Modeling and Simulation for Hybrid Environments

NMSG Conference
21-22 October 2016
Bucharest

Erdal Çayırcı   Murat Atun   Başar Kasım

Agenda

- Conceptual Model for Hybrid Environments by ET-043
- Modeling and Simulation as a Service (MSaaS)
- HAVELSAN Training and Experimentation Cloud (hTEC)
- Conclusions

Hybrid Warfare

"Hybrid Warfare is underpinned by comprehensive hybrid strategies based on a broad, complex, adaptive and often highly integrated combination of conventional and unconventional means, overt and covert activities, by military, paramilitary, irregular and civilian actors, which are targeted to achieve (geo)political and strategic objectives. They are directed at an adversary's vulnerabilities, focused on complicating decision making and conducted across the full DIMEFIL spectrum in order to create ambiguity and denial. Hybrid strategies can be applied by both state and non-state actors, through different models of engagement, which may vary significantly in sophistication and complexity. Adversaries employing hybrid strategies will seek to remain ambiguous, claim pursuit of legitimate goals and aim to keep their activities below a threshold that results in a coordinated response from the international community. This includes avoiding direct military confrontation, if possible; although the use of overt military action as part of a hybrid strategy cannot be discounted".

Reference: PO(2015)0673, "Strategy on NATO's role in countering Hybrid Warfare"

DIMEFIL: Diplomatic, Information, Military, Economic, Financial, Intelligence, Legal

What is new?

*“The use of hybrid strategies in conflict are not new, but what is new for NATO is the way a wide range of **political, civil and military instruments are combined** and coherently applied, aiming at particular vulnerabilities of targeted nations and international organizations in order to achieve strategic objectives. Common to the state and non-state models is the simultaneous, opportunistic, synergistic and sophisticated combination of **conventional/regular, subversive/irregular and criminal/corrupt actions** in designated geographic areas **to achieve political aims**. **Globalization, underpinned by technological advances**, particularly in the field of communications, including those in cyber space, **has led to increased vulnerabilities** in nations and international organisations that can be exploited in a variety of scenarios that **fall short of direct military conflict**. Increasingly sophisticated cyber-attacks, far reaching **complex propaganda and misinformation campaigns**, as well as **targeted and coordinated political and economic pressure** are indicative of modern hybrid warfare scenarios, which represents a challenge to the defence of Allies’ populations and territory that is broader than just a military threat. Furthermore, hybrid strategies aim at **complicating, delaying and impeding timely decision making** and undermining the ability of an Ally or the Alliance as a whole to respond to such a threat swiftly, firmly and effectively”.*

De-Mystifying

HYBRID WARFARE IS:

- Highly integrated (**synchronized**)
- Combination of **conventional** and **unconventional** means
- **Overt** and **covert** activities

Military, paramilitary, irregular and civilian actors

- Directed at an adversary's **vulnerabilities**
- Complicating **decision making**
- Across the full **DIMEFIL** spectrum
- Creating **ambiguity** and **denial**
- Both State and Non-State actor

+

WHAT IS NEW:

- **Combined**, political, civil and military **instruments**.
- **Political aims** achieved through conventional/regular, subversive/ irregular, criminal/corrupt actions.
- Increased vulnerabilities through **globalization** emphasized by **technological** advances.
- **Fall short of direct military conflict**.
- Complex **propaganda** and misinformation campaigns.
- **Targeted and coordinated** political and economic pressure.
- **Complicating**, delaying and impeding timely **decision making**.

