A MODEL TO DESCRIBE HYBRID CONFLICT ENVIRONMENTS

Erdal Cayirci[a], Agostino Bruzzone[b], Francesco Longo[c], Hakan Gunneriusson[d]

[a]The Research Center for S.T.E.A.M., FMV Işık University, Üniversite Sokak, Şile, İstanbul, 34980, Türkiye
[b]D.I.M.E., University of Genoa, Via Opera Pia 15, 16145 Genova, ITALY
[c]DIMEG, University of Calabria, Via P. Bucci, 45C, 87036 Rende (CS), Italy
[d]Dep of Ground Ops and Tactics, Swedish Defense University, Drottning Kristinas väg 37, 114 28 Stockholm, Sweden

[a]erdal.cayirci@isikun.edu.tr, [b]agostino@itim.unige.it, [c]f.longo@unical.it, [d]Hakan.Gunneriusson@fhs.se

ABSTRACT

This article focuses on the definition, implementation and testing of a model to describe Hybrid Conflict Environments. Without the need of citing specific cases or countries, it is clear that hybrid strategy and warfare are becoming more important. A hybrid strategy can affect policy makers, military operations, economics and financial trends, intelligence and legal activities as well as information and media. A conceptual model is introduced to define and to gain further insight into hybrid environments. The model is then implemented and tested by running experiments to provide evidence on its relevance. Finally, results are presented and discussed.

1 INTRODUCTION

Hybrid warfare is a new approach to warfare (Berzinš 2014)(Davis 2014) (Hoffman 2009a). It is described as the black version of comprehensive approach because it aims the destabilization of the targeted nation/community by exploiting it's weaknesses at the maximum extend. The most of the research in the field is for obtaining a better insight into it and hence for developing more effective techniques to counter the adversaries implementing a hybrid strategy. Hybrid warfare is also called as nonlinear warfare by some nations.

A hybrid strategy is based on a broad, complex, adaptive and often highly integrated combination of conventional and unconventional means, which include overt and covert activities by military, paramilitary, irregular and civilian actors (Berzinš 2014)(Davis 2014) (Hoffman 2009b) (Hoffman 2009c). The owner of the strategy, which is typically not known by the public, orchestrates all these means to destabilize the targeted nation or community for achieving (geo)political and strategic objectives. All the vulnerabilities are analyzed carefully and exploited at the maximum extend. A hybrid warfare is conducted across the full Diplomatic/Political, Information, Military, Economic, Financial, Intelligence, Legal (DIMEFIL) spectrum (Cayirci and Marincic 2009). Ambiguity is created, the denial is always possible especially for the creator of the strategy, and the decision making processes are overly complicated for the defendant. 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, and even maintaining economic and diplomatic relations if possible; although the use of overt military action as part of a hybrid strategy cannot be discounted.

Hybrid Warfare involves threats that can be categorized into four broad classes; traditional,

irregular, catastrophic terrorism and disruptive. Asymmetric warfare, information warfare and cyber warfare (Cayirci and Ghergherehchi 2011) (Gunneriusson and Ottis 2013) are important domains for hybrid warfare that can be fought on three battlegrounds: within the conflict zone population, home front population and the international community.

As the definition implies, hybrid warfare requires modelling and simulation in various domains, such as, conventional, cyber and information warfare (Cayirci and Ghergherehchi 2011), social and human behaviour modelling (Bruzzone et.al. 2014) both with local and international perspectives, threat networks and asymmetric warfare. Although modelling and simulation requirements for many of these fields have been studied extensively, hybrid warfare as a domain has not been addressed holistically yet. Moreover, a model that describes hybrid environments and its dynamics is not available to understand better what to tackle with. Our research, conducted as an international exploratory study titled as "Exploratory Team 043 Modelling and Simulation for Hybrid Warfare" under NATO's Science and Technology Organization, aims to fill this gap. The preliminary results from our research are reported in this paper.

