Information & Security: An International Journal

Vassileva & Zwilling, v.39:3, 2018, 220-234 https://doi.org/10.11610/isij.3919

HYBRID WARFARE SIMULATION-BASED LEARNING: CHALLENGES AND OPPORTUNITIES

Bistra VASSILEVA and Moti ZWILLING

Abstract: In the past few years, the body of knowledge on hybrid warfare grew considerably, as did its importance both in practice and in academia. This article provides a current overview of the existing body of the literature in the field of simulation-based learning and the hybrid warfare issues of key importance. The authors present here an original framework related to simulation-based learning environment which provides students or trainees the opportunity to acquire knowledge and skills to deal with different situations in hybrid warfare impacting both the private and the public sector. Research questions driving this study are as follows: First, to identify key topics of hybrid warfare which should be taken as mandatory topics during the training sessions; second, to evaluate the possibilities to apply simulation-based learning to hybrid warfare issues, and, third, to propose a methodological framework of simulation-based learning environment about key hybrid warfare topics and related technological issues.

Keywords: hybrid warfare, simulation-based learning, applied competences, cyber security.

1. Hybrid Warfare as a Learn-changer

Two of the most notable characteristics of 21st century world are discontinuity and complexity. Continuous change is characterized by unstable economic conditions, rapidly changing technologies, global competition, workforce diversity, and new organizational structures. We live in a world of shrinking boundaries and shifting economic fortunes.[1] Disruptive technologies, rapid structural changes and economic turbulence are impacting the global economy by accelerating the rise of complexity. Complexity becomes a new norm in contemporary world which requires a new perspective both from theoretical and applied point of view. The exponential change (irrespective of the level) generally creates significant chaos which frequently becomes the progenitor of conflict.[2] From the point of view of nonlinear dynamics, our traditional way of thinking about international relations, international conflicts and even about learning reached a bifurcation point – a turning point, where a minor fluctuation in any part of the system can cause a radical change in the system's direction.

Hybrid warfare as a relatively new phenomenon challenges our mind-sets and teaching-learning approaches.[1] It certainly could be defined as a learn-changer.

1.1. The Concept and the Challenges of Hybrid Warfare

According to the U.S. Capstone Concept for Joint Operations "… future conflicts will appear as hybrids comprising diverse, dynamic, and simultaneous combinations of organizations, technologies, and techniques that defy categorization."[3] The most popular definitions of hybrid war tend to emphasize the blending of regular and irregular approaches to warfare in novel and unexpected ways. Hybrid warfare is the visible part of a complex phenomenon (i.e. the top of the iceberg) while hybrid conflicts and hybrid threats which trigger the warfare are hidden below the surface. Hybrid treats are 'hybrid' in two aspects. First, the actors involved comprise a combination of state and non-state entities. Second, a diverse mix of conventional, irregular, terrorism and criminal [2] means or activities are used in the operational battlespace. In hybrid wars, these means are emerging into the same force in the same time and in the same battlespace.

Hoffman proposes that the evolving character of conflict that we currently face is best characterized by convergence in several aspects:[4] (1) physical and psychological, (2) kinetic and non-kinetic, (3) combatants and non-combatants, (4) military force and interagency community, and (5) state and non-state actors. Philp and Martin suggest another important aspect called temporal convergence when "… the human perception of events in time, and the time-depreciating-value of knowledge in the face of opposition and uncertainty, may map onto a future goal-state."[5] Contemporary conflicts differ substantially from past conflicts in terms of frequency (time) and character. The predominant notion features future conflicts as multi-modal or multi-variant rather than a simple black or white characterization of one form of warfare.

The increase in information technology and information data had recently provided an incentive to many firms to invest in cyber technology, in order to be prepared to the future hybrid warfare. As stated, the explosion of information had produced many challenges to military commanders, industry and academic researchers. One of the main challenges is the need to train both military organizations as well as industries to be able to plan and react to cyber-attacks before they occur, especially the so called "zero day" attacks. Such preparations require the organization to map its assets, and in addition to develop a strategy how to transfer, store, recognize and filter data

---

1 Some authors argue that during the history, many wars have had both regular and irregular components, but these components occurred in different stages, theatres or formations. See for example Anton, "Hybrid Pedagogies for Hybrid War."

