Security in the 21st Century

Hybrid Warfare and

Comprehensive Security

GEN Jerdwut Kraprayoon
Special Advisor RTArF HQs

@ SSC
Feb 9, 2021

Outline

- Introduction
- Hybrid Threats
- Comprehensive Security

Introduction

- นรม. และ ผบ ทบ พูดถึง Hybrid Warfare แต่ยังอาจจะสับสันเรื่องความหมาย และนิยามที่เกี่ยวข้อง (ควรใช้ Hybrid Threats)
- เนื่องจากเป็นเรื่องใหม่ เป็นภัยคุกคามในรูปแบบใหม่ ซึ่งเรายังไม่มีหลักนิยม และโครงสร้าง รองรับ
- ยังไม่มีนิยามทหารที่เป็นสากล
- ปกติ ในแง่ทางการเมือง เราจะไม่ใช่คำว่า Warfare เพราะสังคมจะเข้าใจว่า เป็นแนวคิดทหารสำหรับ ต่อสู้กับประชาชน

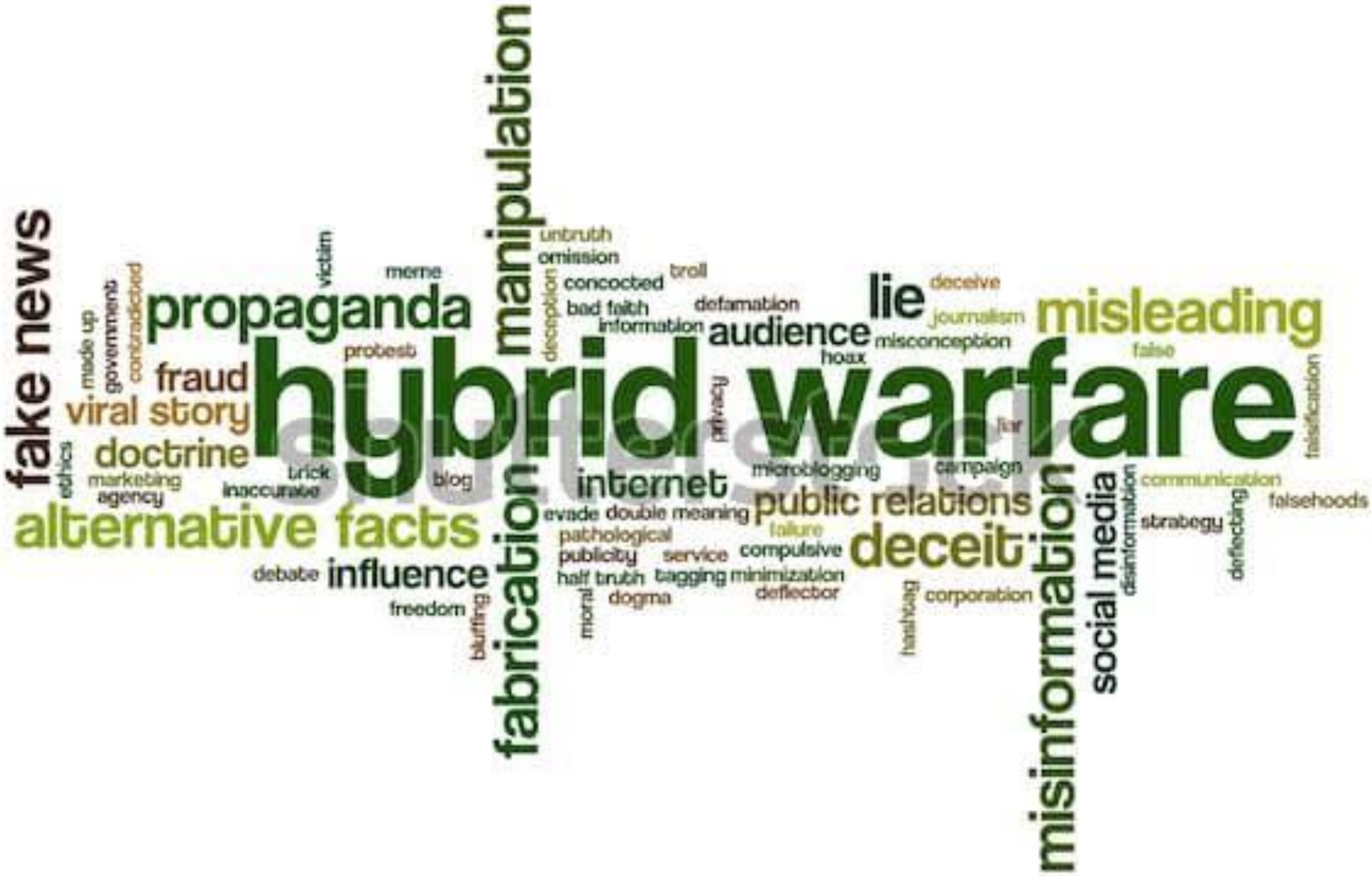
What is Hybrid Warfare?

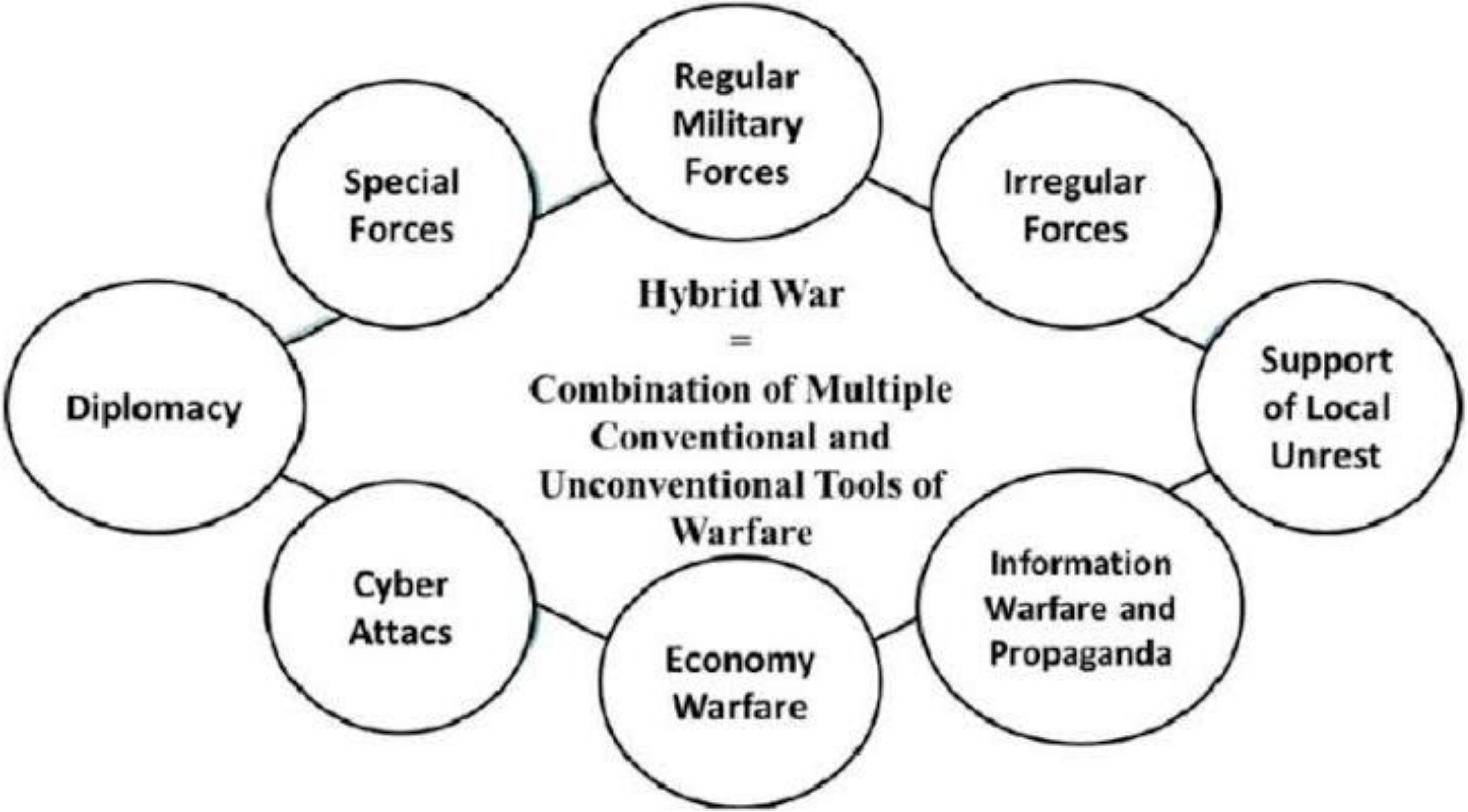
- Hybrid warfare is an emerging, but ill-defined notion in conflict studies. It refers to the use of unconventional methods as part of a multi-domain warfighting approach. These methods aim to disrupt and disable an opponent’s actions without engaging in open hostilities.

- While the concept is fairly new, its effects and outcomes are often in the headlines today. Russia’s approach to Ukraine is an example of this form of warfare. It has involved a combination of activities, including disinformation, economic manipulation, use of proxies and insurgencies, diplomatic pressure and military actions.

- The term hybrid warfare originally referred to irregular non-state actors with advanced military capabilities. For example, in the 2006 Israel-Lebanon War, Hezbollah employed a host of different tactics against Israel. They included guerilla warfare, innovative use of technology and effective information campaigning.