In Section 2, we explain our model called the conceptual model for hybrid environments (CMHE). The dependent parameters in the model are the objectives of the owner of a hybrid strategy. We relate these objectives to a set of independent parameters in the model. In Section 3, we analyze the dynamics between the independent and dependent parameters in our model through experimentation. We conclude our paper in Section 4.

2 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 offenders 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 (Bachmann and Gunneriusson 2015) (Bachmann and Gunneriusson 2015b). 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. Of course 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.

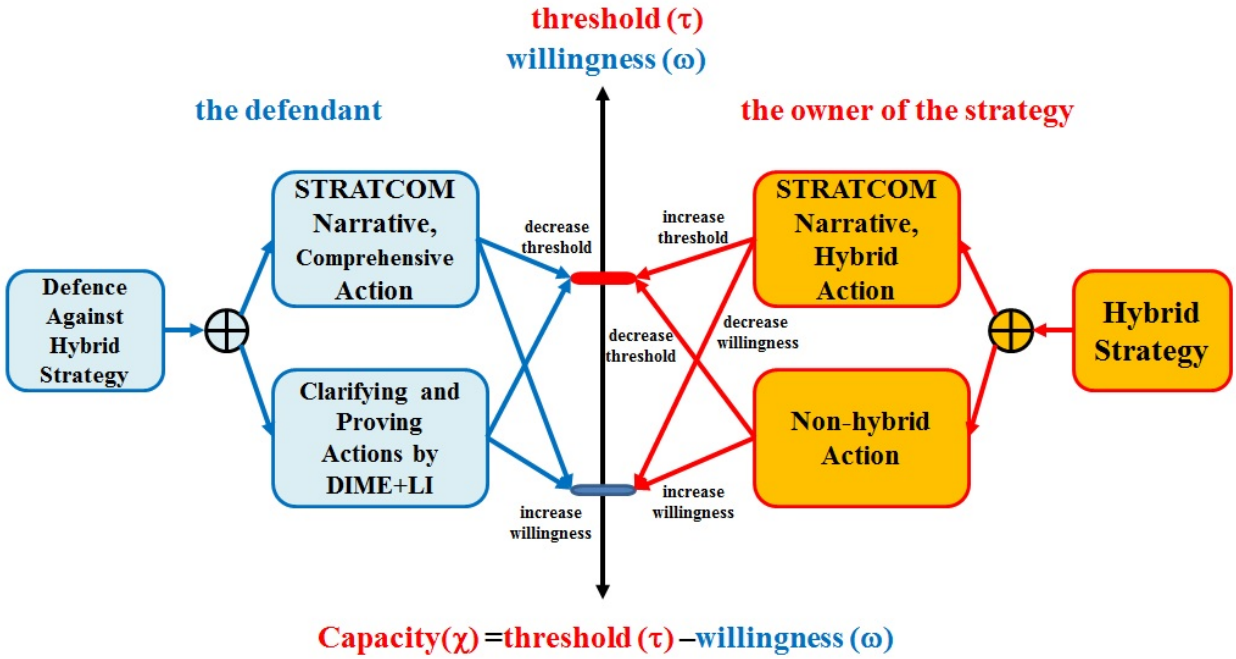

Figure 1: The top level depiction of the conceptual model for hybrid environments.

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.

2.1 Modelling the threshold for CMHE

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.

The threshold depends on four parameters, the normalization ν of the current level of instability (i.e., the defendant is getting used to the situation), STRATCOM by the opponent s_o, STRATCOM by the defendant s_d and the power p_Σ of the defendant in all DIME+LI domains p_δ (diplomatic), p_ι (informational), p_ϕ (military), p_ε (economic), p_λ (law enforcement), p_σ (intelligence) as given in Equations 2 and 3. Please note that the weight μ of each DIME+LI domains in overall power p_Σ of the defendant may be different from each other. In these equations, s_o, s_d and p_Σ are real numbers between 0 and 1 (i.e., $s_o \in \Re$, $s_d \in \Re$, $p_\Sigma \in \Re$ and $0 \leq s_o \leq 1$, $0 \leq s_d \leq 1$, $0 \leq p_\Sigma \leq 1$)