2 Hoffman (2009: 35) defines the threats as traditional, irregular, terrorist, and disruptive.

which is presumed as malware in real time attacks. In military, most of these attacks as published are defined as NCW (network centric warfare).

The way in which organizations are planning to prepare for a hybrid warfare which is supported by internet infrastructure, had led many decision makers to think that technology is not sufficient to assist organizations to handle cyber-attacks; they rather need to invest time in developing concepts which would help all operations that are triggered by decision makers, computers agents, or initiated in response to physical weapons or attacks on infrastructure.

One of the main challenges is to build a conceptual view of the NCW, while viewing the assets network as a network of many processes, which could be handled and monitored through a SOC (Security Operations Centre). According to this concept, the CSO (Chief Security Officers) should manage the SOC, while handling in "real time" many events such as: to monitor and block intruders to exploit security breaches and penetrate the perimeter network of the organization. Phister and Plonish had already shown in their study that many military organizations around the world had already built warfare applications to handle "real-time" combats and evaluate the different scenarios.[6] Such a concept, which was demonstrated by the authors already in 2004, had developed and became more sophisticated in the recent years while influencing organizations by building concepts and tools to defend themselves from cyber-attacks. These tools are evaluated from the concept of performance and cost.

Further, according to Phister and Plonish "commercial technologies are more computationally based, while military applications are based more on supporting courses of actions." [6] Moreover, as the amount of data and technology in organizations increases, the demand to evaluate data that is resourced from many devices increases as well. This phenomenon will also influence the aspects of software framework and architecture or infrastructure that is intended to support and enable integration of many components fused to one control and monitor central system.

1.2. 'Hybrid' Teaching Methodologies for Hybrid Warfare

As it was mentioned above due to the influence of hybrid warfare new educational approaches are needed. There is increasing consensus [2,7,8] that traditional educational system which is based on conformity and compliance should be transformed by the implementation of creative pedagogical approaches to develop innovative thinking and to stimulate strategic thought. Beyond knowledge and skills training, the learning process should emphasise the following: (1) developing a mindset which is global; (2) working through a model of cross-cultural reconcilement; and (3) emphasising "relational" skills.

Facing the challenges of hybrid warfare, a combined methodology of training and education should be applied, and it should be able to: (1) develop cognitive skills; (2) provide situational knowledge; (3) stimulate critical thinking. Under these conditions teaching is not merely a way of "covering the curriculum" or transferring the knowledge directly from the 'expert' to the learner, but a way of encouraging initiative, creativity and responsibility for the decisions which are taken.

Research suggests that hybridity of war requests the use of both material and cognitive approaches to warfare,[9] i.e. it needs both training ("field" training to develop skills) and education (to generate knowledge). The educational requirement is far more about teaching students "how to think" (process) than "what to think" (objects). One of the key skills needed to counteract hybrid war is the spirit of adaptability.[3] In a situation of asymmetrical environment students should be "trained for certainty and educated for uncertainty." Students must do more than just listen: they must read, write, discuss, or be engaged in solving problems.[10] Further, students must be engaged in such higher-order thinking tasks as analysis, synthesis, and evaluation; they have to be actively involved. Thus, strategies promoting activities that involve students in doing things and thinking about what they are doing may be called active learning. Performing these activities, especially in a team environment, forces students to take responsibility for their decisions.