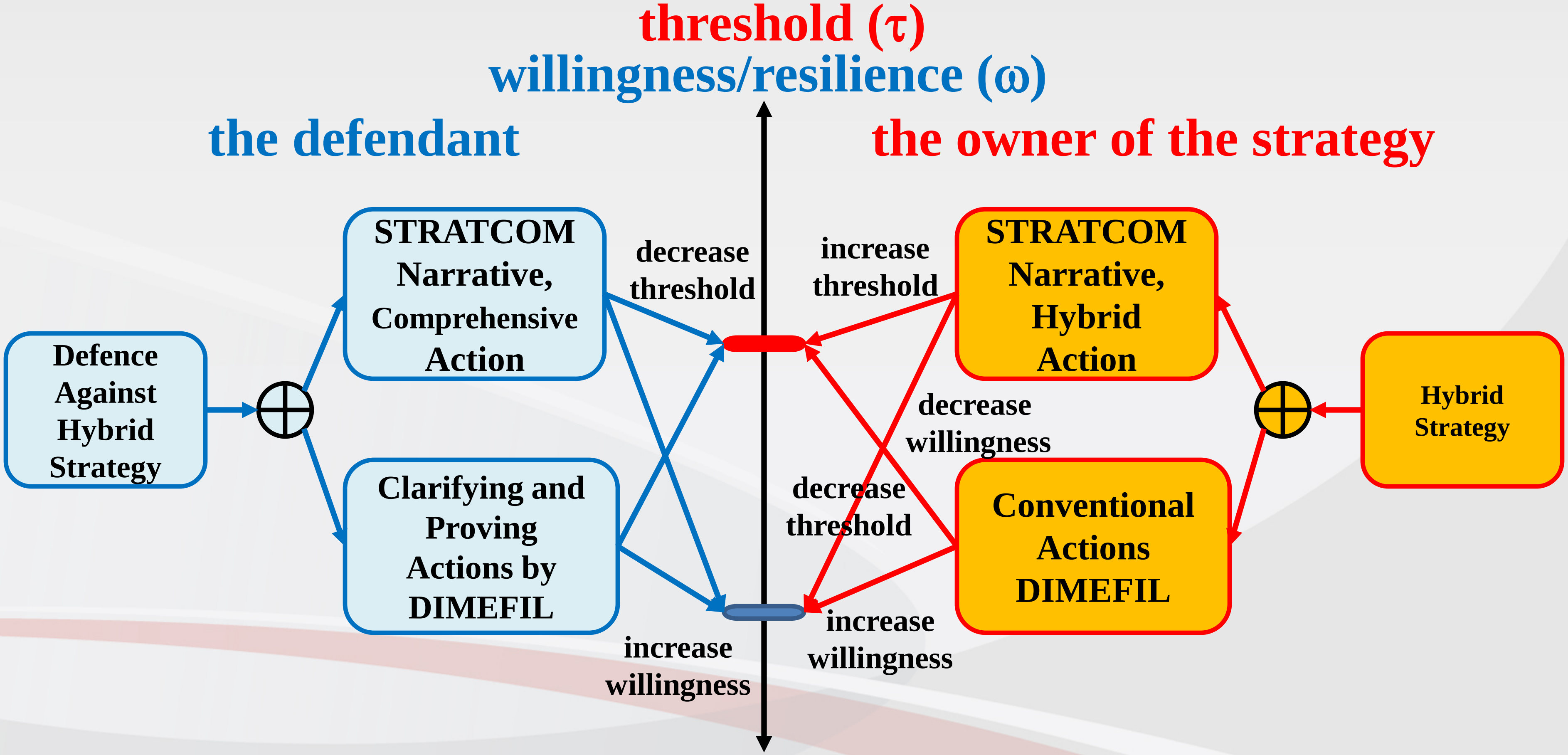
Components of a Hybrid Strategy

HAVELSAN
Training is our business!

- **Strategic intent**
  - The will of the Alliance – causing action or in-action (ambiguity or coercion)
- **Battle for the Narrative**
  - Including deception, duplicity, falsify attribution to create ambiguity
- **Exploitation of Weaknesses**
  - PMESII (later DIMEFIL)
- **Adaptive Actions over a Broad Spectrum**
  - NATO’s counteraction results in shift of opponent’s effort
  - Maintain strategic initiative
- **Exploitation of Laws, Treaties, Conventions, and Norms**
- **Use of Armed Forces**
  - Hybrid model without use of armed forces is possible

Conceptual Model for Hybrid Environments by ET-043

HAVELSAN
Training is our business!


threshold (τ)
willingness/resilience (ω)
the defendant
the owner of the strategy
Defence Against Hybrid Strategy
STRATCOM Narrative, Comprehensive Action
Clarifying and Proving Actions by DIMEFIL
decrease threshold
increase willingness
increase threshold
decrease willingness
decrease threshold
increase willingness
STRATCOM Narrative, Hybrid Action
Conventional Actions DIMEFIL
Hybrid Strategy

$$\text{Capacity}(\chi) = \text{threshold } (\tau) - \text{willingness/resilience } (\omega)$$

Cayirci E., A. Bruzzone, F. Longo and H Gunneriusson, 2016. ‘A Model to Describe Hybrid Conflict Environments’, I3M.

The Analytical Model

$$v = \sqrt[d^h]{\prod_{c=1}^{m_i}\left(\prod_{k=1}^{n}(1-R_{ck\alpha})\right)^{t_i/n}}$$

$$v_i = \frac{R_\rho}{t} v_{i-1} \underset{.}{+} \left(1-\frac{R_\rho}{t}\right) v$$

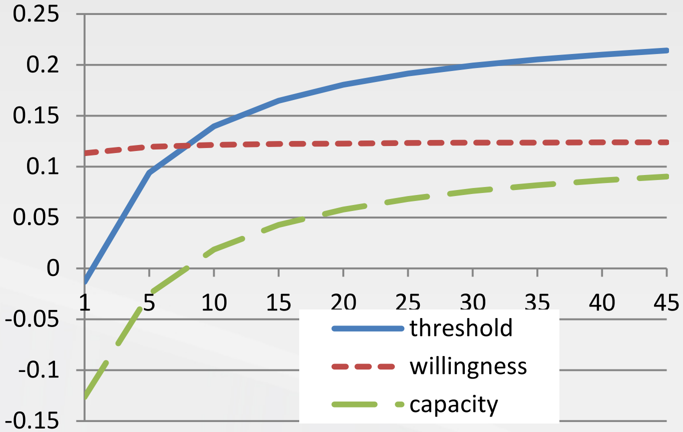
$$a_i = \prod_{c=1}^{m_i}\left(\prod_{k=1}^{n_l}(a_{ol})_{ck}{}^{1/1+(a_d)_{ck}}\right)^{t_i/n}$$

$$a_r = \prod_{c=1}^{m_i}\left(\prod_{k=1}^{n_n}(a_{on})_{ck}{}^{1+(a_d)_{ck}}\right)^{n/t_i}$$

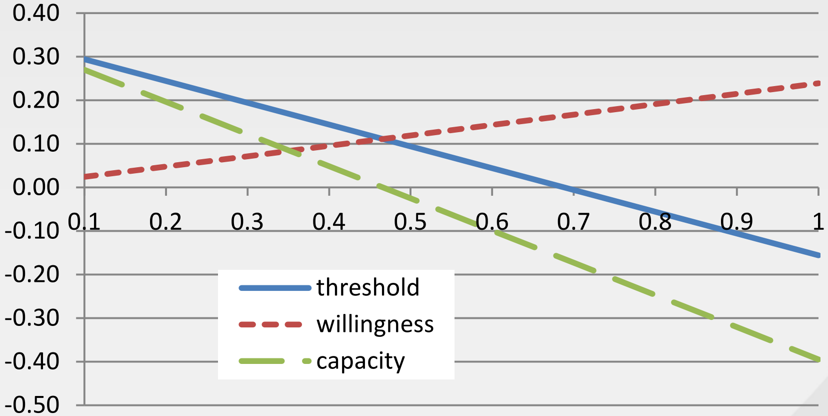
$$\omega = \frac{p_\Sigma\, s_d\, a_i - (1-\, p_\Sigma)\, s_o\, a_r}{d^h}$$

Cayirci E., A. Bruzzone, F. Longo and H Gunneriusson, 2016. ‘A Model to Describe Hybrid Conflict Environments’, I3M.

