Australian Government
Department of Defence
Defence Science and Technology Group

Conceptualisation of Hybrid Warfare

NATO 9th Operations Research And Analysis Conference 22-23 Oct 2015

Donald Lowe and Thitima Pitinanondha
Defence Science and Technology Group, Australia

Acknowledgments: Rick Nunes-Vaz, Cayt Rowe, Ivan Garanovich, Li Jiang

For further information, please contact:
Donald Lowe
e: donald.lowe@dsto.defence.gov.au
p: +61-2-61287374

Introduction

- Hybrid warfare: *A pithy term that attempts to capture the complexity of current conflict that goes beyond "traditional" military warfare?*
  - "widely understood to blend conventional/unconventional, regular/irregular, and information and cyber warfare" (Van Puyvelde, 2015)
  - "terrorism and criminal behaviour" (Hoffman, 2014)
  - "financial manipulation; kidnapping and illegal border crossings" (Kramer et al., 2015)

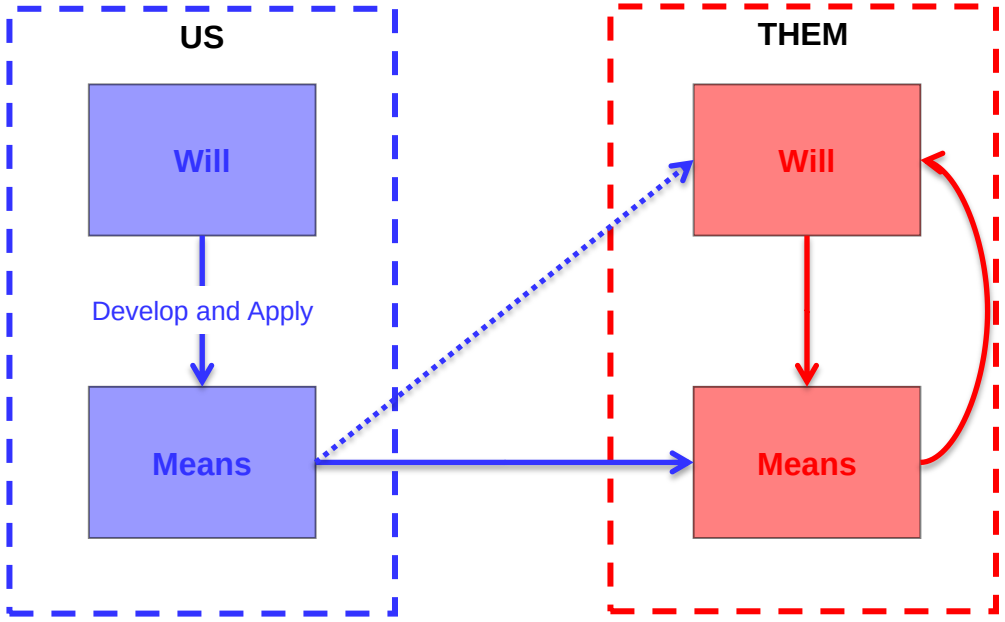
- The Challenge
  - How to design a set of entities that is capable of containing or defeating the adversary/ies undertaking "hybrid warfare"?

- The Approach?
  - This requires a modelling approach that can describe this interconnected space, provide insights into the nature of this complexity and usefully guide the design of the collection of entities.
  - *Caveat: this is a **very early** exploration of a potential approach*

Clausewitz (really) simplified

- "War therefore is an act of violence to compel our opponent to fulfil our will".
- "Violence, that is to say physical force … is therefore the means; the compulsory submission of the enemy to our will is the ultimate object. In order to attain this object fully, the enemy must be disarmed; and this is, correctly speaking, the real aim of hostilities in theory."

(Carl von Clausewitz, "On War")



This is still fundamentally true today, as to stop an adversary you address either the Means or the Will (or both):

- You attack their Means to prevent them imposing their Will on you.
- You "attack" their Will so that they do not feel disposed to using their Means.

We would simply expand "violence" and "physical force" to any forms of influence or coercion (including positive ones!).

In simple terms, *Hybrid Warfare* expands upon Clausewitz as to the *Means* used, as well as the Adversary's *Means* attacked and perhaps more directly addressing their *Will*.

