International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:5, No:11, 2011

Infrastructure means for Adaptive Camouflage

Jiri Barta and Albert Srnik

***Abstract*—**The paper deals with the perspectives and possibilities of "smart solutions" to critical infrastructure protection. It means that common computer aided technologies are used from the perspective of new, better protection of selected infrastructure objects. The paper is focused on the co-product of the Czech Defence Research Project - ADAPTIV. This project is carrying out by the University of Defence, Faculty of Economics and Management at the Department of Civil Protection. The project creates system and technology for adaptive cybernetic camouflage of armed forces objects, armaments, vehicles and troops and of mobilization infrastructure. These adaptive camouflage system and technology will be useful for army tactic activities protection and for decoys generation also. The fourth chapter of the paper concerns the possibilities of using the introduced technology to the protection of selected civil (economically important), critical infrastructure objects. The aim of this section is to introduce the scientific capabilities and potential of the University of Defence research results and solutions for the practice.

***Keywords*—**ADAPTIV, Adaptive camouflage technology, CAMouflage, Cybernetic Active Camouflage

I. Introduction

THE risk of various extremist and terrorist actions is very serious in the present time. I believe this danger is rather underestimated due to the inclusion of the Czech Republic into the group with low terrorist attack risk [2]. Despite the above mentioned, our country middle rating regarding terrorist threats, this topic became a much discussed subject in professional community. Here, particular areas, technologies or states, that could be the next terrorist targets, are controversial and often fuzzy [6].Terrorist attacks represent the events, which are not only well planned but also very well procured with material assets by their perpetrators. To ensure the defence against these attacks on time, various instruments of security, crisis, and emergency management are used. Their basic parts consist of the activities covered by contingency and emergency planning which are based on the analysis and assessment of risks and threats. It is an expert analyse of the required goals which identifies the appropriate ways of goals achievement, and person-oriented leadership that supports the creative work and mutual collaboration [2].Our era of new global threats global economic situation asks new control/regulation behaviour of the organizations, human corporations and their Process Systems [4]. This situation indicates the priorities of never-ending crisis management, which can't use quantitative behaviour of participant and actor's entities.

J. BARTA works as a lecturer at The Department of Civil Protection of University of Defence. Kounicova 65, 662 10 Brno, Czech Republic. (e-mail: jiri.barta@unob.cz)

A. Srnik is studying a doctorate at the University of Defence, Kounicova 65, 662 10 Brno, Czech Republic. (e-mail: albert.srnik@unob.cz).

II. Problem Formulation

The question of appropriateness and of the diagnosis of required objectives has been opened in the European Union recently. Its results were published in the Directive of the European Union Council. The directive refers to the identification and designation of European Critical Infrastructure and the assessment of the needs to improve their protection [8]. The basis is to highlight the vulnerability of some critical infrastructure elements or critical infrastructure elements systems. Its disruption would have a significant impact on national security, security of basic needs of population, human health or economy of the state.

The directive deals with the concept of European Critical Infrastructure and emphasises the increased protection of critical infrastructure elements. Their disruption could have a significant impact on other member state or member states of the European Union as well [8].

Adequate response to this European Union normative act has been absent in the Czech Republic legislation for a long time. But University of Defence is in solution of this problem [4]. Czech infrastructure is ranked only marginally as a possible target of a terrorist attack. Recently, the amendment of the Law [9], that changes the way of understanding the risks of attacking the infrastructure, was published. Finally, the importance of infrastructure, especially the critical one, together with the European critical infrastructure is emphasises sufficiently and understood to be a serious threat to the state and its inhabitants from the perspective of possible terrorist attacks.

Preventive measures protect critical infrastructure elements are the most effective but they require the availability of necessary technologies, economic resources and personal qualities. In developed states, instruments for security management are used that help to ensure the high security of critical infrastructure elements.

The technology is a key factor in protecting critical infrastructure elements [1]. It is not necessary to invent and develop new technologies for the protection and security of individual subjects. It is possible, and for economic reasons often necessary, to use common technologies with a slight modifications or in a new Use Case.

These procedures create opportunities to secure the selected infrastructure objects at relatively low costs.