Simulation-based learning is a form of active and experience-based learning (or experiential learning). Its distinguishing feature is that the experience of the learner occupies central place in all considerations of teaching and learning. This experience may comprise earlier events in the life of the learner, current life events, or those arising from the learner's participation in activities implemented by teachers and facilitators. A key element of simulation-based learning is that learners analyse their experience by reflecting, evaluating and reconstructing it (sometimes individually, sometimes collectively, sometimes in both ways) in order to draw meaning from it in the light of prior experience.[15]

Sadowski and Becker distinguish between the following two types of learning approaches to warfare: material and cognitive.[11] They suggest that the latter should be applied in education in the scope of hybrid warfare. The basic operating assumption of this approach is mind as the key factor in hybrid warfare. It is considered that mind through distraction, deception, deterrence, or dissuasion, disrupts the will of the adversary. Effective education in this respect should bypass material assets and focus on mental processes, emotions, feelings, perceptions, behaviours, and decisions.

---

[3] Attributed to Joseph J. Thomas, director of the Lejeune Leadership Institute, Marine Corps University.

A group of authors proposed that the beginning of the twenty-first century could be called 'The Quantum Age' – time of changing paradigms, from Newton's mechanistic laws of classical physics to the theories of chaos and quantum mechanics.[12,13] These authors suggest that new sciences provide the conceptual foundation for a new skill set for decision makers – a set of skills that can enable to view conflict from a new perspective, but also to respond to conflict in new ways. This paradigm shift affects the view point to conflicts and respectively to the skills required to deal with conflicts. During the last few years several authors are using quantum theory in their research work as a metaphor for the development of a new set of skills aimed at decision makers, called quantum skills.[2] The concept of quantum skills corresponds to the goals of simulation-based learning and will be used by the authors as a cornerstone of their methodological framework to hybrid warfare.

2. Research Methodology

The research methodology is divided into three interrelated modules: benchmarking analysis, qualitative study, and quantitative study. Present paper presents the first two modules.

Benchmarking is an analytical management technique, which may be used to compare internal performance with the best external performance to identify strengths and weaknesses. According to Havas, it can reveal good practice that can be replicated and implemented to improve performance beyond previous levels, on a continuous basis.[14] Benchmarking is a learning tool and works best when systematically applied. Bessant and Rush reported that benchmarking involves looking at focused core processes along two key dimensions – performance and practice.[15] The performance dimension in benchmarking can provide the motivation for learning because it identifies gaps and differences in performance. But it does not tell anything about how those gaps arose. Practice benchmarking involves looking at how particular processes operate to achieve output performance. On the basis what is compared, Fageberg identified four types of benchmarking applications, namely strategic benchmarking, performance benchmarking, process benchmarking, and competence benchmarking.[16] The last one is the most recently developed type of benchmarking. Literally, a benchmark is a standard for comparison and an indicator of past success. According to Dévai, Cahill and Gallagher,[17] it is (i) a reference or measurement standard for comparison; (ii) performance measurement that is the standard of excellence for a process, and (iii) a measurable, best-in-class achievement.

As it was mentioned above, quantum skills are used as a benchmark to build the anatomy of knowledge areas in the field of hybrid warfare education.

The qualitative study comprises in-depth interviews and focus group discussions. Five lecturers and three representatives from the IT industry were interviewed using in-depth interviews. Two focus group interviews with students from the Naval Academy and the University of Economics, both in Varna, Bulgaria were conducted. The focus group interviews were videotaped. Qualitative methods were chosen to construct our methodological framework of simulation-based learning environment of counter-hybrid warfare. Two focus groups of six students each were selected to include male and female students. Age was not a factor taken into consideration when selecting the focus groups.

Three key areas were identified following the analysis of the qualitative data gathered at focus groups and in-depth interviews, namely attitudes (including awareness), behaviours, and structures/systems which are interrelated in a form of triangle.

Attitudes include the actors' perceptions and misperceptions of each other and of themselves. These can be positive or negative, but in violent conflict actors or parties tend to develop positive and negative misperceptions also known as "enemy imaging."

Behaviours can include cooperation or coercion, gestures signifying conciliation or hostility. Violent conflict behaviour is characterised by threats, coercion and destructive attacks. Co-operative behaviours could include: recognition of rights of the opponent, recognition of the existence of the opponent, recognition of the right of a people to live in peace and security, etc.