- Following that war, in 2007, American defence researcher Frank Hoffman expanded on the terms “hybrid threat” and “hybrid warfare” to describe employing multiple, diverse tactics simultaneously against an opponent.


hybrid warfare
manipulation
fake news
propaganda
misleading
lie
audience
alternative facts
fabrication
misinformation
social media
deceit
public relations
internet
influence
doctrine
viral story
fraud
made up
government
contradicted
victim
meme
protest
ethics
marketing
agency
trick
inaccurate
blog
debate
freedom
bluffing
untruth
omission
deception
concocted
troll
bad faith
defamation
information
deceive
journalism
misconception
hoax
false
privacy
fraud
liar
microblogging
campaign
evade
double meaning
pathological
failure
publicity
service
compulsive
half truth
tagging
minimization
deflector
moral
dogma
hashtag
corporation
communication
falsehoods
strategy
disinformation
deflecting
falsification



Hybrid War
=
Combination of Multiple Conventional and Unconventional Tools of Warfare

Regular Military Forces

Irregular Forces

Support of Local Unrest

Information Warfare and Propaganda

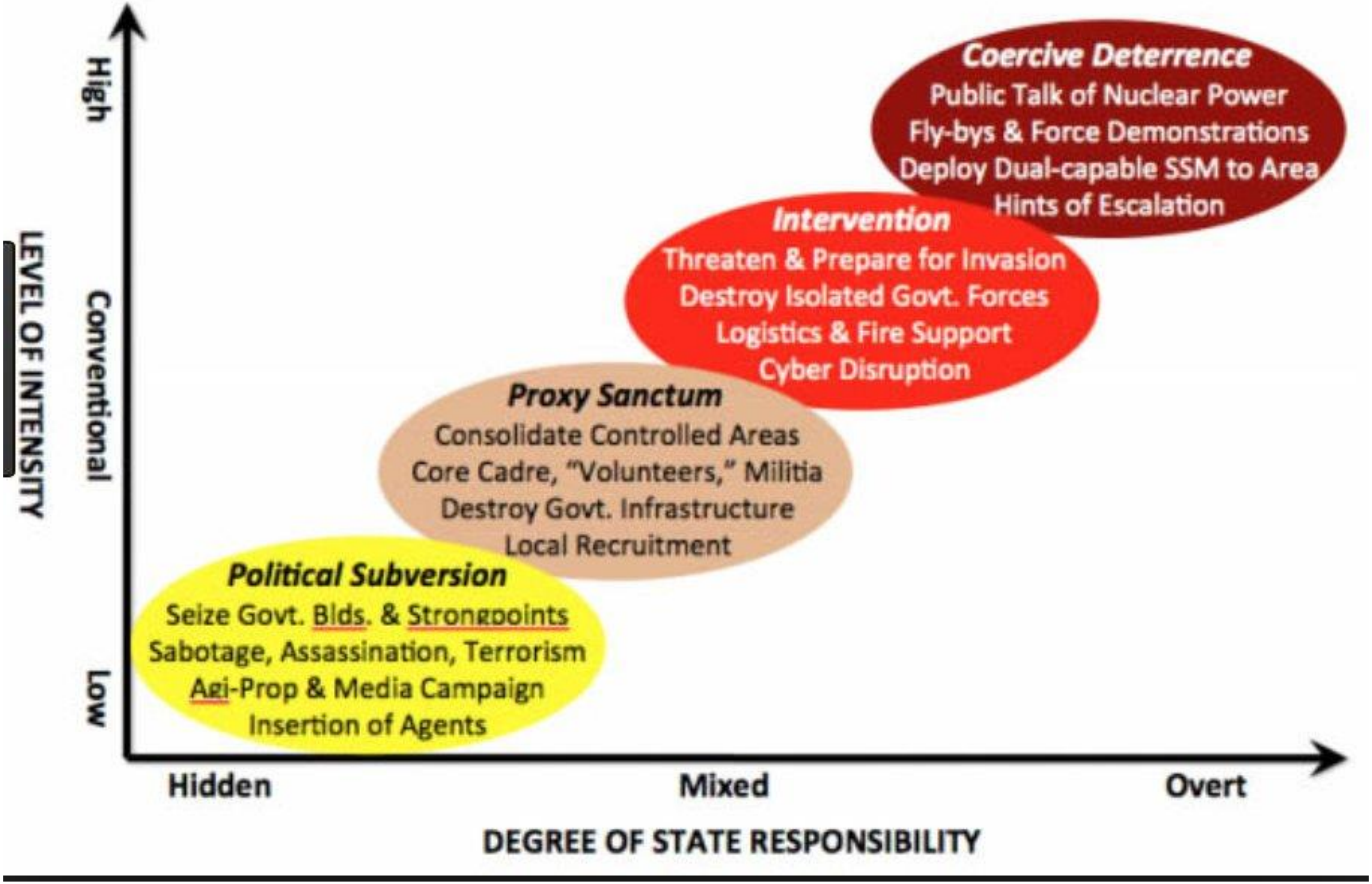
Economy Warfare

Cyber Attacs

Diplomacy

Special Forces

Russian Style *Hybrid Warfare* in Ukraine



Coercive Deterrence

Public Talk of Nuclear Power
Fly-bys & Force Demonstrations
Deploy Dual-capable SSM to Area
Hints of Escalation

Intervention

Threaten & Prepare for Invasion
Destroy Isolated Govt. Forces
Logistics & Fire Support
Cyber Disruption

Proxy Sanctum

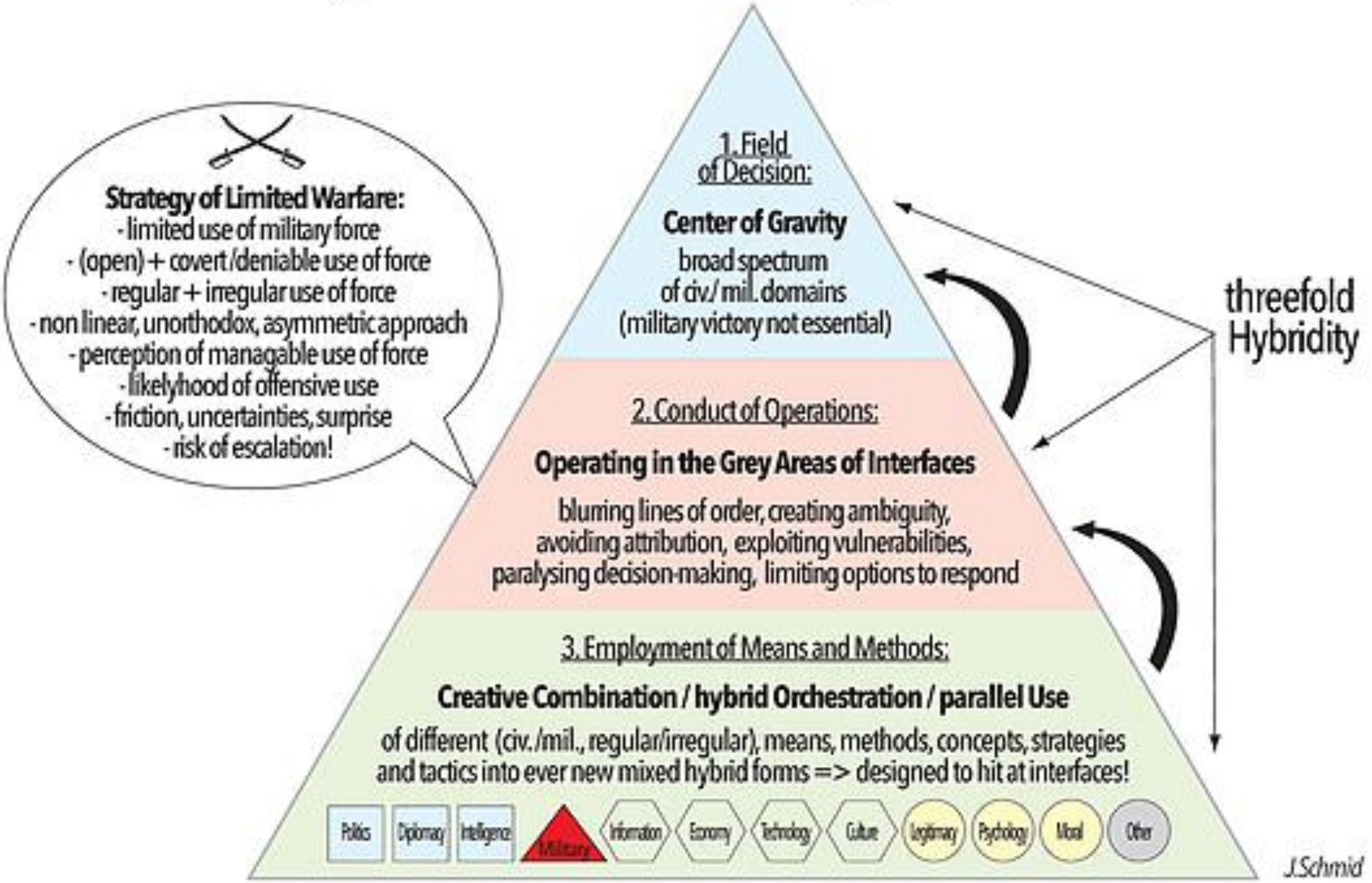
Consolidate Controlled Areas
Core Cadre, "Volunteers," Militia
Destroy Govt. Infrastructure
Local Recruitment

Political Subversion

Seize Govt. Blds. & Strongpoints
Sabotage, Assassination, Terrorism
Agi-Prop & Media Campaign
Insertion of Agents

The “paradoxical” Trinity of Hybrid Warfare

Three key characteristics / tendencies & their hybrid interaction / orchestration



Strategy of Limited Warfare:
- limited use of military force
- (open) + covert /deniable use of force
- regular + irregular use of force
- non linear, unorthodox, asymmetric approach
- perception of managable use of force
- likelyhood of offensive use
- friction, uncertainties, surprise
- risk of escalation!

1. Field of Decision:

Center of Gravity

broad spectrum of civ./ mil. domains (military victory not essential)

2. Conduct of Operations:

Operating in the Grey Areas of Interfaces

blurring lines of order, creating ambiguity, avoiding attribution, exploiting vulnerabilities, paralysing decision-making, limiting options to respond

