RESEARCH CONCERNING THE SECURITY IMPROVEMENT IN THE INFANTRY SHOOTING RANGE

Cristian-Emil Moldoveanu, Neculai-Daniel Zvîncu, Alexandra-Mihaela Olar-Pop, Thomas Gaden

[1]*Military Technical Academy „Ferdinand I“,Bucharest, ROMANIA, cristian.moldoveanu@mta.ro*
[2]*ECAM Strasbourg, FRANCE, thomas.gaden@ecam-strasbourg.eu*

Abstract: *By computing the useful information obtained with the internal and external ballistics, the theoretical trajectory of a bullet can be calculated. In order to get the most accurate values, preliminary knowledge is needed. So by using appropriate tools and software, a bullet's trajectory can be calculated if the correct values are provided (mass, diameter, initial angle, initial speed). Using the physical model for the trajectory and the experimental means we obtain the bullet impact and ricochet.*

Keywords: *Ricochet, impact, ballistics, accuracy*

1. Introduction

In order to compute the trajectory of the bullet, the different forces and phenomena occurring during the flight need to be assessed. The most effective way to do that is to express all the forces applied to the bullet and to establish the equations of the movement. Some hypotheses are taken in account: the bullet is studied for a short-range; the Corriolis force is neglected etc. There following forces are considered to be applied to the system: weight (G) and drag (R):

$$G = mg \tag{1}$$

$$R = \frac{1}{2}\rho V^2 S C_x \tag{2}$$

with:

- ρ, density of the air [kg/m3];
- V, speed of the bullet [m/s];
- S, cross sectional area [m²];
- C_x, drag coefficient.

Next we can establish the equations needed to study the bullet movement. We use the fundamental principle of dynamics. The following equations are obtained:

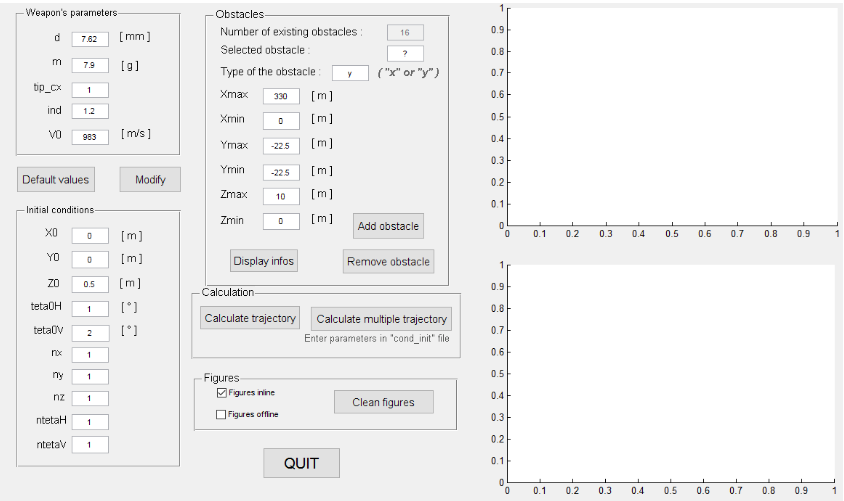
$$\begin{gathered} \frac{dV}{dt} = -\frac{1}{2}\frac{\rho}{m} V^2 S\, C_x - g\, sin\theta \\ \frac{d\theta}{dt} = -\frac{g\, cos\theta}{V} \end{gathered} \tag{3}$$

In order to obtain the bullet trajectory we use the following initial conditions:

- the initial speed V_0= 700 m/s;
- the initial angle θ_0= 5 °;
- the initial position (x_0, y_0) = (0 , 0);
- the mass m = 9 g;
- the bullet diameter d = $7.62 * 10^{-3}$ m.

2. The computational program

Using the equations presented above we set up a computational program having the aim to calculate the single or multiple trajectories (fig.1). The impact points of the trajectories are obtained by taking in account some obstacles.



Weapon's parameters
d 7.62 [mm]
m 7.9 [g]
tip_cx 1
ind 1.2
V0 983 [m/s]

Initial conditions
X0 0 [m]
Y0 0 [m]
Z0 0.5 [m]
teta0H 1 [°]
teta0V 2 [°]
nx 1
ny 1
nz 1
ntetaH 1
ntetaV 1

Obstacles
Number of existing obstacles : 16
Selected obstacle : ?
Type of the obstacle : y ("x" or "y")
Xmax 330 [m]
Xmin 0 [m]
Ymax -22.5 [m]
Ymin -22.5 [m]
Zmax 10 [m]
Zmin 0 [m]

Calculation
Enter parameters in "cond_init" file

Figures
☑ Figures inline
□ Figures offline

Figure 1. *The interface of the computational program*

In the **Weapon's parameters** section, the user can modify: the diameter of the bullet, the mass, the drag coefficient, and the initial velocity. In the **Initial conditions** section are the firing parameters: initial position (X_0, Y_0, Z_0), the horizontal and vertical angles (Vθ_{0H}, θ_{0V}), and the number of different position for each parameter ($n_X, n_Y, n_Z,\ n_{\theta H}, n_{\theta V}$).

Two other buttons were also added: the "**Default values**" button will modify the values of the two section so that they correspond to the defaults conditions of firing (d =7.62mm, m =7.9g, tip_cx =1, ind =1.2, $V_0 = 983$m/s, $X_0 = 0$m, $Y_0 = 0$m, $Z_0 = 0.5$m, θ_{0H}=0°, θ_{0V}=1°, $n_X = n_Y = n_Z = n_{\theta H} = n_{\theta V0} = 1$); the "**Modify**" button is used to save the weapon's parameters and the initial conditions before a simulation.

In the **Obstacles** section, the user can:

- see the details of every existing obstacles, by entering the number of the and then clicking on "**Display infos**". The user will access to the type of the obstacle (perpendicular to the x-axis or y-axis), and the minimum and maximum coordinates along the different axis. If the entered value is above the number of existing obstacles, the program will display the information of the last obstacle. If the entered number is null or negative, it will display the information of the first obstacle.
- create an obstacle, by entering its number, its type, and the minimum and maximum values of its coordinates and then clicking "**Add obstacle**". If the obstacle is an x-type, the $X_{\min}$ and $X_{\max}$ coordinates must be the same. If it is an y-type, $Y_{\min}$ and $Y_{\max}$must be equal. The user can either create a new obstacle by entering a number above the number of existing obstacle, or replace one by typing the number of one already existing.
- remove an obstacle, by typing the number of the obstacle and then clicking "**Remove obstacle**".