$$p_\Sigma = \mu_\delta p_\delta + \mu_\iota p_\iota + \mu_\phi p_\phi + \mu_\varepsilon p_\varepsilon + \mu_\lambda p_\lambda + \mu_\sigma p_\sigma \tag{2}$$

where $\mu_\delta + \mu_\iota + \mu_\phi + \mu_\varepsilon + \mu_\lambda + \mu_\sigma = 1$

$$\tau = (\nu s_o) - (p_\Sigma s_d) \tag{3}$$

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. Please note also that social computing is a critical media to disseminate the STRATCOM narrative by the defendant, as well as the disinformation by the opponent.

In Equation 4 and 5, the normalization parameter ν 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. We call this parameter as the memory parameter ρ. The number of events (i.e., hybrid and non-hybrid actions taken by the opponent) n in the last period i that the normalization parameter is evaluated for, and the length t_i of the time interval between the last normalization evaluation and current time give the frequency (n/t) of events. Please note that the unit (i.e., months, weeks or days) for time intervals does not make an impact on the model. However, there is at least one event in every time interval and therefore the length of time intervals is not a fixed value.

It is also an important parameter how disturbing α an action is. We call this parameter as the difficulty, which needs categorization of events in space and character. In our model, the number of categories m is not a fixed value and may change in every evaluation period i as the length of time intervals do.

The frequency (n/t) is typically controlled by the designer of the hybrid strategy. On the other hand, the memory parameter ρ and the degree of difficulty α change from community to community, and there is an uncertainty associated with them. It is not easy to treat this uncertainty in aleatory domain at least for the time being. Still we refer them as random variables, i.e., $\rho:\Omega\rightarrow\Re^{+}$ and $\alpha:\Omega\rightarrow\Re^{+}$, where $R_\rho(\Omega, \Im_\rho, P_\rho)$ and $R_\alpha(\Omega, \Im_\alpha, P_\alpha)$ are the related random processes, Ω is the set of positive real numbers between 0 and 1 and including 0 and 1 (i.e., $0 \leq \Omega \leq 1$), $\Im_\rho$ is the set of values for how much the past influences the perception about the current situation (i.e., the weight of the past on the current perception), $\Im_\alpha$ is the set of values for how difficult to normalize an event, P_ρ and P_α are the probability density functions and statistics that fits best to the defendant.

The other important parameters for calculating the normalization factor ν are ethnical and religious divisions d (i.e., the number of ethnical and religious groups) and how much these divisions discriminate or tolerate (or even to support the opponent) h each other. The division parameter d is a positive integer greater or equal to one (i.e., $d \in Z$ and $d \geq 1$). The discrimination parameter h is a real number greater than zero and less than or equal to two ($h \in \Re$ and $0<h\leq 2$).

$$v = \sqrt[d^h]{\prod_{c=1}^{m_i}\left(\prod_{k=1}^{n}(1-R_{ck\alpha})\right)^{t_i/n}} \tag{4}$$

$$v_i = \frac{R_\rho}{t}v_{i-1} + \left(1-\frac{R_\rho}{t}\right)v \tag{5}$$

Please note that there is at least one event in each category c (i.e., for $\forall$c, $m_i \geq 1$). Otherwise the category does not exist. Therefore, ν is a real numbers between 0 and 1 (i.e., $\nu \in \Re$ and $0\leq\nu\leq 1$).

2.2 Modelling the Willingness for CMHE

The following parameters affect the willingness: STRATCOM by the opponent s_o, STRATCOM by the defendant s_d, the power p_Σ of the defendant in all DIME+LI to clarify and communicate the facts, the effectiveness of the comprehensive actions a_d by the defendant, hybrid a_{on} and non-hybrid a_{ol} actions by the opponent as shown in Equations 6-8, where a_d, a_{ol} and a_{on} are real numbers between 0 and 1 (i.e., $a_d \in \Re$, $a_{ol} \in \Re$, $a_{on} \in \Re$ and $0\leq a_d \leq 1$, $0\leq a_{ol} \leq 1$, $0\leq a_{on} \leq 1$). The division d and discrimination h parameters already explained in the previous subsection. A part n_l of the number of events n are non hybrid, and the other part n_n are hybrid actions. Therefore, $n=n_l+n_n$.