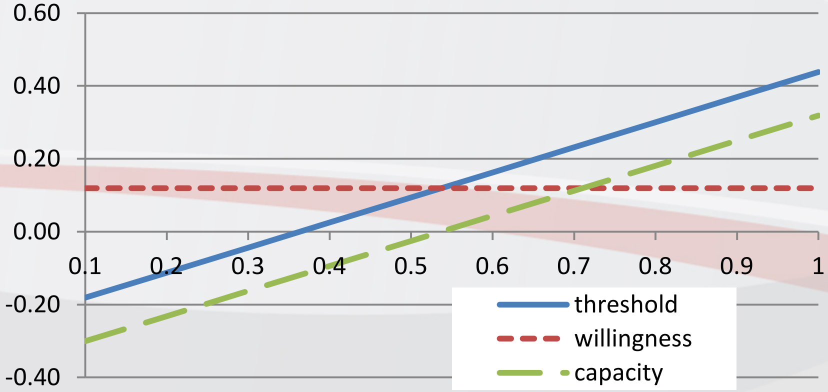
Results from the Model



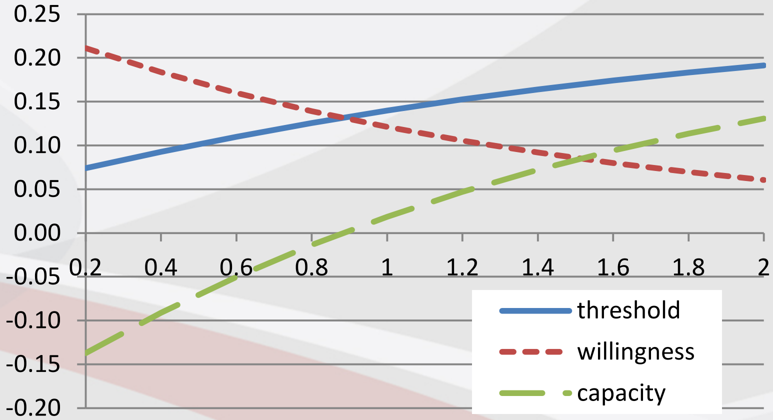
frequency



STRATCOM by defendant



STRATCOM by oponent



discrimination

Cayirci E., A. Bruzzone, F. Longo and H Gunneriusson, 2016. ‘A Model to Describe Hybrid Conflict Environments’, I3M.

Hybrid Threats

Hybrid Warfare for operational level includes threats from the following domains:

Threat	Notes	Current M&S Status
Traditional	Covert and overt military operations including CBRN	Mostly ready, Multi-resolution, JISR Needs To Mature More
Irregular	Guerilla Warfare, Asymmetric Warfare, Etc	Need Threat Network Models
Catastrophic Terrorism	Mass Casualties, Impact On Social And Economic Life	Not Ready… Individual Models For Parts But Not Integrated
Disruptive	Cyber, Critical Infrastructure,	**Definitely Not Ready For Joint Operational Level. Not Integrated.**

Focus Area

Cyber Defense

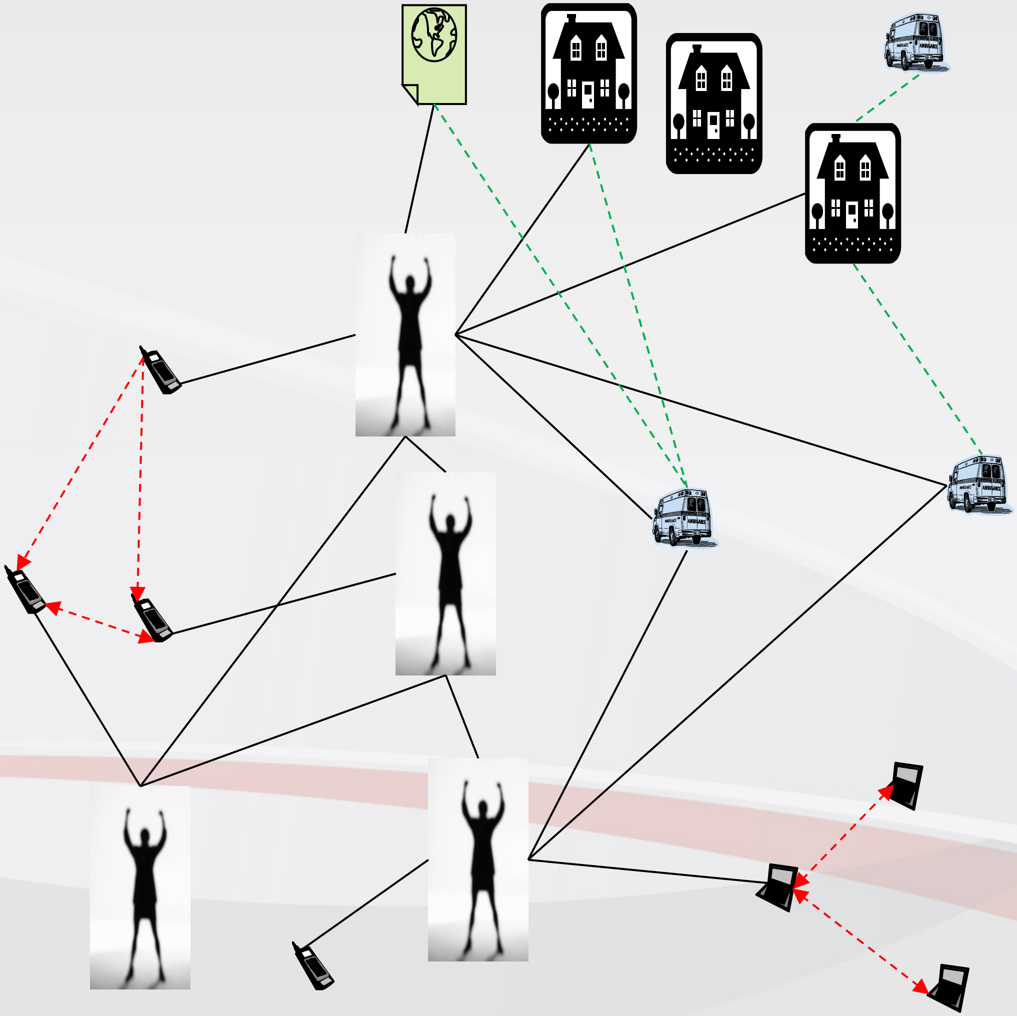
- Joint operational level dilemmas and challenges
- Human Behavior Effect
- Rational decision making under cyber attack
- Planning in joint operational level for cyber incident response and recovery
- Relations with other important domains such as STRATCOM, social/human behavior modelling

Focus Areas

Critical Infrastructure and Their Networks

- Within hybrid warfare context
- Dilemmas and challenges in joint operational level
- Relations with other domains such as STRATCOM, irregular warfare, disruptive attacks, catastrophic terrorism, etc.