In the **Calculation** section, the user has two choices: calculate one trajectory with the initial parameters entered in the "Initial conditions" section; calculate multiple trajectories on the same figure with the parameters entered in the "cond_init" file of the program's directory.

Finally, on the **Figures** section, the user can choose where to plot the figure: in the interface, in the two already existing graphs (by choosing "Interface Figures"), or in new appearing windows (by choosing "Outside Figures"). The two different options can be chosen at the same time.

3. Numerical results

We will use the computational program presented in Fig 1 in order to calculate the two distances d_1 and d_2 of the associated obstacles, for the following type of firing range (fig. 2). The aim is to obtain a best configuration for the firing range in order to avoid the ricochet and the impact points outside the area of the firing range.

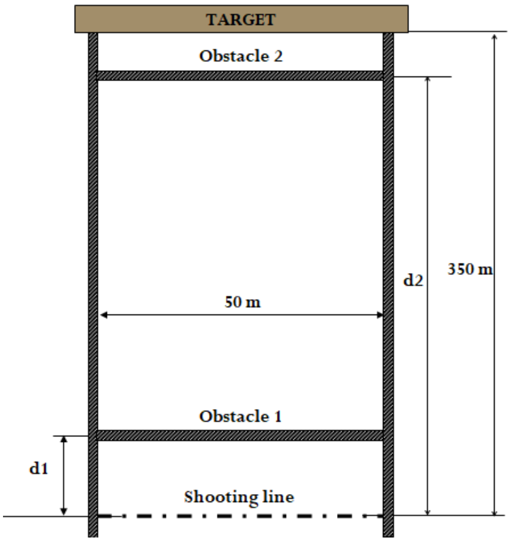


Figure 2. *The firing range configuration*

The bottom position of the obstacles is considered at 4m and the top is considered at 10m, and for the target wall the bottom is at ground level and the top at 10m.

The problem can be considered as a geometrical problem: the best disposition is made such as the first and second obstacles occupy the biggest surface possible. It also implies that, for a maximum efficiency, they need to only block specific trajectories and not trajectories that the other ones could block (fig. 3).

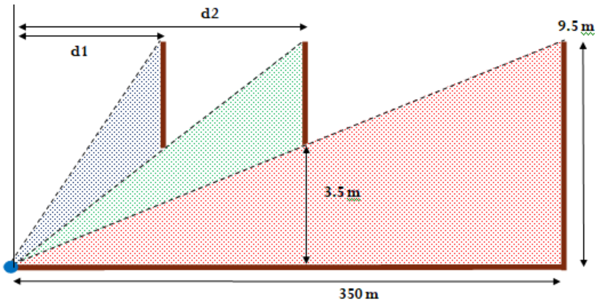


Figure 3. *The geometrical problem of the firing range configuration*

By running a simulation with the following parameters: $X_0 = Y_0 = 0m,\ Z_0 = 0.5m,\ \theta_{0H} = 0^0$, and by making , θ_{0V} from 0^0 to 11.4^0, are obtained the results presented in fig. 4.

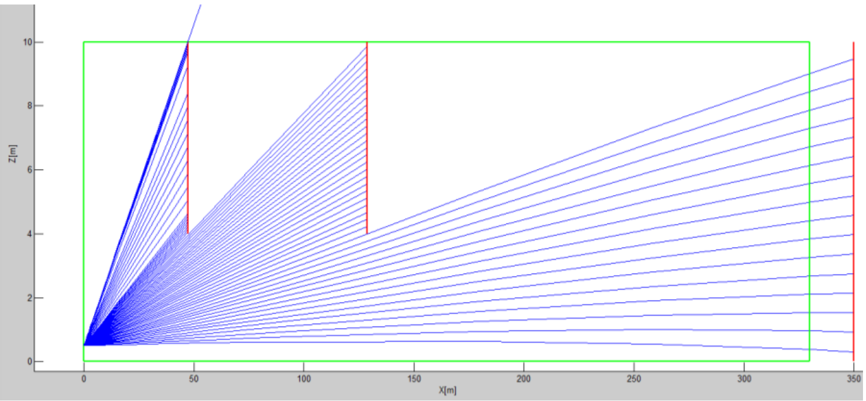


Figure 4. *The trajectories obtained for the best firing range configuration*

The set of two obstacles positions, respectively at 47.5m and 128.9m and the target wall placed at 350m, we can stop trajectories for $\theta_{0V} < 11.4°$.

4. Conclusions

In this study we ran a physical analysis conducting to a final equation system whose parameters were included in a ballistic model for computing the ricochet parameters of the bullet. Implementing it on computer program by creating a code with an interface enabled us to find an approximate solution of the system using the Runge-Kutta method. It can simulate a trajectory whose order of magnitude in terms of range and velocity is matching with real firing parameters and results. This program can calculate the impact point using the different types of obstacles.

The experiments about the ricochet velocity of a bullet highlight a few points: the initial velocity of a bullet varying from one experiment to another, while the firing conditions are the same; the angle of the target has an important influence on the bullet ricochet angle and velocity: for high incident angles, the bullet will be deflected with a lower velocity.

Acknowledgments

This work was carried out through the Project Research Concerning the Improvement of the FIRING Security in Shooting Range, 2016.

REFERENCES

1. R. Brouchu, R. Lestage, Three-Degree-of-Freedom (DOF) Missile Trajectory Simulation Model and Comparative Study with a High Fidelity 6DOF Model, DRDCVALCARTIER-TM-2003-056, Technical Memorandum, Defence R&D, Canad-Valcartier, 2003;

2. T. Sailaranta, A. Siltavuori, S. Laine, B. Fagerstrom, On Projectile Stability and Firing Acuracy, Proc. Of the 20th International Symposium on Ballistics, pp. 195-202, Orlando, Fl, 2002.