$$a_i = \prod_{c=1}^{m_i}\left(\prod_{k=1}^{n_l}(a_{ol})_{ck}^{\,1/1+(a_d)_{ck}}\right)^{t_i/n} \tag{6}$$

$$a_r = \prod_{c=1}^{m_i}\left(\prod_{k=1}^{n_n}(a_{on})_{ck}^{\,1+(a_d)_{ck}}\right)^{n/t_i} \tag{7}$$

$$\omega = \frac{p_{\Sigma}\, s_d\, a_i - (1 - p_{\Sigma})\, s_o\, a_r}{d^h} \qquad (8)$$

Since a_d, a_{ol} and a_{on} are real numbers between 0 and 1, the willingness ω is also a real value between 0 and 1, and therefore the capacity χ from Equation 1 will be a real value between -2 and 2 (i.e., $\chi \in \Re$, and $-2 \leq \chi \leq 2$).

3 EXPERIMENTAL RESULTS

Through Monte Carlo Simulation, we experiment with our model and observe how it behaves as we change the independent parameters. In our experiments, random numbers are generated for the memory parameter ρ and the degree of difficulty α according to normal distribution with various mean values. The sensitivity of the threshold τ, the willingness ω and the capacity χ against the changes in the other parameters of the CMHE is examined. The preliminary results from our experiments are provided and analysed in this section.

In Figure 2, the sensitivity against the changes in frequency (n/t) of the actions by the opponent is depicted. The values assigned to the other parameters during these tests are given in the caption of Figure 2. As expected, the community gets used to the hybrid environment as the frequency of events increase, and therefore the threshold increases, which also means better capacity for the opponent. As the frequency gets higher, its effect on the threshold gets lower. The sensitivity of the willingness is less against the frequency comparing to the threshold.

In Figures 3 and 4, the relations between the capacity and STRATCOM are shown. Both the threshold and the willingness are affected by the effectiveness of the STRATCOM by the defendant. Better defendant STRATCOM results in an increase in the willingness and a decrease in the threshold and the capacity. An opposite relation is observed between the threshold and the STRATCOM by the opponent as expected. There is another difference between the effects of STRATCOM by the opponent and the defendant, which is the sensitivity of the willingness against the changes in STRATCOM by the opponent is much less comparing to the STRATCOM by the defendant.

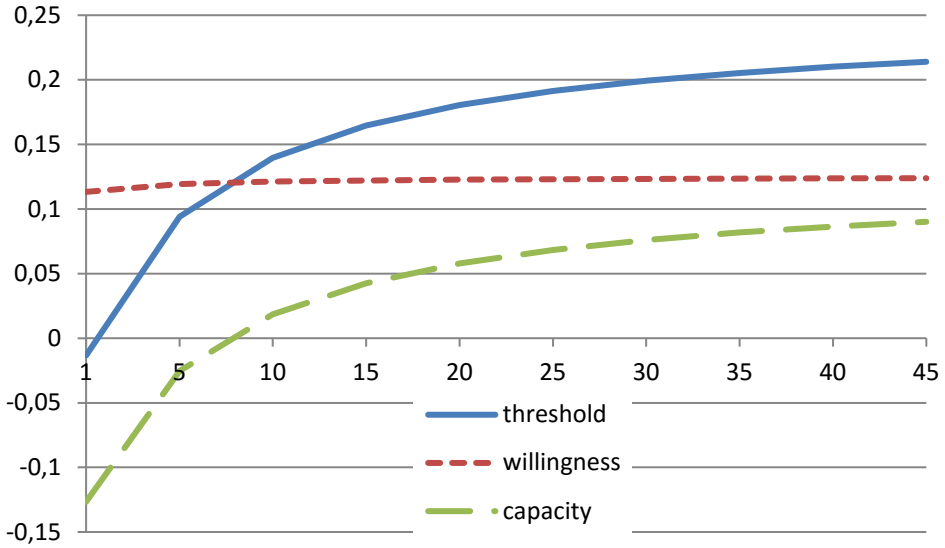

Figure 2: The sensitivity against frequency (n/t) when α=0.5, P_{Σ}=0.5, s_o=0.5, s_d=0.5, a_d=0.5, a_{ol}=0.5, a_{on}=0.5, d=2, h=1.