Focus Areas



Threat Networks

- Collecting intelligence
- Effect Propagation
- Scenario and MEL/MIL Consistency
- Links with catastrophic terrorism
- Links with disruptive incidents

Focus Areas

Social/Human Behavior Modelling

- Within hybrid warfare context
- Dilemmas and challenges in joint operational level
- Relations with other domains such as STRATCOM, irregular warfare, disruptive attacks, catastrophic terrorism, etc.
- Immigrants, IDPs, etc.
- Epidemics

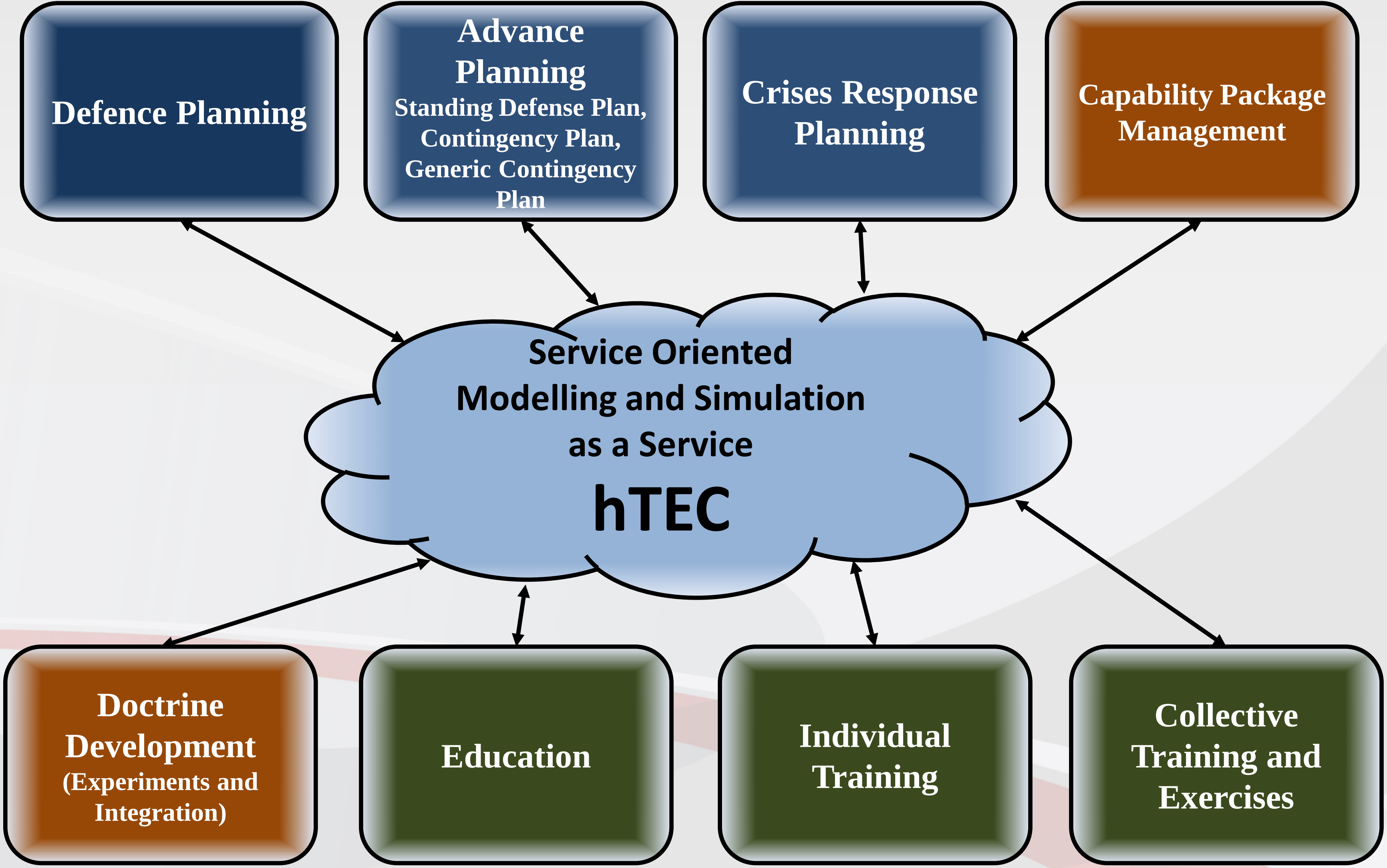
Challenges

- Hybrid scenarios will be different in every conflict. Different elements of hybrid strategies will be combined in different ways. How do you model that?
- Classification levels
- National caveats
- Geographical displacement of stakeholders
- Warfare is at the last phase of HW. Is it a warfare?

Defense Process

HAVELSAN

Training is our business!



Defence Planning

Advance Planning
Standing Defense Plan, Contingency Plan, Generic Contingency Plan

Crises Response Planning

Capability Package Management

Service Oriented Modelling and Simulation as a Service

hTEC

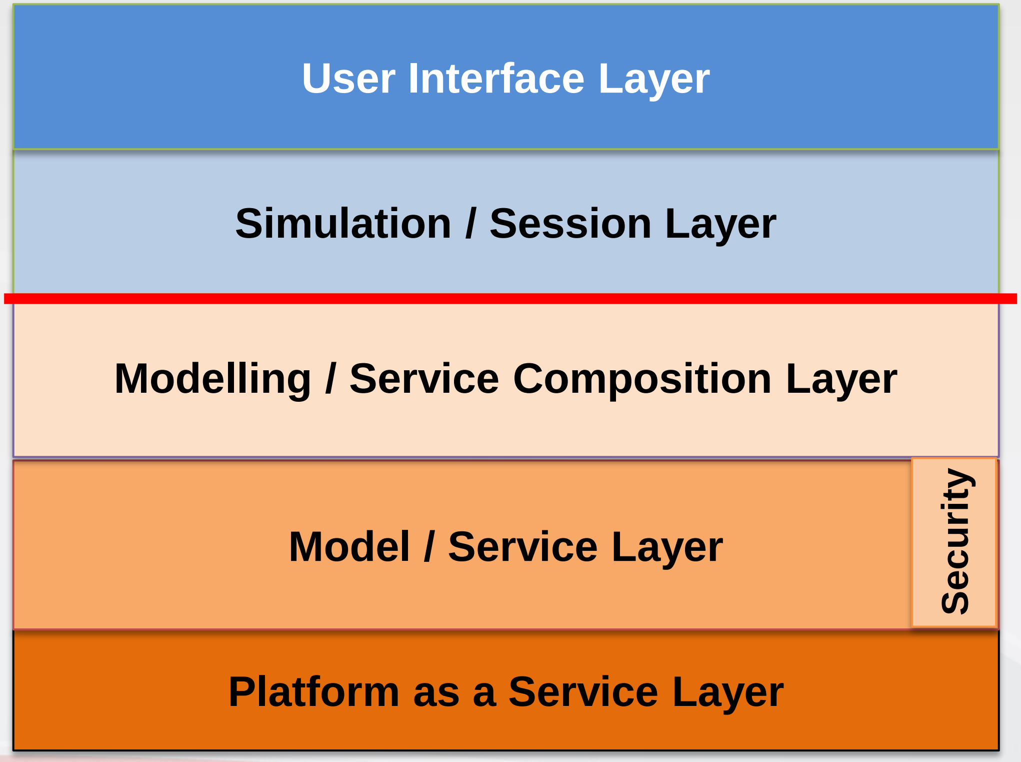
Doctrine Development
(Experiments and Integration)

