Conceptualization of information warfare

Petra Vejvodová

9 October 2018

Why is information important in conflict?

Information warfare

- Information is **not a new component** to conflict
- Information about the enemy crucial for all sides of any conflict

- **Deception**

- For centuries, cryptography has been used to hide and reveal messages (Enigma)

Day D – operation Bodyguard

- Code name for 2WW military deception employed by the Allied nations during the 1944 Normandy landing
- To mislead the German high command as for the location of the invasion (Normandy vs. Pas de Calais)
- Fictional army and fake vehicles
- Fake radio broadcasting
- Double agents giving wrong

  information to the Nazis

https://www.youtube.com/watch?v=a3w9pmvpyDM

https://www.youtube.com/watch?v=dlRFs1C4l0Q
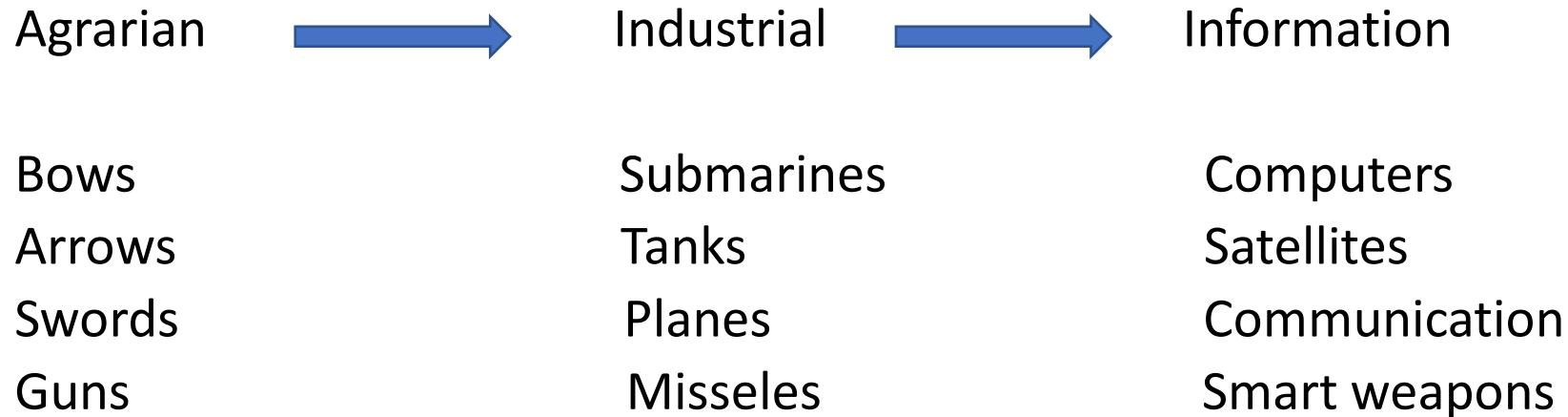
Operation Infektion

- Code name for operation of USSR against the US during CW
- First half of 1980s
- Case of AIDS showed up - opportunity for KGB agents to blame Americans
- US ministry of defence blamed that it developed the virus and it spreads it among people

Gulf War in 1990s

- George Bush administration has learnt lessons from the Vietnam War about the importance of public support and controlled discourse during the crisis

- TV coverage portrayed all U.S. policy actions and U.S. military intervention in an extremely positive light

- In October 1990, a 15-year old Kuwaiti girl testified that she witnessed Iraqi soldiers removing fifteen new-borns from incubators in Al-Adan Hospital in Kuwait City and had seen them left to die on the floor of the hospital

Information Warfare

- The information age, however, has developed in extraordinary improvements in collection, storage, analysis, and transmission of information

- Tofflers talk about third wave of warfare (Revolution in Military Affairs) – information is crucial, information win battles (since1970s improvement in technical means)

Agrarian   →   Industrial   →   Information

Agrarian	Industrial	Information
Bows	Submarines	Computers
Arrows	Tanks	Satellites
Swords	Planes	Communication
Guns	Misseles	Smart weapons

Information warfare

- Libicki (1995): *information warfare as a conflict involving the protection, manipulation, degradation and denial of information*

- *Any action to deny, exploit, corrupt, or destroy the enemy`s information and its functions, protecting ourselves against those actions, and exploiting our own military information functions*

