NATO
OTAN

TRANSFORMATION THROUGH TRAINING

BYDGOSZCZ - POLAND

Transformation for Training

Interview with Major General Wilhelm Grün, the Commander of the Joint Force Training Centre

NATO - Georgia Exercise

Another Milestone in the Development of Long-standing Military Cooperation

JOINT FORCE TRAINING CENTRE

Test Your Capabilities and Get Ready for the Future to Keep Our Nations Safe

CWIX 2017

ISSN: 2084-8358

The Magazine of the Joint Force Training Centre

September 2017 - Issue No: 10








TABLE OF CONTENTS

„Transformation Through Training“

The aim of this magazine is to provide a forum for exchange of information and expertise among training and educational institutions across NATO in the area of training, military professional education, and related technological support. In the context of The NATO “Smart Defense” approach, there is growing importance for cooperation with partner states and international organizations, such as the United Nations, the European Union, the Organization for Security and Cooperation in Europe and others. With the above in mind, the JFTC invites authors from countries and institutions beyond the NATO environment, to publish in the Transformation Through Training magazine. The magazine will focus on the best practices in the areas of command and staff training, professional military education, simulations and simulation technologies, distributed training, military training development as well as other related areas. The JFTC also welcomes recommendations for the application of the most recent experience and lessons learned from ongoing operations, training events and recent innovations in the field of simulations and information technologies. The magazine will also briefly cover the life of the international community at the JFTC with the aim of promoting the centre within NATO and among the partner nations. The magazine will be published twice a year, during the spring and fall, by the NATO Joint Force Training Centre in Bydgoszcz.

The articles published in this magazine represent opinions of their authors and do not necessarily reflect the official policy of NATO.

Publishing Institution:
Joint Force Training Centre Bydgoszcz (JFTC)

Managing director:
Brigadier General Ladislav JUNG,
JFTC Deputy Commander / Chief of Staff

Editor-in-Chief:
LTC Eric PARTHEMORE, JFTC Director of Management

Publishing Editor:
Ms. Radosława KUBICZEK, JFTC Public Affairs Specialist

Editorial Board:
Mrs. Kamila SIERZPUTOWSKA, PhD, Kazimierz Wielki University, Poland

Advisory Support:
Mr. Tomasz OCIŃSKI, JFTC Language Specialist

Editorial Contact Information:
Public Affairs Office
Joint Force Training Centre
ul. Szubińska 2
Bydgoszcz, 85-915, Poland.
E-mail: pao@jftc.nato.int

ISSN: 2084-8358

Scan the QR code with your mobile device. This will take you to the archive of *Transformation Through Training* magazine.

Transformation for Training

Interview

with Major General Wilhelm Grün

the Commander of the Joint Force Training Centre

Sir, we are talking a year after you assumed the position of the Joint Force Training Centre Commander. This time let you get familiar with the place but your memories of the first days here are still fresh. Can you share with us some of your first thoughts and impressions right after coming to Poland?

I always underline that throughout recent years every NATO post has brought me closer to my country, to Germany. In 2010 I started my service at the Joint Force Command Lisbon, Portugal. In 2013 I moved to Turkey, where for three years I worked as the Deputy Chief of Staff Operations at the Land Command Izmir. Last year, I started my service here at the Joint Force Training Centre – approximately 4 hours of driving from the Polish-German border.

However, I must admit, that although Bydgoszcz is not far from Germany and I had, of course, a rough idea about the country, I did not know exactly what to expect. And it turned out to be like homecoming. Poland is very close to Germany – and I am not talking about the distance, or not only about it. I am talking about culture, social aspects of life, people, etc. - not to mention the climate or food.

Bydgoszcz is a fantastic city with open and kind people. It is a really good place to live. I am very happy to be here.

And your first impressions related to JFTC - does the Centre differ from HQs you were assigned to in the past?

Yes – it is a bit different from what I know from the past. In my previous positions, I was focused more on operations. Both Joint Force Command Lisbon and Land Command Izmir were part of the Allied Command Operations' structure. Being a part of the Allied Command Transformation's family, JFTC is responsible for the collective training – be it pre-deployment preparation for soldiers going to Afghanistan or higher headquarters battle staff training, it is something different than I was responsible for in the past. But this is why I am sure that my experience on

the operational side, is a good asset I can use to improve and reinforce the JFTC's support to NATO Force Structure (NFS) and NATO Command Structure (NCS) training.

When I became the JFTC Commander, the centre already had a solid reputation as the flagship of NATO pre-deployment training. And I knew it was a good basis for further shaping.

From the very beginning I was impressed by the staff. My first observations are related to my induction and the Change of Command. It was prepared very well. But also first training events and exercises I participated in as the centre's Commander showed that the team was well organized and fully committed to the mission. And flexible – which was visible especially during the first NATO-GEORGIA Exercise in November 2016 in Krtsanisi, Georgia. The event was new for JFTC, and still prepared and executed on a high level. And these are not only my words. The exercise has been recognized by many high-ranking political and military leaders.

You mentioned "further shaping" of JFTC. On numerous occasions you underlined the JFTC position of a key player in NATO training, yet still you emphasized the Centre's transformation. In opening remarks to the last issue of the TTT magazine you wrote: "While contributing to the transformation of NATO by providing high quality training to our diverse training audiences, we have to keep transforming ourselves as well". Why change something that works well?

The rapidly changing geopolitical situation makes the role of training and simulation even more important than some years ago. You can see this in outcomes of the latest NATO summits. They show the increasing role of NATO training, and thus lead to a higher interest in JFTC as a venue for NCS, NFS and national headquarters' training, training for Major Joint Operations (MJO) and even more advanced operations.

JFTC – one of the two NATO training centres – needs to adapt to this situation. JFTC has to be ready and able to answer to the current and future needs of the Alliance, to requirements set up by the Supreme Allied Commander Transformation (SACT) as well as by the Supreme Allied Commander Europe (SACEUR), through his Annual Guidance for Education, Training, Exercises and Evaluations.

The mission in Afghanistan has been our main focus for years and Resolute Support remains our priority. But we receive more and more tasks. In response to the Readiness Action Plan agreed to in Wales in 2014 JFTC has taken responsibility for NATO Response Force (NRF) Continuation Training, TRIDENT JOUST. In 2017 SACEUR has provided guidance to place Alliance Defence at the core of the training program. The change in focus has JFTC at the forefront of the transformation of the NATO training continuum.

We have already proven – with support to Multinational Corps Northeast, German--Netherlands Corps and Rapid Reaction Corps-France for example - that we are a perfect venue for this type of exercises. We have also proven that JFTC is not only a venue or a static training centre - we are able to deploy teams of training experts to various locations - where our customers need us.

Additionally, we have a strong team working on new technologies, modelling and simulation solutions in support of NATO training. Since 2011 we have been the home for the Coalition Warrior Interoperability eXploration, eXperimentation and eXamination eXercise (CWIX) – NATO's premier exercise for testing and experimentation. The importance of this event is increasing year by year and requires more and more attention. This year we had the pleasure to host both, the North Atlantic Council and the Military Committee during the CWIX Distinguished Visitors' Day. We also play a key role in Balkan Bridges Exercise that utilizes the South Eastern Europe Exercise and Training Network (SEETN) as a medium for communication, data exchange, and simulation. These two capability development events demonstrate the crucial role of testing, experimenting and developing innovative solutions in support of military operations. And this is also the direction JFTC will follow, as innovation becomes the second pillar of our work.

We identified potential, which can be used to better support the Alliance in nowadays' areas of concern. Now we have to develop on it.

So what exactly are the new directions of JFTC's transformation in support of NATO training?

Throughout the 13 years the Centre has built its solid basis – it is a well-known and appreciated place for pre-deployment training but also a trusted location where NCS and NFS Commanders want to train with their staffs. As we have full expertise, know-how and capabilities in pre-deployment training, there is still more that we can – and have to - offer to NATO and national headquarters. Some adjustments are, of course, required, however the basis is already here.

And this is what we are doing right now – we are building on the foundations laid by former commanders and staff members to respond to the current and future needs of the Alliance, expressed by our superiors.

Our aim is to be able to fully support commanders from Multinational Brigade up to Joint Force Command level and their staffs in becoming fully operational - while being clearly delineated from our sister training centre in tasks, in order not to duplicate our resources.