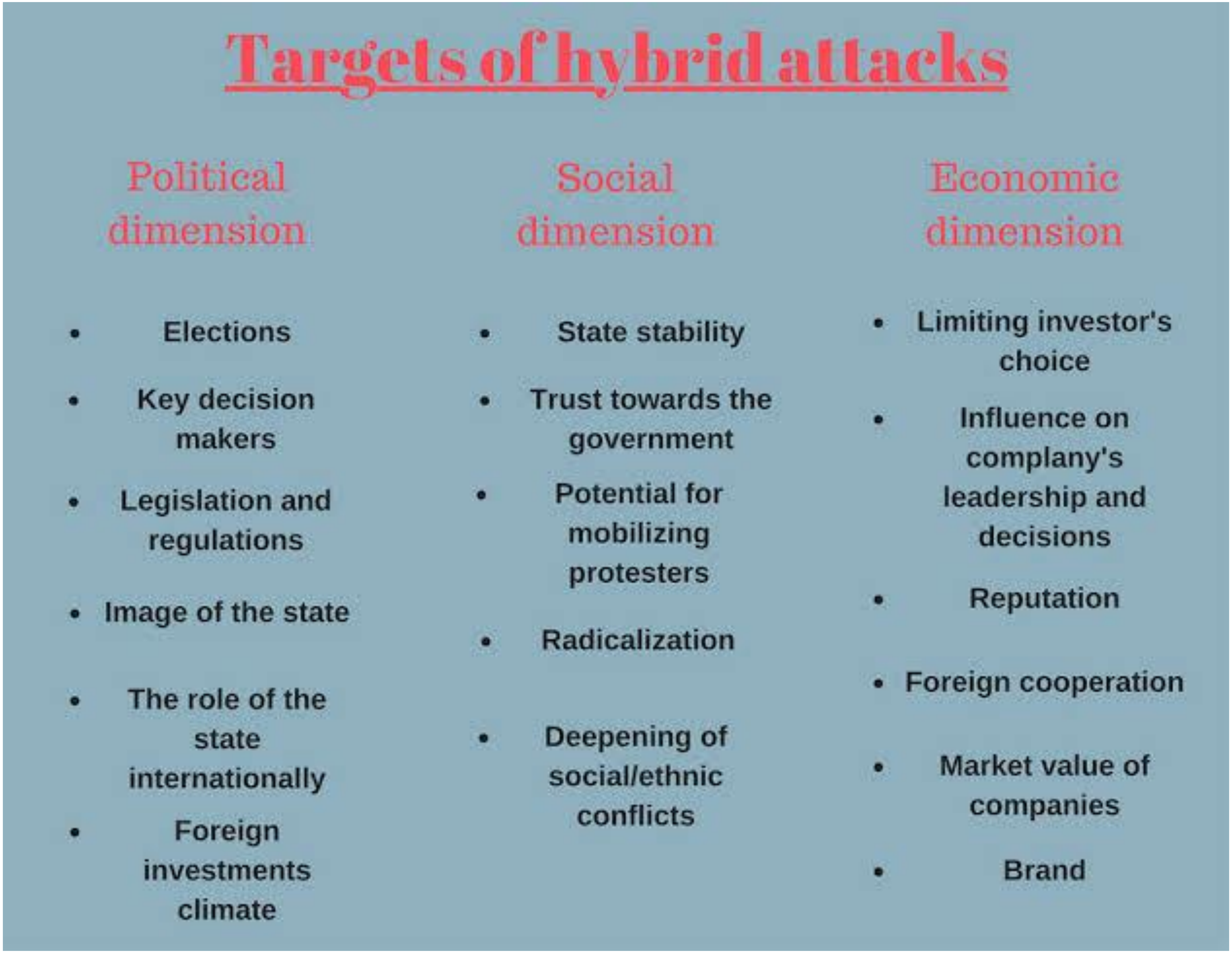
3. Employment of Means and Methods:

Creative Combination / hybrid Orchestration / parallel Use

of different (civ./mil., regular/irregular), means, methods, concepts, strategies and tactics into ever new mixed hybrid forms => designed to hit at interfaces!

threefold Hybridity

J.Schmid



Targets of hybrid attacks

Political dimension

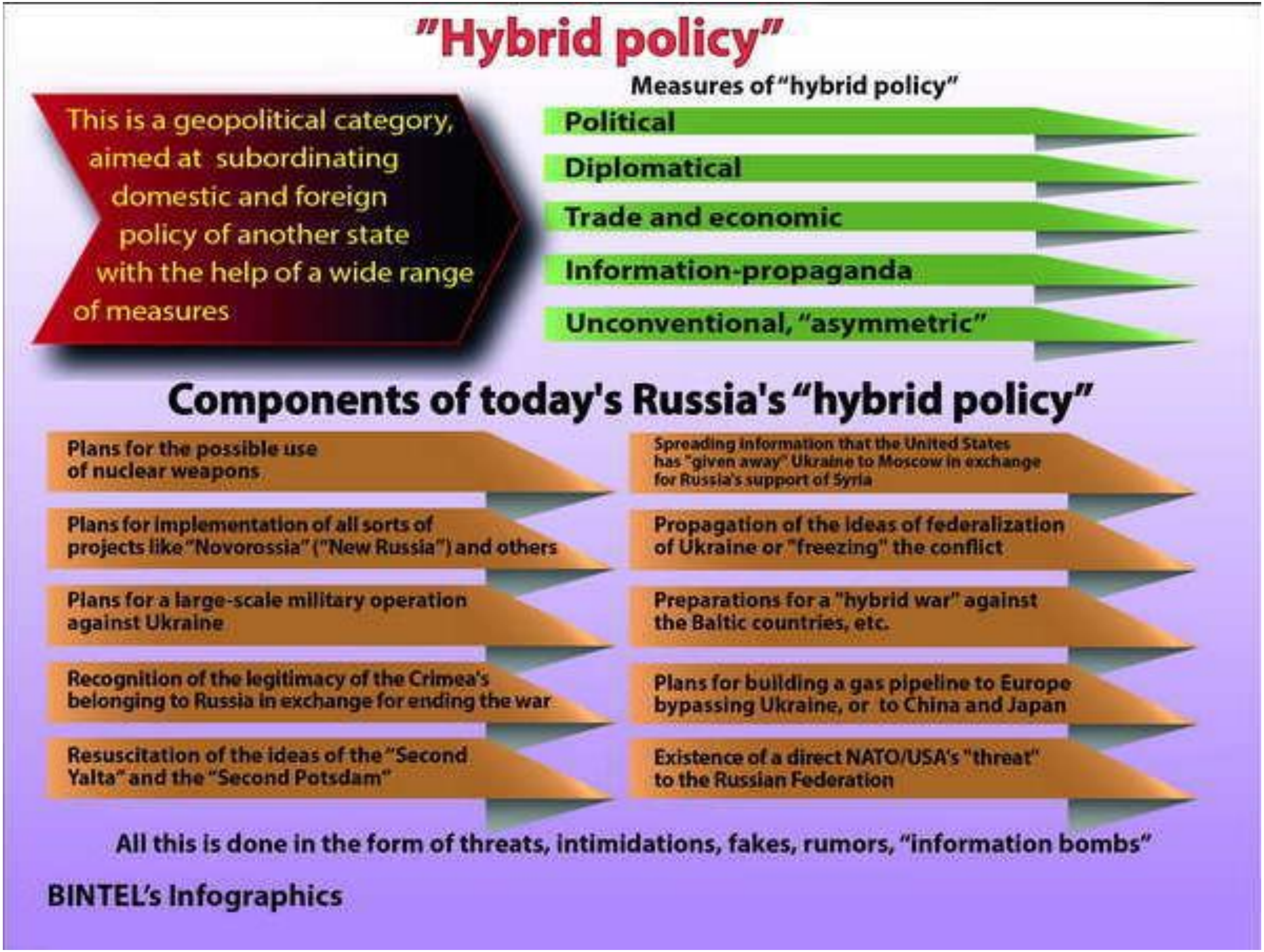
- Elections
- Key decision makers
- Legislation and regulations
- Image of the state
- The role of the state internationally
- Foreign investments climate

Social dimension

- State stability
- Trust towards the government
- Potential for mobilizing protesters
- Radicalization
- Deepening of social/ethnic conflicts

Economic dimension

- Limiting investor's choice
- Influence on complany's leadership and decisions
- Reputation
- Foreign cooperation
- Market value of companies
- Brand



"Hybrid policy"

This is a geopolitical category, aimed at subordinating domestic and foreign policy of another state with the help of a wide range of measures

Measures of "hybrid policy"

- Political
- Diplomatical
- Trade and economic
- Information-propaganda
- Unconventional, "asymmetric"

Components of today's Russia's "hybrid policy"

- Plans for the possible use of nuclear weapons
- Plans for implementation of all sorts of projects like "Novorossia" ("New Russia") and others
- Plans for a large-scale military operation against Ukraine
- Recognition of the legitimacy of the Crimea's belonging to Russia in exchange for ending the war
- Resuscitation of the ideas of the "Second Yalta" and the "Second Potsdam"
- Spreading information that the United States has "given away" Ukraine to Moscow in exchange for Russia's support of Syria
- Propagation of the ideas of federalization of Ukraine or "freezing" the conflict
- Preparations for a "hybrid war" against the Baltic countries, etc.
- Plans for building a gas pipeline to Europe bypassing Ukraine, or to China and Japan
- Existence of a direct NATO/USA's "threat" to the Russian Federation

All this is done in the form of threats, intimidations, fakes, rumors, "information bombs"

BINTEL's Infographics

NEW ERA OF GLOBAL COMPETITION

ASYMMETRICAL HYBRID WARFARE

THE MODERN BATTLEFIELD IS EVERYWHERE

UNRESTRICTED WARFARE

NON-MILITARY

- Economic Warfare*
- Financial Warfare*
- Transaction Warfare*
- Trade Warfare*
- Resources Warfare*
- Regulatory Warfare*
- Legal Warfare*
- Education Warfare*
- Technological Warfare*
- Sanction Warfare
- Media Warfare
- Propaganda Warfare
- Culture Warfare
- Ideological Warfare
- Religious Warfare
- Poisioning Warfare

TRANS-MILITARY

- Espionage Warfare*
- Information Warfare*
- Intelligence Warfare*
- Industrial Warfare*
- Resources Warfare*
- Pirating Warfare*
- DarkNet Warfare*
- Smuggling Warfare*

CYBER WARFARE

- Drug Warfare*
- Infiltration Warfare*
- Deterrence Warfare*
- Psychological Warfare
- Diplomatic Warfare
- Subversion Warfare
- Environmental Warfare

MILITARY

- Biological Warfare
- Chemical Warfare
- Ecological Warfare
- Space Warfare / EMP
- Electronic Warfare
- Guerrilla Warfare
- Terrorist Warfare
- Conventional Warfare
- Kinetic 'Smart' Warfare
- Nuclear Warfare