DIME and effects

- The concept of instruments of national power has evolved in the U.S. since the 1970s. At the turn of the century, the Department of Defence formalised them as four specific elements of national power: Diplomatic, Informational, Military, and Economic (DIME) (Department of Defense, 2000)

- It became a pillar of the emerging concept of Effects-Based Operations (EBO) in the US during the early part of this century. However, EBO failed to be successfully operationalised which resulted in it being eventually discarded (Mattis, 2008).

- Despite the failure of EBO, the ideas of instruments of national power and effects are both enduring concepts which are perhaps useful to try to better align and integrate all elements of hybrid warfare (including cyber).

Viewing hybrid warfare as DIME

Amongst some quarters, there is a view that hybrid warfare can be viewed simply as the use of the extant DIME model:

- "So I thought I would open my remarks today just addressing this hybrid war, … really, it is a collection of tools that we've seen in warfare before … we use a model called DIME, diplomatic, informational, military, and economics" (General Philip Breedlove, NATO Supreme Allied Commander Europe, 2015)

- "Diplomatically, Russia is trying to push the argument that Ukraine's authorities are the problem. In the information sphere, we see an information and disinformation campaign aiming to mask Russia's intentions. Militarily, we see daily troop movements, cross-border shelling and the use of all [types of] military capabilities. And, lastly, economic warfare through [the manipulation of] energy supplies," (General Philip Breedlove, NATO Supreme Allied Commander Europe, 2014)

- "Strategic deterrence involves the development and implementation of a complex system of interrelated political, diplomatic, military, economic, informational, and other measures aiming to pre-empt or reduce the threat of destructive actions from an attacking state (or coalition of states)" (Government of Russia, 2009), which (Franke, 2015) notes "The measures thus enumerated in the strategy are very similar to the Western DIME, spelled out as Diplomatic, Information, Military and Economic power."

- "As discussed by Russia in its new doctrine the military instrument per se plays only a limited role. Instead all of the instruments of power are employed: diplomacy, information, military, and economic (DIME). The purpose of using these instruments in this synchronized way is to pressure, influence, and destabilize other countries, i.e. destroying or at least permanently weakening regimes that oppose Russian interests." (Thiele, 2015)

Utilising "Effects" to more broadly describe operations

- An *effects lexicon* is required that is capable of generically describing effects.
  - Lowe and Ng (2004) provide a draft foundational lexicon that connects effects, actions and entities.

- Also an *effects framework* is also required that, in conjunction with the lexicon, facilitates the construction of concept maps of systems.
  - Lowe et al. (2006) provide a framework of functions, services and domains that can be used to categorise types of generic actions and their impact.

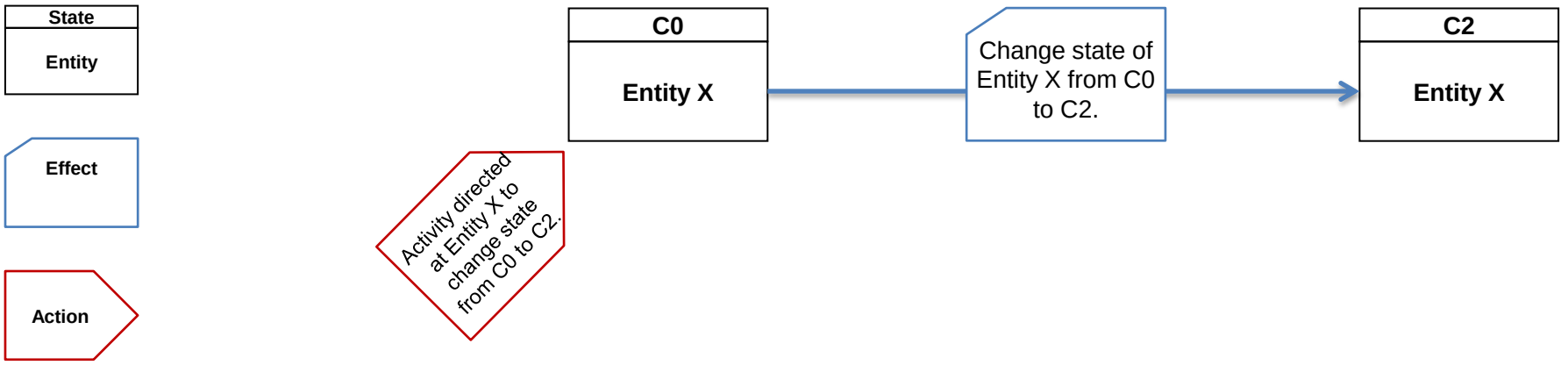
An effects-based lexicon

The protoype effects-based lexicon of (Lowe and Ng, 2004) describes *entities* as existing in actual *states* and having potential other *states*.