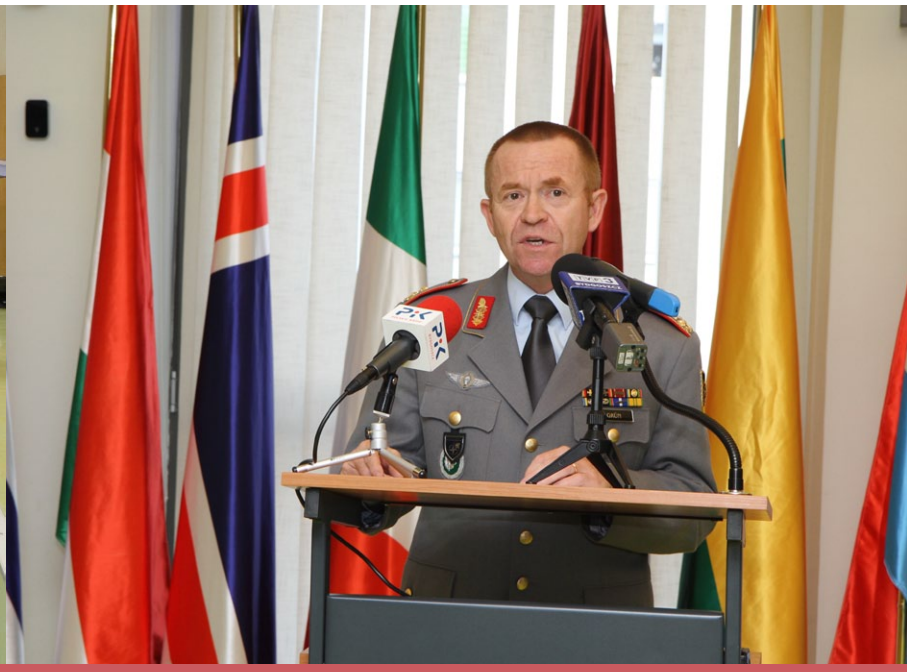
What are the main fields of JFTC transformation? How does the Centre adapt to new challenges?

While our motto is "Transformation through Training", we are currently transforming for training, for better training.

Internally, I would define two main fields of this transformation – optimization of the Centre's structure and infrastructural development.

In the first area, we are now preparing ourselves for a new structure tailored to better respond to current needs related to both training and innovation. Our manpower of approximately 150 soldiers and civilians will be reorganized once the new structure is approved.

Meanwhile, the JFTC compound is also expanding. We have already finalized construction of the Command Post area – with all installations and security systems required. This makes JFTC a unique training facility within NATO where exercising headquarters can deploy elements of their Command Post structures and therefore train with systems and equipment they



would use in real operations. We are also expanding our office space to accommodate current and new staff members in order to increase JFTC's capacity up to 1000 workplaces, for both the training audience and exercise control staff at a time.

Two areas where JFTC is using training to implement transformation are STEADFAST PINNACLE and STEADFAST PYRAMID, and the NATO-Georgia JTEC Mentorship program. In STEADFAST PINNACLE and STEADFAST PYRAMID, of which JFTC will become ODE starting in 2018, SHAPE intends to use this high level staff training venue to rehearse new operational and strategic concepts, and harness the knowledge of senior leaders assigned to NATO. Mentoring the Georgian Joint Training and Evaluation Centre (JTEC) is a Partner Development mission that will improve the capability and capacity of the Georgian Training Centre and allow it to function within NATO Guidelines for future use by NATO members.

What do these changes mean for the Centre? Will its priorities change?

I would not say "change" – we will still be focusing on Resolute Support mission pre-deployment training. We will also continue testing, experimenting and building NATO's interoperability during CWIX. And additionally, we will stand ready and are fully prepared for new training needs defined by SACT, SACEUR and the outcome of the NATO Exercise Program Review, which is related to MJO training. These are the reasons JFTC is transforming and remains in close coordination with our higher headquarters, the Allied Command Transformation.

We are focused on two main areas – training and innovation. The JFTC transformation aims at reorganizing and thus enhancing our training capacity on one side. On the other, we are working on increasing our innovation abilities, including experimentation as well as capability development that will also support the Allied training. For example, the Battle Lab that is now being implemented at JFTC is a useful tool in conducting exercises and experimentation.

What the changes will bring, is JFTC's enhanced ability to act as Officer Directing Exercise for Multinational Brigade up to Joint Force Command level exercises, to fully support NCS/ NFS commanders in Collective Defence training, and development of new, innovative capabilities. Therefore, our current second and third priority will gain momentum. JFTC will be more capable – in terms of manpower, structure and infrastructure, while being flexible enough to provide ad hoc training and to respond to the needs of Commanders, and thus the Alliance.

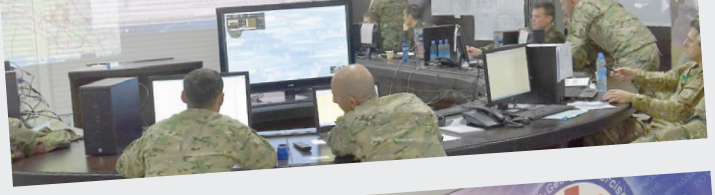
Big changes and significant development of capabilities and capacities will certainly result in a heavier workload for the Centre. How do you envision the upcoming months at JFTC?

These will be very intensive months. Developing our new structure, adjusting to a new reality will require a high level of flexibility, understanding and dedication from the staff. However, the people at JFTC are very committed and I am sure the transition will be smooth and successful. It will not be easy, but to achieve more we have to intensify our efforts. And we are ready for that.

Thanks to all the improvements, our support to the Alliance will be even more streamlined. We will be more efficient in responding to NATO's changing requirements. JFTC is a reliable, flexible training provider for NCS and NFS, and will become the primary location for Land Centric training. JFTC is a first class venue for training and will maintain a state-of-the-art platform for experimentation.

JFTC will remain at the very heart of NATO's training aspirations and transformation. As the importance of both training and testing will undoubtedly grow, JFTC will remain on the cutting edge of enhancing NATO's ability to defend the Alliance, deter adversaries and project stability. ■

Questions asked by
JFTC Public Affairs Office



NATO-Georgia Exercise

Another Milestone in the Development of Long-standing Military Cooperation

LTC Leon Soroko,
While preparing this article, the author was a member of JFTC Training Division

Introduction

In November 2016 Commander Joint Force Training Centre (JFTC), together with a substantial part of the JFTC staff, travelled down to Georgia in order to fulfil the role of the Officer Directing the Exercise (ODE) in the NATO-Georgia Exercise 2016, the first in a series of exercises to be held in Georgia with NATO- and partner nation participation.

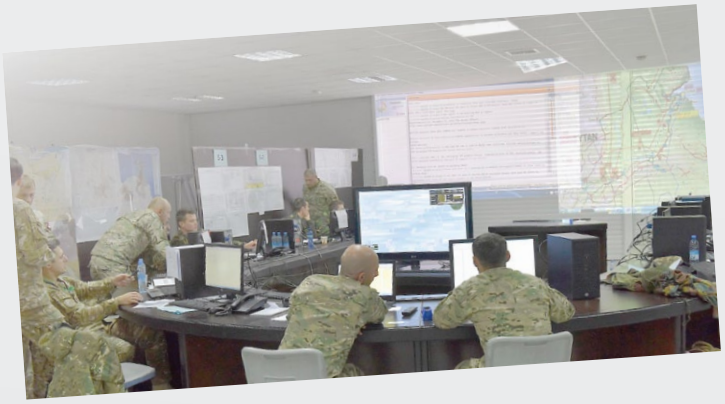
You might ask: "What does NATO have to do with leading an exercise in Georgia?", as these were the exact thoughts that came to my mind when I heard about this in the fall of 2015. However, after being appointed the Officer with Primary Responsibility (OPR) from the JFTC, I started to understand more of the background details. In this article I will try to explain to you some of the reasons behind it and will describe how we planned, prepared and executed this exercise. Furthermore, as this will not be a one-time event, I will try to lift a tip of the veil on possible future mentoring support from JFTC and the NATO-Georgia Exercises to come.

Background of the NATO – Georgia Exercise

At the Wales Summit in September 2014, a substantial package of measures was launched to strengthen Georgia's ability to defend itself and advance its preparations for membership. Further steps to intensify cooperation to help strengthen Georgia's defence capabilities, interoperability and resilience capabilities were taken at the NATO Summit in Warsaw in July 2016[1].

A number of pillars have been identified within the Substantial NATO Georgia Package (SNGP), ranging from Defence Planning to Military Police capabilities and from STRATCOM to aviation development.

One of the pillars of defence capabilities and interoperability is the strengthening of the Joint Training and Evaluation Centre (JTEC), which provides a full range of training for the Georgian



armed forces, from section level life fire training up to Brigade level Command Post training. They are currently mentored and advised by a team of advisors mainly from the Nordic and Baltic States, Germany and the United Kingdom.

In order for the JTEC to become ready for taking on the full responsibility for exercise planning, preparation and execution of a NATO exercise in the future, the NATO-Georgia series of exercises have been created as a vehicle to achieve this.

Initial ideas for JFTCs' involvement took shape during a visit of JFTC's DCOM/COS to the exercise Agile Spirit in Georgia in the summer of 2015. Agile Spirit is an annually held US-led exercise with participation of Georgian-, NATO- and other Partner Nations units and staffs. It is executed in the Krtsanisi Training Facilities (KTF) approximately 40 kilometres south of Tbilisi, Georgia. What started out as a few JFTC members supporting the existing Georgian team with advice and remote support turned into a full blown ODE role. This included scenario development, MEL/MIL development and scripting and manning of the key EXCON positions during the execution phase, raising the JFTC participation during this particular exercise up to 38 staff members from across all divisions.

I will describe some of the key aspects of the exercise below.