"ANYTHING WARFARE"
ABSENT OF ANY RULES

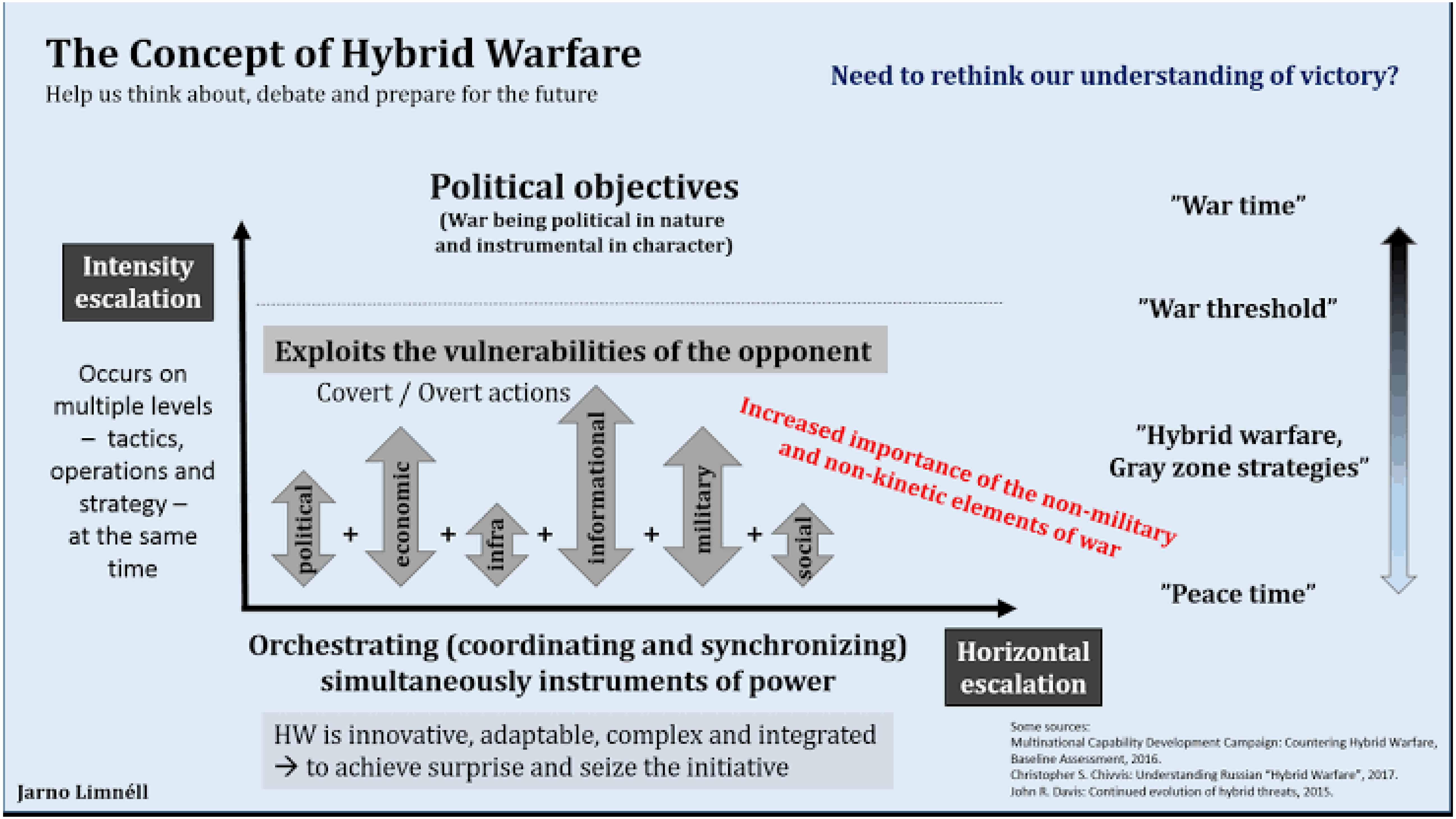
Espionage is the core focus and fabric of AHW

* Related to Economic and Transaction Warfare

Cyber Warfare functions as the key accelerator to all warfare methods

BLACKOPS PARTNERS

SPECTRE.



The Concept of Hybrid Warfare

Help us think about, debate and prepare for the future

Need to rethink our understanding of victory?

Political objectives

(War being political in nature and instrumental in character)

Intensity escalation

Occurs on multiple levels – tactics, operations and strategy – at the same time

Exploits the vulnerabilities of the opponent

Covert / Overt actions

Increased importance of the non-military and non-kinetic elements of war

"War time"

"War threshold"

"Hybrid warfare, Gray zone strategies"

"Peace time"

Orchestrating (coordinating and synchronizing) simultaneously instruments of power

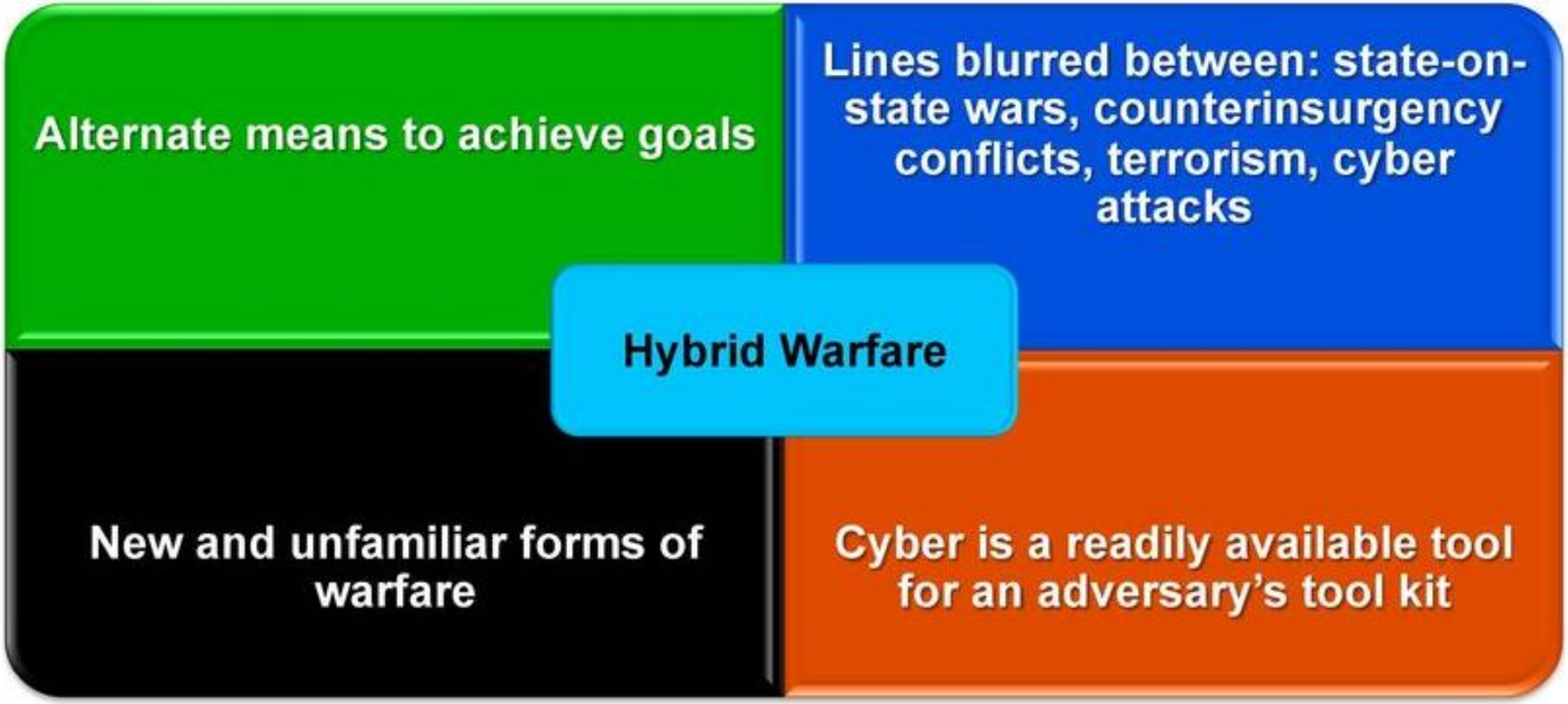
Horizontal escalation

HW is innovative, adaptable, complex and integrated
→ to achieve surprise and seize the initiative

Some sources:
Multinational Capability Development Campaign: Countering Hybrid Warfare, Baseline Assessment, 2016.
Christopher S. Chivvis: Understanding Russian "Hybrid Warfare", 2017.
John R. Davis: Continued evolution of hybrid threats, 2015.

Jarno Limnéll

Characteristics of Hybrid Warfare



Alternate means to achieve goals

Lines blurred between: state-on-state wars, counterinsurgency conflicts, terrorism, cyber attacks

Hybrid Warfare

New and unfamiliar forms of warfare

Cyber is a readily available tool for an adversary's tool kit

Clausewitz: "War is more than a true chameleon that slightly adapts its characteristics to the given cause"

Source:

- HYBRID WARFARE ASSESSMENT – FOLLOW-ON TASKING FROM THE WALES SUMMIT, 7 Nov 2014
- *Hybrid Warfare*, edited by Williamson Murray and Peter R. Mansoor, Cambridge University Press