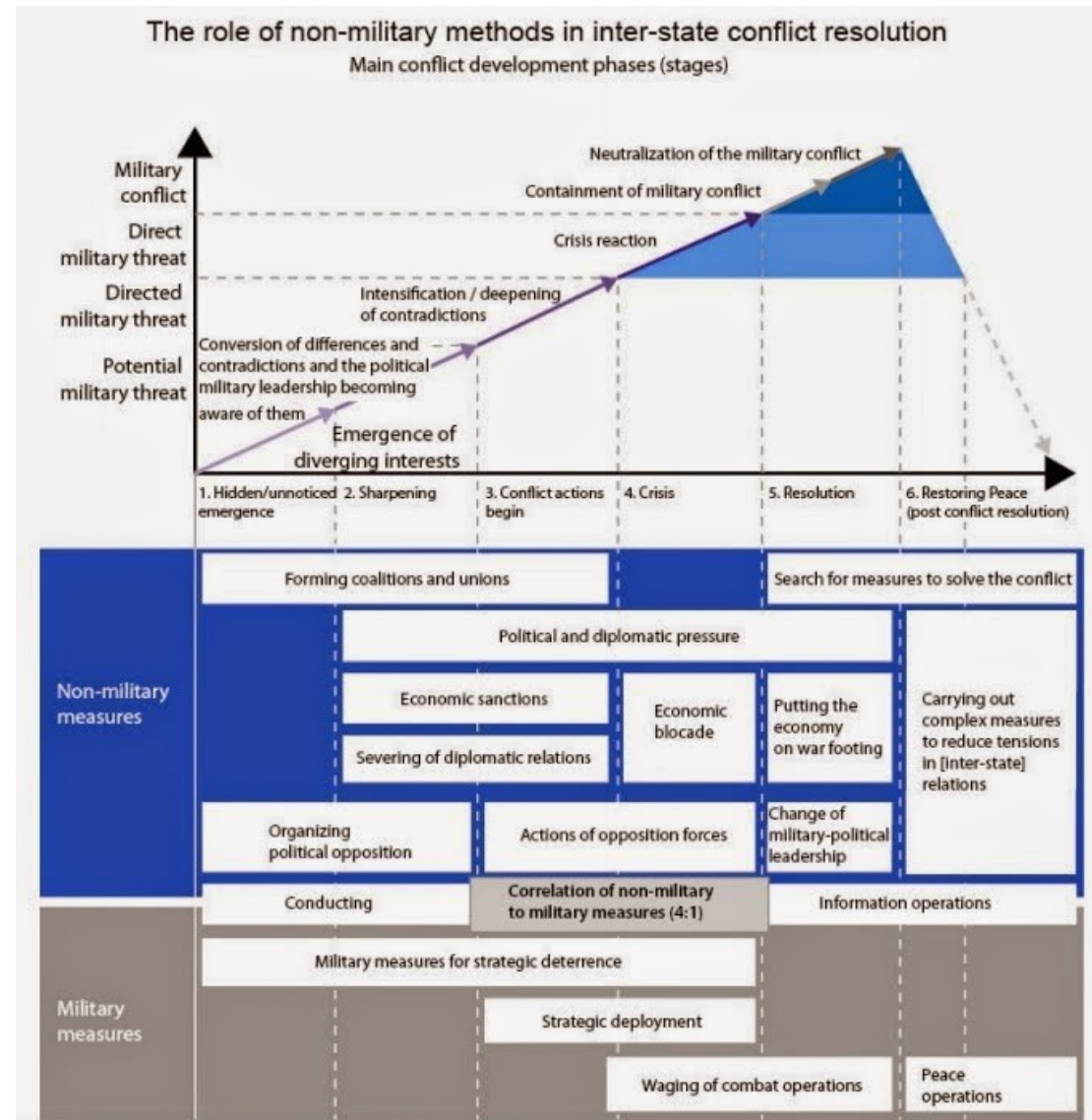- **Information as a weapon and target**

What constitutes Information Warfare?

1. **Psychological Operations**
2. **Electronic Warfare**
3. **Physical Destruction**
4. **Intelligence Warfare**
5. **Economic information warfare**

US vs. Russian approach towards IW

- The **US military** focus tends to favor **technology** – electronic warfare, cyberwarfare + **tool during military operations**

- The U.S. Joint Chiefs of Staff define information operations as "*the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation, to influence, disrupt, corrupt, or usurp the decision of adversaries and potential adversaries while protecting our own.*" (Teyloure Ring, 2015)

- **Russia** uses much broader term including **psyops and propaganda**

- Russian understanding of information warfare: "*influencing the consciousness of the masses as part of the rivalry between the different civilizational systems adopted by different countries in the information space by use of special means to control information resources as 'information weapons.'*". (Teyloure Ring, 2015)

Gerasimov doctrine (2013, Russia)

The role of non-military methods in inter-state conflict resolution

Case of Russian information warfare

- IW as geopolitical tool of influencing internal state affairs
- Combination of tried and tested tools of influence with a new modern technology and capabilities
- Adaptation the principles of subversion to the internet age

- New investments cover three main areas:

1) Both internally and externally focused **media with a substantial online presence** (e.g. RT),

2) Use of **social media and online forums** as a force multiplier to ensure Russian narrative achieve broad reach and penetration (trolls),

3) **Language skills**, in order to engage with target audience in their own language.

Russian IW: media

- Investments in human capabilites – recruitment of staff for online media, journalists

- Coordination of messaging with centralized direction

- RT, Sputnik (national branches in European countries)

- Spring 2014: annexation of Crimea - media in Europe were „buying" what Russian media outlets were selling (Western media were reporting Russian disinformation as a fact)

Russian IW: media

- Pro-Russian and anti-EU/NATO narratives
- Fueling existing tensions by manipulation (emotions)
- Dissemination of fake news (Lisa case)
- Dissemination of alternative realities

- „Trust nobody", „Everybody lies"
- political apathy or radicalisation (→far right parties)

Russian IW: trolls

- Spreading false information, polarizing the debate at social networks and forums, targeting emotions

https://www.youtube.com/watch?v=6CjR82EYwBc