Exercise Specifications[2]

Exercise Aims

The aim of the exercise was two-fold: First: 'To educate and train the Georgian General Staff in the NATO Exercise Planning Process' and second: 'To train a Multinational Brigade Headquarters in planning and conducting a Non-Article 5 Crisis Response Operation'. I.e. the actual conduct of the exercise was the ultimate vehicle to go through the process of Exercise Planning within a NATO environment where Georgian General Staff was fulfilling the role of the Officer Conducting the Exercise (OCE).

Land Command Izmir (LC) was assigned the role of mentor for the OCE. In order to guide the OCE Core Planning Team (CPT) along the path of processes, procedures and milestones of the Exercise Planning Process as described in the Bi-SC 75-3, a team from LC G-7 went regularly to Georgia to prepare the CPT members for the various meetings and assisted them with the creation of the required inputs for these meetings and to develop the necessary planning guidance and products.

The JFTC as the Officer Directing the Exercise (ODE) was tasked to support the OCE where required.

Exercise Objectives

Besides training the Georgian General Staff on the NATO Exercise Planning Process there were several other objectives to be achieved by executing this exercise. These were:

a. Improving GAF interoperability in Command and Control as well as utilizing GEO simulation capabilities;
b. To practice coordination and liaison with IOs/GOs/NGOs and
c. To promote Strategic Communications (STRATCOM) visibility for Georgia as a Defence Capacity Building and Enhanced Opportunities Partner.

Stake holders and participants

Allied Command Transformation (ACT) sponsored this exercise whereby SACT acted as the Officer Scheduling the Exercise (OSE). As such ACT was responsible for several important processes within the exercise planning process, of which Exercise Budget Holder, LEGAD support for the Technical Arrangements, STRATCOM planning and execution and DV-Day organisation are just a few examples. The NATO Liaison Office in Tbilisi and the permanently posted members of the SNGP team in country were also a big help during the setup and execution of the exercise. Their local knowledge, contacts and Subject Matter Expertise in several areas diminished the need to organise additional SMEs from other NATO institutions.

Planning

Already during the development of the Exercise Specifications (EXSPEC) it was clear that the normal exercise planning timeline of 18 months would not be achievable. From the start of the exercise planning until start execution there were only 10 months left. Furthermore, as we were planning for an ad-hoc Multinational Brigade Headquarters, comprised of a core Georgian Brigade Headquarters augmented with multinational participation and Georgian armed forces representatives, we assessed we could only bring the full HQ staff together once. We therefore needed to relocate some of the milestones, which need to take place before exercise execution, into the execution part of the exercise. Key leader training (KLT), Battle Staff Training (BST) and Crisis Response Planning (CRP) were

all executed in Georgia at the front end of the actual execution, i.e. phase III-B.

Preparation

All of the Exercise Planning conferences (Initial Planning C, MPC, FCC and CPTMs to prepare these) were held in Georgia, which required extensive travel for some members of the JFTC team. It gave us a good opportunity to assess the facilities in use and to make recommendations for future developments. The MEL/MIL scripting week however was held at the JFTC due to the available CIS infrastructure and the ability to use the NATO FASs in Georgia.

We decided to use the CERASIA Scenario and modify it to the needs of a Non-Article 5 Crisis Response Operation for a MN Brigade in a NATO environment.

Execution

Participants

As mentioned before the Multinational Brigade Headquarters (MNB HQ) was the Primary Training Audience and consisted of 80 Personnel. The Brigade Commander was LTC Khvichia, who is the Commander of the 4th Brigade in Vaziani. He brought along a portion of his own brigade HQ and was augmented with personnel from within the GEO Armed Forces as well as Multinational participants. In total 28 officers and NCOs from BEL, BGR, HUN, LTU, LVA, NLD, ROU, SVN, TUR and UKR worked in the Headquarters.

Preparation

Preparation started already on 2 November, when the advance party of JFTC Protocol, Real Life Support, CIS and NCIA arrived in the Krtsanisi Training Area. All the infrastructure for Training Audience (TA), EXCON and Exercise Support were set-up, networks prepared and installed and the Functional systems and connectivity tested. Most of the EXCON arrived on Tuesday 6 November, when we started with EXCON preparation and training.

Exercise Conduct

Training Audience in-processing was executed on 9 November and on Thursday 10 November we started in the Vaziani Barracks with the required security, real life support and exercise in-briefs, followed by the opening ceremony and an ice breaker for all.

Training Audience Key leaders received their first training on 11 November. It covered a short introduction to start off with, as it was the first time the key leaders actually met. Furthermore presentations and discussions on the MDPM in general, the scenario in depth, the IPB delivery by the Bde S2 and information dissemination on Legal aspects and cooperation with IOs/ GOs/NGOs prepared them for the next step in the conduct of the exercise, which was the Crisis Response Planning phase.

For three days the newly formed Bde HQ planned the lay-down of the forces in country, looked at several tasks already given to them by the Higher Commanders Headquarters, played by LANDCOM and gave orders to their sub-units. In the same time the sub-units, represented in LOCON and other players prepared themselves during the continuation of the EXCON preparation and training. Scripting was finalized and CAX Startex parameters and locations generated.

In order to bring the Headquarters up to speed for the execution phase of the operation, a one-day session of Battle Staff Training was scheduled just before Startex. This gave the Brigadede Commander and Chief of Staff ample opportunity to give direction and guidance to the newly formed staff on how the information flow should be optimized and coordination achieved across the headquarters.

Exercise play lasted three and a half days, in which several major incidents were played, battle rhythm events and working groups respectively boards were held and handover briefs were delivered. Media and STRATCOM played a major role as well as the interaction with international organisations and role-players from the host nation, creating a Comprehensive Environment in which a unit conducting a Crisis Response Operation needs to operate.

On day 3 of the execution phase (Thursday 17 November) ACT organised a well-visited DV Day, where approximately 140 guests were hosted, amongst others the President, several ministers and the CHOD of Georgia, CHODs from various NATO countries, a host of ambassadors and defence attaches accredited to Georgia and many dignitaries from the political, civilian and military society in Georgia.

After Action Review

The after action review on the last day of the exercise focused on three separate parts: firstly the achievement of the training objectives and the overall lessons learned for exercise preparation, setup and execution. The second part analysed the Multinational Brigade performance and gave advice on improvements regarding processes and standing operating procedures. The last part was conducted with limited participation and focused on providing feedback on NATO-GEO JTEC facilities and capabilities, future mentoring and the next iteration of the NATO-Georgia Exercise. All output was captured and discussed during the Post Exercise discussion, conducted two months after the exercise.

Support

Every exercise we execute requires extensive support from NCS/ NFS entities and other organisations. The NATO-GEO Exercise was not different in this respect. I will only mention major players who supported us during the preparation and execution of the exercise, with the risk of forgetting some other important players. For EXCON augmentation we were supported by LANDCOM personnel for depicting the Higher Commanders' Headquarters (HICON). The Joint Multinational Simulation Centre from the USAREUR filled positions in the Training Team and the Observer/Analyst Team, supporting us with knowledge and

know-how on Brigade Level Exercises.

The CMDR COE and MP COE assisted with specialists required for running a Crisis Response Operation and for the interaction with the IOs/GO/NGOs. We were able to secure participation from UN OCHA, Save the Children and ICRC during the preparation and execution phase, which was favourable to build understanding within the MNB HQ regarding the aspect of operating in a Comprehensive Environment.

We were reinforced by a delegation of US NAVY Reservists from the Chicago Detachment, which took on several demanding supporting roles within the EXCON structure. Furthermore, Slovenia and the UK provided LOCON cells on Battalion Level to create realism during the execution phase and last but not least, the Georgian Armed Forces provided multiple shadow EXCON members in order to train these personnel for future exercises.

Commander JFTC, MG Grün, was the Exercise Director and he shared this responsibility with Col Chelidze, Commander NATO-GEO JTEC. JFTC personnel filled most of the key positions in EXCON and the structure was augmented through individual participation of several NATO and Partner Nation members. The total amount of personnel within the EXCON structure was 173, which included all functionalities like Security, RLS, Protocol, Media, Cyber Defence, Information Security, STRATCOM, etc.

Challenges

A new concept executed outside of the headquarters always brings challenges along in planning, preparation and execution. Most of them were a result of a shortened timeline for preparation and were already mentioned somewhere in this article, but I would like to mention a couple of them separately:

a. Building up the CIS environment: We shipped servers, routers and switches, laptops and other equipment to Georgia and integrated them within the existing infrastructure at the JTEC. Thanks to the hard work and support of NCIA and JFTC technicians we were able to create a stable environment in which the core services, the MEL/MIL and CAX were able to operate, a Common Operational Picture could be displayed and other systems functioned;
b. High Visibility: As this was the first of its kind, the NATO-GEO Exercise attracted much attention from local, regional and NATO entities and required a robust STRATCOM organisation to cover all. ACT was ultimately responsible for the planning and execution of the DV-day which was well visited and thoroughly executed;
c. Facilities: Although the NATO-GEO JTEC has been up and running for a longer period of time now and infrastructure is generally sufficient to run the execution phase of a Brigade size exercise, it lacks the resources to have classes, training and FAS-instruction at the same time. Therefore, if preparation time allows, the BST, KLT and FAS training part should be separated from the execution part;
d. Multinational participation: It was difficult to attract NATO and Partner Nation Participation within the Training Audience and EXCON cells. This was partly due to the limited timeframe available to announce the exercise and resulted in late announcement of participation. This in turn did not allow informing all participants on the scenario, the latest developments and the requirements.

