„Training in the information age – Cyber warfare and beyond”

Various technical capabilities and new ways to communicate are influencing today’s society. Characterized by the shift from traditional industry to an economy based on information technology, this new time is generally known as the information age. These changes are also influencing the way, how military and civil operations have to be executed in the future to be successful. This includes, that also the training of tactical leaders has to be adjusted to these new framework conditions. With focus on command and staff training (CAST), it will be outlined, which new objectives have to be trained in this new age.

The main objective of CAST is to train the decision making process of military and civil leaders at all steps of an operation. Embedded in realistic real-time simulation, in which every action has an influence to the whole scenario, the training audience will be empowered to handle every kind of operation. Besides that, CAST is also being used for mission rehearsal to prepare for a specific operation or to test different tactics to define standard operation procedures.
Common characteristics of these training contents are that a current situation has to be evaluated by the training audience. This includes the analysis of all existing and further influencing factors. Based on that, all operational activities like the deployment and movement of own forces have to be planned to fulfill the defined tasks successfully. And finally, all activities have to be coordinated by the commanders and their staff taking into account the changing conditions of the operation.

In classical military training scenarios, it is possible to identify a clearly defined mission type, with specific objectives. The opposing forces are known and their tactical behavior is mostly predictable. In addition, the behavior of other involved groups in the area of operation is well-known or can be assumed.
Civil scenarios are mainly characterized by a major incident, which leads to the challenge of coordinating the responds forces and activities in the area of operation. Besides that, other corresponding activities like coordinating movement up to evacuating the population has also to be taken into account.

Before it is possible to answer the initial question, how training in the information age has to be designed, the general characteristics of the information age have to be pointed out.

As a result of the technical evolution, systems are getting more and more complex. The world is confronted with digitalization and a direct and fast connection between people due to the internet. New communication channels like social media are giving everybody a platform to share personal ideas or opinions with others. On the other hand, these new possibilities bearing the risk of an information overflow and a clash of cultures. Such confusing situations for an individual could be exploited by radicals to recruit them for their thoughts of hate.

Our modern society is faced with a new quality of threats, which are directly connected with these mentioned characteristics. The imbalance of military power in areas of conflict, with a simultaneous unrestricted availability of information, leads to new tactics commonly known as asymmetric or also hybrid warfare. Terrorist organizations are able to execute diverse attacks by individually radicalized persons easily. Fake information is deliberately used to influence the general opinion of the public and the number of cyber attacks is increasing dramatically over the last years. Aggressors focusing more and more on vital targets like public transportation, media or power supply, generally known as critical infrastructure.

Considering these aspects, modern training settings need to be adapted to ensure the simulation of realistic scenarios for the training audience. Beside the classical mission settings, military leaders are recently confronted with the fact, that asymmetric opponents are mostly unpredictable and invisible. Communication channels, which are normally used to coordinate own activities, can also be corrupted or interrupted by cyber attacks, without recognizing the infiltration. Besides that, alternative communication channels, like social media, are used by the involved parties to coordinate activities or just exchange information. Nowadays modern weapon systems are mostly digitalized and threatened to be attacked directly by cyber forces.

Emergency responds forces are confronted to the fact, that a major incident is combined with potential additional incidents, assumed[1] and also fake incidents[2]. The

[1] Assumed incidents are based on subjective perception of person, who interpret it wrongly as an incident

[2] Fake incidents are based on intentional misreports, to suggest a real incident

information overflow, due to individual status reports via social media channels, makes it more complicated for a crisis manager to get an overview about the whole situation. In addition to that, aggressors could also take advantage of a real incident by spreading fake information to interfere rescue measures, leading to ‘fake incidents’. Besides that, the behavior of the population is getting more and more unpredictable and the coordination of emergency response forces and activities on the ground becomes a challenging task for a commanding officer.

Modern CAST has to combine all possible aspects of an operation to ensure a realistic training for military and civil leaders. Therefore, new training objectives need to be implemented. Cyber has to be integrated to increase the awareness of cyber-attacks. The training audience has to understand the different strategies to attack modern systems and learn how to avoid them by specific counter-measures. In addition to that it has to be trained how the security of own systems can be improved and how to deploy cyber-forces efficiently for an operation.
Social media used as a communication channel becomes more and more important for military and civil operations. Trainees have to understand how information is exchanged and influences the mind of the population – or even the forces on the ground. They also have to be aware of the effect of falsified or colluded information and learn how to use tools or techniques to include social media in their own operational planning processes and actions.
Because of the fact that conflicts are shifting into urban terrain, the impact of attacks against critical infrastructure has to be simulated. For a successful execution of an operation, it is essential to know how people will behave and how this behavior could be influenced by specific actions like the deployment of forces or the broadcast of information via different communication channels like social media.

Modern training settings have to take all these aspects into account. For a successful training of military and civil leaders, preparing them for the future challenges, it is essential to change the intensity and the impact of these different factors easily. Current training systems need to be able to simulate all of these factors and be flexible enough to adjust them to the specific training objectives.
With CAE´s constructive simulation system GESI, it is possible to create such complex and demanding training scenarios. Acting in their own command posts, the

training audience receives realistic information in real-time, to fulfill every possible scenario. GESI includes various tools and modules enabling instructors to simulate every aspect of military or civil operations in a customized intensity and focused on specific training objectives.

The information age is influencing todays and future military and civil operations dramatically. To be prepared to these challenges CAST has to be rethought. New settings and new factors have to be considered in designing modern training contents. Also the used training systems have to be performant and flexible enough to simulate all possible scenarios.
CAE’s GESI supports tactical military and civil leaders to stay well prepared for the future.