3. Moldoveanu C E , Sava A C. Şomoiag P,NistoranG D (2016) Study of the Effect of 7.62 mm Caliber Ammunition, on Concrete. Comparative Analysis between Eastern and Western Types Ammunition, *Romanian MoD Research Project*

SECURITY OF CRITICAL INFRASTRUCTURES UNDER THE EVOLUTION OF ADVANCED TECHNOLOGIES

Benedictos Iorga

Spiru Haret University, Faculty of Engineering and Computer Science, Bucharest, Romania

E-mail: iorga.ben.mi@spiruharet.ro; iorgaben@yahoo.com

***Abstract**: The transformation speed of human society in the last decade is overwhelmingly due to technological developments, based on the artificial intelligence implementation, the global expansion of the cyber environment, the IoT emergence, and last but not least, the dual-usage operationalization of systems and technologies. The technology change has a profound impact on critical infrastructures security, both through the emergence of new threats and risk levels and through the diversification and repositioning of old threats. Thus, both technology and risk diversity carry security adaptation systems for critical infrastructures protection.*

In this context, the adaptation of security systems to new innovative technologies to ensure critical infrastructure protection becomes an almost continuous measure.

The fast understanding of amplification and diversification directions of threats and risks generated by the "twisted effect" of advanced technologies and the effective implementation of new architectures and solutions to counter security vulnerabilities manifested in critical infrastructures will differentiate between the relevance and irrelevance of integrated security systems in the future.

My current research work aims to identify the advanced technology development in the spectrum of threats to critical infrastructure security and to determine potential implementable technical solutions for an effective response to new threats amplified by the disruptive technology evolution.

Keywords: *artificial intelligence, security, integrated system, risk, threat, drones, critical infrastructure*

The impact of advanced technology evolution on critical infrastructure security

Critical infrastructure comprehensively defined by US law as ”*systems and assets, whether physical or virtual, so vital (....) that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters*" **[1]** has undergone a remarkable evolution in terms of extending interdependence and interconnectivity between component systems, generated by the development in information technology.

Ever since the Roman Empire, one of the most important aims of the defense system and policies has been the protection of what we today call *"critical infrastructure (CI/CNI)"* of the old empire. Roman fortresses were relying, during the glory of the empire, on a circular, concentric security system identified today under the concept of *“defence in depth”* **[2].** Thus, any Roman fortress was defended and protected by at least 4 security (concentric) rings, which had in the epicenter the “critical Roman infrastructure” represented by the governor's house and the respective Roman power centers: senators' residences, senate, forum, “*comitia centuriata*” **[3],** etc. Regardless of the defense strategies implemented or the specific techniques, ensuring the security and protection of critical infrastructure has taken precedence over any other activity, and its basis was the specialized human staff.

In today's age, governed by digital technology, ensuring the security of a state's critical infrastructure, or on a small scale, a “smart city”, is no longer an exclusively human or technical task.

This implies a complex, hybrid activity carried out by specialized human factor and technical factor, based on a conglomeration of interconnected subsystems under the concept of *integrated security systems.* Security functions specific to critical infrastructure protection are ensured through specialized and dedicated subsystems, being mainly developed for the complementary counteraction of multi-spectrum threats such as unauthorized physical or logical access to infrastructure, unauthorized access to infrastructure-specific data and information, preservation of the functions of security systems /equipment that protects infrastructure, limiting and denying the critical infrastructure or related systems functionality, circumvention of security rules by staff operating the critical infrastructure, etc. In the context, advanced security systems dedicated to critical infrastructure protection may be defined as integrated systems specialized in ensuring the protection, security and active monitoring of infrastructure and its essential components aiming at maintaining basic functionalities, increasing resiliency level and prohibiting any destructive action on infrastructure elements, whether physical or logical.

The sizing, development and deployment of security systems dedicated to critical infrastructure protection are currently performed under complex security risk analysis, infrastructure reference industry case, and threat materialization impact in recent history, the evolution of security systems technology, depending on the experience of specialized personnel and not least on the ability of states to assimilate, develop and implement advanced protection technologies.

While in the past digital technology and security systems changes have gradually evolved linearly, the emergence of dual-use disruptive technologies such as autonomous platforms (underground, ground, air, sea drones), cyber technologies, cyber-attack/protection platforms, robotics, artificial intelligence, satellite surveillance systems and miniaturization of sensors will require exponential evolution of technical security systems dedicated to critical infrastructure protection, regardless of the area it serves.

Defining a security architecture in the new technological context shall consider a broad and innovative spectrum of threats, to the detriment of legislative, budgetary limitations or case-related impact. The main future features of dedicated security architecture and systems shall be “resiliency” and “adaptability” to advanced technology threat actions. While in the past the main threat to any critical infrastructure was *the human factor and its direct action,* the future threat will be *autonomous drone platforms (UAV/UAS, UNV, and UGV), intrusive cyber-systems and destructive-handling artificial intelligence capabilities.*

The evolution of security systems, from analogic to digital platforms, has taken around 20 years and has been driven mainly by the evolution of information technology and network environment. In our assessment, currently, the developmental state of security systems dedicated to critical infrastructure protection, although accelerated by technology, lies at the border between digital technology and artificial intelligence.

The evolution of dual disruptive technologies mentioned above will generate a major conceptual, operational and technical impact for integrated security systems, as follows:

a. *The expansion and miniaturization of autonomous civil-military dual-use drone platforms* will result in a shift of the threat spectrum to the critical infrastructure security, *now on the ground, to a multi-spectrum area* (underground, air, land/sea);

b. *The use of offensive cyber systems and unhindered access to intrusive cyber-assets and technologies* by non-state actors and civil companies *will increase the threat to electronic and cyber-preservation of security capabilities through remote intrusive access or direct electronic spectrum actions in the electronic spectrum on the critical infrastructure essential components;*

c. *The liberalization of artificial intelligence capabilities and the possibility of handling machine-learning algorithms will result in diversification and simplification of illicit documentation activities of critical infrastructure vulnerabilities, using the common infrastructure interconnection environment.* The future interconnection level of any critical infrastructure will increase, as the outcome of digitalization and unification of network processes and architectures across the states.

d. *The large-scale materialization of the IoT* **[4]** *concept and increase in the number of devices/equipment* dependent on an internet connection or online updates, within critical infrastructure, even in dedicated protection systems, will lead to *security vulnerability of any critical infrastructure,* without any concrete possibility of countering these threats, using current technologies and resources;

e. Wide-scale acquirement by civil entities and companies of *the capabilities to scan, observe and document security solutions dedicated to critical infrastructure protection will require the development of new protection capabilities and the scaling of security risk analysis in terms of threats.*

The five technological evolution trends rapidly developing in today's interconnected society, call for a rethink of the threat spectrum and profile towards the critical infrastructures of the states as well as the conceptual change of the current organizational mode and implementation of security solutions toward the most effective use of bilateral cooperation in the field of advanced technologies and counteracting the proliferation of disruptive effects.