Conclusions

The NATO-Georgia Exercise 2016 was a success in all respects. The Georgian General Staff was guided through the complex labyrinth of the NATO Exercise Planning process, executing each step themselves and producing all the required documentation including the Exercise Planning Guidance and a full-fledged Exercise Plan. The Multinational Brigade HQ proved that with limited preparation time, multinational staff officers could be integrated within a Georgian framework brigade and function well as a staff, planning and conducting operations. Furthermore JTEC personnel have been involved in the planning, preparation and execution of the exercise and will soon start planning the next iteration of the NATO- Georgia Exercise.

Future

NATO-Georgia Exercise 2019 and Onwards

As mentioned in the introduction, the NATO-Georgia Exercise 2016 was not a one-time show, but was a part of a series of exercises. During and after the exercise lots of discussions have been held and current status is that the next exercise will take place in spring 2019. During the next iteration JTEC will take on the role of the Officer Directing the Exercise, which reduces JFTC role to mentoring, advising and assisting where needed. This gives the NATO-GEO JTEC the opportunity to gather the right people, prepare them for their roles and start the Exercise Planning Process for the NATO-GEO Exercise 2019. JFTC will help them along the way, advising them where needed and assisting them with the necessary entry points within the NATO structure in order to facilitate a smooth preparation.

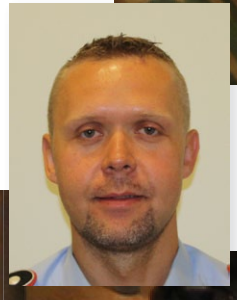
Mentoring the JTEC

Currently JFTC is working on the Mentor Plan 2017 – 2020 in order to assist in developing enduring exercise planning and exercise delivery capacities within the NATO-GEO JTEC. ■

[1] Source: NATO Website (http://www.nato.int/cps/en/natohq/topics_38988.htm#)
[2] ACT Exercise Specification NATO – GEORGIA Exercise 2016 dated 13 July 2016.

Remaining Focused on Afghanistan

Resolute Support Training Maintains Its Momentum



LTC Lars Zacharias,
JFTC Training Division

Welcome to 1396

Afghanistan. Welcome to 1396. Almost 16 years of NATO mission history. What have we achieved? Where did we succeed? Where did we fail?

From 25 January to 3 February 2017, 223 participants from 22 contributing nations joined the Resolute Support (RS) Training Event (TE) 17-1, the first in a series of four RS TEs in 2017 at JFTC. Bearing in mind similar questions as mentioned above, the whole training audience was listening to the opening remarks given personally by the Chief of Staff RS, Lieutenant General Juergen Weigt. He drew a broad picture of the western engagement over the last decades, pointed out achievements, illustrated challenges and designed the way ahead up to 2020. No more, no less. He described the year 2016 (1395 according to the Solar Hijri Calendar, which is the official calendar in the Islamic Republic of Afghanistan) as equilibrium, as a year of survival for the Government of the Islamic Republic of Afghanistan (GIRoA) in fighting against a multiple layered insurgency. He explained the concept of the RS mission and shared the RS vision of a 2020 desired end state; how to enable the Afghans to provide a sufficient level of security by themselves.

This essay will follow his analysis and illustrate the importance of a continuous focus on a dedicated pre-deployment training prior to each individual RS deployment. In a nutshell: the Resolute Support Mission (RSM) is an advisory mission and without well prepared advisors, it will not be successful.

Afghanistan: Achievements and Challenges

Afghanistan is a multi-ethnic country with a complex and dynamic mix of cultures, still far away from peace and stability. Corruption, violence and organized crime structures are only examples of a wide spread variety of risks and problems which the local authorities are facing on a daily basis. A multi-layered insurgency is hampering the efforts of the international community as well as the field work of local, regional and international aid organizations. The Taliban are operating from the Pashtun areas in the South and East, expanding especially into the area of Kunduz. People are disappointed about the slowly progressing development process and afraid of the so called "strong foreign cultural influence", especially in rural areas. Outside Kabul and larger cities, traditional power structures are unbroken.

Nevertheless, there are indicators of progress. During the last 15 years the life expectancy has increased by 20 years, and today more than 60% of the Afghan population has access to clean water and one of the 2,200 healthcare facilities. The number of students in public schools has increased by a factor of 10, up to 9 million today, and the literacy rate has reached 38% instead of 9% in 2001. All over the country 175,000 students are enrolled in universities. These are still poor numbers, no doubt, but compared to the 2001 situation it shows tremendous efforts of the international community in nation building.

The problem is that nation building does not follow a short term approach; it requires a long term guided process. Nation building does not last months or years; it lasts generations and mindsets. A 10-year-old child from 2001 will enter public services by 2010, and will become effective by achieving their first leadership positions by 2020 at the earliest. For the senior leadership positions this timeline is 2030 and beyond. We have reached equilibrium indeed, a turning point in Afghan history, where a new and independently educated generation is stepping in, but there is no alternative than to sustain the engagement until achieving self-sustainability. The baseline for any further effort is a safe and secure environment.

Looking back at European history, Germany seems to be the best example for a long term nation building process. After the Second World War it took 15 years to initially set up new security forces, and almost 25 years to become self-sustainable. When joining NATO in 1956, German chancellor Adenauer was asked if the senior leadership of the new armed forces would recruit out of the same personnel who were in engaged in the World War before. His answer was of simple logic: "I don't believe NATO will accept 18-year-old Generals." Finally, the presence of International Security Forces in Germany ended after 49 years in 1994.

NATO Resolute Support Mission

Key factors for Afghan self-sustainability are effective and self-sustainable Afghan Security Forces, which can provide a safe, secure and stable environment. Without this essential precondition any further development efforts will be at risk of failure. Therefore the core principle of the NATO Resolute Support Mission (RSM) is to Train, Advise and Assist (TAA) the Afghan National Defense and Security Forces (ANDSF). RSM follows the Security Force Assistance (SFA) concept in order to mature the systems, processes, and institutions that are required to sustain a modern army and police force. Coalition advisors conduct "Functionally Based Security Force Assistance" to develop Afghan Security Institutions' capacity to fulfill their tasks properly and ensure long term sustainability. All coalition efforts have to be aligned with Afghan efforts; this remains the key to success.

But what does this mean in practice? "Functionally based" describes the shifting of the emphasis of advising from a unit-based approach, as conducted during the former ISAF mission at Battalion and Brigade levels, to advising along eight Essential Functions (EF), which are identified as critical for achieving sustainability throughout all levels of command. These functions are interdependent, they span across all levels of government and defense, from the lowest tactical to the highest strategic level. Each EF is vertically oriented and contains a variety of processes and procedures. Coalition advisors focus on enabling their Afghan counterparts on all levels to solve their problems within their own domain, within their own means and capabilities. The focus is to understand and engage the Afghan information flow and ensure the interaction from the executive and strategic level (Ministry of Interior, Ministry of Defense) down through the operational

levels (Police Zone Headquarters, Army Corps Commands) to the operating forces (field units) and back up the chain again.

In fact, advising is the main effort of RSM. In a daily work, every advisor will face multiple challenges out of all defined EFs. Therefore, a particular part of the staff on RS HQ level as well as on Train Advise and Assist Command (TAAC) levels is appointed as specialists to each EF. These staff officers are responsible for vertical integration, horizontal coordination, analysis and synchronization of the information process issues within their EF. Their main task is to identify key friction points in a particular Afghan system in order to coordinate influencing efforts. This analysis is a foundation for the daily advisory work. The advisors coordinate with all EFs on a regular basis and set up their advisory efforts along the identified key issues, to encourage their advisees to find their own solutions to their challenges. A well-organized framework of interaction between EF staff and advisors is essential for the success of RSM. Enabling a determined advising effort remains the key task for all RS personnel.

The Resolute Support Pre-Deployment Training Program

Having a clear understanding of RSM, JFTC delivers a pre-deployment training program which is tailored to meet the specific requirements of the Training Audience (TA). The main effort of RS TE's is to educate the TA in the specifics of the mission, to train personnel who are filling advisory and/or command and control positions within RS as well as the personnel assigned to advisor roles and create conditions for team building within and between both TA groups. Although it is initially designed for RS HQ requirements, personnel assigned to other coalition agencies and commands in Afghanistan are also invited. It has to be clearly pointed out that RS TEs are not designed to provide "on-the-job training" for advisors and EF staff. The focus remains on ensuring a common understanding of Train, Advise

and Assist (TAA) in the framework of the Functionally Based Security Force Assistance concept of operations. The TA should become familiar with the operational environment and understand their roles within the RSM framework. Therefore JFTC is only simulating the mission environment. In case of a TAAC participation, which represents the tactical level of RSM, an additional aim for this TA group is to build up capable, confident and cohesive staff and advisory teams in order to enable the TAAC to carry out its mission.