Education

Individual Training

Collective Training and Exercises

Havelsan Training and Experimentation Cloud (hTEC) and MSaaS



User Interface Layer

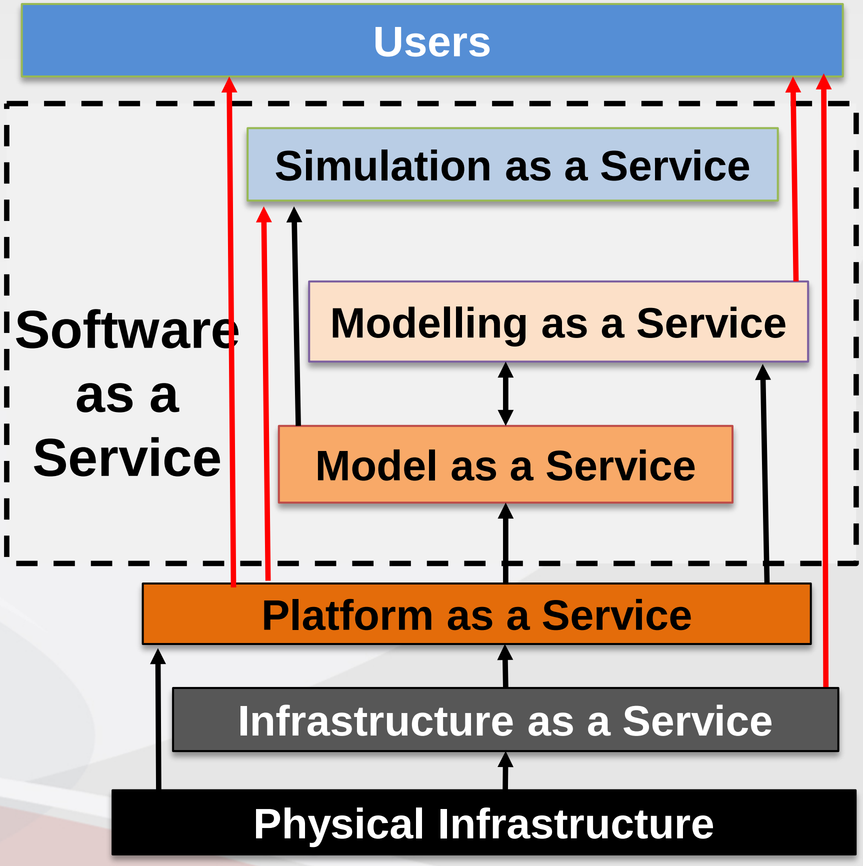
Simulation / Session Layer

Modelling / Service Composition Layer

Model / Service Layer

Security

Platform as a Service Layer



Users

Software as a Service

Simulation as a Service

Modelling as a Service

Model as a Service

Platform as a Service

Infrastructure as a Service

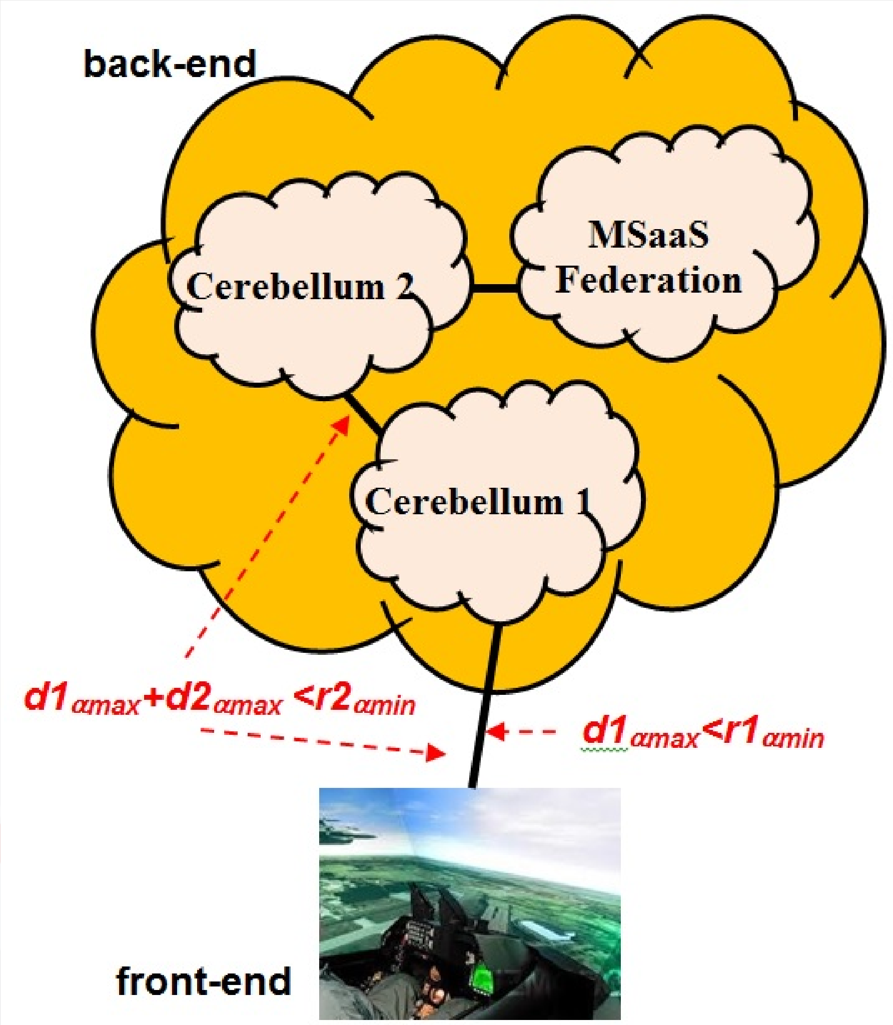
Physical Infrastructure

a. hTEC Layers

b. Cloud Service Models Including MSaaS