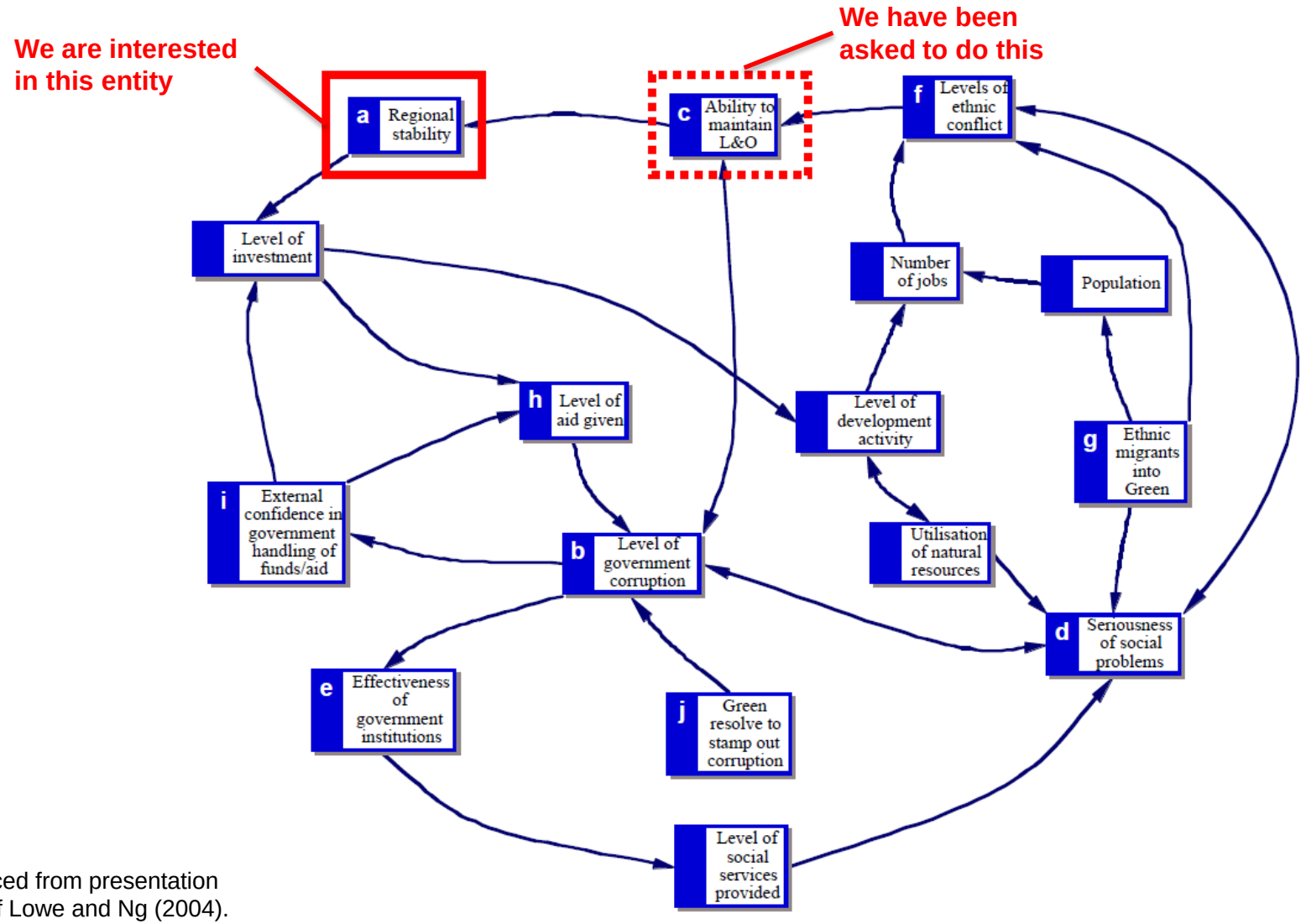
An *effect* is *a change of state* of an *entity* from its current *state* to one of its potential *states*.

An *action* is some activity that is directed at an *entity* or the system of which it is a part. Often, it is done to produce a particular *effect*, but it can only be causally linked if it is successful.