Threat spectrum generated by technological evolutions in the area of critical infrastructures

a. *The duality of advanced technologies – drone systems.*

The threat footprint of disruptive technologies on critical infrastructure security, particularly on the ground, is continuously expanding, mainly due to the civil-military duality of the new autonomous platforms and systems. On the one hand, current technical systems such as autonomous drone platforms are dual and developed for civil purposes (research, medical, industrial, economic, social), but they can be used offensively, for destructive purposes through small adaptations, operationalization and implementations, to carry out destroying activities of critical infrastructure elements, particularly toward the energy distribution systems, transport infrastructure elements or communications networks. For instance, a commercial drone operationalized with artificial intelligence systems for the flight path and usually used in urban activities to determine the cadastral situation, atmospheric characteristics and terrestrial photography, can have a destructive use, by simply changing the flight path, the operating area, and by using improvised explosive devices and means.

For port-critical infrastructure dedicated to transport/storage of energetic resources, a fleet of autonomous sea platforms such as UMS oceanic/maritime research systems used successfully in ocean research and aquatic applications can be a vector of the direct threat to critical underwater communications infrastructure or energy resource transport routes. Almost identically, the emergence of nano drones, similar in size to ordinary insects, with a range of more than 30 minutes, wirelessly or solar charging, capable of transmitting images, positions and documenting a whole critical infrastructure can be a real danger for the protection and physical security of critical terrestrial infrastructure elements, without being effectively counteracted by the actual security systems capabilities.

The duality of autonomous platform technologies is a current reality that will be generalized shortly so that defining new critical infrastructure security and protection capabilities becomes a stringent necessity.

b. *The offensive network environment cybernetisation can preserve the security functions* (video surveillance, access control, and detection), *electro supply systems or SCADA* **[5]** *control systems* by advanced malware, APT-type attacks, and zero-day exploit in network equipment, IP cameras and operating systems and by the destructive use of offensive means in the electromagnetic spectrum. *During the last decade, when SCADA systems were using standard protocols and hardware/software as in administrative IT systems, differences between SCADA systems and IT systems were reduced. Also, the connectivity between SCADA systems and other systems increased* **[6, p.4].** In the technological future context, the totality of the cyber risks that are now manifested in the network environment, will migrate in the critical infrastructure security environment, generating an extrapolation of risk level.

c. *IoT technology.* The massive interconnection of network infrastructures supported in the future by development of 5G-technology will make critical infrastructure dependent on the connection environment and simultaneously on equipment, subassemblies and software manufacturers. Any current critical infrastructure, be it the energetic environment, transport system, financial systems or the medical field, depends on the hardware components and software platforms. The IoT environment will generate the integration of these components with the global interconnection environment and the level of security risk will be both from the outside to the internal infrastructure environment and from inside to the outside environment. The relationship between technology manufacturers, interconnection service providers and software manufacturers will define the security level of critical infrastructures shortly, regardless of the ability of states to ensure their protection and security.

Conclusions and proposals for adaptation and development of integrated security systems

The dynamics of technological change over the last decade has left its mark on the upward evolution of critical infrastructures threats in such a profound way that the notion *adaptation* of integrated security systems will most likely be replaced in the future by notions such as *innovation and reinvention.*

The effective response to new threats is found in technology, as well as in the growth of culture and security training of specialized personnel while rethinking the security procedures. Technically, technological changes will bring about a rethink of how to integrate security systems component modules, subsystems, and a systemic change by implementing new advanced capabilities and technologies, as follows:

a. *Security system integration currently performed at the physical/network layer* (third layer of the OSI model) *needs to be performed at the application/software level of the OSI architecture*. Thus, each security system related to critical infrastructure will additionally cover the other systems in a wider spectrum of threat, and data and information obtained can be integrated, interpreted, processed and exploited centrally, thereby achieving a synergy of security functions and protection actions. Security functions interconnection at the software/application level will also enable artificial intelligence algorithms deployment to optimize threat analysis and security monitoring processes, thus excluding human subjectivity.

b. *The development of security systems dedicated to critical infrastructure protection shall be modular, using „in-house" technologies, by national industry companies* or operating in partner countries, able to ensure transparent management throughout both the production and the life cycle, while also seeking to reduce dependence on external suppliers, unknown or from states with totalitarian regimes outside bilateral alliances and agreements.

c. *The integration and interconnection of security systems across all critical infrastructures shall be a closed but extended one, meeting INFOSEC security criteria, in EAL* **[6]** standard, exclusively using a network environment, redundant, controllable, and inspected and within the protected perimeter.

d. *Video surveillance systems, control access systems to critical infrastructure elements and smart monitoring systems of all functions of critical infrastructure shall be developed in an integrated way, through the implementation of AI* „machine learning" and „deep learning" technology. Thus, the ability to document threats and limit vulnerabilities will no longer be passive but will allow identification and preemptive warning of possible threats, but also the determination of a possible pattern of their future intruding actions. For instance, the human ability to predict potential cyber threats is limited by the experience and the speed of response to the threat, but the ability of artificial intelligence algorithms to preemptively identify a potential threat or intrusive action is based on objective learning, thus increasing system responsiveness and threat identification capabilities.

e. *Physical protection and security of critical infrastructure require a rethink in terms of increasing threat identification capacity from the spectrum of physical intrusive access* to critical elements. This requires the interconnection of all infrastructure access areas through the network environment and the use of detection, recognition and identification tools enhanced by biometric technologies.

f. *The human security factor and the critical infrastructure monitoring and control systems*. The critical infrastructure monitoring and control system developed in current technologies needs to be *changed into a proactive integrated management security-critical infrastructure system*, encompassing all security components. This will allow multi-spectrum threat control and a comprehensive assessment of risk and security events. The cyber defence component will become mandatory in the future integrated security management architecture of critical infrastructure, along with the ongoing human resource training and motivation factor.

Human management and security factor will also undergo a technological process, with future protection action being a combined personal – human – autonomous platform. The level of human staff training to ensure security management will be technically high, adapted to the technologies used and the evolution of new generation platforms and sensors (cyber, autonomous platforms, artificial intelligence, software). In addition to the technological change of future technical security architectures, a procedural re-think of inter-institutional cooperation systems is required to increase the pro-activity of security platforms and systems. Thus, the critical infrastructure security cannot be ensured in the future without bilateral cooperation between states that have access to the same infrastructure or inter-institutional cooperation at the level of a state.