Structures/ systems refer to the political, economic, societal, etc. mechanisms, processes and institutions that influence the distribution and satisfaction of basic needs and interests of people, which include physical and military security, economic security, societal security and ecological security.

3. Methodological Framework of Simulation-based Learning Environment Countering Hybrid Warfare

3.1. 'Hybrid' Teaching Methodologies for Hybrid Warfare. Anatomy of Knowledge Areas

Quantum skills concept is used as a benchmark to specify the knowledge areas which are applicable to hybrid warfare education *(SIM4hWarfare).* A summary of these areas is provided in Table 1.

Table 1: Quantum skills in hybrid war learning methodologies

Quantum skills	Provided ability	Core characteristics	Applicability to hybrid pedagogies to hybrid warfare
Quantum seeing	The ability to see intentionally	The underlying assumption: beliefs reinforce perceptions and perceptions reinforce beliefs This ability enables managers to consciously select their intentions. The competent person possessing this skill can model the ability to identify and test assumptions and beliefs.	To develop capacity to observe and analyse the gaps between objective vs perceived reality expectations and beliefs (intentions) which lead to conflict Teaching tools: ▪ Appreciative Inquiry (AI) ▪ "Two-column" technique [18] ▪ "Ladder of assumptions"[19]
Quantum thinking	The ability to think paradoxically	The opposite of logical, linear, black and white thinking skills (so called binary thinking). It is grounded in capacity to find a fully acceptable solution to divergent points of view.	To identify and analyse perceived paradoxes, especially socially constructed polarities. To learn to see beyond the paradox and find win/win solutions. Teaching tools should stimulate the right hemisphere of the brain with a focus on visual images instead of verbal language and logic, i.e. to train the process of imagistic thinking.
Quantum feeling	The ability to feel vitally alive	Higher levels of energy and vitality could be maintained simply by choosing to focus on the positive aspects of experiences.[20] Seeing "negative" events from a positive perspective does require one to think paradoxically	This skill will have an enormous impact on issues such as motivation, burnout, stress, and job satisfaction. Teaching tools: ▪ to train students to be able to choose between every external stimulus and subsequent internal response ▪ to focus on the positive aspects of all events [20]

Quantum knowing	The ability to know intuitively	Quantum knowing is the ability to connect in non-sensory ways with information in this quantum field of potentiality. Langer' research (theory of mindful decision making) suggests that gathering information does not necessarily lead to better decisions [21]	To avoid positivistic paradigm (positivistic, reductionistic, mechanistic thinking) in knowledge creation. Teaching tools which enable: ▪ developing intuitive knowing as much as rational analysis ▪ to train the skills for 'staying aware' (mindfulness) ▪ to develop internal intuition ▪ to train the process of discovering highly creative solutions to the most difficult challenges Accelerated Learning techniques could be applied
Quantum acting	The ability to act responsibly	Quantum acting is the ability to act with concern for the whole (the whole self, the whole organization, the whole society, and the whole planet). i.e. the quantum concept of interconnectivity. The quantum principle of non-separability puts a new perspective on social responsibility in decision making.	This skill can be used to design lives of impeccable actions that focus on intentions that are good for both self and for the larger system. Using the skill of quantum acting leads people to choose to make responsible choices. Responsible choice also mandates a commitment to making managerial choices ever more conscious.
Quantum trusting	The ability to trust life's process	It is derived from chaos theory. Strange attractors provide managers with visual images of a world in which structure emerges out of chaos.	To develop skills which enable managers to ride the rapids of conflict without attempting to actively manage the course of resolution. By practising this skill people become less intent on manipulating the world and more intent on simply appreciating it. This allows self-organization to occur.

Quantum being	The ability to be in relationship	This skill recognizes the relational nature of the universe.	To develop the ability to see the world through the other's eyes which is a prerequisite to win-win conflict resolution.