This simple approach allows one to define *actions*, *effects* and *entities* so that these can be linked coherently.

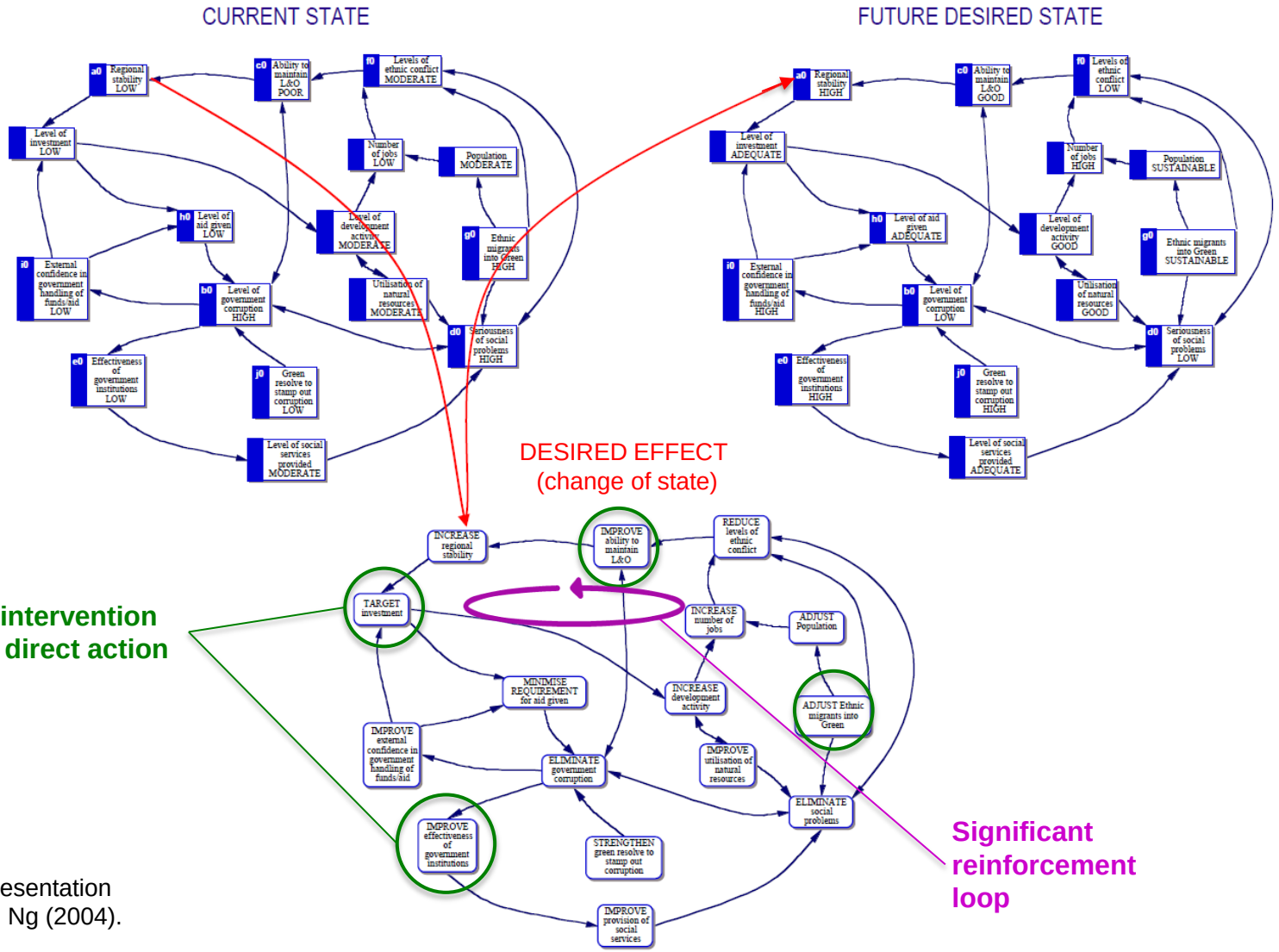


Simple Exemplar – Stabilising a failing nation-state



Reproduced from presentation version of Lowe and Ng (2004).

Crafting a set of actions



Reproduced from presentation version of Lowe and Ng (2004).