Providing a level of security in the future of advanced technology for states' critical infrastructures will migrate from the reactivity spectrum toward the spectrum of pro-activity and anticipation of threat evolution, to decrease the level of vulnerability by proactive neutralization of potential aggressors. The advanced technology evolution and the effects of its destructive intended use can also be countered by technology and by improving the level of training, specialization, the adaptation of staff knowledge and skills to new security systems and technology platforms.

References

[1] Section 1016(e) of the USA PATRIOT Act of 2001 - 42 U.S.C. 5195c(e).

[2] Security in depth (DID/SID)", a term derived from defense techniques that are preferentially used in the cyber environment, https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

[3] http://www.novaroma.org/nr/Comitia_centuriata_(Nova_Roma)

[4]https://www.internetsociety.org/resources/doc/2015/iot-overview?gclid=EAIaIQobChMIkp3U4KX66wIVRubtCh0AEwn9EAAYAiAAEgID_vD_BwE

[5] Wei & Morris, Thomas & Reaves, Bradley and Richey, Supervisory Control and Data Acquisition (SCADA). Drew On SCADA Control System Command and Response Injection and Intrusion Detection, ECrime Researchers Summit (ECrime), 2010.

[6] Kovacevic, Ana & Nikolic, Dragana, Cyber Attacks on Critical Infrastructure: Review and Challenges (draft),2015

[7] Nancy Mead, The Common Criteria, 05, July, 2013, Carnegie Mellon University 2005-2012, available at https://us-cert.cisa.gov/bsi/articles/best-practices/requirements-engineering/the-common-criteria

LASER SAFETY FOR EU DEFENCE FORCES - E-LEARNING PLATFORM

LYUBOMIR LAZOV, ERIKA TEIRUMNIEKA, EDMUNDS TEIRUMNIEKS, NEDKA ATANASOVA

Faculty of Engineering, Rezekne Academy of Technologies,
115 Atbrivosanas aleja, LV-4601 Rezekne, Latvia, lyubomir.lazov@rta.lv

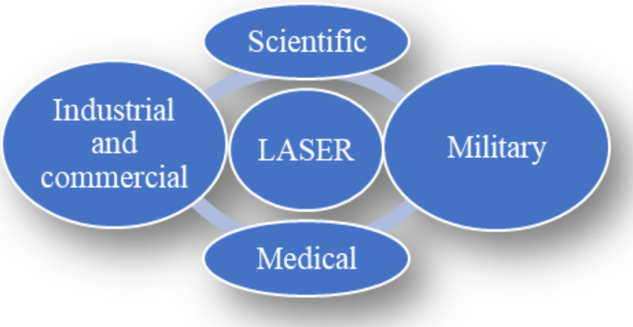
***Abstract**: With the development of laser sources in the last 60 years, the field of applications of lasers is developing as well. From vision correction to driving vehicles, from spaceflight to fusion, from material processing to presentation pointers, lasers are still finding their application in unexpected areas. Should be noted, that the lack of laser safety skills in the professions and sector bound up with lasers is already present and, unfortunately, reality. With the development of laser sources in the last 60 years, the field of application of lasers has been developing. From vision correction to driving vehicles, from spaceflight to synthesis, from material processing to presentation pointers, lasers are still being used in unexpected areas. It should be noted that the lack of laser safety skills in the professions and sector related to lasers is already present and, unfortunately, a reality.*

This article presents the highlights and results of a European project in the field of laser safety in several European countries. The project "Laser models for web safety for vocational education / training" is aimed at improving professional skills in the field of laser safety by developing, testing and validating innovative web-based training modules in accordance with the norms and standards of the European Union.

***Keywords**: Laser Safety, Laser Technology, e-learning platform, VET, Lasers in the Military*

Introduction

Laser is an electronically optic system which produces artificial, coherent, highly monochromatic electromagnetic radiation with ability to reach extremely high energy densities. The applications of lasers in our lives are extremely versatile and extensive[1 – 3]. In general, we can define the application of the laser in 4 groups, see Figure 1.



.

Figure 1 General areas of the Laser applications

Photonics and laser technology are now a priority of the Europe's defence ministries and an essential to enhance the combat capabilities of NATO-led armies, as stated in the documents and strategies. The introduction of new and different laser sources and weapons in the military sectors requires the development of new skills and competencies of the military and command staff of the army subdivisions in the field of laser safety. According to NATO (North Atlantic Treaty Organization), a number of significant technology-related trends – including the development of laser weapons, electronic warfare and technologies, that impede access to space – appear self-possessed to have major global effects that will impact on NATO military planning and operations. In addition, the photonics and laser technologies sector is an essential contributor to the European defensive economy and, that its advancement is vital to the development of other digital technologies and flagship programmes and indispensable to European security and defensive.

In the past years European Norms and Standards in this area „Laser Safety" have become obligatory for all European countries. But, the lack of laser safety skills in the sector is already in place and, unfortunately, traditional military institutions cannot meet this demand. The dangers of laser radiation can be diverse and at the same time devastating for the health and fitness of army.

The purpose of this report is to provide useful information about the purpose and results of a European project developed by us with a civic focus in the field of laser safety for the needs of vocational training. Our desire is for this attempt to serve as a basis and bridge to the creation of training modules for training in the military.

1. Erasmus+ Laser Safety Project

The project aims to improve professional skills for laser safety through online training in vocational education and training in small and medium enterprises. Details of the project can be found in Table 1.

Table 1 Details of the project

Title:	Web-Based Laser Safety Modules For Vocational Education/Training
Project No.:	2018-1-LV01-KA202-056957
Programme:	Erasmus+
Key Action:	Cooperation for innovation and the exchange of good practices
Action:	Strategic Partnerships
Project Start Date:	01-09-2018
Project Total Duration:	24 months
Applicant Organisation:	Rezekne Academy of Technologies, Latvia
Webpage:	lasersafety.rta.lv

Project has gathered partners from five European Union countries: Bulgaria, Germany, Hungary, Latvia, Romania.

Organizations involved:

- Rezekne Academy of Technologies, Latvia;
- iTStudy Hungary Kft., Hungary;
- SWA Bildungsakademie GmbH, Germany;
- Universitatea Din Pitesti, Romania;
- European Center for Science and Innovation in Education, Bulgaria;
- University of Ruse Angel Kanchev, Bulgaria;

- Veda Consult, Bulgaria.