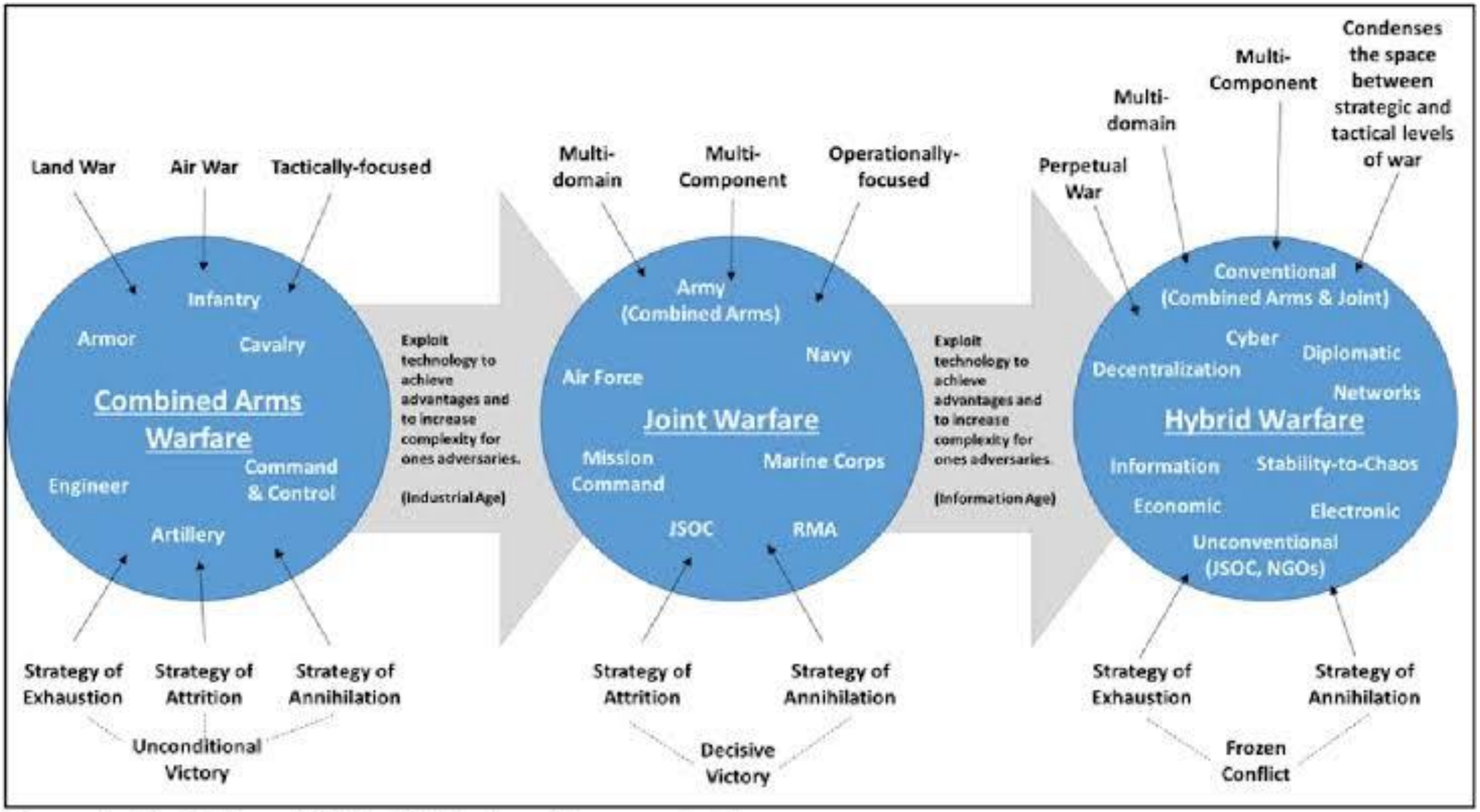
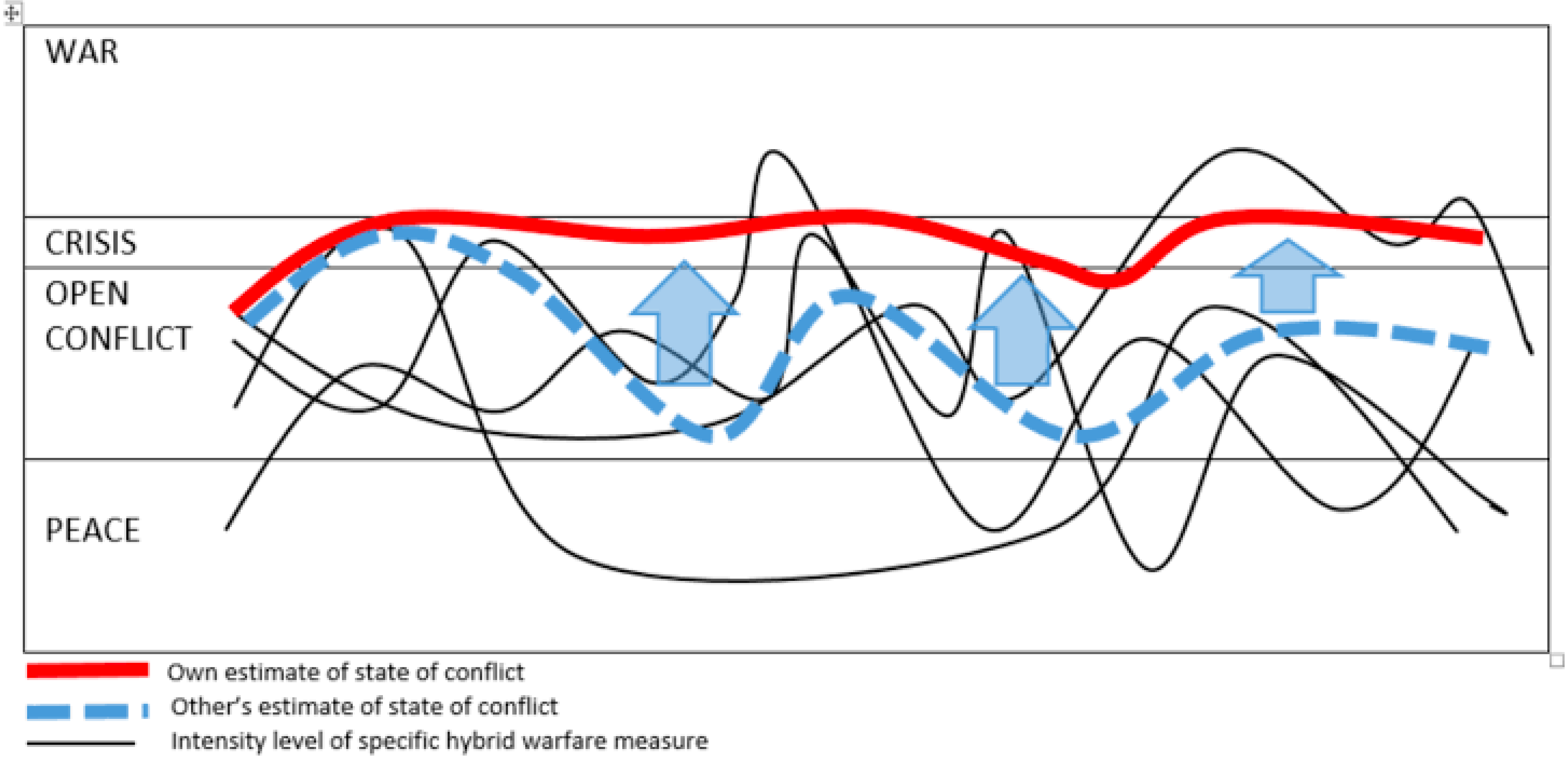
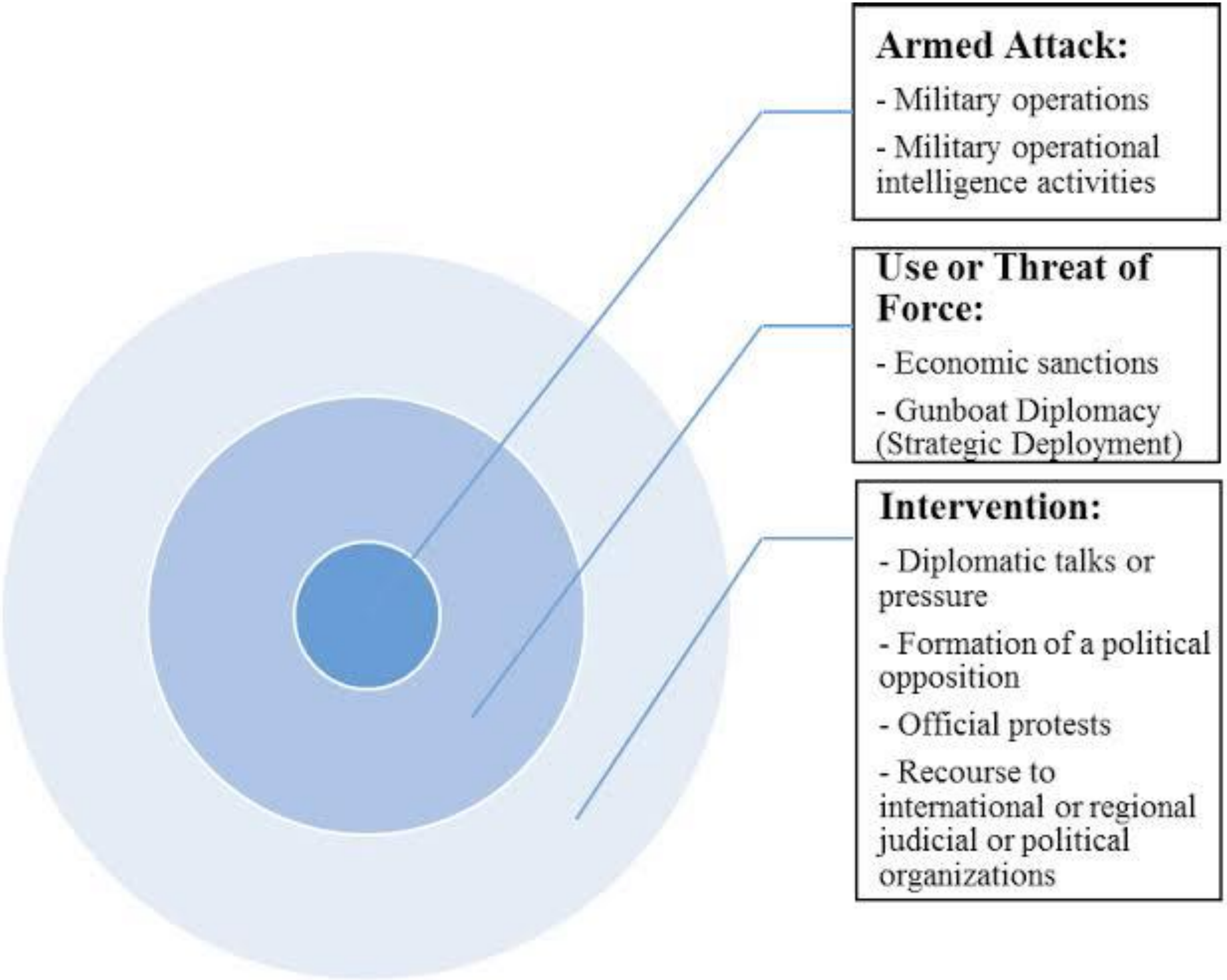


Figure 1. Evolution of Hybrid Warfare. Source: Author.

Miscalculation (overestimating)


WAR
CRISIS
OPEN CONFLICT
PEACE
Own estimate of state of conflict
Other's estimate of state of conflict
Intensity level of specific hybrid warfare measure



Armed Attack:

- Military operations
- Military operational intelligence activities

Use or Threat of Force:

- Economic sanctions
- Gunboat Diplomacy (Strategic Deployment)

Intervention:

