Russian Approach to Information Warfare

Jeff Malone
School of Engineering and IT
Australian Defence Force Academy
September 2014
Scope

- Historical Context
- Russian Approach to IO
- Operational Vignettes
- Emerging Issues
Historical Context
Impact of History and Geography

- Key historical influences on Russian approach to use and manipulation of information in warfare are rooted in influence of Mongol approach to warfare and Russian geography
- Mongols in Russia largely fought and won outnumbered; made effective use of deception and intimidation (a primitive but effective combination of PSYOPS and kinetic operations/PPP) as an effective force multiplier
- Mongols effectively employed then extant technologies (carrier pigeons, dedicated communications dispatch riders) to enhance speed of own C2; also specifically targeted the same in adversaries
- More generally, the flatness of the steppes makes it difficult to employ natural camouflage and concealment, places emphasis on active deception means

Depiction of the Battle of Kulikovo in 1388 – a Russian victory over the Mongols, using their own tactics of concealment, deception and ambush against them
Revolutionary Era Influences

• In early Soviet era, keen interest in use of propaganda for both internal mobilisation and loyalty, and as a weapon to subvert adversaries

• This also entailed the use of disinformation, proxies and false-front organisations for propaganda dissemination

• Soviets identified then emergent media technologies (mass newspapers, radio, cinema) as critical dissemination means

• Correspondingly recognised vulnerability of own population to foreign influence, leading to a strict regime of censorship and media control in the Soviet state

“We can and must write in a language which sows among the masses hate, revulsion, and scorn toward those who disagree with us.” - V.I. Lenin
Maskirovka

- Entails the coordinated employment of OPSEC, passive camouflage and concealment, MILDEC and counter-intelligence and counter-ISR activities

- Concept first emerges in the 1920s, but is refined on the basis of its employment and operational experience in the Great Patriotic War

- Particular interest in relationship between maskirovka and surprise, particularly in the crucial initial period of warfare to achieve decisive victory; lessons from German success at start of Operation BARBAROSSA

- The concept is applicable from the tactical up to the national level, and is to be integrated with other information-based activities

Diagram illustrating the environmental, technical and operational dimensions of maskirovka
Radioelectronic Combat

- REC emerged in the early 1960s as an operational concept that integrated maskirovka, EW, and offensive (kinetic) fires
- Entails both defensive/protective and offensive actions and acts as a force multiplier
- Key missions in REC:
  - Protecting friendly C2
  - Disrupting adversary C2
  - Obtaining intelligence on adversary REC capabilities
  - Denying adversary intelligence on friendly REC capabilities
  - Achieving surprise in the initial stage of war
- Similarity to later US concepts of C3CM and C2W, but precedes them by over a decade

The Soviets made significant investments in REC and REC-enabling capabilities; pictured here is the *Ural*, a dedicated C2 and REC vessel for the Soviet Far East Pacific Fleet.
The Military Technical Revolution

- Term gradually emerged from late 1960s onwards, to describe the impact of emerging information technologies on the conduct of warfare
- Identifies that the increases in the speed of C2 and the increasing precision of effects would have transformational implications; lessons from Vietnam Conflict and Arab-Israeli wars
- Key issue for Soviets was that effective Western exploitation of technology would render Soviet numerical advantage irrelevant, lethality of conventional forces would approach those of tactical nuclear weapons
- Develop the concept of the Reconnaissance Strike Complex, which builds on REC with automated, networked links between C2, sensors and effect generators – NCW in Western terms
- US response to MTR prompts early thinking about C3CM and an information-based RMA

The concept of the MTR and RSC was rooted in Soviet fears that Western military integration of information-based technologies would render traditional forces – particularly tank-heavy ground forces – operationally vulnerable and therefore strategically irrelevant
Reception of the 1991 Gulf War

