Modelling and Simulation for Hybrid Environments

Erdal Çayırcı
Research Center for S.T.E.A.M.
FMV Işık University
TURKEY

erdal.cayirci@isikun.edu.tr

Başar Kasım and Murat Atun
Simulation, Training and Test Systems Department
HAVELSAN, Ankara
TURKEY

bkasim@havelsan.com.tr, matun@havelsan.com.tr

ABSTRACT

NATO Modelling and Simulation Group Exploratory Team ET-043 developed a conceptual model and made a gap analysis for the modelling and simulation requirements of the hybrid environments. A hybrid strategy is based on a mix of overt and covert activities by all kinds of actors and involves the full spectrum of diplomatic, information, military, economic, financial, intelligence and legal domains. Therefore, the adaptation and integration of models from various fields, level of resolution and fidelity is required. Modelling and simulation as a service (MSaaS) introduces many advantages in fulfilling this requirement. HAVELSAN training and experimentation cloud (hTEC) is an architecture designed to maximize the advantages of MSaaS for modelling and simulating hybrid environments.

1.0 INTRODUCTION

Hybrid environments are characterized by the employment of a large set of hybrid approaches *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* [3][8][9]. Comparing to the conventional warfare, the main difference is how various strategies are mixed together to achieve a goal. A hybrid strategy involves the full Diplomatic/Political, Information, Military, Economic, Financial, Intelligence, Legal (DIMEFIL) spectrum [4]. The owner of the strategy wants to create ambiguity and to be able to deny because a hybrid strategy may not always comply with the international law and ethics, and the actors aim to meet their objectives without affecting their diplomatic and economic relations. They avoid direct and open involvement in any kinetic action. In other words, the break of a conventional war may mean the failure and the end of a hybrid strategy.

NMSG exploratory team ET-043 made a gap analysis for modelling and simulation (M&S) of hybrid environments, and developed a conceptual model to describe it. In their model, the capacity of a hybrid threat is related to the defenders' willingness to explicitly engage with the offender and the threshold up to which the defending society can tolerate the hybrid actions. The ET-43 gap analysis indicates that human and social behaviour modelling is an important part of the M&S requirements for hybrid environments, and although there are tools and techniques available to fulfil a high percentage of hybrid environment

M&S requirements, these tools and techniques need to be adapted and integrated.

M&S as a service (MSaaS) has emerged as the result of new cloud computing technologies for the last decade [5]. HAVELSAN training and experimentation cloud (hTEC) is an MSaaS architecture for training and experimentation. Our hTEC project is an opportunity to extend the military modelling and simulation support to fill the gaps described by ET-43 for hybrid environments.

In Section 2, we explain the conceptual model for hybrid environments (CMHE) developed by ET-043 [7]. In Section 3, hTEC is explained. We also elaborate on why hTEC fits the requirements for hybrid environment M&S. We conclude our paper in Section 4.

2.0 THE CONCEPTUAL MODEL FOR HYBRID ENVIRONMENTS

The top-level depiction of CMHE is in Figure 1. As it is clear in the Figure, a hybrid strategy is an offensive strategy. There are two key values related to the community/nation under attack, namely the willingness and the threshold. The willingness is the level of desire and stamina by the targeted community to engage with the offender. It also implies the support by the international community to the defendant. When the willingness is over the threshold, the targeted community approves tackling with the offender, even an armed conflict, after which the hybrid environment may become a theatre of operations unless the offender backs off. Of course, after this point, the offender's homeland may also become a theatre of operations, and hence, the conflict is not a proxy war for the offender anymore.

Therefore, the offender aims to keep the threshold as high as possible, while managing the willingness as low as possible. Vague environment, denial and all sort of perception management are the main tools for this [1] [2]. Strategic communications (STRATCOM) is a key both for the defence and the offence in hybrid environments. Apart from STRATCOM, the offender can take hybrid actions which can be denied, and may have to take also non-hybrid actions from time to time. Non-hybrid actions increase the willingness and decrease the threshold.

The defendant aims completely the opposite, i.e., decrease the threshold and increase the willingness. The main reason for this is that the capacity of the offender depends on the difference between the threshold and the willingness. For this, the defendant needs to clarify and prove what the reality is. All the components of diplomatic, informational, military, economic, law enforcement and intelligence (DIME+LI) domains should be used to achieve that. The aim is to stabilize the community/the nation under hybrid attack and to gain the international and legitimate support for eliminating the hybrid threats. Therefore, comprehensive approach and STRATCOM are the main tools for the defendant.

In Figure 1, the results of the actions are shown as "increase or decrease threshold/willingness". However, the passive case (i.e., no action is taken) has also a result which is complete opposite of the results shown in the Figure. For example, if the defendant is passive and taking no comprehensive action or does not have a proper STRATCOM narrative, the threshold increases and the willingness decreases.