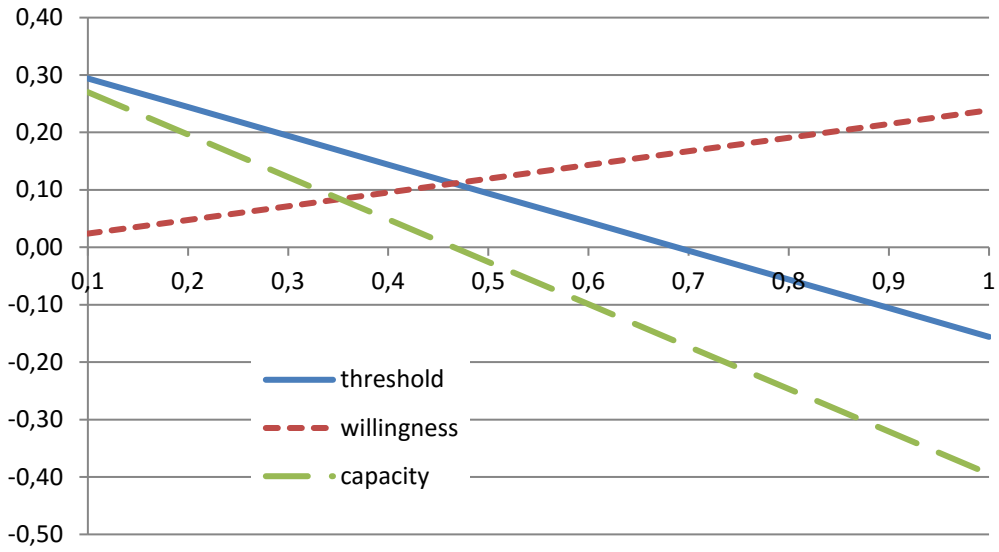

Figure 3: The sensitivity against STRATCOM by the defendant (s_d) when $\alpha=0.5$, $P_\Sigma=0.5$, $n/t=10$, $s_o=0.5$, $a_d=0.5$, $a_{ol}=0.5$, $a_{on}=0.5$, $d=2$, $h=1$.

In Figure 5, the results from the tests for the discrimination parameter h are illustrated. How much the divisions in a community discriminate each other is an important weakness that can be exploited easily by the opponent. This is clearly observable in Figure 5. When the discrimination is higher, the willingness of the community to tackle with the opponent is lower. On the other hand, the higher the discrimination is, the higher the threshold and the higher the capacity of the opponent become.

