What undermines “Deterrence by Punishment”?*
* Attribution Problem: difficult / time-consuming to identify attacker.
* Anonymity does not leave return address to retaliate.
* Forensics takes months; anonymous attack seconds.
* Can’t credibly threaten retaliation.
* 2 Credibility Problem: although cyber is Offensive Dominant, states keep their offensive capabilities secret. Revealing capabilities decreases their effectiveness. Use and Lose phenomenon.
* Asymmetry Problem – not all actors are equally digitalized. And sometimes hacktivists or criminals. Difficulty to retaliate in kind.
* *What undermines “Deterrence by Denial”?*
* Credibility Problem: defense is seen as inherently weaker than offense. Can’t threaten denial.
* EW hardly possible, in contrast to conv, sub conv and non conv realms.
* Alternative view
* Deterrence by Resilience” – emerging novelty – absorbing the strike, mitigating the harm, and quickly recovering.
* Attribution is difficult, but possible. Improvements in Forensics, Intel Disciplines and International Cooperation.
* Attribution problem is also a liability for attacker. Significant energy and resources. May be that’s why we have not yet seen deadly CNA.
* Coercion and Deterrence demands some level of disclosure, to communicate your demands as in other forms of strategic interactions.
* Second strike capability can be preserved in cyber-domain +
* Reverse Asymmetry & CDD: Conventional retaliations against cyber strikes are possible. Another 2nd strike tool. – Cross Domain Deterrence
* EW possible: Strategic context and Fast Detection.

**Does Cyber Empower Strong or Weak Actors?**

Empowering Strong:

* Exclusivity of CNO. Only really strong actors will be able to develop significant military grade CNO (attack) capabilities. Weak will be left behind.
* Ineffective Asymmetries. Weak actors can utilize their asymmetrical advantages only up to a certain (not critical) level.
* Backing Cyber with other forms of Power. Cyber warfare should be backed by traditional military, political and economic capabilities to achieve real strategic effects and to exploit cyber effects. (Estonia ,Gruzia and Ukrain can be paralyzed but you need more power to achieve real outocomes). Thus, it only extends the existing disparities between strong and weak actors.

Empowering Weak:

* Expanding strategic toolkit of the weak and power projection capabilities.
* Accessible Capabilities due to Diminishing Costs. The costs of what was considered a significant cyber attack last year is diminishing as the code becomes accessible for reverse engineering. Little development expertise and capacity is needed.
* From Quantity to Quality - multiple aggressive actors with global reach capabilities (even if minor) may harm and increase global political disorder.

**Does Cyber Favor Strategic Stability?**

* Yes:
* Operating Under the Violent Threshold: cyber enables to attack and to promote strategic goals without turning to traditional forms of war. Substitute for devastating and apocalyptic alternatives
* Not enough Violent to be considered a War
* Cyber War is Not Coming due to interconnectivity. Self Deterrence.
* Enhanced Cooperation & Diffusion of technology may enable more modes of cooperation between various, state and non-state actors around the world that share common goals and adversaries.
* No:
* Large – N of cyber actors and fragmentation of traditional coherent IR players increases complexity. Power moving away from the governments.
* Second Order Consequences – accidents and misinterpretations of big powers.
* Favors Cyber Arms Race. No international arms control regulation in this field. Low probability for verification procedures and CBM as in the nuclear or conv. realms.
* Offense Dominance Temptation to use it in light of the Attribution Difficulty.
* Active Defense Temptation – temptation to overcome defense inefficiency by preemption.
* Poor strategic depth (long time between experiencing an attack and deciding where to respond and how) may favor Cyber Dooms Day Machines (automatic responses). Inadvertent escalation from minor cyber exchange to major conventional war.

So What? Why these questions matter? Because different strategic communities think, act and invest resources according to the answers to these questions.

Their answers may be unique and may vary. Different actors conceptualize cyber according to their strategic mentalities, strategic traditions and military cultures.

Today, the US, Europeans, Russian, Israeli, Iranian, Chinese conceptualizations of cyber warfare differ from each other. This corresponds with the intellectual histories of the earlier military innovations and demonstrates different cultures of military innovations across the globe.

Let me briefly address peculiarities of the Russian approach and contrast & compare it with the others.

Russian approach manifests continuity in its strategic tradition.