An effects-based framework

- While the lexicon provides a simple way to link actions, effects and entities, in order to be useful in describing and understanding the broadness and complexities of hybrid warfare, a more detailed description of entities is desirable.

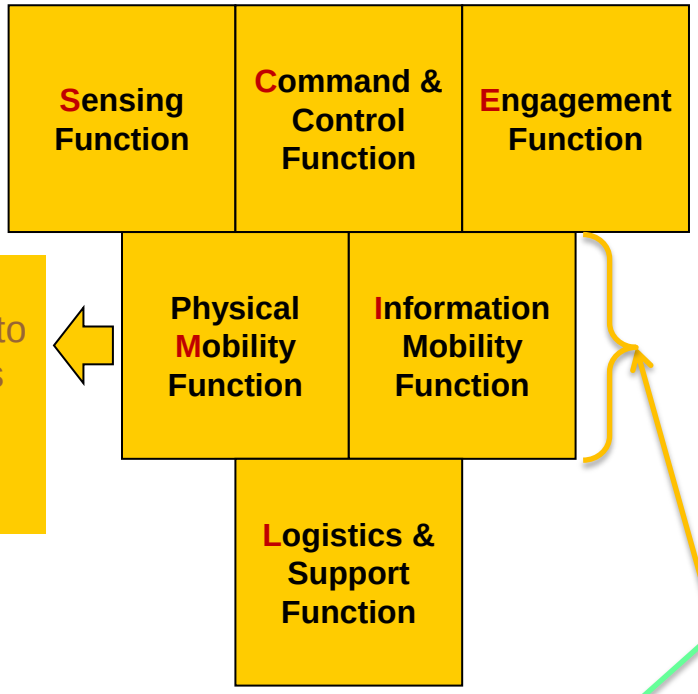
- Entities can be fairly comprehensively described as possessing six basic functions which perform six related actions (or services) in three basic domains (Lowe et al., 2006).

- These were specifically derived from an expansion of concepts introduced with Network-Centric Warfare (NCW) which introduced
  - Four Grids (*Command, Engagement, Sensing, Information*)
  - Three Domains (*Physical, Information, Cognitive*)

From NCW to SCMILE

SCMILE "converted" the four NCW Grids to similarly named functions (SCEI).

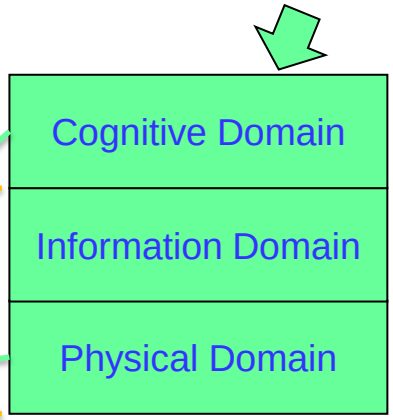
As NCW was focussed upon information networking, it didn't include the more material *Physical Mobility & Logistics & Support* functions which are added to make up SCMILE .



Note that the *mobility functions* refer naturally to the movement of entities in two of the domains:
- Physical
- Information

The three NCW domains are interconnected aspects of the material world.

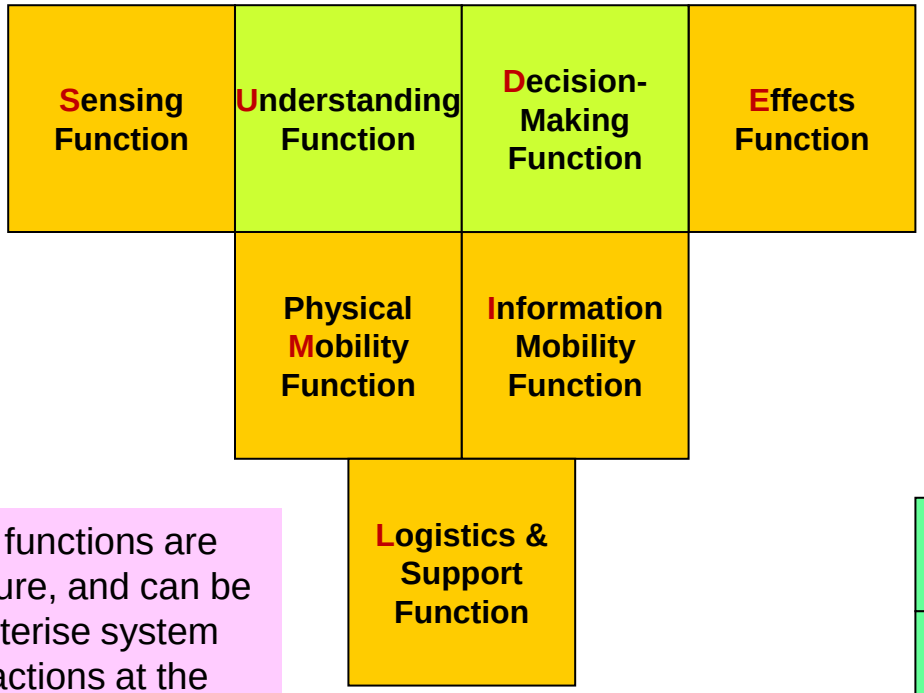
Entities fundamentally inhabit the physical world, but have identifiable related properties in the other domains.