Major General Thorsten Poschwatta, the Deputy Commander of the Bundeswehr Joint Forces Operations Command (BwJFOCOM), who welcomed the participants during the opening ceremony for RS TE 17-1, underlined exceptional value of events tailored this way: "The Resolute Support Training Event 17-1 – bringing together future members of the RS Headquarters, TAAC-North Headquarters and various advisory teams – is a unique opportunity for a common, yet individually shaped training throughout all tiers of the mission to create mutual understanding for each other and form a team."

JFTC usually conducts four RS TEs per year in the role of Officer Directing the Exercise (ODE), which means it is the provider of the training. Before this article was completed, in total three 2017 RS TEs had been conducted. The requesting authority is Allied Joint Force Command Brunssum (JFCBS), which covers the role of the Officer Scheduling the Exercise (OSE) and the Officer Conducting the Exercise (OCE). Usually during two of four TEs per year, personnel of the German led TAAC-North join the training as well and the BwJFOCOM takes the role as a co-OCE. In 2016 the number of trainees was approximately 80 for each of the even-numbered TE's and 220 for the ones with TAAC-North participation. The number of the first 2017 even-numbered TE (17-2) increased to approximately 120 due to the participation of personnel of the Italian led TAAC-West.

What does a RS TE at JFTC look like? Every RS TE is a multi-modal training event which consists of two main parts: an academic phase (Mission Specific Training, MST); followed by a practical phase which includes Battle Staff Training (BST), and a Mission Rehearsal Exercise (MRE) for TAAC level TA. During the academics phase JFTC provides introductory briefings, lectures, panel discussions and Functional Systems Training for all TA. During the practical phase the staff receives training based on stand-alone and cross-functional vignettes which are snapshots of practical working situations in theatre. Different groups of TA are combined and work on RS-related issues together through pre-scripted vignettes as well as self-prepared working groups and boards. During this phase, selected HQ RS personnel receive specific function-related training at JFCBS.

To achieve these objectives and be able to provide the most up-to-date training framework, it remains crucial that JFTC receives support from Subject Matter Experts (SMEs). SMEs are NATO personnel or civil experts who have relevant theater and/or mission experience; ideally they are recently redeployed from mission or directly join the TE out of theatre. JFTC's training concept incorporates this expertise and to enhance realism it is augmented further by the participation of leaders from the ANDSF. Additionally JFTC staff visits theatre during every TE preparation phase.

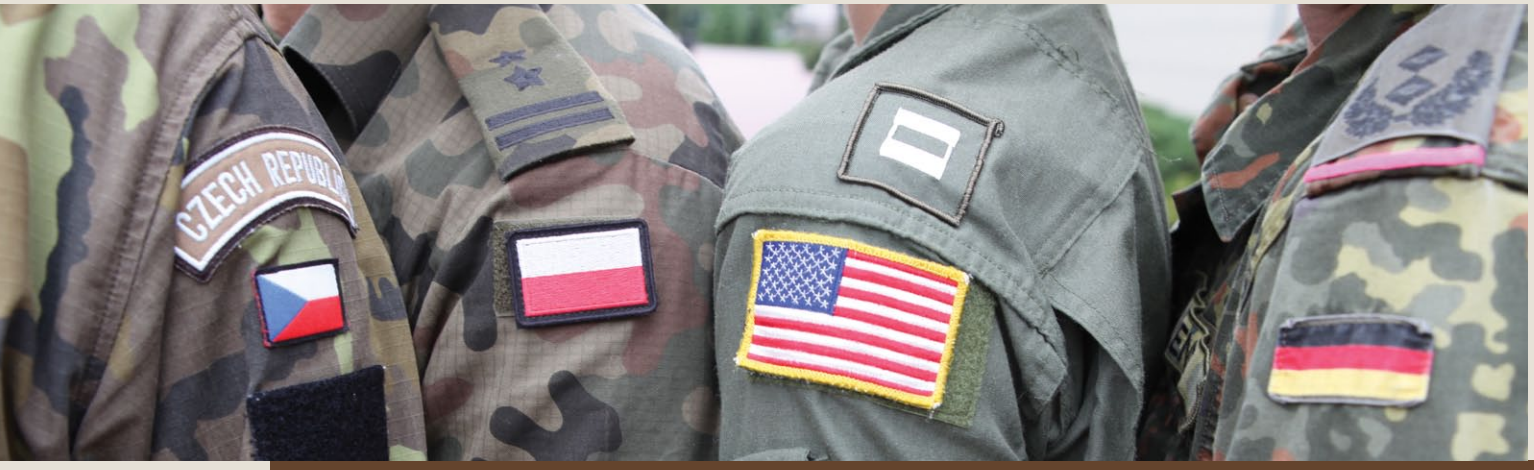
Blueprint or Snapshot? The Resolute Support Training Events in 2017 and the way ahead

After TE execution is before TE execution – conducting this kind of full scale training four times a year might spread the impression that RS TEs are a routine job at JFTC. In fact, usually every RS TE is based on its previous iterations, and almost 75% of the content remains the same. But the mission still evolves, and due to a dynamic mission environment about 25% of the content has to be adjusted for every subsequent TE. Attending an RS TE within a time difference of 18-24 months, a participant would experience a lot of changes in staff procedures and current mission related topics. In any case the expectations of the TA are quite high: the training should be up-to-date in order to prepare for the upcoming deployment; and, it should provide good knowledge about procedures and processes at the respective levels of command as well as introduce specific tasks related to individual positions. Therefore a continuous review of all TE content remains mandatory.

Like all the previous RS TEs, the 2017 events are a mix of both standardized training and unique event, blueprint and snapshot. The beating heart is the RSM, and the rhythm of its heartbeat is the rhythm of RS TEs. Any pre-deployment training has to follow reality, there is no way to practice the other way around. Future TEs will have to follow the same approach. Professionalism and passion are defining the identity of JFTC in conducting each single TE. Regardless of rapidly changing conditions, the quality of pre-deployment training will remain as the standard achieved in 2017.

The Resolute Support Mission Pre-Deployment Training remains JFTC's priority. With the recently conducted event of this type, JFTC underlined its unique position with regards to NATO current mission preparation training within the NATO training landscape. Nevertheless, JFTC stands ready for future adjustments and therefore continuously monitors the transition planning to a post-RS engagement by the Alliance. The current training design can be easily converted to support any mission adjustment. However, the main guidelines for a future NATO engagement in Afghanistan are still to be defined. Besides that, until the end of 2018 four RS TEs per year are pre-booked on the JFTC Program of Work.

Lieutenant General Erich Pfeffer, Commander of the Bundeswehr Joint Forces Operations Command summarized the RS TE during his address to the TA with the following words: "In recent days you have received a picture of your future tasks in Afghanistan. It was presented as realistically as possible. You are well prepared now. Thanks to this, as soon as you set your foot in Afghanistan, you will be able to quickly start your mission." ■



Test Your Capabilities and Get Ready for the Future to Keep Our Nations Safe

CWIX 2017

LTCDR Hubert Winiczenko,
JFTC Training Division

New technologies bring considerable changes and new opportunities for the global society. They definitely influence the way the future multi-domain battlefield will look like (e.g., increased speed of exchange of information, use of big data or even Artificial Intelligence to assist decision making process, activities in the cyber domain impacting physical domain). Looking ahead it seems that conventional military aggression against the Alliance or its members is unlikely but not impossible. The most probable threats for the Allies are rather unconventional. Among the possibilities of attacks by international terrorist groups, use of soldiers without insignia dubbed "little green men", or information activities that seek to change perception of reality, cyber-attacks of varying degrees of severity are more and more frequent. Whenever we face a military strategy that combines conventional warfare (employing a military Instrument of Power (IOP) of a modern state, economic, informational, and diplomatic IOPs) together with irregular warfare and cyberwarfare - the so called hybrid warfare, the implications for NATO preparedness and readiness are obvious. They include the definition of security, its strategy for deterrence (or "hybrid deterrence" as General Sir Adrian Bradshaw, the former Deputy Supreme Allied Commander Europe called it), its need for a military transformation, its ability to make decisions rapidly, and its reliance for help on countries and organizations from outside the Alliance. So are we ready for the emerging threats and capable of facing them?

CWIX – the event to test your capabilities

Every year, NATO Allies and Partners have an opportunity to check it.

They test their capabilities during the annual Coalition Warrior Interoperability, eXploration, eXperimentation, eXamination, eXercise (CWIX). The last event of this kind took place between 12 and 29 June 2017 at the Joint Force Training Centre (JFTC) in Bydgoszcz, Poland.

CWIX takes interoperability and readiness as the foundation for all NATO operations as they allow forces to deploy together, be effective from the very beginning of the operation and communicate as one cohesive force synchronizing activities towards common objectives. The 2017 event was another edition of this largest annual NATO-approved interoperability event which provides active support for the Readiness Action Plan (RAP), the Federated Mission Networking (FMN), the Smart Defense and Connected Forces Initiative (CFI). Again, CWIX showcased interoperability testing and FMN confirmation of current specifications supporting NATO Education Training Exercise and Evaluation (ETEE) and interoperability certification. It validated and verified Communications and Information Systems (CIS) for achieving combat readiness of the NATO Response Force (NRF), Very High Readiness Joint Task Force (VJTF), followed by the Steadfast Cobalt 2017, Trident Joust/ Juncture 2017 or conducted at the level of a Major Joint Operation "Plus" (MJO+) - Trident Javelin 2017 exercises. Cyber interoperability supporting cyberspace as a domain (recognized by NATO a 'domain of operations' at the Warsaw Summit in 2016) was an important aspect of CWIX 2017.