- Reception of the 1991 Gulf War an important influence on evolution of IO/IW thinking in post-Soviet Russia
- Success of US C3CM/SEAD campaign seen in some quarters as a validation of MTR/RSC concepts
- Failure of Iraqi C2 and IADS – closely modelled on Soviet REC principles – leads to questioning of the value of Soviet-era concepts (with counter-argument regarding Iraqi effectiveness in implementing such concepts)
- Theorists note of the implications of real-time global television reporting on the conflict for mustering domestic and international support
- Also leads to questioning of whether Soviet command economy could deliver IT underpinning required to implement a MTR in the Soviet armed forces

Soviet reception of the Gulf War was signally important in shaping post-Soviet views on IO/IW and the implications of the emerging global real-time media environment
Russian Approach to IW
IW in Russian Military Doctrine

• Current ‘Military Doctrine of the Russian Federation’ promulgated by Presidential edict on 5 February 2010; effectively a statement of defence/military policy for the Russian Federation

• “Constitutes a system of views officially adopted...for the armed protection of the Russian Federation.” (para 2)

• Characteristic of contemporary war: “the intensification of the role of information warfare.” (sub-para 12d)

• “Military action will be typified by the increasing significance of precision, EM, laser, and infrasound weaponry, computer-controlled systems, drones and autonomous maritime craft...” (para 15)

• Features of modern conflicts: “the prior implementation of measures of information warfare in order to achieve political objectives without the utilisation of military force...” (sub-para 13d)

• Equipping the armed forces entails: “…develop(ing) forces and resources for information warfare.” (sub-para 41c)

• Notably does NOT offer a specific definition of ‘information warfare’; this is defined elsewhere in the hierarchy of Russian military concepts and documents
IW in Russian Military Theory

• A variety of (unclassified) definitions of IW have been offered in Russian open literature

  • “IW is a way of resolving conflict between opposing sides. The goal is for one side to gain and hold an information advantage over the other. This is achieved by exerting a specific information/psychological and information/technical influence on a nation’s decision making system, on the nation’s populace, and on its information resource structures, as well as by defeating the enemy’s control system and his information resource structures with the help of additional means, such as nuclear assets, weapons and electronic assets.” (Russian General Staff Academy definition)

  • “IW is a complex of information support, information counter-measures, and information defence measures, taken according to a single design, and plan, and aimed at gaining and holding information superiority over an enemy while launching and conducting a military action/battle.” (definition published in article by COL S.A. Komov in the journal Military Thought)

• Emerging (since 2007) concept of Information Strike Operations (transliterated Russian abbreviation: IUO) which extends the REC/RSC concept of operations by incorporating ‘electronic fire’ (an extension of EA arguably including DEWs) and ‘information strike’ (CNO)
SVR Approach to IW

- Sluzhba Vneshnik Razvedka (SVR) is the Russian Federation’s external intelligence (and covert operations) agency
- Head of SVR has defined IW as:
  - “…a concept that includes establishing control over other states’ information resources, deterring the development of information technology in countries which are potential enemies, possibly disrupting or completely putting out of operation information networks and communications systems, and developing information weapons and systems for safeguarding the security of a country’s own information structure and information flows.”
- Suggests a more expansive, national-level approach to IW than a narrowly military one, which specifically includes peacetime measures intended to influence or shape the information environment
- Includes broader national policy instruments such as export controls, embargoes and ‘information blockades’ to achieve national security outcomes
Information Security Doctrine

• ‘Information Security Doctrine of the Russian Federation’ promulgated in 2000 articulates Russian approach to the role of information in national security

• Originally administered by the Federal Agency for Government Communications and Information (FAPSI – Russian strategic SIGINT agency); from 2003 administered by the Federal Security Bureau (FSB – Russian Federation successor to the KGB)

• Provides a broad overview of the role of information in national security, and information-based threats to the security of the Russian Federation

• Specific issues include security of government information, cyber security, cryptography, media operation and control, and censorship