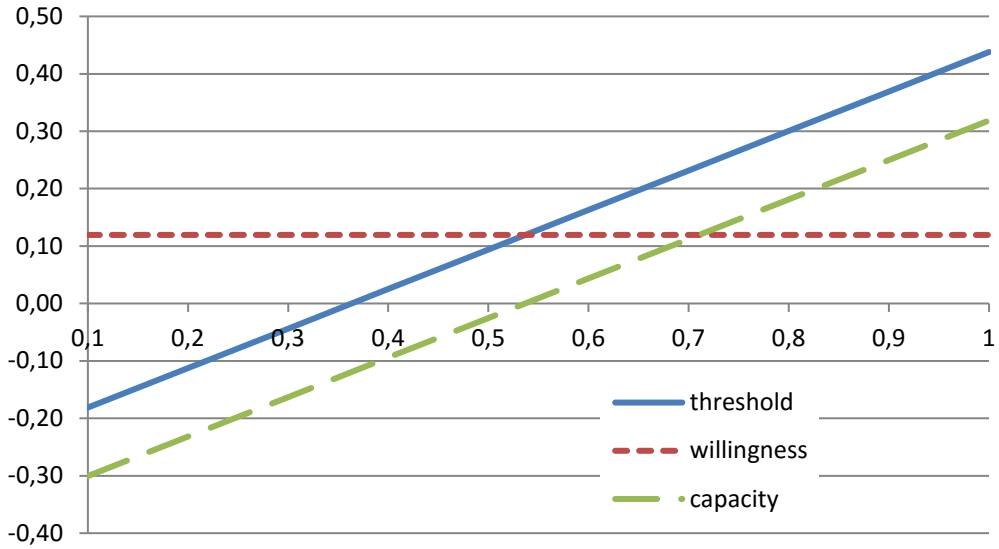

Figure 4: The sensitivity against STRATCOM by the opponent (s_o) when $\alpha=0.5$, $P_\Sigma=0.5$, $n/t=10$, $s_d=0.5$, $a_d=0.5$, $a_{ol}=0.5$, $a_{on}=0.5$, $d=2$, $h=1$.

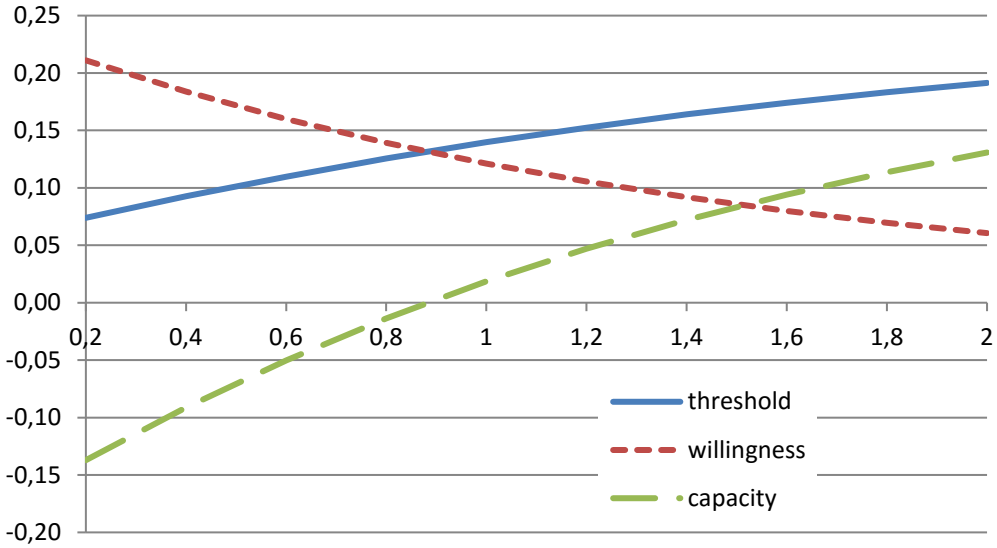

Figure 5: The sensitivity against discrimination (h) when $\alpha=0.5$, $P_{\Sigma}=0.5$, $n/t=15$, $s_o=0.5$, $s_d=0.5$, $a_d=0.5$, $a_{ol}=0.5$, $a_{on}=0.5$, $d=2$.

As shown in Figure 6, as the actions by the opponent gets more difficult (i.e., more disturbing) for the defendant, the threshold decreases, because those events are more difficult to be normalized (i.e., more difficult to get used to). The willingness of the community changes in positive direction but much less comparing to the threshold.