The main execution site for CWIX was JFTC. The Centre was additionally connected with several distributed locations in Europe and North America via the Combined Federated Battle Laboratories Network - the so called CFBLNet. CFBLNet enables nations to work together in all areas of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR).

CWIX is the only NATO-led interoperability event that involves the NATO Enterprise, NATO Agencies and other organizations, NATO and Partner Nations, NATO Centres of Excellence and International Organizations such as the European Union. This year, within a really large family of experts, including more than 1000 representing 88 commands from 26 NATO and Partner Nations, the participants tested military capabilities to enhance and improve technical interoperability of Communication Information Systems (CIS) through exchange of ideas and brainstorming new ones. Coming to JFTC for CWIX was an excellent chance to practically apply and test NATO standards and procedures before undertaking NRF validation and certification to actually de-risk CIS. The exercise also allowed to increase overall performance of the Alliance and Partners in response to the likely future threats.

CWIX testing as an important component of capability development lifecycle

There were 16 Focus Areas (FAs) and 8 Working Groups (WGs) during CWIX through which test cases were prepared, coordinated and executed. For example the Operational Command (OP COMD) FA was the coordination point for all Joint/ Operational level capabilities. One of its aims was to provide an operational background and drive for the execution of vignettes and test cases. The OP COMD FA in close coordination with the Joint Vignette Coordination Working Group (JVC WG) built up and managed a fictitious joint scenario to provide an operational background to the interoperability testing activities. The scenario established flow of communication and operational data between the OP COMD FA acting as the deployed Joint HQ and the FAs as Component Commands (CCs). This testing platform allowed capability developers to take risks that can be introduced within a controlled environment to further mature capabilities and improve future

readiness and prepare the Alliance to meet the emerging challenges without fear.

Cyber defense - resilience of NATO and national networks

There have already been cyber-attacks against NATO systems and they are increasingly sophisticated and damaging in an evolving and complex threat environment. NATO Secretary-General Jens Stoltenberg has said that there were 500 dangerous cyberattacks on NATO facilities every month in 2016. The figure represents a 60-percent increase as compared with the previous year. We have to bear in mind that the risk of a large-scale attack on NATO's C2 systems could lead to consultations under Article 4 or possibly even to collective defense measures under Article 5. The most intriguing aspect of our era is that events in one part of the world are far more likely than in the past to have repercussions elsewhere while the attribution of a cyber-attack is difficult.

Effective cyber defense requires Allies to yet better cooperate to fight against unconventional threats such as cyber-attacks in order to improve their capabilities to prevent and recover from the attacks. Improving resilience of computer networks can have a "deterrent-by-resilience" effect dissuading possible attackers by demonstration of the futility of their approaches. CWIX encourages Partner participation, building capacity and forms multinational solutions to common security concerns. Partner and non-NATO nations are force multipliers in NATO operations when they are fully interoperable with NATO forces. Therefore CWIX is also seen as an avenue to improve the resilience of NATO and national networks and capabilities for current and future NATO operations through collaboration and exercising on an artificial scenario with fictitious cyber threats that reflect real ones.

Through exchange of best practices, information sharing and international cooperation CWIX is the right place to raise awareness about the effective cyber defense and practically test the Allies' and Partners' cyber capabilities.

Interoperability and readiness – two core pillars of the Alliance success

NATO's Comprehensive Political Guidance "requires Allies to continue the process of transformation, including conceptual and organizational agility and the development of robust capabilities that are deployable, sustainable, interoperable, and usable." Without doubt the Alliance will face a range of security challenges and threats in the future. To respond to them military forces from different countries and services must assemble rapidly and act fast across all domains in order to achieve common goals. Therefore NATO military forces should grow more interoperable and agile to apply dynamic operational principles and be supported with critical elements for success on the future battlefield. Interoperability in this case means that different information systems will be able to communicate effectively across our formations at different echelons of command.

Conclusion

Safety of our nations depends, among many factors, on our readiness to react to future challenges. To react swiftly and successfully we need to practice and stress procedures, protocols, and compatibility of our IT systems by identifying and resolving interoperability gaps. The sooner we find possible solutions the better we will execute future exercises and operations. NATO has been engaged in continuous transformation for many years to ensure that it has policies, capabilities, and structures required in the changing international security environment, to deal with current and future challenges. That is why every year we meet and work together at the Coalition Warrior Interoperability, eXploration, eXperimentation, eXamination, eXercise, proving that one NATO is stronger than the sum of its parts. ■

Distinguished Guests Explored CWIX

NATO Deputy Secretary General, Rose Gottemoeller, Polish Undersecretary of State in the Ministry of National Defence, Tomasz Szatkowski, NATO Supreme Allied Commander Transformation, General Denis Mercier, NATO Deputy Chairman of the Military Committee, Lieutenant General Steven M. Shepro, and NATO Commander Joint Force Training Centre, Major General Wilhelm Grün, welcomed NATO's leading political and military bodies, the North Atlantic Council and the Military Committee, to the Coalition Warrior Interoperability Exercise (CWIX) on June 22nd to discuss NATO's continuous adaptation in a complex international security environment.

"All 29 Allies – and many more partners around the world – need to be able to operate seamlessly across a wide spectrum of activities and missions. And the exercise will help us do exactly that."
- the Honourable Rose Gottemoeller, NATO's Deputy Secretary-General

"It is my strong belief that CWIX demonstrates NATO at its best. (…) The large number of participants from NATO bodies, Allied Nations and Partners underscores NATO's adaptation and transformation."
- Lieutenant General Steven M. Shepro, Deputy Chairman of the Military Committee

"By federating national security centres on a classified NATO network, employing the Cyber Range for preliminary testing – and it is the first time it has ever been done – the exchange of information can be made possible to improve our common defence as well as integrate cyber effects provided voluntarily by Nations."
- General Denis Mercier, Supreme Allied Commander Transformation

"As JFTC's main effort is training, we are really honoured that starting from 2011 we have also been the home for this biggest annual NATO interoperability event and thus played an even more active role in enhancing NATO's ability to defend the Alliance and project stability"
- Major General Wilhelm Grün, Commander of the Joint Force Training Centre

Innovation & Development of JFTC Infrastructure on the Road to the Corps Level Exercises

Mr. Jaroslav Barilla
JFTC Plans, Analysis and Programs Management Office

Instability and rapidly changing geopolitical situation are the main features of today's world. It forces NATO to cope with numerous challenges at all levels spanning from the strategic level, through operational and down to the tactical level. But there are also opportunities to be sized and utilized.

Threats to the NATO south flank, illegal migration, global terrorism, failing states, cyber warfare as well as threat to NATO political cohesion are just a few challenges that represent the top of "*the NATO iceberg of challenges*". NATO reacts to such situations by adapting and adjusting its strategies and policies. The Alliance's Strategic Concept sets the requirement that NATO carries out the necessary training, exercises, contingency planning and information exchange to assure defence against a full range of conventional and emerging security challenges. Inevitably, such situation affects the NATO training domain and requires the Alliance to deliver a proper capability to train its forces.

To cope with the above stated challenges and opportunities, and in order to provide platforms for the necessary training, NATO has to continuously invest into its training facilities, including JFTC and JWC. Based on the character and circumstances, there are numerous options how to address shortfalls spanning from the initiation of a standalone project, through addendum of the existing Capability Package (CP), the Urgent Requirements procedure or the NATO Security Investment Program Minor Works project.

The Minor Works Project

The main goal of the Minor Works Procedure is to serve as a simpler, faster, and less bureaucratic way to request and process an NSIP authorisation than through

the normal process. The purpose is to simplify procedures so that less effort is devoted to individual Minor Works projects leaving more time for managing higher value and more difficult projects. Therefore, the use of the Minor Works Procedure should result in an earlier satisfaction of military requirements, in avoidance of cost rises resulting from inflation, and in demonstration of responsiveness of NSIP to the needs, frequently of a Minor Works nature, of the many local site commanders and improved NSIP financial planning and implementation management. A Minor Work is defined as a discrete project, straightforward, self-standing, and completely usable, not a part of a currently proposed project.

The whole process starts with identification of shortfalls. Once we see that our capabilities or capacity do not meet the existing standards or requirements of supported HQ's, we conduct an internal analysis and risk assessment. In order to properly plan, coordinate and mitigate the impact of NSIP projects on the JFTC Program of Work, JFTC has established the NSIP project implementation and coordination team. Plans and Analysis and Program Management Section of the JFTC are in lead of the team in initiation and planning phases, while the Headquarters Support Division in execution/ construction phases of the projects.

From the technical point of view, it is critical for successful projects that the solution proposed is in accordance with the applicable "Criteria and Standards" (e.g. Peace Headquarters C&S) and the project meets the Minimum Military Requirements. In other words, the solution must not exceed the requirements and be cost-effective.