Profile of participants includes three universities with their own research institutes (including photonics and laser technology), one NGO, two VET centers and an ICT company. The project team aims to develop, test and validate four innovative training modules (Figure 2) in line with the needs of the European photonics and laser technology field. Using the right environment, learning modules will be web-based and accessible to students, laser workers / operators and all other players related to the fields of photonics and laser technologies.

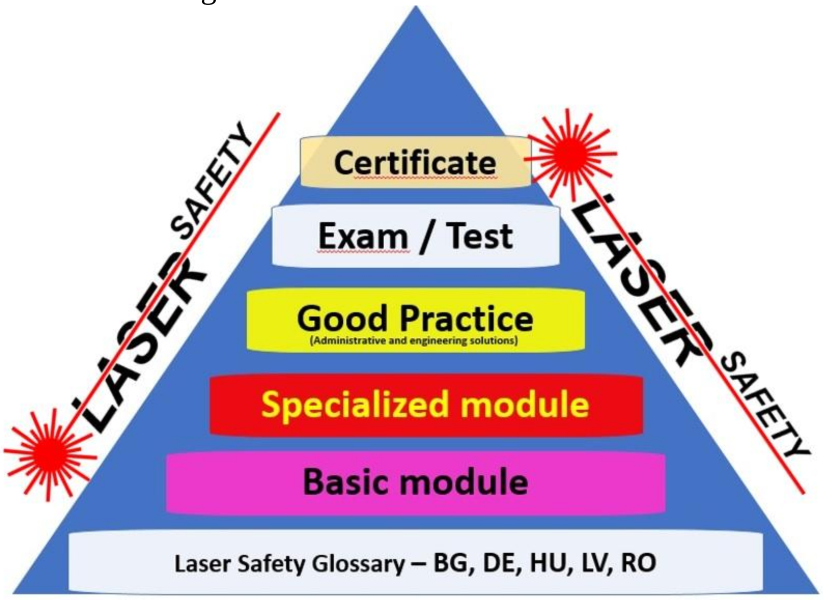


Figure 2. Innovative training modules in Laser Safety

The Laser Safety Course will be free of charge translated into 5 languages and web based and interactive. In substantive terms, it will comply with EU Directive 2006/25 / EC. It will give an opportunity to those who want to improve their knowledge and get a European certificate in Laser Safety.

The final results that will be expected to be obtained during the development of the project and its dissemination are:

□ Improvement of vocational education and training in the field of laser safety by using new interactive methods.

□ Enhancing the professional skills of photonics and laser technology specialists by enhancing their knowledge of laser safety.

□ Creating specialists with skills and competencies in the field of laser safety.

□ Support for the development and implementation of European laser safety norms and standards in the project partner countries.

□ Improving the employability of the European labor market.

□ Increasing the motivation of young people for vocational training and work in the field of innovative photonics and laser technology.

□ Changing people's thinking about the dangers of laser radiation and creating safe working conditions when operating with laser, laser systems and complexes.

The educational product for e-learning that is created under this project is built on the basis of:

➢ analysis of existing VET programs and ongoing training in the laser safety sector in the partner countries;

➢ identification of the needs of workers related to the use of laser in 5 partner countries.

The survey and analysis methodology is based on special questionnaires. The team of participating project partners developed two sets of questionnaires. They are designed to provide the necessary information for:

- the current state of the laser safety problem;
- specific proposals for new skills needs for training modules.

After approval of the survey questions by the project partners, the questionnaires were translated from English into the national languages of the participating project partners: Latvian, Bulgarian, Romanian, Hungarian and German. The project partners then surveyed each in their country on (5) companies related to the use of lasers and the laser system and on (25) workers / operators.

Today, a number of SMEs are working successfully to produce new competitive products based on photonics and laser technology. Distributors of laser equipment are required under European laws to warn of the dangers inherent in their product. In turn, the laser operators and other laser technology consumers are required to examine in detail the operating instructions supplied with the safety instructions before putting the laser device into service.

This study showed that in some countries such as Bulgaria, Romania and Hungary in the years before the transition there was a system for control and training on laser safety, but in the years of transition due to the great administrative and economic changes in these countries these good practices are lost. Since 2006, with the adoption of the European Directive, the necessary administrative control structures for monitoring have not yet been deployed, and there are no professional training centers offering certified Laser Safety courses.

Another difficulty that would impede the widespread and rapid implementation of the directive is that it will require the removal of employees from their direct work responsibilities, which impedes employers and disrupts the pace of work in the enterprise. The activities and results of this European project "Creating Laser Safety Modules for Training / Training" will contribute to solving this problem. At the same time, it has saved both time and money for both trainees and employers.

The methodology offered to work on the project is a mixed model of training that could help achieve the project goals in the most appropriate way. Combined learning as a method of learning includes elements of distance learning and attendance training, optimally combining the strengths and benefits of each. The use of combined learning is intended to partially address the main task of modern education - with a limited number of teachers to help a large number of learners get the skills they need in the shortest possible time.

- Combined learning is a flexible technology that combines virtual and direct communication, in which discussions, debates, exchanges of experiences and practices, deep self analysis of parts of the matter through online technologies are held. These allow you to save time actively exercising and learning certain skills and habits in the classroom.
- Combined Learning develops critical thinking and creates skills for independent learning and work, relevant information (exploration, analysis and selection of materials) is used in training and career development.
- In combined learning, training materials are provided not only in print but also in accessible electronic text and / or media option, which allows students to choose individual mode of learning (access to the materials as many times as they need at a convenient time and place).
- Combined learning is interactive, it provides the opportunity for communication "teacher-learner" and "learner-learner", expression of personal opinion and perspective, exchange of opinions and possibility of changing topic directions in the studied material.

- In combined learning, individual psychological characteristics of the trainee are taken into account, because the combination of various forms of work enable students to express themselves with their different temperament and speed of absorption of matter. Thus, combined learning fits and supports the ideas of personality-oriented approach to training.

The complexity, versatility and multifactoriness of the learning process in learning contexts dictates the need for a methodologically new approach to learning from the standpoint of individualisation of learning. The use of combined learning nowadays is associated with solving the problem of the individualization of learning, its intensification and optimization. The ability of the online environment to individualize learning, enables a new way to approach the possibilities of using combined learning in the educational process.

EU Workplace Safety Regulations oblige each company to take all necessary safety and health measures at work, document them and periodically monitor for compliance, but on the other hand there is big problem about monitoring enterprises whose are related with laser beam use, because there is insufficient information about the laser systems purchased and implemented in the countries under study. This and many other problems will be solved if more people will have experience and knowledge in the field of laser safety after completing a full training course in accordance with European norms and standards, as well as obtaining a laser safety certificate.