III. Using the Results of Science and Research

There are many universities and research institutes dealing with science and research in camouflage technologies. They toy with the question of the use of common security technologies and other security options that use the principle

of COTS (Commercial Off The Shelf) as much as possible [6]. That means the maximal utilization of commercial products and services to create a specific system or technology [3].

In this group of institutions there is the University of Defence. Its researchers are working on various scientific research projects of military and security character. The basic issue of this article is to protect the critical infrastructure. Therefore, the focus is put only on research in security for the protection of these elements.

The Department of Population Protection of the Faculty of Economics and Management at the University of Defence solves many projects within its research activities in the field of safety. One of these projects addresses the novel camouflage and simulation technique.

University of Defence operates under the auspices of the Ministry of Defence. This project focuses on the masking of selected infrastructure elements and other objects.

IV. ADAPTIV

The Camouflage is concealment [5] by means of disguise. The likely root of the word camouflage is camoufler, a French term meaning smoke blown in someone's face as a practical joke. Word origin is in Italian camuffare. The Camouflage is a method of avoidance of observation that allows an otherwise visible object (organism or structure to remain indiscernible from the surrounding environment through deception.

ADAPTIV is an acronym for project of the Defence Research which deals with the draft and assertion of new adaptive technology for simulation and camouflage in the operational environment of the armed forces of the Czech Republic and for infrastructure protection.

The primary goal of the ADAPTIV project is to create a system and technology for the adaptive cybernetic camouflage of armed forces objects, armaments, vehicles, and troops, as well as of the civil infrastructure [5].

The main purpose of camouflage is to mask an object or hide some activity. The project ADAPTIV deals with possibilities to pretend activity in places where nothing happens or show artificial objects that in fact do not exist. The possible application of this project is the imitation or simulation of security or various types of the security of selected infrastructure objects.

Last baseline of interoper-mobile wireless application for disaster events crisis and emergency management arises from CAMou*flage*™. The CAMou*flage*™ means previous baseline of University of Defence R&D´s project acronym **C**omputer **A**ided **M**obile R**o**aming **u**niversity made NET **f**or **la**st sta**ge** mile. Its functional improvement follows from innovative architecture making and dynamic modelling & simulating & crisis scenarios creation ability via the method UML,(UP)/ DYVELOP by means of its dynamic blazons development. They are enabling to serve for relevant entities (actors and domains) behaviour of disaster events driven human activities of crisis / emergency management practitioners in various environments [6].

V. DATASAM

The basis of this project is a modular system of assembled screens, which can be used independently or together to camouflage a bigger object. Bogus reality is then projected on the screen or screens.

The basic unit of the screens systems is a screen called DATAsam (Figure 1). Its material cannot be published; its composition is in secrecy regime. DATAsam overall construction and configuration is a patented process. The system consists of special screens enabling front and rear projection. These basic units can be assembled into a structure that best suits the needs of masking the infrastructure object. After assembly, he screens system is docked and ready for projection of camouflaged reality. Suitable types of camouflaged reality projection are selected by specific characteristics depending on particular use. They have to correspond to the weather conditions and the needs of masking.

Another part of the system is a freely accessible data projector. That could be bought in any shop with audio-visual equipment - according to the principle of COTS. Output quality and credibility of the projected image could be sometimes precarious. The higher image quality is required, the better projector has to be used. The basic parameter of projector quality for this type of use is its luminosity.

Fig. 1 The basic unit of a special projecting screen – DATAsam (Source: created by author)

VI. TESTING

By definition, the purpose of camouflage is to blend with surroundings and be invisible. Camouflaged object must minimise the differences between camouflage and natural background with regard to human senses, technology and the angle of observation.

During testing, it is necessary to take into account the fact that the intensity of illumination is very variable over time. This complicates the stability of projected camouflage and the projected image must be modified to the light spectrum. This confirms the variability of the system and the possibilities of its use for different types of light conditions.

The test was made at different distances and different observing angles. All the results were recorded and the restrictive conditions for using this technology in real situations were defined.The result was a test environment illustrating the real usage of the camouflage system. The results were recorded and evaluated on several levels. The first level was the visual observation and the confirmation of suitability for image masking. There has been little difference between the actual and DATAsam projected realities. The observations was performed from various distances but was limited to the size of camouflage and test space. The rule is that the camouflage is more credible from longer distance from the masked object compared to the closer one, and thus more easily to expose.On the second level of evaluation, the main task was the measurement of the comparability of light spectrum camouflage images with reality. The observations of spectral properties for anticipated masking were performed. The adaptation of the camouflage reality was compared with changes in the light spectrum over time [7].This technology has been tested on the International Fair of Defence and Security Technology – IDET too (Figure 2).