• Role of information in national security further developed in 2008 ‘Strategy of Information Society Development in Russia’ and 2009 ‘National Security Strategy’

The Information Security Doctrine provides the overall framework for Russian Government control of information and information infrastructure for national security purposes; picture here is from a protest against Internet censorship in early 2014, the text reads “censorship”
Operational Vignettes
First Chechen War – 1994-96

• Initial effort to create an independent Chechen state in the wake of the collapse of the Soviet Union in 1991; after several years of disorder, results in (initially undeclared) Russian armed intervention in 1994

• Arguably represented a continuation of Soviet-era brute-force COIN (as previously demonstrated in Afghanistan) but now on a former Soviet territory

• Russians – though generally poorly equipped – employ REC-type capabilities against the Chechens; Chechens successfully exploit commercially acquired technologies (satellite phones, RF jammers, etc) to significant effect

• Chechens able to leverage access to global media as a key dissemination mechanism for PSYOPS campaign; Russian performance in this regard – and in trying to deny Chechen access to global media – regarded as poor

• Russian performance essentially regarded as a failure; arguably demonstrated rationale for tightened controls on media in post-Yeltsin Russia
Lessons from Kosovo 1999

• Russia not a direct protagonist in Operation ALLIED FORCE, but (arguably) provided some degree of covert assistance to Serbia

• Detection anddowning of F-117 aircraft demonstrated innovative radar techniques could defeat low-observability (‘stealth’) technologies

• Effective Serb use of decoys and camouflage demonstrated continuing relevance of maskirovka in countering an air campaign

• Noted that ultimate decisive factor in campaign was not military defeat of Serbian armed forces, but the political isolation – both domestically and internationally – of Serb leadership

• Demonstrated the utility of Internet (both directly and via hacking and defacement of adversary webpages) as a propaganda dissemination mechanism

The downing of an F-117 Nighthawk aircraft demonstrated the limitations of low-observability technology which had proved so useful in the 1991 Gulf War
Second Chechen War – 1999-2000

- Russian intervention arose out of unresolved issues from first war, and in response to terrorist attacks attributed to Chechens in Russia proper.

- Main phase of operations Aug 1999 to May 2000; but insurgency continued until 2009; Russian military handed operational lead to security services in Apr 2002.

- Russian employment of IW demonstrated evolution in Russian approach to IW through 1990s, integrated information-technical and information-psychological aspects:
  - Enhanced EW, ISR and precision targeting capabilities acquired since first war were effectively employed within an RSC approach.
  - Able to exert far great control of domestic and global media (and Internet); were effectively able to counter Chechen narrative in the infosphere.

- Russian experience here shaped further refinement of military’s approach to IW into the 21st century.


Chechen graffiti taunting Russian troops during the Second Chechen War; text reads: “Welcome to Hell, Part 2”
2007 Estonian Cyber Attacks

• Significant cyber attacks on Estonian information infrastructure lasted 22 days between April and May 2007; coincided with protests/rioting by Russian ethnic minority in Estonia and economic sanctions by Russian Government

• Triggered by Estonian government’s decision to relocate a Soviet era monument to Great Patriotic War away from central Tallinn (Estonian capital)

• Entailed both significant DDOS attacks on Estonian (public and private sector) information infrastructure and defacement of Estonian Government websites

• Depicted by Russian Government as grass roots activism for which it was not responsible and had no control

• Despite some circumstantial evidence (IP addresses for launching attacks, dissemination of advice on how to conduct DDOS attacks) full extent of official Russian complicity remains controversial and contested

A prominent feature of the 2007 Estonian cyber attacks was the hacking and defacement of Estonian government webpages; a common motif in defaced webpages was the replacement of Estonian government symbols with images relating the Soviet era and the ‘Great Patriotic War’
Georgia - 2008

- Roots of conflict go back to immediate post-Soviet era; commenced with Georgian response to attacks by Russian-backed separatists in Ossetia; Russia responds with more general assault on Georgia (however Russian cyber attacks precede actions by separatists)