Source: Adapted from Darling,[12] Darling and Fogliasso,[22] Shelton,13 and Shelton.[23]

The following steps are proposed in order to elaborate the abovementioned knowledge areas:

Step 1: Analyse academic content standards.

Academic content experts should be trained to use the *SIM4hWarfare* system and related tools. There should be at least two experts in each area, given the need for discussion on applicability of specific taxonomy items.

Step 2: Identify the related academic skills required for competent performance in the occupation.

Step 3: Crosswalk the skills and knowledge=

Step 4: Develop contextual statements that bring together the academic content standards and occupational skills standards using real life examples.

As it was mentioned above, students should be "trained for certainty and educated for uncertainty." During the last few years we apply mission-based learning as a tool to develop applied competences. Mission (Figure 1) is defined as an assignment which requires a practical completion of a task or a sequence of tasks based on a certain knowledge. Missions are accompanied by clear instructions and a feedback form. The feedback form is used for validation and it serves as an assessment tool thus providing transparency and creating a competitive environment among students.

The mission-based methodology flows from the initial mission to the completion of the final mission. The methodology allows for mission re-ordering depending on desired learning outcomes.

3.2. Process Model of Simulation-based Learning Environment

The final goal of the proposed phase model of simulation-based learning environment is to create competent hybrid combatants. In the begining of the process students/ trainees should pass through so called "military" training which includes training how to read instructions (of the missions), how to follow instructions, and how to report. The process itself (Figure 2) combines knowledge development, creativity stimulation, innovativeness encouragement, and intuition.

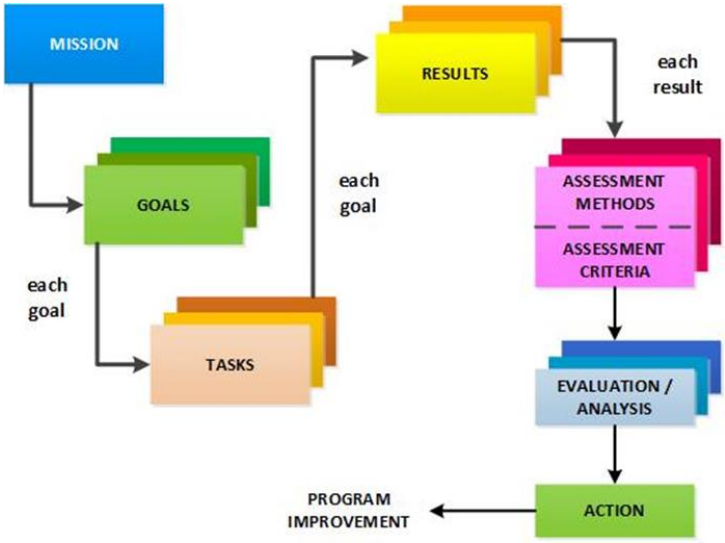

Figure 1: Mission as a core component in simulation-based learning.

The focus is placed on developing the following three groups of skills. First, cognitive skills which require capability to cope with difficulties provoked by hybrid warfare. These skills are recognized as the main human capabilities, as it requires mental agility and tolerance for ambiguity or uncertainty to recognize or quickly adapt to the unknown. Second, decision-making skills, especially to understand the true areas of disagreement (conflict) which contribute to solving the right problems and manage the true needs of the parties. Third, tactical abilities.

These skills as a background for quantum skills development could be achieved by applying the OODA (Observation – Orientation – Decision – Action) framework.[5] Observation is the means by which one collects/registers information about the state of the external world and corresponds to the key area of structures/systems. Orientation comprises the internal processes by which observations are compared with prior knowledge and experience to update an understanding of the world. It corresponds to the key area of attitudes. Decision is the internal process by which various tentative solutions are assessed and one selected for action. Action is the process by which the internally constructed solution is applied to the world. It corresponds to the key area of behaviour.

3.3. Research methodology

Based on *SIM4hWarfare* conceptual model the following research methodology is proposed (Figure 3).