The activities and content of the modules developed under this project will enable the students to receive knowledge and the opportunity to apply for Laser Safety Officer position in companies related with lasers, that would be monitored on national level by “Safety work environment” institutions in every EU country.

2. Lasers in the military

The use of lasers by the military continues to increase. Many armies of different countries are using a wide variety of lasers in many different ways. Traditional troops, such as infantry, artillery, naval and airborne subdivisions, now recognize the laser as an essential teaching element for increasing the accuracy and effectiveness of combat (Fig.3).

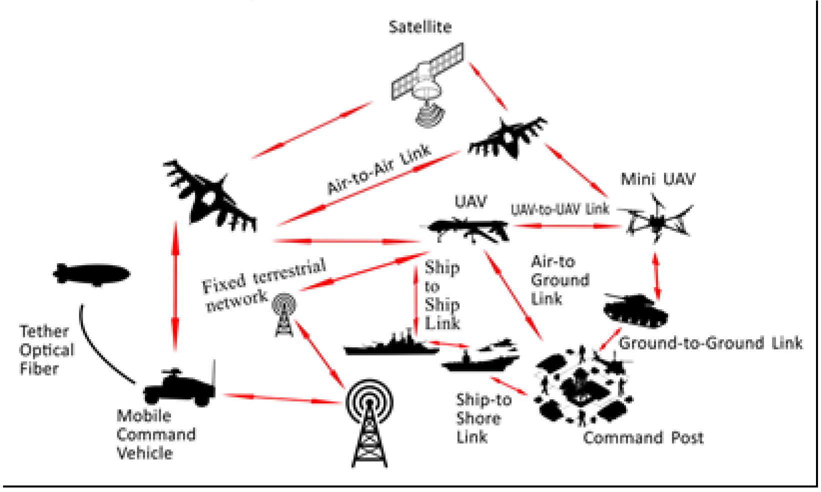


Figure 3. Illustration of military laser applications and their technological diversity

Lasers are also an element in a number of trainings related to the educational process of the Army staff.

How much exposure to laser light is hazardous? To answer this question, you have to take into account the output characteristics of the laser.

Those characteristics include wavelength, output energy and power, size of the irradiated area, and duration of exposure. If you’re using a pulsed laser, you also must consider the pulse repetition rate.

The output power of modern day military lasers ranges from milliwatts to megawatts (in cases where they deliver continuous output power), or even petawatts (10^{15} W) for short pulse lasers. In military terms, lasers with continuous output powers greater than 20 kW are classified as High Energy Lasers (HEL). Output powers in the range of kilowatts or even megawatts allow the creation of laser beams with potential harmful intensity over distances of up to several hundred kilometres. These beams can be used to heat up targets,which then may lead to structural failure of the target object.

The sensitivity to a given wavelength of laser radiation varies considerably from person to person. Maximum exposure limits (MPEs) show the highest exposure that most people can tolerate without injury.

Table2 gives the maximum allowable eye exposure for different lasers operating at different radiation levels.

Table 2. Maximum perssimible exposure limits (MPe) level W.cm^{-2}

	0,25 s	**10, s**	**10, min**	**500, min**
CO$_2$ (CW) λ = 10,6 µm	-	100. 10^{-3}	-	100. 10^{-3}
Nd:YAG (CW) λ = 1,33 µm	-	5,1. 10^{-3}	-	1,6. 10^{-3}
Nd:YAG (CW) λ = 1,064 µm	-	5,1. 10^{-3}	-	1,6. 10^{-3}
Nd:YAG (Q swiched) λ = 1,064 µm	-	17,0. 10^{-6}	-	5,1. 10^{-6}
GaAs Diode CW λ = 0,840µm	-	1,9. 10^{-3}	-	610,0. 10^{-6}
HeNe (CW) λ = 0,633 µm	2,5. 10^{-3}	-	-	17,6. 10^{-6}

**Krypton-(CW) λ = 0,647;
0,568;
0,530 µm**
	2,5. 10^{-3}
	31. 10^{-6}
	16,7. 10^{-6}
			364. 10^{-6}
			2,5. 10^{-3}
			2,5. 10^{-3}
				28,5. 10^{-6}
				18,6. 10^{-6}
				1,0. 10^{-6}

Argon (CW) λ = 0,514 µm	2,5. 10^{-3}		16,7. 10^{-6}	1,0. 10^{-6}
XeFl-(Eximer CW) λ = 0,351 µm	-	-	-	33,3. 10^{-6}
Xel-(Eximer CW) λ = 0,308 µm	-	-	-	1,3. 10^{-6}

The hazard evaluation procedure used is based on the ability of the laser beam to cause biological damage to the eye or skin during intended use, and is related to the classification of the laser or laser system from Class 1, considered to be nonhazardous, to Class 4, very hazardous. Lasers or laser systems are certified by the manufacturer for the specific hazard class in accordance with the EU standard of laser products.

The classification of lasers is based on the concept of accessible emission limit (**AEL**); these are defined for each laser class. AEL takes into account not only the output of the laser product but human access to the laser emission. Lasers are grouped into seven classes: the higher the class, the bigger the potential to cause harm (Fig.4). The risk could be greatly reduced by additional user-protective measures, including additional engineering controls such as enclosures.

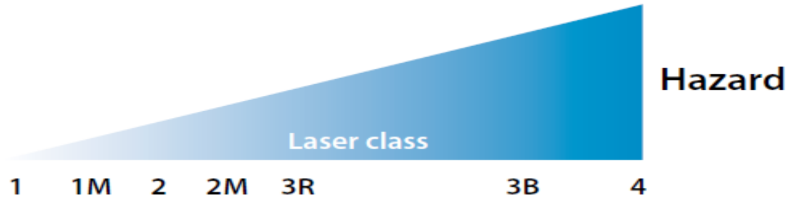


Figure 4. Laser classes and the hazard

Class 1

Laser products that are considered safe during use, including long-term direct intrabeam viewing, even when using optical viewing instruments (eye loupes or binoculars). Users of Class 1 laser products are generally exempt from optical radiation hazard controls during normal operation. During user maintenance or service, a higher level of radiation might become accessible.

Class 1M

Safe for the naked eye under reasonably foreseeable conditions of operation, but may be hazardous if the user employs optics (e.g. loupes or telescopes) within the beam.