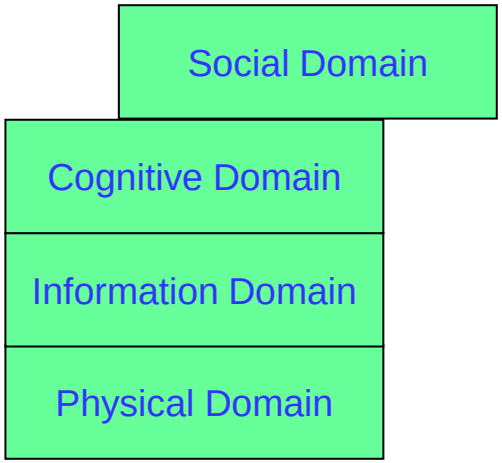
Clausewitz already refers to two of these domains:
- Will = Cognitive
- Means = Physical

From SCMILE to SUDEMIL

SCMILE has been modified by breaking *Command & Control* into its components of *Understanding* and *Decision-Making*. This has been done to better expand the utility for specific military functions (notably Intelligence). Additionally, a fourth domain has been added, the *Social Domain*, which characterises the behaviour of the groups of people.



As the Social Domain is in some respects an *emergent property*, it does not perfectly align with the other three domains, which generally apply to single entities.



The SUDEMIL functions are scalable in nature, and can be used to characterise system functions and actions at the tactical, operational and strategic levels.

SUDEMIL Effects-Based Approach (SEBA)

- The SEBA Framework consists of
  - Seven functions
  - Four types of actions (seven if expanded)
  - Three domains (four if expanded)

Entity SUDEMIL Functions	Entity DIME(FIL) Actions	Domains
Sensing	Diplomatic	Physical
Understanding	Information	Information
Decision-making	Military	Cognitive
Effects	Economic	(Social)
Information Mobility	(Financial)	
Physical Mobility	(Intelligence)	
Logistics & Support	(Law Enforcement)	

- Any entity can be described holistically as a set of the seven functions
  - These functions serve as attributes of the entity, as well as potential actions the entity may perform.
- Within an effects-based paradigm, the engagement function is expressed as the four (seven if expanded) potential actions.
- These functions and actions exist simultaneously in the three domains:
  - They manifest materially in the physical domain
  - They have data and metadata that is associated with them that exists in the information domain
  - They impact on the knowledge systems of individuals and entities in the cognitive domain
  - (They may also further emerge as shared knowledge in the social domain)
- Together, these potentially provide a framework to consistently characterise hybrid warfare.

Discussion of the SEBA Framework

- The SEBA Framework provides a way to categorise both the entity attributes being targetted as well as the capabilities required in hybrid warfare.

- Note that the aim is NOT a "perfect systems model", which is unattainable. The aim is to be able to systematise actions in a more integrated fashion and promote shared understanding as to their logic and their ultimate efficacy. This model is sufficient to generate the first order comprehension of the activities and results of hybrid warfare.

- This might be built upon with other models. For example,
  - PMESII (political, military, economic, social, information, infrastructure) may be useful when looking at a target nation's key systems, or
  - Maslow's hierarchy (of needs) could be useful if targetting the state of individuals or social groups.

Cyber warfare SEBA characterisation

The following table exemplifies the use of the SEBA framework to characterise specific cyber attacks in a systematic way, breaking down the specific actions undertaken, effects sought, functions under attack and the primary domains where the activity occurred.

The aim is to be able to use this standard taxonomy to better and more comprehensively model systems and design capabilities and actions.