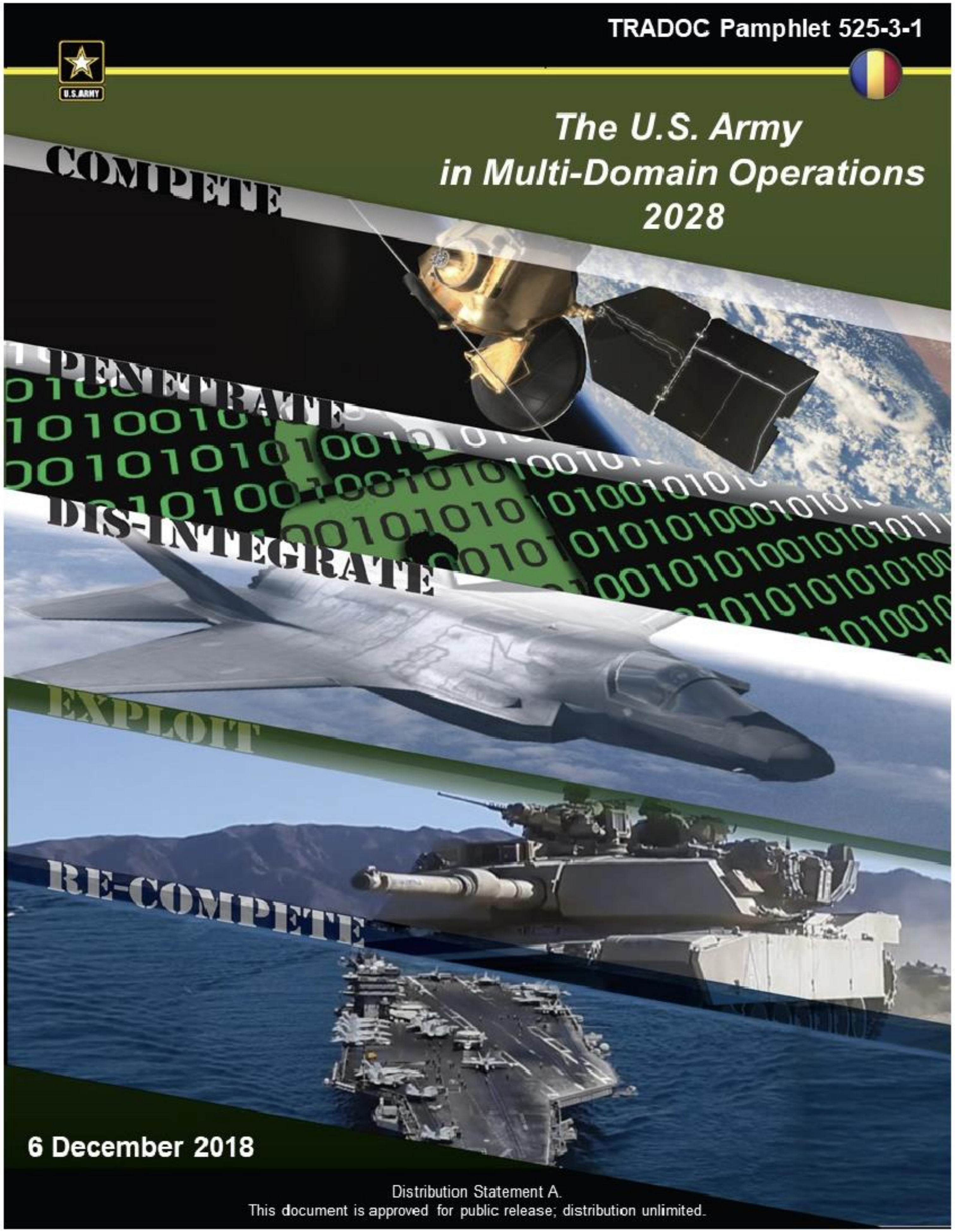
- Diplomatic talks or pressure
- Formation of a political opposition
- Official protests
- Recourse to international or regional judicial or political organizations

Hybrid Warfare

- Military Strategy? Or National Security Strategy?
- Political Warfare
- Conventional Warfare
- Irregular Warfare
- Cyber Warfare
- Information Warfare (fake news),
- Diplomacy
- Lawfare
- Foreign Election Intervention.
- By combining kinetic with subversive efforts, the aggressor intends to avoid attribution or retribution.

Notes

- US military Multi Domains Operation (To Counter China’s and Russia’s AA/AD Strategy)
- Grey Zone Operation
- US Army School Published Manual for Regime Change Intervention
- Israel defines Hybrid Warfare as Social Warfare



TRADOC Pamphlet 525-3-1

The U.S. Army in Multi-Domain Operations 2028

6 December 2018

Distribution Statement A.
This document is approved for public release; distribution unlimited.

Tenets of the Multi-Domain Operations

- The Army solves the problems presented by Chinese and Russian operations in competition and conflict by applying three interrelated tenets: calibrated force posture, multi-domain formations, and convergence.

- Calibrated force posture is the combination of position and the ability to maneuver across strategic distances.

- Multi-domain formations possess the capacity, capability, and endurance necessary to operate across multiple domains in contested spaces against a near-peer adversary.

- Convergence is rapid and continuous integration of capabilities in all domains, the EMS, and information environment that optimizes effects to overmatch the enemy through cross-domain synergy and multiple forms of attack all enabled by mission command and disciplined initiative.

- The three tenets of the solution are mutually reinforcing and common to all Multi-Domain Operations, though how they are realized will vary by echelon and depend upon the specific operational situation.

What is Grey Zone?

Related to hybrid warfare, the term political warfare commonly refers to power being employed to achieve national objectives in a way that falls short of physical conflict.

Such warfare is conducted in the “grey zone” of conflict, meaning operations may not clearly cross the threshold of war. That might be due to the ambiguity of international law, ambiguity of actions and attribution, or because the impact of the activities does not justify a response.

Recent discussions, including last week’s speeches, focus on the newer aspects of these concepts – specifically activities in the information domain.

Our increasing connectivity and reliance on information technology is a vulnerability that is being targeted by two key threats: cyber attacks, and the subversion of our democratic institutions and social cohesion. Both are recognised challenges to our national security.

These are “hybrid threats” as they may be employed as part of a broader campaign – including political, criminal and economic activities. And because they feature the ambiguity associated with the grey zone, they are well suited to achieve political outcomes without resorting to traditional conflict.

While cyber attacks are carried out by a variety of actors, there is an ongoing low intensity cyber conflict between nation states. This includes attacks and counter-attacks on critical infrastructure, such as power grids, reported between the US and Russia.

Grey Zone Operation

- Public speeches by Australian Defence Force Chiefs are irregular enough that people sat up and took notice when General Angus Campbell used his address at the Australian Strategic Policy Institute’s 2019 “War in 2025” conference to outline the increasing threat represented by political warfare – a term not likely to be familiar to the average Australian.

- Political warfare involves so-called grey-zone operations or hybrid warfare, which include activities such as subversion, foreign interference and utilization of unmarked military forces. These measures are provocative and escalating but still designed to be non-kinetic and non-lethal. As they aim below the threshold of outright warfare, they do not necessitate or justify a warlike response.

Grey Zone Operation

The ‘grey zone’ has received much publicity over the past decade as certain nation-states have employed indirect methods to gain advantages over their opponents without resorting to open kinetic warfare.

Grey zones can be an important element of ‘hybrid warfare’.

The definition of hybrid warfare remains subject to debate, but inherent in the term is the idea that covert and unconventional methods, which may include non-kinetic effects, are employed in addition to conventional military force.

Grey Zone Operation

- Grey zone operations are coercive and intended to achieve change, but they seek at the same time to limit an adversary's ability to respond.

- In most, but not all, circumstances, they're 'deliberately designed to remain below the threshold of conventional military conflict and open interstate war' and 'are meant to achieve … gains without escalating to overt warfare, without crossing established red-lines, and thus without exposing the practitioner to the penalties and risks that such escalation might bring'.

- While a substantial proportion of such operations have occurred purely on land in recent years, such as the Russian-sponsored campaigns in Georgia and Ukraine, they have also been used at sea and to key strategic effect.

Recent grey-zone activity in maritime Asia suggests an increase in hybrid warfare. The lines between military, economic, diplomatic, intelligence and criminal means of aggression are becoming increasingly blurred.

Hybrid warfare is warfare with the following aspects:

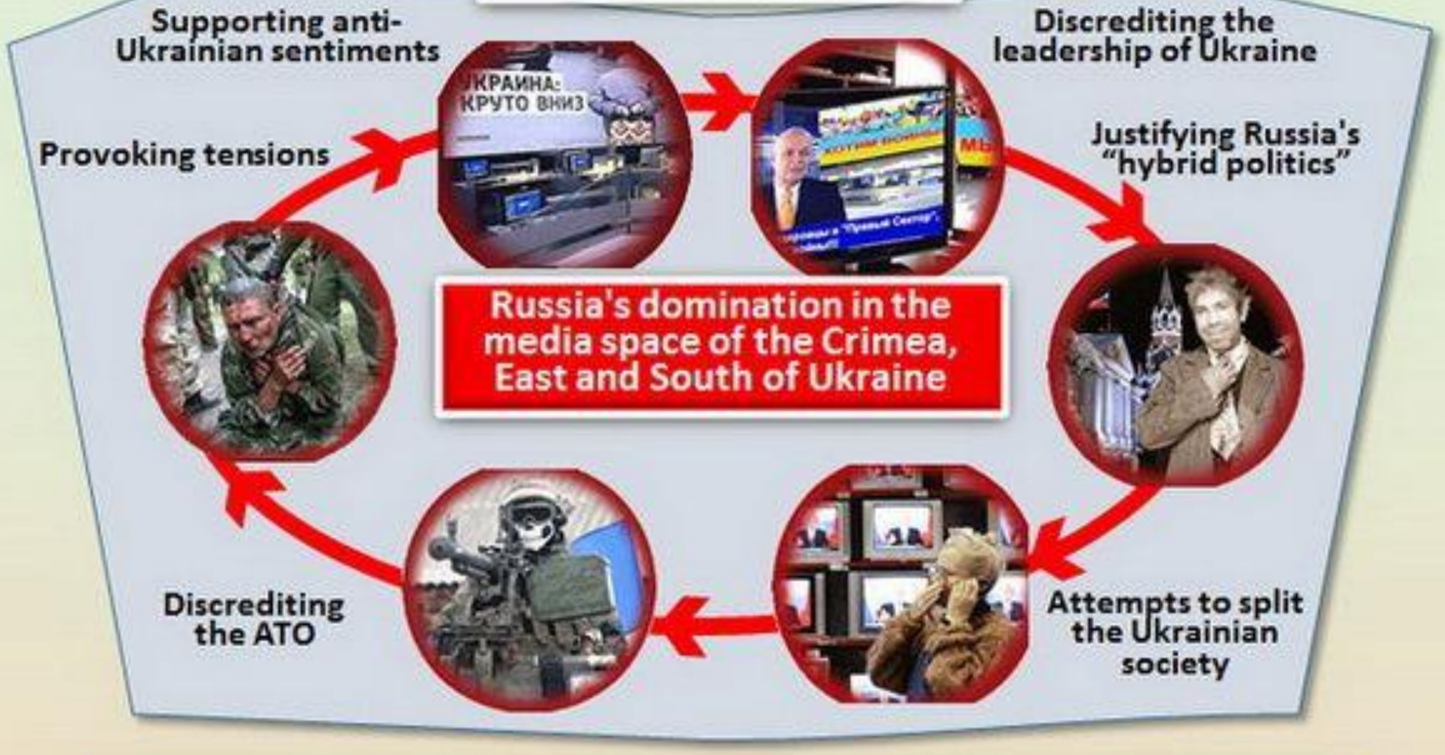
A non-standard, complex, and fluid adversary. A hybrid adversary can be state or non-state. For example, in the Israel–Hezbollah War and the Syrian Civil War the main adversaries are non-state entities within the state system. These non-state actors can act as proxies for countries but have independent agendas as well. For example, Iran is a sponsor of Hezbollah but it was Hezbollah's, not Iran's, agenda that resulted in the kidnapping of Israeli troops that led to the Israel–Hezbollah war. On the other hand, Russian involvement in Ukraine can be described as a traditional state actor waging a hybrid war (in addition to using a local hybrid proxy). Note that Russia denies involvement in the Ukraine conflict.