Class 2

Laser products that emit visible radiation and are safe for momentary exposures, even when using optical viewing instruments, but can be hazardous for deliberate staring into the beam. Class 2 laser products are not inherently safe for the eyes, but protection is assumed to be adequate by natural aversion responses, including head movement and the blink reflex.

Class 2M

Laser products that emit visible laser beams and are safe for short time exposure only for the naked eye; possible eye injury for exposures when using loupes or telescopes. Eye protection is normally provided by aversion responses, including the blink reflex.

Class 3R

Direct intra-beam viewing is potentially hazardous but practically the risk of injury in most cases is relatively low for short and unintentional exposure; however, may be dangerous for improper use by untrained persons. The risk is limited because of natural aversion behaviour for exposure to bright light for the case of visible radiation and by the response to heating of the cornea for far infrared radiation.

Lasers should only be used where direct intra-beam viewing is unlikely.

Class 3A lasers—rated in power from 1 milliwatt to 5 milliwatts—cannot injure a normal person when viewed with the unaided eye but may cause injury when the energy is collected and put into the eye as with binoculars. Most laser pointers fall into this category. A danger or caution sign must label the device, depending on its irradiance.

Class 3B

Hazardous for the eyes if exposed to the direct beam within the nominal ocular hazard distance (NOHD). Viewing diffuse reflections is normally safe, provided the eye is no closer than 13 cm from the diffusing surface and the exposure duration is less than 10 s. Class 3B lasers which approach the upper limit for the class may produce minor skin injuries or even pose a risk of igniting flammable materials. Lasers from 5 milliwatts to 500 milliwatts can produce eye injury when viewed without eye protection. This class of laser requires a danger label and could have dangerous specular reflections. Eye protection is required.

Class 4

Laser products for which direct viewing and skin exposure is hazardous within the hazard distance and for which the viewing of diffuse reflections may be hazardous. These lasers also often represent a fire hazard. Lasers above 500 milliwatts in power can injure you if viewed directly or by viewing both the specular and diffuse reflections of the beam. A danger sign will label this laser. These lasers can also present a fire hazard. Eye and skin protection is required

Artificial optical radiation sources are widely used by the military: Searchlights; Lighting at military airfields; Infrared communication systems; Laser target designators; High Energy Lasers and others. During combat operations, commanders may need to take decisions on the cost/benefit of courses of action to weigh the small risk of real injury if the exposure limits are exceeded against the risk of serious injury or death from other hazards. Military uses of artificial optical radiation may include:

In order to use laser beams as weapons, a significant amount of laser output power is necessary. The output power depends heavily on the actual target. For the so-called soft targets, the minimum power to cause harm can be very low. Blinding lasers, for example, are designed to blind the human eye temporarily or permanently [4]. As the eye is very sensitive, these weapons require only a small amount of output power. Blindness can be caused in several ways: apart from burning the retina, a laser pulse can also break blood vessels inside the eye or cause a process of slow decline of the retina. At a distance of some meters, even an output power of a few milliwatts can damage the eye because the ocular focuses the beam onto the retina. This dramatically increases the intensity of the beam. Blinding lasers were used in the Falklands conflict and in the Iran/Iraq war of 1980s [5]. However, in 1995, these weapons were officially banned under International Humanitarian Law. If the aim is to destroy hard targets rather than to blind the enemy, however, the laser requires an output power which is many orders of magnitude higher than that of blinding lasers.

As mentioned above in this article, many countries and research institutes develop and test lasers with continuous output power over 20 kW or impulse power over 1 kJ [6]. As stated above, the use of blinding laser weapons is illegal under International Humanitarian Law. In particular, these weapons violate the Fourth Protocol (1995) to the Convention on Prohibitions or Restriction on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects. This protocol outlaws the use and transfer of laser weapons which are intended to cause blindness. Additionally, the signatories are obliged to take the necessary steps to prevent blindness caused by other laser weapon engagements [7]. However, the protocol is not applicable if collateral blinding occurs as a result of military laser applications that are otherwise considered legitimate. As a consequence, the protocol might be applicable to High Energy Lasers (HEL) weapons only, if they are especially designed for blinding purposes. Nevertheless, the protocol seems to have had some positive effects so far. The protocol the first step towards a comprehensive ban of all laser weapons. This would be the first step towards preventive arms control, a concept which was developed to ban the introduction of new destabilising weapon systems [8]. Whether and to what extent a complete ban is realistically achievable is obviously another question.

Acknowledgments

This work has been supported by the Erasmus+ programme, KA2 – Cooperation and Innovation for Good Practices within the project Nr. 2018-1-LV01-KA202-056957 “Web-Based Laser Safety Modules For Vocational Education/Training”.

References

1. Poprawe, R., H. Weber, G. Herziger, (2004), *Laser Applications*, Springer, 495 p., ISBN: 978-3-540-00105-8

2. Estudillo-Ayala,J., R. Rojas-Laguna at al. (2015) *Sub- and Nanosecond Pulsed Las ers Applied to the Generationof Broad Spectrum in Standard and MicrostructuredOptical Fibers*, Springer Science & Business Media, ISBN: 978-94-017-9480-0

3. Angelov, N., *Determination of Working Intervals of Power Density and Frequency for Laser Marking on Samples from Steel HS18-0-1*, Proceedings of the Union of Scientists - Ruse, Book 5 Matematics, Informatics and Physics, Volume 12, pp. 125-130, 2015

4. Peters, A., (1995) *Blinding Laser Weapons: The Need to Ban a Cruel and Inhumane Weapon*, Human Rights Watch Arms Project, September, vol. 7, no. 1, , pp. 1–49

5. McCall, J. H. Jr, (1997) *Blinded by the Light: International Law and the Legality of Anti-Optic Laser Weapons*, Cornell International Law Journal, vol. 30, no. 1, 1997, pp. 1–44

6. US Defense Threat Reduction Agency, “Section 11: Lasers and Optics Technology” , in US Department of Defense, Devloping Science and Technologies List, Ft. Belvoir, 2000, http://www.dtic.mil/mctl/DSTL/Sec11.pdf.

7. ICRC, “Treaty database of the International Comitee of the Red Cross”, http://www.icrc.org/ihl.nsf/WebFULL?OpenView –viewed May 2005.

8. T Petermann, M Socher & C Wennrich, Präventive Rüstungskontrolle bei Neuen Technologien. Utopie oder Notwendigkeit?, Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag 3, Edition Sigma, Berlin, 1997.