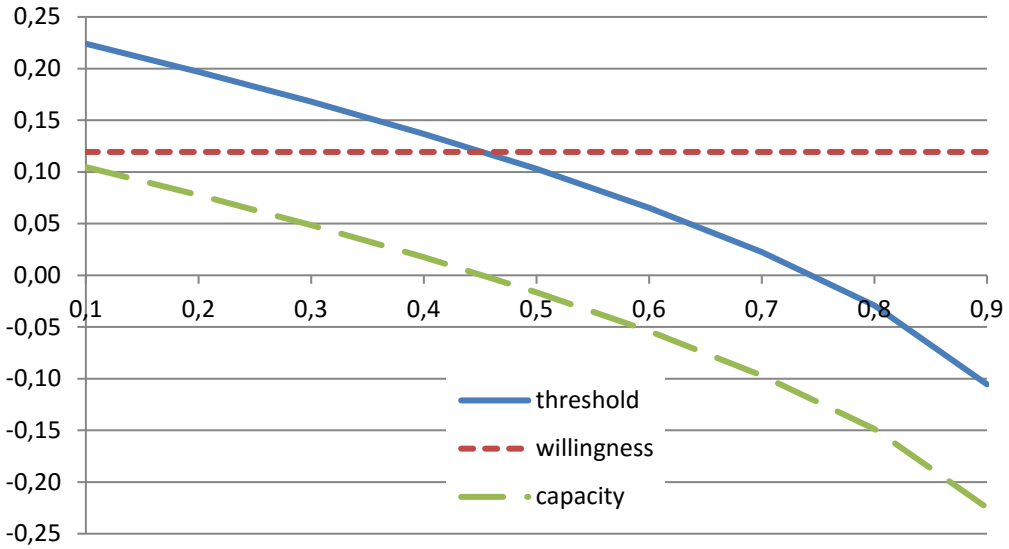

Figure 6: The sensitivity against the difficulty (α) of the opponent actions when $P_{\Sigma}=0.5$, $n/t=10$, $s_o=0.5$, $s_d=0.5$, $a_d=0.5$, $a_{ol}=0.5$, $a_{on}=0.5$, $d=2$, $h=1$.

Our final experiment is about the effectiveness of the comprehensive actions by the defendant. They do not change the threshold but the willingness, which gets better as the comprehensive actions by the defendant becomes more effective. However, the effectiveness of the comprehensive actions is not much if they are not supported by a consistent STRATCOM narrative.

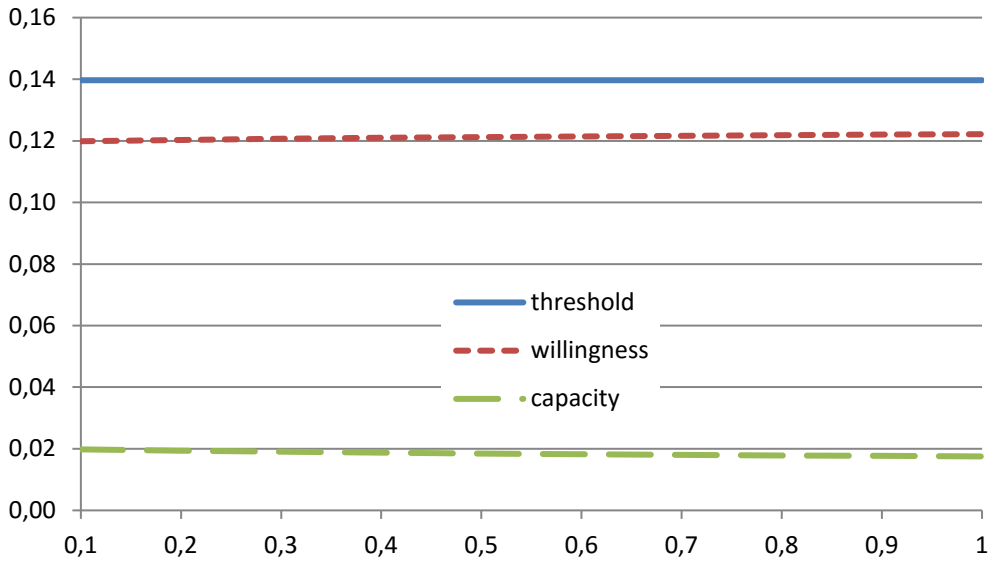

Figure 7: The sensitivity against comprehensive actions (a_d) of the opponent actions when $\alpha=0.5$, $P_\Sigma=0.5$, $n/t=10$, $s_o=0.5$, $s_d=0.5$, $a_{ol}=0.5$, $a_{on}=0.5$, $d=2$, $h=1$.