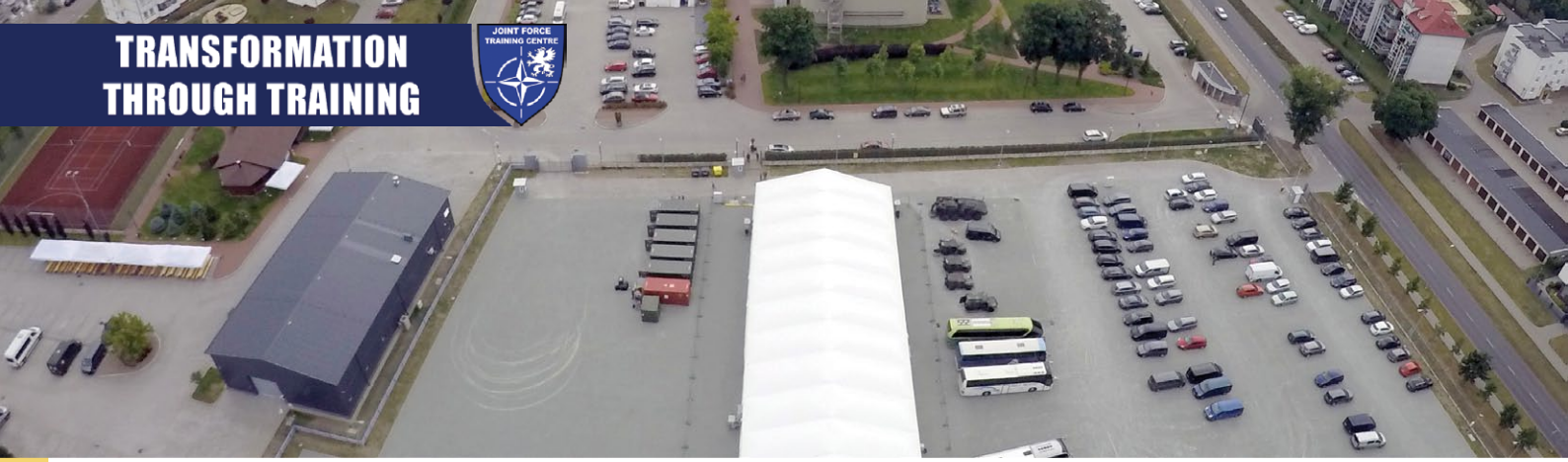
In the recent years, NATO authorities approved five NSIP Minor Works projects that would bring more than 3.6 million EUR of investments into JFTC infrastructure. In addition, we have initiated the sixth project – an upgrade of the JFTC security infrastructure, which is currently processed by the Host Nation (HN) POL NSIP Agency in Warsaw.

Overview of approved JFTC - NSIP Minor Work Projects:

Project	Scope
Training Area	Project provides supported HQ's with a unique opportunity to train in the configuration as they would fight. • *"Train as you fight"* • *"Plug and train"* • All weather surface, gravel • Power and CIS drop points • Access control.
Warehouse	Projects addresses shortfall of any internal JFTC storage capacity. • 600 m2 of general purpose storage capacity.
Temporary Office Space	Project addresses the shortfall of work space for permanent staff members. • Temporary container based office space for permanent staff members in security class II area configuration.
Patio Roofing	Project is supposed to protect patio from accumulating snow falls that cause static stress to the building. • Addresses Building 5 design shortfalls • Metal-glass construction
Audio / Video Displays Upgrade	Project is supposed to replace obsolete audio and video displays. • Increased resolution • Management of multiple sources of information

Overview of initiated JFTC - NSIP Minor Work Projects:

Project	Scope
Upgrade of Security Infrastructure	Project is supposed to replace obsolete Security infrastructure.



Capability package addendum

The scope of the minor works is limited by the total cost up to 1.5 M EUR for a single project. Therefore, the major infrastructure development projects must be addressed through the Capability Package Addendum.

Statistics of the exercises from the recent years clearly indicate that JFTC capacity delivered by the Capability Package is insufficient. We are more and more reliant on the capacity extension through the contracted tents. Lack of capacity is relevant to all categories of training support that we provide. It is the case of current operations support with Resolute Support pre-deployment training events, capability development events such as CWIX as well as future operations training support with NRF/ NCS/NFS training events such as Trident Joust or Citadel Bonus exercises. The 36th BiSC CP Board recognised this shortfall on 26 May 2016 and initiated Capability Package Addendum 1.

The road from the identification of the shortfalls to the mitigation solution in place is not a short one in case of the Minor Work Project, but is definitely more complicated when it comes to Capability Package Addendum (See Picture 1 and Picture 2). As of now, ACT in close cooperation with JFTC and JWC developed CP Addendum 1 for submission. Submission, however, is delayed due to Allied Command Operation proposal to synchronize CP Addendum with outcomes of the NATO Exercise Programme Review.

With the submission, CP Addendum enters the political level of screening, endorsement and approval. International Staff and International Military Staff screen the CP Addendum and produce the Joint Staff Screening Report. Further, the Joint Staff Screening Report must be endorsed by the Resource Policy Planning Board (RPPB) and the Military Committee (MC) where national representatives to RPPB and MC provide their national view's and inputs to the respective CP. If the outcome of screening and endorsement are positive, the North Atlantic Council (NAC) will approve the CP.

JFTC plans and expects to gain the NAC approval by the end of 2017. After that HN POL NSIP Agency will request for the Advanced Planning Funds for development of the Technical Feasibility Concept and the Project Cost Estimate. NATO Office of Resources will study the concept and if supportable, approve it.

The approval will initiate the phase when HN POL must develop the design of the project, select supervisors and contractors through bidding process. In our case, the plans indicate that the construction will not start before 2020 with completion in 2022.

JFTC CP Addendum 1 addresses the shortfalls in training workspace and CIS infrastructure in the following areas: Workspace for permanent staff; Workspace for training audience; Workspace for EXCON; Showers and changing rooms; CIS infrastructure.

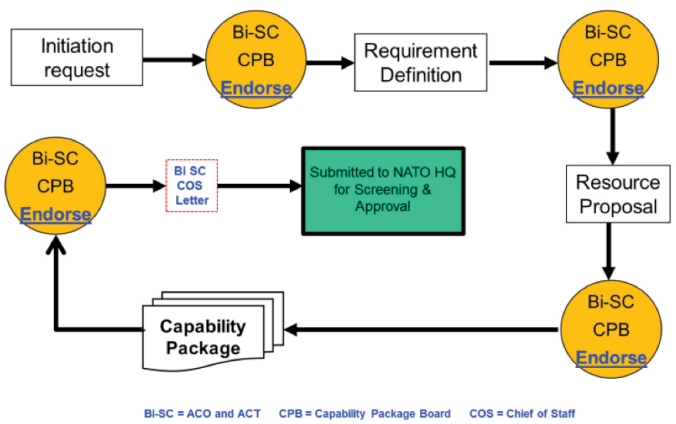
Conclusion

The main attributes of the future training programme are relevance, reliability, flexibility and sustainability within acceptable risk margins. The future JFTC training support capacity and capability must guarantee the above stated characteristics. Furthermore, our training support must meet rapidly changing demands and needs of NATO Command Structure and NATO Force Structure Headquarters.

The NSIP serves as a vehicle for the implementation of NATO military capabilities. JFTC NSIP Implementation and coordination team utilizes all available forms of investment into our infrastructure to meet the evolving training support requirements and to keep the facility competitive and "in the state-of-the-art".

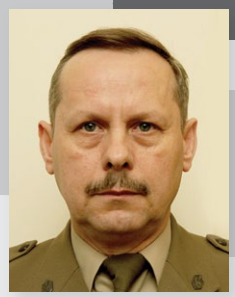
Since the process of the approval of the infrastructure investment is rather lengthy and complicated, early identification of the shortfalls, proper evaluation and risk assessment and immediate reaction are crucial preconditions for success. ■

NATO Capability Package Development



On the Way to Certification

JFTC Support to Citadel Bonus 2016 and Ultimate Sword 2016



LTC (ret.) Cezary Haracewiat
JFTC Training Division

In the 4th quarter of 2016 Joint Force Training Centre (JFTC) hosted two separate however very similar exercises. The first, known as Citadel Bonus 2016 (CIBS16), executed in the second half of November was conducted by the Rapid Reaction Corps – France (RRC-FR) with its headquarters located in Lille, France. The other one, named Ultimate Sword 2016 (ULSD16), was held in the first half of December and was executed by 1st German-Netherlands Corps (1GNC) with its command centre located in Münster, Germany.

Since both Headquarters (RRC-FR and 1GNC) were on their way to assuming the NATO Force Structure Joint Task Force Headquarters (NFS JTF HQ) role in 2017/2018, they had to be issued NATO certificates first. The certification process is a relatively long procedure, including a series of training events and exercises. It starts with an internal individual & collective training and finishes with a major NATO exercise. For both RRC-FR and 1 GNC the main certification exercise was the Trident Jaguar 2017 (TRJR17) executed in March/April 2017 at the Joint Warfare Centre (JWC) in Stavanger, Norway.