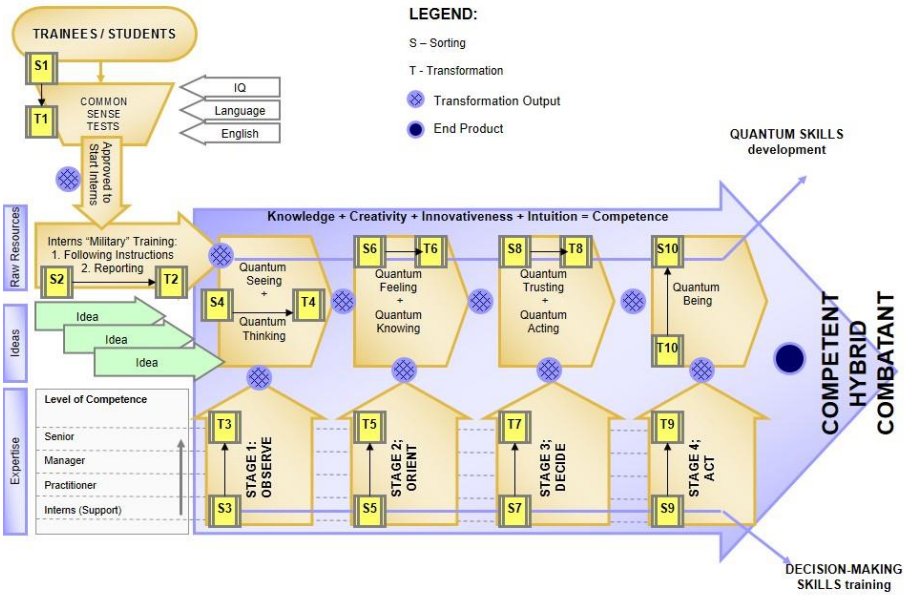

Figure 2: Conceptual model of SIM4hWarfare.

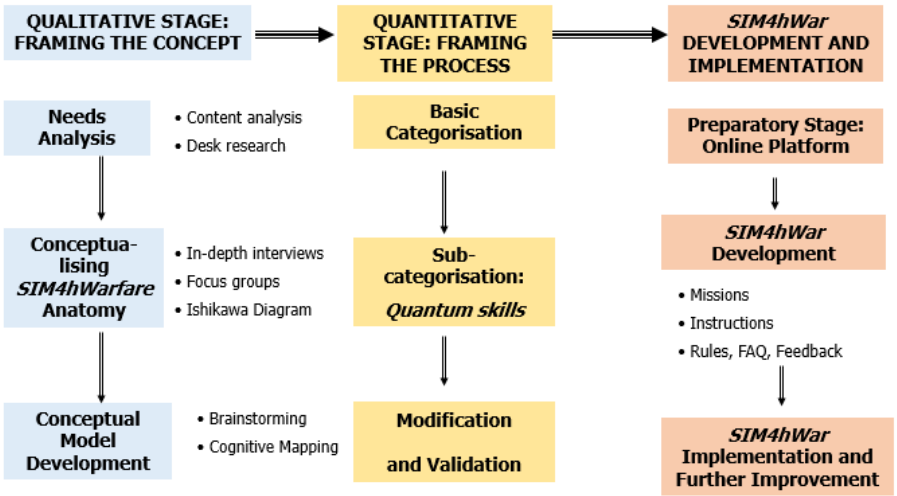

Figure 3: Research methodology.

It will be conducted as a preliminary research for "Cyber security" course as follows.