- Russians employ REC-type activities to undermine Georgian C2 and air defence capabilities; some problems caused by US blacking out of GPS and poor performance of Russian GLONASS system

- Despite generally overall operational poor performance by Russians, appear to have learned lessons from Chechen conflicts; in particular control of access by global media to conflict area

- Cyber attacks conducted by both sides; effect of Russian cyber attacks on Georgia less effective than in Estonia because Georgia less ‘wired up’ as a nation, therefore less dependent/vulnerable

- Arguably first instance where ‘kinetic’ manoeuvre operations have been directly combined with CNO against infrastructure targets

As in Estonia in 2007, one focus of Russian-based cyber attacks on Georgian targets was the hacking and defacement of government web pages
Ukraine - 2014

- Current on-going operations in Ukraine demonstrate – at least in part – the further evolution of the Russian approach to IW

- Emphasis of bulk of IW activities thus far has been in the information-psychological domain; involving both overt and covert/proxy activities

- Campaign has been successful within Russia and annexed portions of Ukraine; distinctly less so elsewhere

- Has arguably demonstrated the risks of devolved use of social media (e.g.: social media based reporting has seemed to indicate direct separatist involvement in the downing of MH117)

- Scope of REC/RSC type information-technical activities thus far has been somewhat limited, given the extent of combat operations between Ukraine and Russian/separatist forces; extent of cyber attacks along the lines of those experienced by Estonia and Georgia has been limited

Countering imagery associated with the downing of MH17 – apparently by Russian-backed Ukrainian separatists – has now become a major challenge for the Russian IW campaign
Emergent Issues
Reflexive Control and Psychotronics

• A distinct feature of the Russian approach to IW has been a specific focus on the human nervous system as the ultimate target of IW-type activities.

• Approach stands astride more traditional division between ‘information-psychological’ and ‘information-technical’ aspects of IW.

• Prospective IW-type activities in this domain referred to by terms such as Reflexive Control, Psychotronics, and other terms.

• Potentially entails a wide range of techniques or technologies to induce intended behaviour change:
  • Directly influencing human mental states via induced EM directly targeting the brain.
  • Imparting subliminal messages by manipulating human-machine interface in C2/situational awareness systems.
  • Weaponisation of psychedelic, psychotropic or other psychoactive substances.

• The chemical agent employed by Russian CT forces in the 2002 Nord-Ost Theatre hostage crisis conceivably represents an actual operational example.

The use of an unknown incapacitating chemical agent – leading to over 100 deaths – during the Nord-Ost Theatre hostage crisis could represent an actual example of this uniquely Russian approach to IW focused on the human nervous system.
Conclusion

• Russian approach to IO/IW quite distinct to US/Western Anglophone one; in particular, closer association between military IO/IW and the role of information in overall national security
• Current approach to IO/IW builds upon historical legacy of the Mongol influence, pre-Revolutionary Russia and the Soviet period
• Emergence of modern (post-Soviet) Russian approach to IO/IW has been strongly influenced by both Russia’s own experience, and lessons drawn from other states (particularly US/NATO application of C3CM in 1991 Gulf War and IO/IW in 1999 Kosovo campaign)
• Military IO/IW closest to Western approach; relationship between Soviet MTR and the origins of the US C3CM concept
• Unique aspects of Russian approach to IO/IW relate to measures intended to target the human organism/nervous system directly; closest other national approach in this respect is arguably some aspects of Chinese approach to IO/IW

IW will become a more prominent feature not only of the Russian military’s approach to operations, but of the national security practices of the Russian state as a whole
References

• Information Warfare in the Second Chechen War
• Information Security Doctrine of the Russian Federation
• Emerging Cyber Threats and Russian Views on IW and IO
• Anatomy of Russian Information Warfare
• The Mind Has No Firewall