4 CONCLUSIONS

In a hybrid warfare, the adversary uses all available means, very often from the black side, to exploit the vulnerabilities of the defendant and to destabilize it. Creating ambiguity, the denial and disabling the defendant in decision making are aimed in every action. The adversary tries to meet its objectives without an armed conflict even without a major change in its diplomatic and economic relations. It manages two parameters related to the defendant, namely the threshold and the willingness. It tries to keep the willingness of the defendant to clarify the adversary's intention and to engage in an armed conflict at the minimum possible level. The willingness also strongly related to the international community's desire to support the defendant. When the willingness is over the threshold, the hybrid warfare is over one way or the other, i.e., either the adversary backs off or has to face an armed conflict with the defendant supported by the international community. Therefore, the adversary does it's best to raise the threshold as much as possible without losing the control on the willingness.

In this paper, we introduce the CMHE that captures all these relations. The CMHE is developed within the NATO exploratory study called ET-043. We also run experiments with the CMHE. The preliminary results are consistent with the theory about the hybrid environments.

REFERENCES

Bachmann S. and H. Gunneriusson. 2015a. *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.

Bachmann S. and H. Gunneriusson. 2015b. *Hybrid Wars: 21st Century's New Threats to Global Peace and Society*. Scientia Militaria - South African Journal of Military Studies.

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.

Bruzzone, A., M. Massei, F. Longo, S. Poggi, M. Agresta, C. Bartolucci, L. Nicoletti 2014. *Human behavior simulation for complex scenarios based on intelligent agents.* Proceedings of the 2014 Annual Simulation Symposium, Article 10.

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

Cayirci E. and R. Ghergherehchi 2011. *Modelling Cyber Attacks and Their Effects on Decision Process*, Winter Simulation Conference 11, December .

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.

Gunneriusson H. and R. Ottis 2013. *Cyberspace from the Hybrid Threat Perspective*. The Journal of Information Warfare. Volume 12, Issue 3.

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

Hoffman, F.G. 2009b. *Hybrid Warfare and Challenges.* Joint Forces Quarterly , 52, 1. Q.

Hoffman, F.G. 2009c. *Hybrid vs. Compound War: The Janus Choice of Modern War: Defining Today´s Multifaceted Conflict*. Armed Forces Journal (Oct.), 1-2.

AUTHOR BIOGRAPHIES

ERDAL CAYIRCI is Professor of Computer Engineering at Isik University. He is also the Director of S.T.E.A.M. Research Center. He holds M.S. and Ph.D. degrees in Computer Engineering from Middle East Technical University and Bogazici University, respectively.

AGOSTINO G. BRUZZONE is Full Professor of at the University of Genoa. He is President of Simulation Team, Director of the International Master Program MIPET, member of the BoD of the Society for Modeling and Simulation International, Director of M&S Net, Senior Lecturer within the PhD program on Modeling&Simulation. He also served as M&S Responsible in NATO STO CMRE, Director of the McLeod Institute of Simulation Science, Vice-President of the Board of MIMOS (Movimento Italiano di Simulazione) He was involved in research projects in cooperation among EDA, Italian and French MoD, NATO M&S CoE. He has published over 200 journal and conference papers.

FRANCESCO LONGO is Assistant Professor at University of Calabria and Director of the Modeling & Simulation Center – Laboratory of Enterprise Solutions (MSC-LES). He holds a PhD in Mechanical Engineering with a special focuses on Modeling & Simulation of complex systems. He has served as Principal Investigator in different research projects and he is actively involved in the organization of the most important Modeling & Simulation international conferences (e.g. EMSS, I3M).

HÅKAN GUNNERIUSSON is the Head of Research of ground operations and tactical areas in the Department of Military Studies at Swedish Defense University, focusing on hybrid warfare, military ground tactics, as well as sociological and historical perspectives on military tactics and culture.