As shown in Figure 1, the capacity χ of the opponent to continue with a hybrid strategy depends on the threshold τ and the willingness ω. This is given in Equation 1.

$$\chi = \tau - \omega \tag{1}$$

When $\chi \leq 0$, it is expected that the offender backs off or an armed conflict starts. The offender tries to keep the capacity χ over zero (i.e., $\chi > 0$) until completely destabilizing the targeted nation/community and creating the environment to reach its geo(political) and strategic objectives.

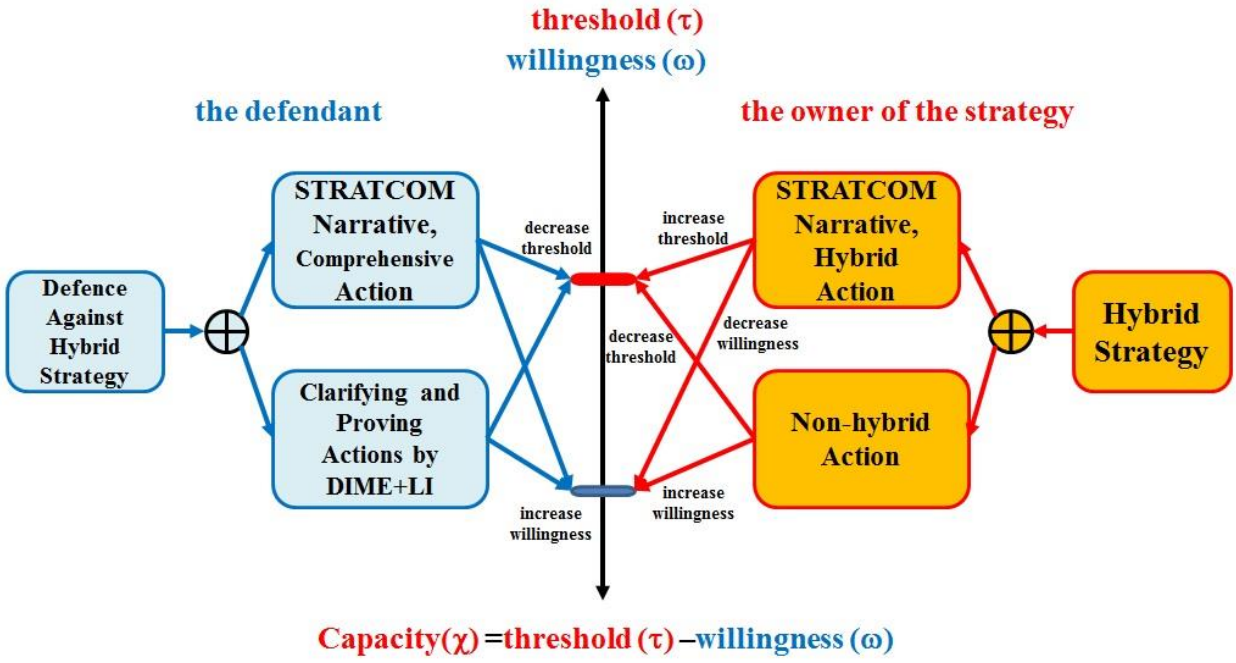

Figure 1: The top-level depiction of the conceptual model for hybrid environments.

The threshold depends on four parameters, the normalization of the current level of instability (i.e. the defendant is getting used to the situation), STRATCOM by the opponent, STRATCOM by the defendant and the power of the defendant in all DIME+LI domains (diplomatic, informational, economic, law enforcement, intelligence. Please note that STRATCOM is not only public affairs. Everything that can pass the messages according to the narrative counts. This includes not only verbal or written messages but also all actions taken. The normalization parameter depends on the history, the types of the opponent's actions and their frequencies. It may change from community to community how well and how long the history is remembered. It is also an important parameter how disturbing an action is. The frequency of actions is typically controlled by the designer of the hybrid strategy. On the other hand, the memory parameter and the degree of difficulty change from community to community, and there is an uncertainty associated with them. The other important parameters for calculating the normalization factor are ethnical and religious divisions (i.e., the number of ethnical and religious groups) and how much these divisions discriminate or tolerate (or even to support the opponent) each other.

The following parameters affect the willingness: STRATCOM by the opponent, STRATCOM by the defendant, the power of the defendant in all DIME+LI to clarify and communicate the facts, the effectiveness of the comprehensive actions by the defendant, hybrid and non-hybrid actions by the opponent. The division and discrimination parameters are also important for the willingness factor. The relations between these parameters and willingness/threshold factors are formally explained in [7].