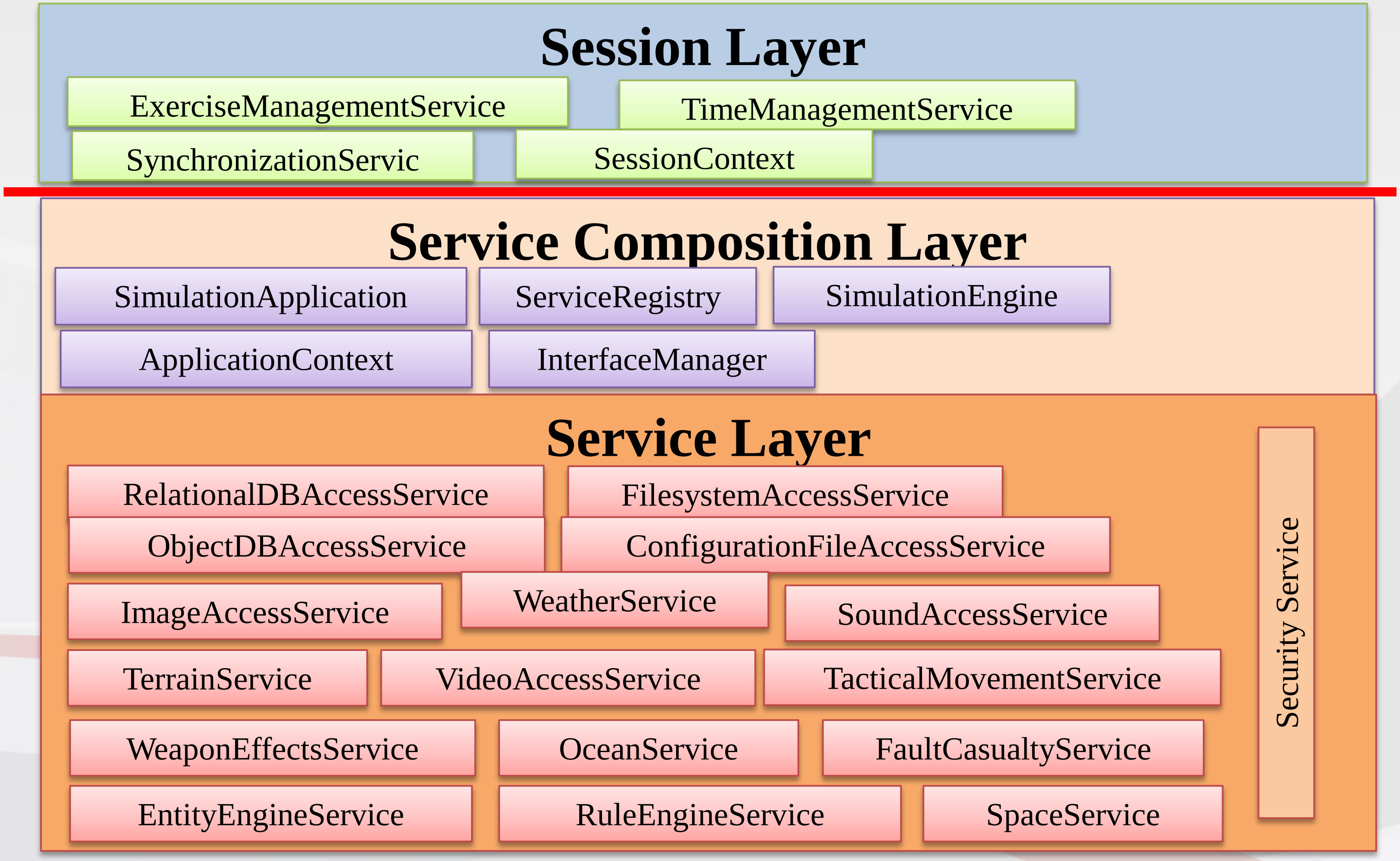
Cayirci E., “ Modelling and Simulation as a Cloud Service: A Survey,” In Proceedings of the 2013 Winter Simulation Conference, edited by R. Pasupathy, S.-H. Kim, A. Tolk, R. Hill, and M. E. Kuhl, Washington DC, December 2013.

Cerebellum Function


back-end
Cerebellum 2
MSaaS Federation
Cerebellum 1
$d1_{\alpha max}+d2_{\alpha max}<r2_{\alpha min}$
$d1_{\alpha max}<r1_{\alpha min}$
front-end

Cayirci E., H. Karapinar and L. Ozcakir, “Cerebellum Function for MSaaS”, The Proceedings of the 27th European Modelling & Simulation Symposium, September 2015.