Event	D.D.O.S. attack on Estonia (Apr 2007)	Stuxnet (2008-10)	Turkey Pipeline Explosion during Russo-Georgian War (2008, suspected)
Source Entity	unattributed	unattributed	unattributed
Source Entity *DIME Action/s*	Information attack (primarily – had some economic consequences)	Combined Military and Information attack (to produce a physical effect)	Information attack (with physical and economic impacts)
Target Entity	Estonian government websites	Iran Natanz uranium enrichment facility	Baku–Tbilisi–Ceyhan pipeline
Target Entity *state transition (Effect)*	functioning websites to non-functioning websites	optimum enrichment to degraded enrichment capability	functioning pipeline to damaged non-functioning pipeline
Target Entity *SUDEMIL Functions* under attack	Targeted Information Mobility Function of Estonian government	Targeted Understanding and/or Decision-Making Function of Iran nuclear facility	Targeted Sensing, Understanding and/or Decision-Making Function of Computer Management System
Domain Activity	Attack within Information Domain via physical networks from remote locations (caused informational mobility damage)	Attack within Information Domain via a proximate physical attack (caused informational and then physical damage)	Attack within Information Domain via physical networks (changing information and causing physical damage)

Ukraine Crisis SEBA characterisation

A recent report hypothesised different phases and actions in the Ukraine crisis (Rácz, 2015).

The following table has selected a single action within each phase to be characterised by the SEBA Framework. This begins to systematise the actions and effects that may have occurred.

Phase	Action	DIME Action	PIC Domain Activity	SUDEMIL Function Targeted
Strategic Preparation	Exploring points of vulnerability in the state administration, economy and armed forces of the target country	I	I	SUDEMIL
Political Preparation	Establishing contacts with local oligarchs and business people; making them dependent on the attacking country via profitable contracts.	DE	P	UDL
Operational Preparation	Mobilizing the Russian armed forces under the pretext of military exercises	MI	PI	SUD
Exploding the Tensions	The media of the attacking country launches a strong disinformation campaign	I	I	SU
Ousting the central power from the targeted region	Disabling the central power by capturing administrative buildings and telecommunications infrastructure in the targeted region	M	P	IL
Establishing alternative political power	Declaring an alternative political centre, based on the captured administrative buildings, by referring to real or fabricated traditions of separatism	DI	PIC	SUD
Political stabilization of the outcome	Organizing a 'referendum' and decision about secession/independence in the target country, all with the strong diplomatic and media support of the attacking country	D	IC	UD
Separation of the captured territory from the target country	attacking country annexes the captured territory (Crimea)	M	P	SUDEMIL
Lasting limitation of the strategic freedom of movement of the attacked country	Loss of territory (economy, population, infrastructure, etc.) results in severe economic hardship, domestic political destabilization and possibly grave humanitarian situation.	M	P	SUDEMIL

Entities and their state from a NATO perspective

The table below records the state of some of the major entities before and after the hypothesised Russian DIME Actions from a NATO perspective (as estimated by the authors where 1 is excellent and 5 is very poor).

While the development of a concept map that relates these entities is beyond the scope of this presentation, this would be a necessary step towards a fuller understanding of the situation and the preparation of actions to shift the entities to more favourable states (from a NATO viewpoint).

ENTITY (SYSTEM)	Russian DIME Action	BEFORE	AFTER	BEFORE	AFTER
GLOBAL					
NATO-Russian relationships	dIMe	3	4		
NATO-Ukraine relationships	DIMe	2	4		
REGIONAL		**Ukraine**	**Ukraine**	**Crimea**	**Crimea**
Political System	DIMe	3	4	3	5
Territory	dIMe	2	4	2	5
Economy	iME	3	4	3	4
Society	DIme	3	4	3	5
Legal	DI	3	3	3	4
Policing	M	2	3	2	4
Military	M	3	4	3	5
Infrastructure, Physical	M	3	3	3	4
Infrastructure, Informational	iM	2	3	3	5

Developing capabilities

- The SEBA Framework potentially provides a systematic method of exploring the initial questions that NATO/EU need to ponder when developing its own response:
  - What are the options for DIME action available to NATO/EU to influence any of the Russian/Ukraine/Crimea entities?
  - What SUDEMIL functions are required to complete these actions?
  - What entities (and associated capabilities) does NATO/EU require to perform these functions?