3.0 HAVELSAN TRAINING AND EXPREMENTATION CLOUD

MSaaS [5] offers many advantages. A layered MSaaS architecture, such as HAVELSAN Training and Experimentation Cloud (hTEC) [11] can promote reusability, interoperability and flexibility. In Figure 2, the hTEC layers and their mapping to cloud service models including MSaaS are illustrated. The bottom layer in hTEC is a platform as a service layer (PaaS). In our test bed called BSigma, ARMADA, which is a HAVELSAN product, is used as PaaS. All the details related to the infrastructure and platforms are autonomously taken care by the PaaS according to the quality of service requirements specified by the

higher layers.

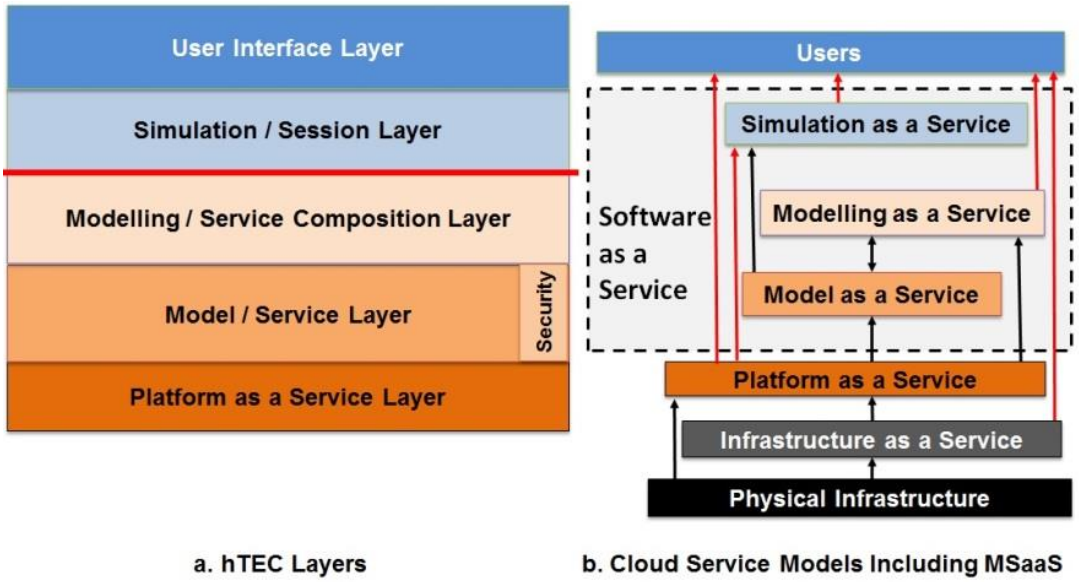

Figure 2: Mapping of hTEC Layers to Cloud Service Models including MSaaS.

The service layer runs on top of the PaaS layer. The models in this layer manage and process the data related to the synthetic environment by using the services from ARMADA. The service layer provides models as services (MaaS) [5], including database management functions. The users can manipulate the synthetic environments by using the services provided by the service layer. Please note that the security service is a sublayer within the service layer.

The service composition layer can compose a service mashup from the models provided by the service layer. It can be mapped to modelling as a service in cloud service models with a difference. Modelling as a service can be used to create new atomic or composed models [5]. In hTEC, the service composition layer is not used for creating new atomic models but models composed of the services provided by the service layer. Please note that, when service composition is complete, a composed model, or in other words a simulation application (i.e., software) is compiled. Therefore, the layers below the red line in Figure 2 are before the compilation of a simulation application, and the layers above the red line provide run time services.

The session layer in hTEC runs the models composed by the service composition. Therefore, it is equivalent to the simulation as a service model [5]. It enables users to run multiple instances of the composed services or even federating them by using various interoperability technologies such as high level architecture (HLA) [10]. Each instance runs with its own image of the synthetic environment; therefore, the master copy of the synthetic environment is preserved for the usage of the others if needed. The instance management service also provides the users with the capability to run each of these instances as different types of simulations such as time stepped, continuous, static or dynamic.

The instance service can also decide on the parts of the services that need to be run in the front end due to stringent end to end delay constraints. The part of a MaaS with stringent delay constraints is called as the cerebellum function of the service [6]. Cerebellum functions are migrated to the machines close enough to the front end (i.e., the machines that satisfy the delay constraints) by the PaaS layer.

In Figure 3, the examples for the services in each hTEC layer are illustrated. hTEC is designed as a distributed architecture. Therefore, there may be thousands of services available around the world when it

is implemented as a public cloud. The hTEC architecture can also be used in a private cloud model where hundreds of services are available.

Software defined networking (SDN) composition and session applications in Figure 3 are the hTEC services for SDN. The interfaces between the control layer and applications are called as the northbound interfaces in SDN. The SDN composition application retrieves the data about the network, such as the average delays between the nodes (i.e., hosts, switches and routers). These data are used for designing an SDN and determining the cerebellum functions and their locations. The SDN session application interacts with the SDN control layer to create and manage the designed SDN during the execution of the simulation.