Examples for hTEC Services



Session Layer

ExerciseManagementService

TimeManagementService

SynchronizationServic

SessionContext

Service Composition Layer

SimulationApplication

ServiceRegistry

SimulationEngine

ApplicationContext

InterfaceManager

Service Layer

RelationalDBAccessService

FilesystemAccessService

ObjectDBAccessService

ConfigurationFileAccessService

ImageAccessService

WeatherService

SoundAccessService

TerrainService

VideoAccessService

TacticalMovementService

WeaponEffectsService

OceanService

FaultCasualtyService

EntityEngineService

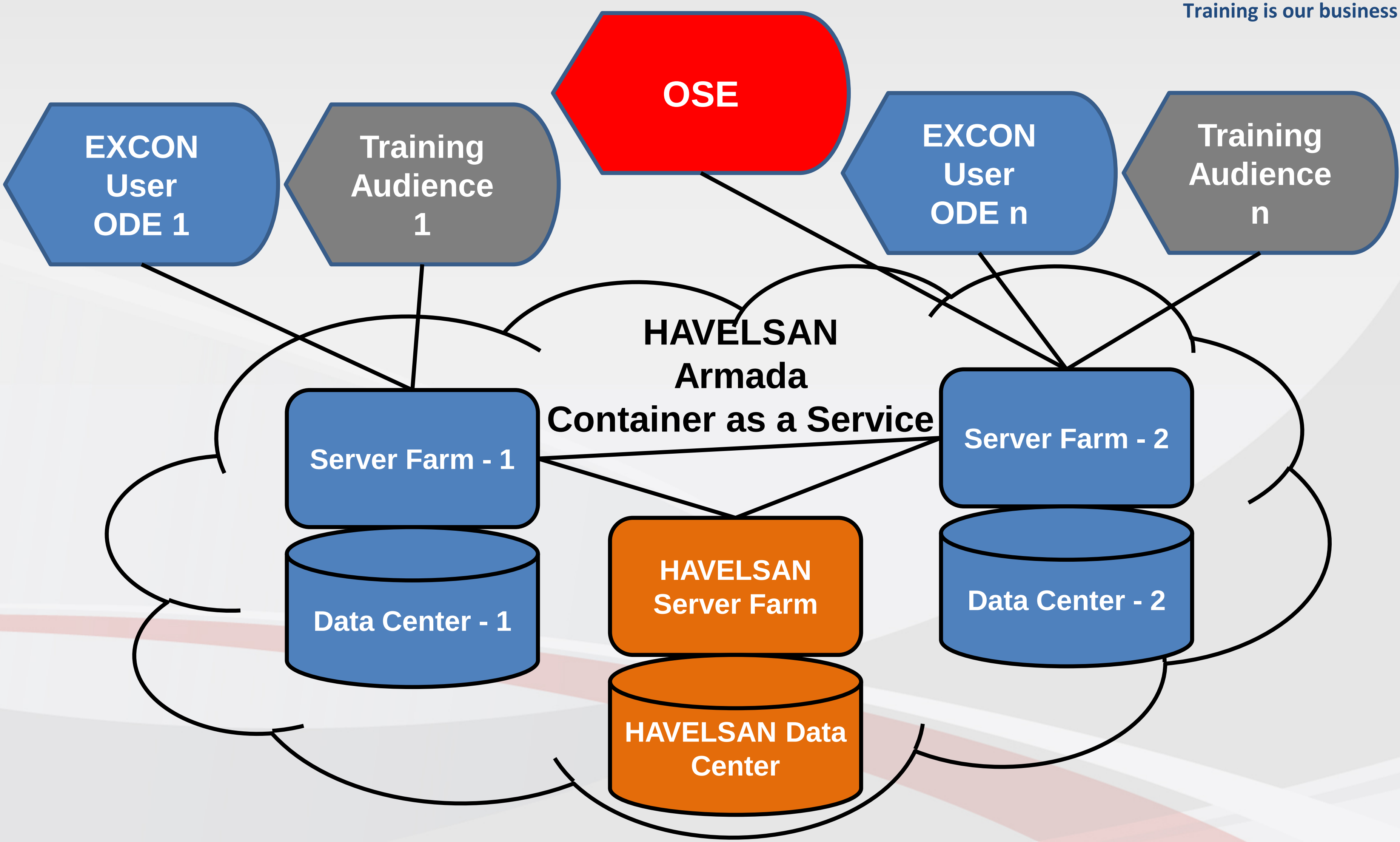
RuleEngineService

SpaceService

Security Service

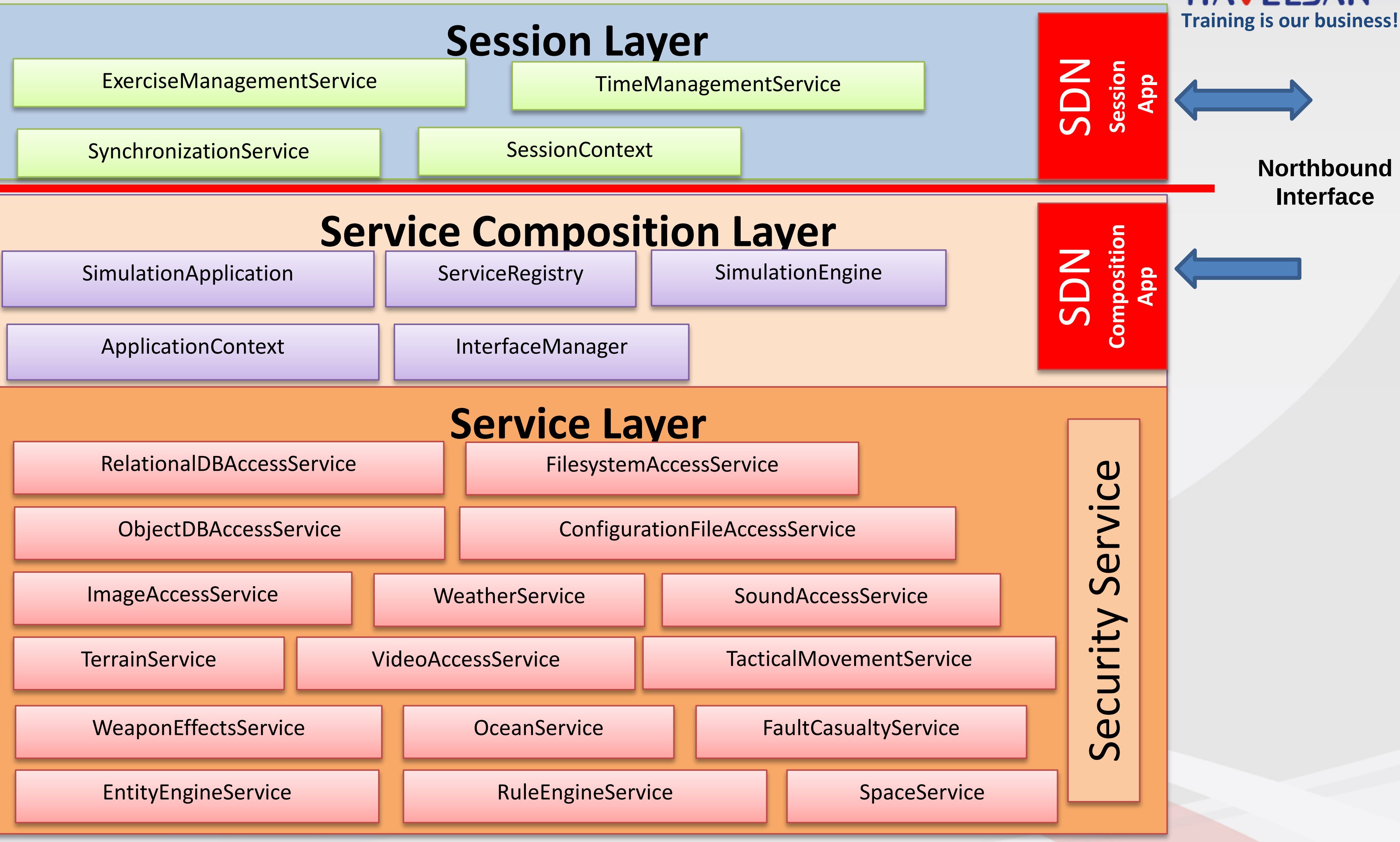
Cayirci E., H. Karapinar and L. Ozcakir, “hTEC: A Layered Architecture for MSaaS”, I/ITSEC, December 2016.