The students will be of two main categories: (1) Students and scholars from academy, and (2) Industrial and Military students. The course will be organised as follows. The first part of the course will include an introduction to cyber security as well as cyber hybrid warfare. In this section terms and definitions will compose the basic knowledge and terminology needed to the following lectures. The course will, in general, provide theory as well as recent publications and research in the field. Teaching material including papers, tools and applications will be given from existing resources which are public, free, and legitimate. The course will be based on books such as "Computer networks," "Computers Security," and "Introduction to cyber security." The second part of the course will include a deep scanning of network security based on tools and examples taken from real scenarios which industrial decision makers in organizations have had to face with. The third part of the course will involve a basic training of programming, mainly focuses on structured programming as well as object oriented (C++ and C#). The students in this section will learn how to write software code. These software code modules are aimed to suit their needs. These pieces of code are actually planned to be simple programs that can assist to evaluate and monitor malware that penetrates into an industrial network. The fourth part of the course will be dedicated to security and encryption – description facilities which are common in many industrial as well as academic institutions. This part will also incorporate exercising. The fifth part of the course will include practical sessions on existing tools and models which aim to expose the student to cope with cyber warfare and cyber-attack scenarios.

During the course, the students will be exposed to different existing tools and case studies, while answering several questionnaires (closed) that will be used to evaluate their pre-experience to cyber-attacks and new cyber technology as well as their expectations from the training sessions alongside their feeling about the contribution of the acquired knowledge which is given through the course. The questions in the survey will be built according to the following hypotheses:

RH1: "Field" training in cyber security raises students' awareness about hybrid threats and hybrid warfare specific characteristics

RH2: There is a difference in students' performance depending on the segment (academy, industrial and military)

Hypothesis will be evaluated through the usage statistics (SPSS). The hypothesis will be used to evaluate the effectiveness of the cyber training course on various students from different segments (either academy, industrial and military), who will be part of representative sample size data.

4. Conclusions and Implications for Future Research

The proposed *SIM4hWarfare* conceptual model provides an opportunity for implementation of simulation-based learning in hybrid warfare specifics. Facing the challenges of hybrid warfare, a combined methodology of training and education should be applied which should be able to: (1) develop cognitive skills; (2) provide situational knowledge; (3) stimulate critical thinking. Under these conditions teaching is not merely a way of "covering the curriculum" or transferring the knowledge directly from the 'expert' to the learner but a way of encouraging initiative, creativity and responsibility for the decisions which are taken.

When applying *SIM4hWarfare* continuously, in a systematic manner, students can gain personal experience through engaging in various activities related to hybrid warfare. The main barriers could be summarised as follows: (1) Administrative barriers due to the restrictive internal rules of the HEI; (2) Misunderstanding of the concept both from the management body of the HEI and lecturers (teachers). Such kind of activities require different type of management and high level of engagement of the teaching staff; (3) Bureaucratic procedures embedded within the educational system which prolong the process of changes and modifications of teaching materials and the process of learning; (4) Extremely low level of administrative flexibility.

Notwithstanding these challenges, the expectation is that competent hybrid combatants will gain diverse educational experiences, will be equipped with all required traditional and new skills, including or together with abilities from domain as cultural intelligence, cyber security and public diplomacy. This will require not just to modify our mindset but also to adapt fast to the changing dynamic environment at both individual and institutional level.

Bibliography

1. Ian Ryder, "Issues and Patterns in Global Branding," in *Securing the Business Benefits of Globalisation: A European Perspective*, ed. Catherine Distler and Bernard Nivollet, Part IV, Chapter 2 (Paris: Prométhée, 2005), 205-226.
2. Charlotte D. Shelton and John R. Darling, "From Chaos to Order: Exploring New Frontiers in Conflict Management," *Organization Development Journal* 22, no. 3 (2004): 22-41.
3. "Capstone Concept for Joint Operations," Version 3 (Washington, DC: Department of Defense, 2009), 1-18.
4. Frank G. Hoffman, "Hybrid Warfare and Challenges," *Joint Force Quarterly* 52 (1st Quarter, 2009): 34-48.