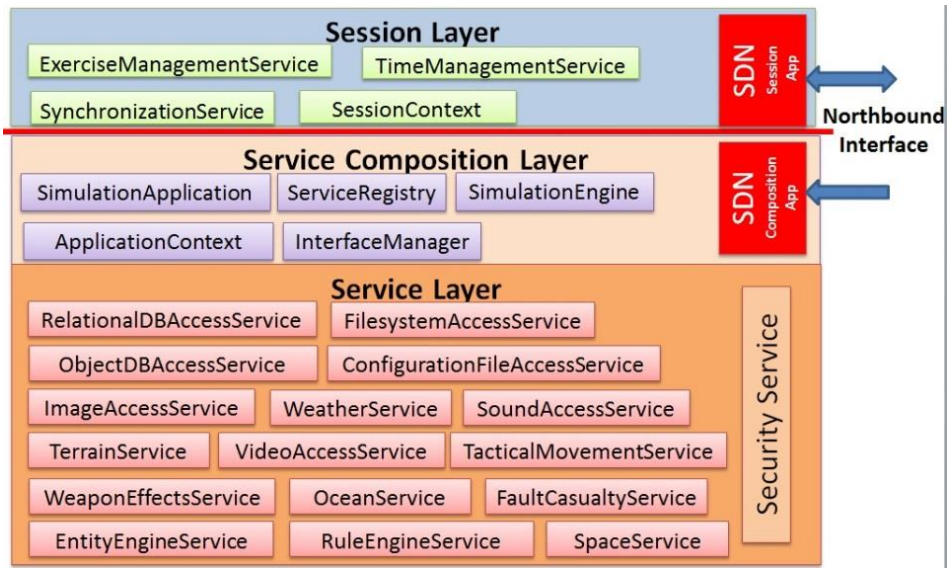

Figure 3: Examples for the Services in hTEC.

4.0 CONCLUSION

hTEC is an MSaaS architecture that improves adaptability, flexibility, reusability, and interoperability. It can provide enhanced modelling and simulating support to training and experimentation events based on hybrid scenarios. It consists of five layers: platform as a service (PaaS), model/service, modelling/service composition, simulation/session and user interface layers. A HAVELSAN product called ARMADA is used as PaaS for our implementation of hTEC. The service layer provides models and also services for database management and data security. The users can manipulate the synthetic environments by using the services provided by the service layer. The service composition layer composes a service mashup from the models provided by the service layer. The session layer in hTEC runs the models composed by the service composition. Finally, the user can run simulations by using the services from user interface layer. hTEC is being implemented and tested over a testbed called BSigma.

REFERENCES

[1] Bachmann S. and H. Gunneriusson. 2015. *Russia's Hybrid Warfare in the East: Using the Information Sphere as Integral to Hybrid Warfare*. Georgetown Journal of International Affairs - International Engagement on Cyber V: Securing Critical Infrastructure.

[2] Bachmann S. and H. Gunneriusson. 2015. *Hybrid Wars: 21st Century's New Threats to Global Peace*

and Society. Scientia Militaria - South African Journal of Military Studies.

[3] Berzinš, J. 2014. *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*. Policy Paper no 02 April, Riga: National Defense Academy of Latvia.

[4] Cayirci E. and D. Marincic. 2009. *Computer Assisted Exercises and Training: A Reference Guide*. John Wiley.

[5] Cayirci E. 2013. *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, pp. 389-400, 8-11 December 2013.

[6] Cayirci E, Karapinar H and Ozcakir L. 2015. *Cerebellum Function for MSaaS*. In Proceedings of the 27th European Modeling and Simulation Symposium (EMSS), Bergeggi, 2123 September 2015.

[7] Cayirci E, Bruzzone A, Lungo F, et al. 2016. *A model to describe hybrid conflict environments.* In Proceedings of the 13th International Multidisciplinary Modeling & Simulation Multiconference, Larnaka, 26-28 September 2016.

[8] Davis, J.R. 2014. *The Hybrid Mindset and Operationalizing Innovation: Toward a Theory of Hybrid.* School of Advanced Military Studies United States Army Command and General Staff College, AY 2014-01, Fort Leavenworth, Kansas.

[9] Hoffman, F.G. 2009a. *Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict*. Strategic Forum 240.

[10] IEEE. 2010. *1516-2010 - IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA)-- Framework and Rules*.

[11] Cayirci E, Ozcakir L and Karapinar. 2016. *hTEC: A layered MSaaS architecture for training and experimentation cloud*. In Proceedings of the 50th Interservice/Industry Training, Simulation and Education Conference (I/ITSEC), Orlando, 28 Nov-2 December 2016.