Hybrid warfare is warfare with the following aspects:

- N*on-standard, Complex, and Fluid adversary*
- *Hybrid adversary can be State or Non-state*
- *Examples:*
- *Israel Hizbollah war*
- *Syria Civil War*
- *Russia Involvement in Ukraine*

Counteracting Russia's propaganda

Enemy`s actions



Supporting anti-Ukrainian sentiments

Discrediting the leadership of Ukraine

Justifying Russia's "hybrid politics"

Attempts to split the Ukrainian society

Discrediting the ATO

Provoking tensions

Russia's domination in the media space of the Crimea, East and South of Ukraine

Creation of an efficient system of the information security of Ukraine

Regulatory and legal framework

Evaluation of the information threats

List of subjects for maintaining information security

Creation of a separate information security system for the Ministry of Defense and the General Staff of the AF of Ukraine

Ukraine's national system of information security should be aggressive and defending Ukrainian national interests

Technical, financial and staffing support

Requirements to Ukraine's Intelligence Agencies in the Context of the "Hybrid War"

Doing all kinds of intelligence with the use of a wide range of methods and means

Counteracting the enemy's "throwing in" of corrupted information (disinformation)

Intelligence in the situation of unpredictability and difficulties with forecasting the developments

Intelligence in constant changing of the nature of threats, variability of the aggressor's tactics

Photos from the site of the Main Directorate of Military Intelligence of Ukraine

Deep analysis of the intelligence and timely information and intelligence support to the top state and military leadership for making decisions in the sphere of national (military) security create favorable conditions for winning a victory in the "hybrid war»

Hybrid warfare is warfare with the following aspects:

- *Uses a combination of conventional and irregular methods.*

- Methods and tactics includes:
- conventional capabilities, irregular tactics, irregular formations, diplomacy, politics, terrorist acts, indiscriminate violence, and criminal activity.

- A hybrid adversary also uses clandestine actions to avoid attribution or retribution.

- These methods are used simultaneously across the spectrum of conflict with a unified strategy.

- A current example is the Islamic State's transnational aspirations, blended tactics, structured formations, and cruel use of terror as part of their arsenal.

Hybrid warfare is warfare with the following aspects:

- *A hybrid adversary is flexible and adapts quickly.*
- For example, the Islamic State's response to the U.S. aerial bombing campaign was to quickly reduce the use of checkpoints, large convoys, and cell phones.
- IS militants also dispersed among the civilian population. Civilian collateral damage from airstrikes can be used as an effective recruiting tool.

Hybrid warfare is warfare with the following aspects:

A hybrid adversary uses advanced weapons systems and other disruptive technologies. These weapons can be now bought at bargain prices. Moreover, other novel technologies are being adapted to the battlefield such as cellular networks. In 2006, Hezbollah was armed with high-tech weaponry, such as precision guided missiles, that nation-states typically use. Hezbollah forces shot down Israeli helicopters, severely damaged a patrol boat with a cruise missile and destroyed heavily armored tanks by firing guided missiles from hidden bunkers. The organization also used aerial drones to gather intelligence, communicated with encrypted cell phones and watched Israeli troop movements with thermal night-vision equipment.

Hybrid warfare is warfare with the following aspects:

- *A hybrid adversary uses advanced weapons systems and other disruptive technologies.*
- These weapons can be now bought at bargain prices.
- Moreover, other novel technologies are being adapted to the battlefield such as cellular networks.
- In 2006, Hezbollah was armed with high-tech weaponry, such as precision guided missiles, that nation-states typically use. Hezbollah forces shot down Israeli helicopters, severely damaged a patrol boat with a cruise missile and destroyed heavily armored tanks by firing guided missiles from hidden bunkers. The organization also used aerial drones to gather intelligence, communicated with encrypted cell phones and watched Israeli troop movements with thermal night-vision equipment.

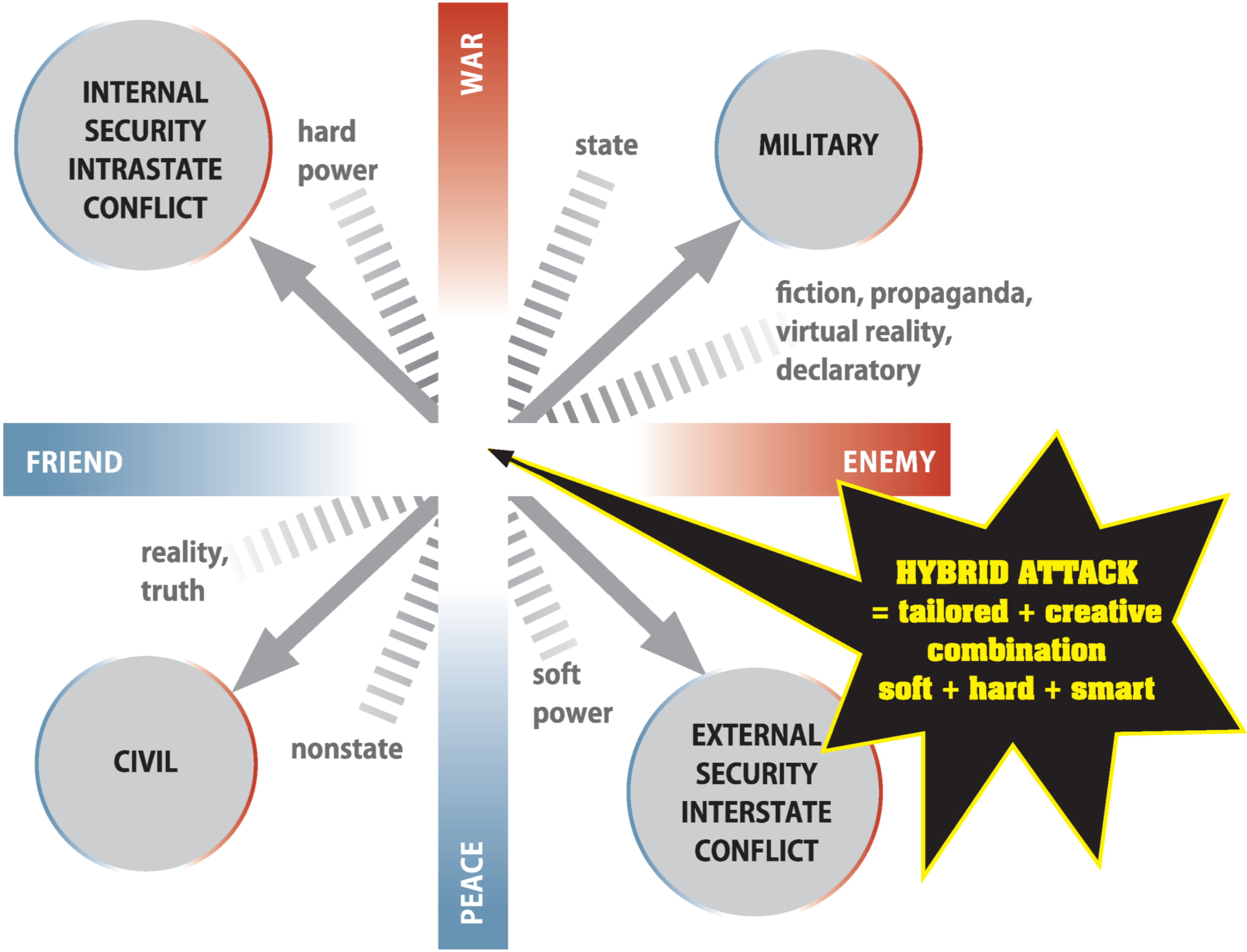
Hybrid warfare is warfare with the following aspects:

- *Use of mass communication for propaganda.* The growth of mass communication networks offers powerful propaganda and recruiting tools. The use of fake news websites to spread false stories is an element of hybrid warfare.

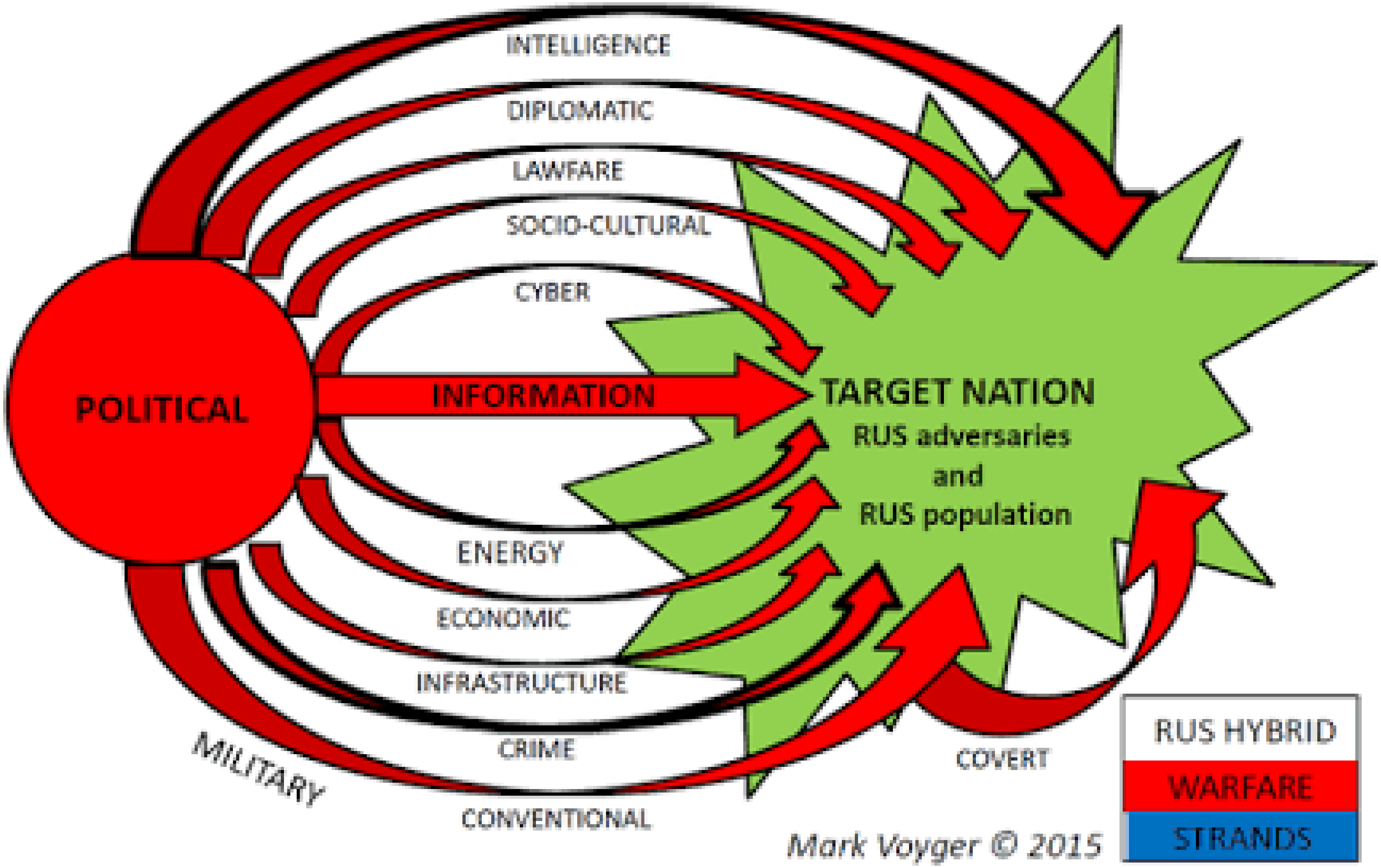
- *A hybrid war takes place on three distinct battlefields.* the conventional battlefield, the indigenous population of the conflict zone, and the international community.