5. Wayne R. Philp and Christopher P. Martin, "A Philosophical Approach to Time in Military Knowledge Management," *Journal of Knowledge Management* 13, no. 1 (2009): 171–183.
6. Paul W. Phister and Igor G. Plonish, "Military Applications of Information Technologies," *Air and Space Power Journal* 18, no. 1 (Spring 2004): 77–90.
7. William Pammer and Jerri Killian, *Handbook of Conflict Management* (New York: Marcel Dekker, 2003).
8. Lee Andresen, David Boud, and Ruth Cohen, "Experience-based Learning," in *Understanding Adult Education and Training*, ed. Griff Foley, Second Edition (Sydney: Allen & Unwin, 2001), 225-239.
9. Mihail Anton, "Hybrid Pedagogies for Hybrid War," *Proceedings of Scientific Research and Education in the Air Force, AFASES 2016*, 18, no. 2 (2016), 509-516, https://doi.org/10.19062/2247-3173.2016.18.2.3.
10. Arthur W. Chickering and Zelda F. Gamson, "Seven Principles for Good Practice in Undergraduate Education," *New Directions for Teaching & Learning* 47 (1991): 63-69.
11. David Sadowski and Jeff Becker, "Beyond the "Hybrid" Threat: Asserting the Essential Unity of Warfare," *Small Wars Journal* (2018), accessed October 18, 2018, http://smallwarsjournal.com/jrnl/art/beyond-the-hybrid-threat-asserting-the-essential-unity-of-warfare.
12. John R. Darling, "Organizational Excellence and Leadership Strategies: Principles Followed by Top Multinational Executives," *Leadership and Organization Development Journal* 20, no. 6 (November 1999): 309-321, https://doi.org/10.1108/01437739910292625.
13. Charlotte Shelton, *Quantum Leaps: 7 Skills for Workplace Recreation* (Boston, MA.: Butterworth-Heinemann, 1999).
14. Attila Havas, "Intelligent Benchmarking: How to Design and Use It for Learning in Central and Eastern Europe," in *Supporting RECORD Centres of Excellence: Conclusions for Policy*, ed. Balász Borsi and Papanek Gábor (Budapest: Budapest University of Technology and Economics, 2004), 73-90.
15. John Bessant and Howard Rush, "Approaches to Benchmarking: The Case of 'Framework Conditions' and ICT-Os" (Centre for Research in Innovation Management, University of Brighton, UK, 1999).
16. Jan Fagerberg, "The Potential of Benchmarking As a Tool for Policy Learning," *IPTS Report* 9(71), (2003), 13-19.
17. Katalin Dévai, Eamon Cahill and Norbert Gallagher, "RECORD's Brighton Conference – A Summary," in *A methodology for benchmarking RTDI organisations in CEE*, eds. Katalin Dévai, Gábor Papanek, and Balász Borsi (Brighton-Budapest, 2002).
18. Chris Argyris, *Knowledge for Action: A Guide to Overcoming Barriers to Organizational Change* (San Francisco, CA: Jossey-Bass, 1993).

19. Peter Senge, *The Fifth Discipline – The Art & Practice of a Learning Organization* (New York: Doubleday, 1990).
20. Doc Lew Childre, *Cut-thru: Achieve Total Security and Maximum Energy: A Scientifically Proven Insight on How to Care Without Becoming a Victim* (Boulder Creek, CA: Planetary Publications, 1996).
21. Kathleen McCarthy, "Uncertainty is a Blessing, Not a Bane," *APA Monitor* (September 1994): 28.
22. John R. Darling and Christine E. Fogliasso, "Conflict Management in the Small Business Firm," *Journal of Contemporary Business Issues* 5, no. 1 (1997): 1-11.
23. Charlotte Shelton, "If Your Only Tool Is a Hammer," *Perspectives* 13, no. 1 (1999): 71-82.

About the Authors

Dr. Bistra VASSILEVA is Associate Professor in the "Marketing" Department of the University of Economics in Varna, Bulgaria, and deputy dean of its Management Faculty. *E-mail*: bistravas@ue-varna.bg.

Moti ZWILLING is Senior Lecturer of Business Administration in the Department of Economics and Business Administration, Ariel University, Israel. In his studies he addresses the interdependence between marketing, cyber security, big data, and machine learning.