**Slide 1: Intellectual Roots, Historical Sources and Drivers of Change**

* 1. The Soviet MTR and the US RMA debates and concepts (Reconnaissance-Strike Complex, Electronic Warfare, Information Dominance, NCW, EBO.
	+ Ogarkov – transformation from massive armies to IT driven operations.
* 2. “Active Measures,” PSYOPS and Information Campaigns
* Lessons learned from: Afghanistan; the USSR collapse, ½ Chechnya Wars; the US information campaigns during GWOT – strategic battle for the narrative.
* Tool of influence - coercion and deterrence
* 3. Equalizer of Conventional Inferiority
* Asymmetrical Trump card - equalizer for conventional inferiority in the IT-RMA era: PGMs, stand-off, and power projection.
* EW and IW may turn in a separate domain that will determine the course and outcome of the future war, may be even without actual fighting.
	+ To weaken C4 of the opponent, at the initial stage of the conflict, to degrade its military effectiveness.
	+ Then, during fighting, to dominate in the battle of narratives and create a positive image in world public opinion.
	+ Or to subdue by IW campaing

**Slide 2: Russian Perspectives on Cyber(Information) Warfare**

**Differences in Conceptualization and Terminology in** Russian and Anglo-sphere

* Information Space (security) vs. Cyber Space (security)
* Russian Cyber Security Strategy, *cyberspace* is part of the *information space*.
	+ Information space – sphere of activity shaping individual & social perception, information itself and information infrastructure.
	+ The latter is a cyberspace - inseparable subset of information space.
* Information Warfare vs. Cyber-warfare
* Cyber warfare relates to foreign concepts and potential aggression acts.
* Russian term - Information Warfare/Struggle (informatcionnaya bor’ba) (sredtstva inf bor’bi) – part of Russian professional discourse but not used in Anglo-sphere.
	+ CNO, EW, PSYOPS, Deception Campaign – Maskirovka (CC&D).

* Information Warfare – tool of statecraft bending the adversary to your will.
* Information potential as enabler of political, economical, and military dominance.
* Cyber attacks are part of the coordinated program of particular state to achieve its strategic goals.
	+ Imposing one’s will without using military force.
	+ To control behavior and resources without physical invasion.
	+ Preparing optimal conditions for the use of force (force multiplier).
* ~~Global info campaign / public diplomacy goals - Improving Russian image abroad.~~
	+ ~~Russia – an indispensible actor of IR.~~
	+ ~~Shape international environment to its liking.~~
	+ ~~Developing FP success (after Syria and Iran.)~~
	+ ~~Defense of Russian culture and promotion of its traditional values~~

**Perception as Center of Gravity;** Reflexive Control as Tool

* Interfering in decision-making process and manipulating consciousness of the individual, government, organization and mass.
	+ Manipulating information to manipulate decision-making process.
* Producing false picture of reality and forcing an actor to act according to in the predicted way favorable to you. (Reflexive control)
* IT - Tool of political subversion and regime change (both defensive and offensive perception)
	+ Fighting for peoples’ minds, hearts and souls – to transform values of particular group of the citizens and turn them into the promoters of the interests of the foreign state.
* Subordinating Elites and Societies.
	+ Use and Abuse of Social Media - Most serious public opinion mobilization tool (+ other mass media).
		- Colored revolutions, protests in Moscow, Arab Spring, protests in Kiev– IW generates offline protests and regime changes. (Some argue that in Estonia 07 and Georgia 08 ,Russia did the same).
* Quest for cyber sovereignty and international regulation of info-space
* Information Control - Source of In/Stability. Deepest Concern – Unrestricted dissemination of inf. over the Internet. Internet Sovereignty.
	+ Desire to introduce international regulations and restrictions on national barriers in cyberspace.
	+ Promoting global agreement on principles of information security – internet sovereignty - to restrict hostile codes and hostile contents. (The West focused on codes and reluctant about contests)
		- Ex1. All White papers in the filed of Information Security aim to prevent intervention in internal affairs.
		- Ex.2. Snowden Affair (total US surveillance) – support of the Russian argument.
		- Ex.3. The Register of Banned (Russian) Sites – “Filtering on the Nationwide level” - After the Arab spring and especially after the 2011 protests – an attempt to introduce the system censoring and controlling Russian blogo-sphere. Looking for offline solutions against actors operating outside Russian jurisdication (Facebook, Twitter). Not very effective yet and not fully imposed. Draft Law.

**Uniqueness of the Russian Approach to IW**

Keep in mind Estonia, Georgia, Ukraine.