HYBRID WARFARE AND THE CONCEPT OF INTERFACES

Operating in the Shadow / Grey Area of Interfaces


WAR
INTERNAL SECURITY INTRASTATE CONFLICT
hard power
state
MILITARY
fiction, propaganda, virtual reality, declaratory
FRIEND
ENEMY
reality, truth
CIVIL
nonstate
soft power
EXTERNAL SECURITY INTERSTATE CONFLICT
PEACE
HYBRID ATTACK
= tailored + creative combination
soft + hard + smart

RUS Hybrid Warfare 'Hydra': Deployable abroad and inside Russia



Mark Voyger © 2015

1 REGULAR MILITARY FORCES
กำลังทหาร ปกติ

2 SPECIAL FORCES
กำลังทหาร รบพิเศษ

3 IRREGULAR FORCES
กองกำลัง ที่ไม่ใช่ทหาร

4 SUPPORT OF LOCAL UNREST
การสนับสนุน จากประชาชน ในท้องถิ่น

5 INFORMATION WARFARE PROPAGANDA
สงครามข้อมูล ข่าวสาร และการ โฆษณาชวนเชื่อ

6 DIPLOMACY
การทูต

7 CYBER ATTACKS
การโจมตี ด้านไซเบอร์

8 ECONOMIC WARFARE
สงคราม เศรษฐกิจ

1 และ 2 เป็นอำนาจของรัฐ

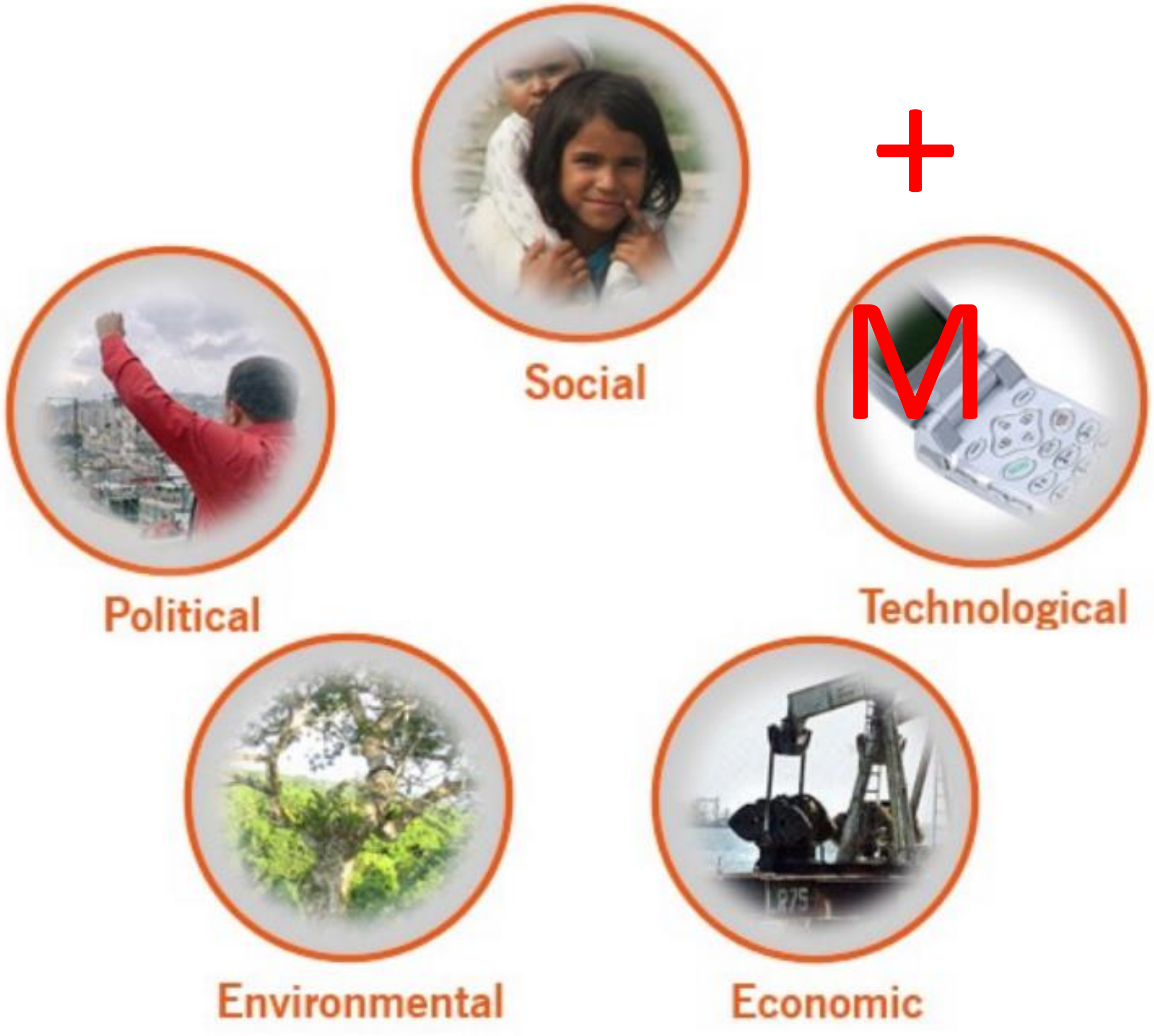
สงครามลูกผสม
HYBRID WARFARE

Comprehensive Security

- Social
- Technology
- Economic
- Environment
- Politic
- Military

Comprehensive Security : STEEPM

STEEP Framework



What is STEEP Analysis?

- The **STEEP** analysis tool is a framework to gauge how the external environment will impact a given company's strategic plan to remain competitive.
- **STEEP** is an acronym for: **Social, Technological, Economic, Ecological (Environmental) and Political**. Other known acronyms derived from STEEP are: PEST, PESTLE, PESTEL, STEP, STEPJE, STEEPLED and LEPEST. The STEEP acronym is well known and used all over the world as a basis for external analysis.

STEEP-M

- Age of Uncertainty
- Strategic Agility

War or peace?

Understanding the grey zone.

Discipline in definition

The impulse to designate this domain as a place of conflict rather than competition is strong. After all, conflict is more likely to command attention and resources than peace. Yet much, but not all, of what we see being conducted in this space could be characterised as features of the difficult, new peace as much as the new warfare.
The range of means being used to project state power is wide and the tempo fierce, but that does not mean that a state of war exists. The contestation we are seeing through unregulated means, in particular in the field of information and subversion, might for all its bumpiness be what the new peace rather than the new war looks like.

The so-called ‘battlespace’ needs decluttering by designating with rigour what activities by foreign states are ‘warlike’, in that they are tantamount to the use of force, and which ones amount to unregulated (and possibly unlawful) competition.
Understanding the difference will help to determine appropriate responses. It will also encourage a more careful use of martial language and a better understanding of the inherent risks of choosing to adopt it.

Broadening the range of activities that are classified as belligerent effectively lowers the threshold for escalation. Governments can’t not respond if they talk of their jurisdiction being attacked. But if they use the language of peacetime, even if the peace is a dirty one, the threshold will be higher. It leaves room for competition, engagement and arbitration. It may ultimately, and importantly, allow for the evolution of rules.

Calibration of response

Sufficient political capacity and appetite needs to be conserved for responding to egregious threats, rather than allowing it to be dissipated in adversarial responses to all perceived activities in the grey zone, many of which constitute a crude form of competition.

There is a conceptual difficulty here, especially for Western powers, whose tolerance for what constitutes competition may have changed in tandem with the shifting balance of global power. Many grey zone activities are functions of a rewired and restructured global economy. To take three of the most potent weapons – information, credit and capital – these used to be monopolised by the same powers that possessed superior firepower and moral authority, namely the US and its allies. That is no longer the case. The weapons, the power and the narratives are more disparately distributed.

China is using its capital and extending its credit on a scale previously unimaginable, and the strategy is paying dividends. Russia has become the most subversive player in cyber space, while China is helping itself to Western IP. It is no surprise that in this new ranking competition is tough and unsettling for those who used to dominate, and it feels sufficiently hostile to be a war.

States will continue to conduct hostile actions against or in foreign jurisdictions by clandestine or deniable means. These actions can be breathtakingly aggressive and occasionally heinous. This small category of activities can constitute a war-like act. Salisbury was close. Sustained cyber pillaging or disabling of national infrastructure might qualify. But the category is best dealt with through existing conventions, robustly applied by law-enforcement agencies and legally governed by intelligence and security counter measures.

Promotion of regulation

Activities in the grey zone are subject to very little, if any, regulation. It is fanciful to imagine a regulatory agreement between states on intelligence or information operations other than in the most exceptional circumstances. But it is possible to imagine at least hot-line exchanges over the most egregious examples of grey zone activity and, incrementally, a setting of boundaries. Historically, this is how regulation to manage new weapons systems has evolved.

More importantly perhaps, it is now possible to imagine the development of a relationship between states and tech and media companies around the ways in which their services are used for propaganda or subversive purposes. There is a delicate balance to be struck between their liberties and new responsibilities, which come as a consequence of being distinctive and powerful actors in the grey zone. There is much to build on given the progress that has made in counter-terrorism and counter-radicalisation.

The strategic goal should be to extend existing conventions and regulations into the activities and means observed in the grey zone. That will require sustained, multilateral effort, and the gains will be incremental. But it will result in the promotion of the rule of law and an inclusion of the grey zone in the realm of peaceful relations between states. The danger is to accept that the grey zone is by definition a place where rules do not apply and that it is growing. This encourages bad behaviour on all sides and raises the risk of miscalculation and escalation. Pacifying the grey zone could prove to be the generational challenge for those states committed to updating and preserving the rule of law.

What’s need to be done?

- Offensive Hybrid Warfare
- Defense Hybrid Warfare
- Strategic = Comprehensive security
- Operational? Tactical?
- No Framework, no Doctrines

Q & A