Fig. 2 DATAsam configuration at IDET fair
(Source: created by author)

Fig. 3 DATAsam configuration at Days of Science in Brno
(Source: created by author)

VII. Conclusion

The result shows that this technology is suitable for camouflage creating. It can be used in cases when the observer will not use optical instruments. It is very difficult to detect the camouflage by naked eye but when optical instruments are used the camouflage detection is highly probable. The objective of camouflage approach is that the observed object or simulated operation is detected as late as possible.

The processed evaluations show that the projection is very credible in terms of visual assessment. During comparing the images with reality, comparison of different distances was made and created images were very credible, resembling the reality. The observation was focused especially on the interface between reality and camouflage.

Evaluation by optical instruments, based on the spectrum analysis of the photographs taken by Nicon 3D camera, confirmed the reality of projected images.

The evaluation of test results showed that it is relatively easy to detect the camouflage technology using optical instruments based on laser. This type of camouflage is not appropriate for masking, when observers will have laser optical instruments. But the question remains: if observer sees nothing suspicious to the naked eye, why focus an optical instrument on the object and reveal his position?

There are many camouflage technologies operating on the basis of camouflage shield or "invisibility shields". Of course, the availability of these technologies and their prices could be prohibiting in some cases. This is the most important advantage of the above described technology. It can be used to camouflage, to simulate a variety of subjects or activities. Options of implementation will depend on the needs of individual cases and limits of technology. This technique is already known, affordable and therefore nothing prevents its using it for the protection of selected infrastructure objects.

Acknowledgment

The article was elaborated within the defence research project with the acronym ADAPTIV – The Draft and assertion of new adaptive technology for simulation and camouflage in the operational environment of the armed forces of the Czech Republic and for infrastructure protection (OVUOFEM 200,801).

References

[1] Ludík, T., Ráček, J. Process Methodology for Emergency Management. IFIP Advances *in Information and Communication Technology, Heidelberg : Springer,* 2011, 359, pp 302-309, ISSN 1868-4238. 2011.

[2] Procházková, D. a kol. (2006). *Bezpečnost a krizové řízení.* 1. vyd. Praha: Police history, 2006. 255 s. ISBN 80-86477-35-5.

[3] Urban, R., Urbánek, J.F. & Lokajová,V. Computer-Aided Dynamic Modelling of New Terrorist Threats Life Cycles, In *5th European Computing Conference (ECC '11),* WSEAS Press, 2011, Paris, France, ISBN: 978-960-474-297-4, pp 228-232.

[4] Urban, Roman & Urbánek, J.F. Computer-Aided Expert System for a Ranking of New Terrorist Threats , In *5th European Computing Conference (ECC '11),* WSEAS Press, 2011, Paris, France, ISBN: 978-960-474-297-4, pp 210-215.

[5] Urbánek, J. F. Application Modelling & Simulation of Data Flow in Disaster Events Management, In *8th Int. Conf. on Simulation, modelling and optimization, SMO '08,* Santander, Spain, WSEAS, 2008, pp 256-260. ISBN 978-960-474-007-9, ISSN 1790-2769.

[6] Urbánek, J.F., Průcha, J. A Development of Wireless Interoper-mobile Application for Outdoor Operation Management, In *8th Int. Conf. on Electronics, hardware, wireless and optical communications, EHAC '09,* Cambridge (UK) : WSEAS Press. 2009. p 57-64. ISBN 978-960-474-053-6. ISSN 1790-5117.ID 609-289, pp 57-64.

[7] Zouhdi, S., Sihvola, A., Vinogradov, A.P. (2008). *Metamaterials and Plasmonics: Fundamentals, Modelling, Applications*. New York: Springer-Verlag. 2008. 316 p. ISBN 9781402094064.

[8] Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [online]. [cit. 2011-6-6]. WWW: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:CS:PDF

[9] Law No. 240/2000 on Emergency Management and on the modification of certain codes (Crisis Code), in latter wording.