* **Holistic Approach Over Domains** (*kompleksnyi podhod*)
	+ Hostile Code and Hostile Content
		- The main divergence from the West and peculiarity of the Russian approach (resemblance to China) is that not only the “code” but also the “content” is seen as threat.
	+ Digital Sabotage and Psychological Subversion
		- Digital sabotage (disorganize/disrupt/destroy state administration) and psychological subversion (discredit leadership, disorient operators, demoralize population) to coerce the actor to make decisions in the interest of the other side.
		- Info-technical strike serves info-psychological pressure. Baits promote particular content.
		- Two types of logic bombs - Syntactical attack - disrupting information system by malicious code & Semantic attack - destructing decision-making process by manipulating the contents.
		- Info-psycho superiority precedes actual fighting; may even render it obsolete. Victory is a psycho act. (Nagovitzin, 2009)
	+ ~~Hence, Holistic Means of IW (CNO, EW, PSYOPS, CC&D)~~
* ~~“Sredstva Informatcionnoi Bor’by,”: CNO, EW, PSYOPS, Deception campaign (CC&D, Maskirovka – both codes and contents).~~
* ~~Ex1. Soviet doctrinal roots of kompleksnost’ (Kinetic, EW, PSYOPS).~~
* ~~Ex.2. Holistic Approach in Action: Countermeasures to 2011 protests - combined application of soft and hard power (promoting alternative content, disrupting discussions, spamming, DDOS of NGOs supporting protesters, bots against particular Twitters, requests to close VKontakte pages, discrediting of opposition leaders (revealing funding information), in parallel with offline actions against the protestors.~~
* **Unity and Hybridity of Efforts (across actors and across domains)**
	+ Synchronization of efforts (IW, Kinetic Campaign, Narratives Battle)
		- * Full spectrum operations: IW, kinetic campaign (Georgia), Public Diplomacy (strategic communications)
	+ Synchronization of effects (On-line & Off-line activism)
		- * Online events/narratives trigger off-line events/behavior and vice versa.
			* Ex1. Estonia: offline and online activism;
			* Ex.2. Georgia: cyber-attack coupled with kinetic military operation; in both cases, but especially in Georgia, supplemented by active measures and psyops.
			* Ex. 3 Crimea/ukraine
	+ Hybridity of actors
* Synergy among various cyber-actors – gov and non-gov.
* Co-opting and co-ordinating Hacktivists, cyber criminals, state cyber capabilities.
* The invisible hand behind the hacktivists. Deniability is part of the modus operandi.
* Ex. Estonia, Georgia, Kirgizstan – light management touch is good enough to put the campaign in motion and light enough to ensure deniability. Loose network or highly empowered individuals cooperating virtually.
	+ For the tacit approval from the Russian government, hackers and criminals proved their botnets for the government at the times of need. (RBN cybercrime group is the best example). Security services cover the network.

- There is no conclusive evidence of Russian gov. involvement in Estonia and Georgia cyber incidents. But, I don’t see the reason not to co-opt hacktivists in future campaigns, if to judge by recent events in Ukrain (titushki).

* **Permanence (across space and time)**
* IW campaign (codes & contents) conducted/uninterrupted in peacetime, in the prelude to war and in wartime.
* On all three levels: T, Op., Str.
* No clear beginning and not clear end.
* Mainly info-psy, with going up on the escalation ladder according to the circumstances. It can be augmented by info-tech (Estonia + Georgia) and kinetic actions (Gerogia).

Three main differences from the Western approach and similarity to Chinese:

* Broader campaign - (not only digital but soft, psychological issues) – but synthetic connection between code &content
* No peace & war times but continuous multidimensional campaign
* Time perspective of the campaign is longer than in the US (not confined to particular crisis/event) but shorter than in China

Bottom Line: Russians are also in the midst of learning and change.

So What? Implications for Israel.

* What are the Israeli views on these questions?
* Are there any other big questions that academics overlook?
* Russian Case in the “Red” and “Blue” context: what can be learned?

**In the midst of cyber learning**

* **Conceptual and organization incoherence**
	+ Russian strategic community is in the midst of cyber learning and strategizing about cyber paradigm.
	+ Opinions of cyber policies and basic definitions are divided giving rise to conceptual confusion and organizational competition.
* **Competing-cooperating cyber actors** (MVD,FSB, FSO, SVR, FSTEK, Military)
	+ Interior Ministry (MVD) – directorate K (computer crimes); FSB - Inf. Sec. service (external virtual threats to national and economic sec. – computer counter espionage); FSO (gov communication and nuclear C2); Federal Servise for Ex&Tech Control (counter-intel of sensitive technology) The military does not have a unified component (diffused across various places GRE/REB), and SVR
	+ All main 5 cyber actors probably have CNO capabilities
* Although most of the places represented as defensive they seem to offensive capabilities. Russian term – bor’ba- incorporates both offensive and defensive.
* Russian DARPA (Fund of Prospective Research) – one of the main focuses and first fund allocations go to cyber.
* **Military Reform** (EW,NCW,C4ISR)
* Lessons Russia learned from Georgia: improved, but still poor performance in info-tech and info-psych domains.
* Reform - main improvements in EW, NCW and C4ISR
* Other components of strategic community have capabilities that the military is seeking (FSO, FSB, SVR).
* **The place of the Cyber troops/command in strategic community**
	+ The place of the cyber troops/command in strategic community is debated.
		- Rogozin (Vice MoD) – proposed in 2012.
		- Shoigy – Gl. OpUpr. – staff work in 2013.
		- Ideas – not GS Directorate, but Branch of Troops (a la SMF) based on the IW components elsewhere in the military.
		- How will it be related to REB and GRU sigint?
* **Intensive learning and emerging corpus of knowledge**
* Despite lack of organizational cohesion - a solid corpus of theoretical knowledge produced during the last 2 decades. – Russian SC – theory before practice or actual capabilities.