hTEC over Armada



SDN for hTEC

HAVELSAN
Training is our business!



Session Layer

ExerciseManagementService

TimeManagementService

SynchronizationService

SessionContext

SDN Session App

Northbound Interface

Service Composition Layer

SimulationApplication

ServiceRegistry

SimulationEngine

ApplicationContext

InterfaceManager

SDN Composition App

Service Layer

RelationalDBAccessService

FilesystemAccessService

ObjectDBAccessService

ConfigurationFileAccessService

ImageAccessService

WeatherService

SoundAccessService

TerrainService

VideoAccessService

TacticalMovementService

WeaponEffectsService

OceanService

FaultCasualtyService

EntityEngineService

RuleEngineService

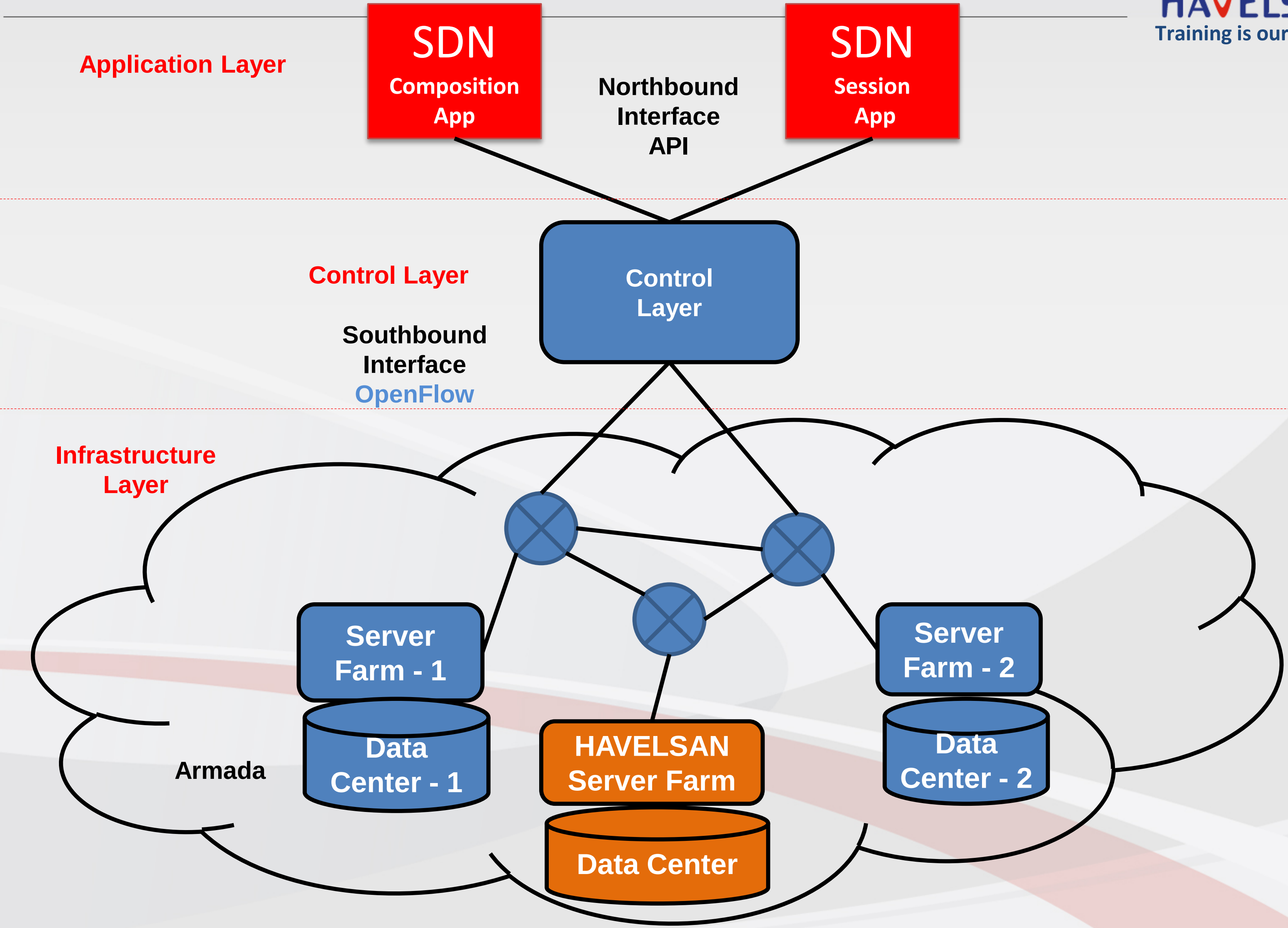
SpaceService

Security Service

Cayirci E., “Configuration Schemes for Modelling and Simulation as a Service Federations,” Simulation Transactions of the Society for Modelling and Simulation International, Vol. 89, Issue 11, pp. 1388 – 1399, November 2013.

SDN for hTEC

HAVELSAN
Training is our business!



Conclusions

- Hybrid Environments
- MSaaS for the Entire Defense Process
- hTEC: HAVELSAN's implementation of MSaaS
- Cerebellum Function
- BSigma: hTEC test bed