Takeaways

- Effects are an enduring and universal concept with general application. In principle, effects could be used to model both traditional (military) warfare and non-traditional (cyber, hybrid) warfare.
- The adaptation of a previously developed effects-based lexicon and services conceptual framework has led to the development of the prototype SEBA framework as an approach to modelling hybrid warfare.
- The SEBA framework aims to provide a consistent characterisation of hybrid warfare activity by systematising the range of actions, effects, functions and domains to.
- The SEBA framework can describe the nature of the capabilities required and the attributes of interest of the target entity.

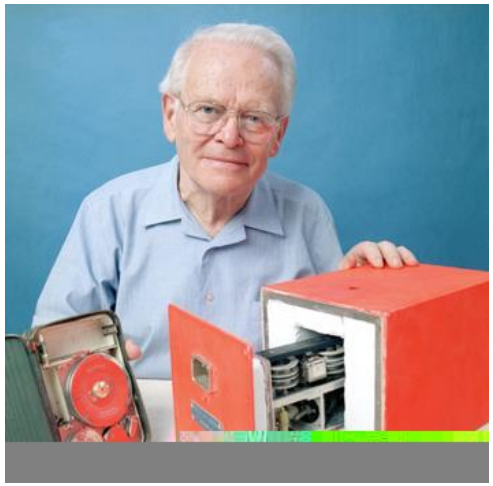
References

- Breedlove, P., 2014. “Die Nato muss auf grüne Männchen vorbereitet sein”, *die Welt*, 17 August. http://www.welt.de/politik/ausland/article131296429/Die-Nato-muss-auf-gruene-Maennchen-vorbereitet-sein.html, accessed 8 September 2015.
- Breedlove, P., 2015. “The Future of Conflict”, *Brussels Forum,* 22 March. http://www.gmfus.org/sites/default/files/22Mar_The%20Future%20of%20Conflict_ccedits.pdf, accessed 2 September 2015.
- Clausewitz, Carl von, “On War”. The complete translation by Colonel J.J. Graham, published by N. Trübner, London, 1873.
- Franke, U., 2015. “War by non-military means: Understanding Russian information warfare”, Swedish Defence Research Agency, Report No. FOI-R—4065—SE.
- Government of Russia, 2009. “Strategy for the national security of the Russian Federation up to 2020”.
- Hoffman, F.G., 2014. “On not-so-new warfare: Political Warfare vs Hybrid Threats”, http://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/, accessed 7 September 2015.
- Kramer, F., Binnendijk, H. and Hamilton, D., 2015. “Defend the Arteries of Society”. http://www.usnews.com/opinion/blogs/world-report/2015/06/09/russia-ukraine-and-the-rise-of-hybrid-warfare, accessed 8 September 2015.
- Lowe, D. and Ng, S., 2004. “Effects-based operations: language, meaning and the effects-based approach”, 2004 Command and Control Research and Technology Symposium, “The power of information age and technologies”, San Diego, 15-17 June 2004.
- Lowe, D., Hayward, J., Bell, J. and Clothier, J., 2006. “The SCMILE Services Framework: A Conceptual tool for designing the NCW force”, 11th International Command and Control Research and Technology Symposium: Coalition Command and Control in the Networked Era, Cambridge, United Kingdom, 26-28 September 2006.
- Mattis, J.N., 2008. “USJFCOM Commander’s Guidance for Effects-based Operations”, *Joint Force Quarterly*, Iss. 51, pp105-8.
- Rácz, A., 2015. “Russia’s Hybrid War in Ukraine: Breaking the Enemy’s Ability to Resist”, The Finnish Institute of International Affairs, FIIA Report 43.
- Thiele, R.D., 2015. “Crisis in Ukraine – The Emergence of Hybrid Warfare”, Institute for Strategic, Political, *Security and Economic Consultancy Strategy Series: Focus on Defense and International Security*, Issue No. 347.
- U.S. Department of Defense, 2000. “The Joint Staff Officer’s Guide 2000”, JFSC Pub 1, National Defense University, Joint Forces Staff College, pp 2-11.
- Van Puyvelde, D., 2015. “Hybrid war – does it even exist?”, *NATO Review*, http://www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/, accessed 7 September 2015.

Questions?

Jindalee Over-the-Horizon Radar

David Warren and his “black box” flight recorder prototype



Nulka Active Missile Decoy