The CIBS16 and ULSD16, scheduled as two-level Command Post Exercises/ Computer Assisted Exercises (CPX/CAX), were RRC-FR and 1GNC's final Battle Staff Training events (BST). During exercises held at JFTC, both HQs demonstrated their capability to plan and conduct the Entry Phase of a NATO Smaller Joint Operations Land heavy (SJO-L) Non Article 5 Crisis Response Operation (NA5CRO) under direct command of SACEUR. That involved a joint and asymmetric complex military, civilian, deteriorating economically and politically failing state environment, focusing on initial combat operation (low intensity) and completion of force integration of a SJO in the framework of the Skolkan Scenario. The RRC-FR and 1GNC also practiced cooperation between Initial Command Element (ICE)

and their main HQs in home bases and support of their Joint Logistic Support Groups (JLSG) in planning and conducting Reception, Staging, Onward Movement and Integration (RSOMI), and theatre level logistics in backing JTF HQ (L) operations.

Although JFTC treats the CIBS16 and ULSD16 events as Phase III in exercise planning process for respective HQs, this was only one step on the way to attain the aforementioned NATO certification (Phase 1D from final TRJR 17 Exercise perspective).

Since both events aimed at the same, they had similar objectives:

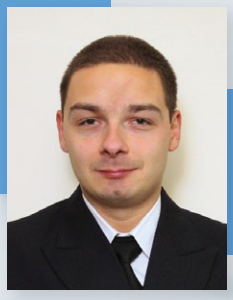
- Demonstrating HQs capability to plan for and conduct the Entry Phase of a NATO Smaller Joint Operation Land heavy (SJO-L);
- Serving as a platform for evaluation of HQ's deployability, Stratcom, Joint Logistic Support, Info-Knowledge Management and RSOMI;
- Facilitating Force/ EXCON initial integration and producing background information in preparation of TRJR CPX;
- Enhancing multinational interoperability in planning and conducting joint-combined operations with an extensive use of NATO LC2IS and FAS;
- Contributing to NATO visible presence in Poland.

Even though the commanders of RRC-FR and 1GNC were both Officers Scheduling the Exercise (OSE) and Officers Conducting the Exercise (OCE), there was a lot left for JFTC to support their training events. Apart from providing the HQs with the main venue for the exercise and the required hardware, our personnel provided them with real life support, particularly with accommodation, individual protocol assistance to each Flag Officer and visitor, transportation and catering. Around 400 participants took part in each of the training and they were supported by approximately 60 dedicated employees of JFTC.

Both exercises were based on the Skolkan 2.0 scenario -a fictitious area located in Scandinavia in northern Europe. It concentrated on several independent countries of the former Skolkan Empire: Arnland, Bothnia, Framland, Lindsey, Otso and Torrike that border NATO countries. Struggling with severe internal issues that may have had an impact on the whole region, Arnland requested NATO forces to provide security assistance. Responding to this official request and with diplomatic support of the United Nations (UN), NATO, as part of a global solution, has accepted to intervene in Arnland. The Arnland Security and Assistance Force (ASAF) mission's task was to help Arnland in resolving the above mentioned international issues and their root causes, and thus enable countering terrorism and organized crime and set the conditions for a secure and stable future in Northern Europe and the Skolkan Region particularly. ■

Cyber Tools in Hybrid Operations

International Law and Cyber Activities Below the Threshold of an Armed Attack



CDR Wiesław Goździewicz,
JFTC Legal Advisor

This article reflects the private views of the author and should not be considered as the official viewpoint of NATO, the Joint Force Training Centre of Polish Armed Forces.
The author would like to express his gratitude to Mr. Andres Muñoz Mosquera, SHAPE Legal Advisor, for sharing his invaluable comments and observations.

1. INTRODUCTION

Cyber tools have the potential, in particular under an economy of force situations, to be highly useful in achieving operational, strategic and political goals. However, if used malevolently, they may threaten regional or even global stability, security and prosperity, as recognised in the 2010 NATO's Strategic Concept[1], adopted during the Lisbon Summit. This is to a large extent caused by growing dependence of countries and private entities on electronic means of communications, entertainment, work, trade, etc.

The fast technological progress has not slipped the attention of NATO – in fact in the years following the Lisbon Summit, the Alliance's policy related to cyberspace has evolved in order to remain current in addressing new security challenges emanating from cyberspace.

In the Wales Summit Declaration[2] Allies declared that international law, to include the Law of Armed Conflict (LOAC), applies fully to cyberspace and actions conducted therein. Member Nations of the Alliance confirmed the possibility of a cyberattack to cross the threshold of an armed attack and thus become the basis for invoking Article 5 of the North Atlantic Treaty. It was reiterated that cyberthreats and attacks would continue to become more common, sophisticated, and potentially damaging. In Paragraph 72, the Alliance declared that:

"*Cyberattacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyberattack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.*"

In a Warsaw Summit Communique, Allies listed cyber threats among others, posed by military forces, terrorist groups and hybrid attacks. Referencing Wales Summit Declaration and reaffirming the commitment to consider cyber defence as a part of NATO's core task of collective defence, NATO recognised cyberspace as an operational domain and declared that the Alliance has to be capable of

operating both in and through cyberspace. Allies reaffirmed their "[…]*commitment to act in accordance with international law, including the UN Charter, international humanitarian law, and human rights law, as applicable[…]",declared to continue "[…]to follow the principle of restraint and support maintaining international peace, security, and stability in cyberspace and welcomed* "[…]*the work on voluntary international norms of responsible state behaviour and confidence-building measures regarding cyberspace*."[3]

During the Warsaw Summit, NATO adopted the Cyber Defence Pledge[4], which – among other provisions – contained confirmation by the Member Nations of their individual and collective responsibilities under Article 3 of the Washington Treaty, in particular in building cyber defence capabilities and strengthening the Alliance's resilience.

Throughout the text of the Warsaw Summit Communique[5], there is a number of instances where linkage is made between cyberattacks and hybrid threats, which should not be a surprise, given the reported (or alleged) use of cyber means in support of hybrid operations observed recently[6]. In one of my previous articles, I tried to address the matters of international law applicable to cyber warfare. This short article attempts to touch upon the issue of international law applicable to cyber actions falling short of armed attacks. In the first part of it, I will try to discuss how international law defines the use of force other than armed attacks, as well as which actions conducted by states or states' agents would be considered as use of force, but not armed attacks, in particular in the cyber arena.

The following part of this article will briefly discuss the principle of non-intervention, in particular in the context of the Nicaragua Case[7] and try to identify cyber activities that might be construed as in breach of the principle of non-intervention.

Fourth section will be dedicated to state responsibility for cyber operations amounting to forcible interventions into internal matters of another sovereign state in the light of the Draft Articles on Responsibility of States for Internationally Wrongful Acts[8].

Subsequently, the use of cyber tools in hybrid operations will be discussed, in particular how cyber actions are used to complicate attribution and blur responsibility.

2. USE OF FORCE OTHER THAN ARMED ATTACK

Article 2(4) of the Charter of the United Nations contains universal prohibition of the use or the threat of use of force. However, interpretation of the clause raised controversies from its very origins, in particular with regards to whether the phrase "use of force" was also meant as e.g. economic coercion[9]. The International Court of Justice (ICJ) ruling on Nicaragua Case has – nevertheless – provided highly useful insight on the meaning of the "use of force" in the context of Article 2(4) of the UN Charter and – among other things – confirmed status of the prohibition of the use of force as not only customary international law, but also *ius cogens* norm[10], despite the practice of states. Scholars argue that states acting in breach of Article 2(4), but trying to legally justify their actions by e.g. appealing to exceptions contained in the same or subsequent articles of the UN Charter, confirm the validity of the rule, rather than weaken it[11]. Similar view is contained in Paragraph 186 of the Nicaragua Case ruling, although the practice of the United Nations General Assembly related to condemnation of certain apparent breaches of Article 2(4) while remaining silent on others, might be construed as challenging such an assertion. Still, failure to condemn should not be interpreted as tacit confirmation of the legality of the use of force[12].

What constitutes the use of force in the meaning of Article 2(4) of the UN Charter? Obviously, an armed attack is a use of force, however this article is meant to address actions not crossing this threshold. The ICJ in Paragraph 191 of the ruling on merits of the Nicaragua Case used the *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*[13] as a reference to reaffirm the obligation of states to "[…] *refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when [such] acts* […] *involve a threat or use of force.", as well as to*"[..] *refrain from organizing or encouraging the organization of irregular forces or armed bands, including mercenaries, for incursion into the territory of another State."*

From this perspective, not only U.S. activities in Nicaragua, but also other examples of the attempts by superpowers to maintain their spheres of influence, even though not formally condemned by the UN General Assembly (and some of them in fact tacitly acquiesced by the international community), have – in the view of the author – constituted unlawful use of force against other sovereign nations in breach of UN Charter Article 2(4)[14] (e.g. U.S. other engagements in Central and South America, organising armed resistance against Fidel Castro's regime in Cuba, Soviet clandestine actions in Afghanistan preceding the full-scale military intervention). These activities would amount to what has recently been referred to as "hybrid warfare", although due to the non-existence of an armed conflict, the author deems terms "hybrid activities" or "hybrid operations" as more appropriate.

Similarly, it seems apparent that employment of military, paramilitary or police forces or clandestine agents on the territory of another state would constitute use of force and thus violation of UN Charter Article 2(4)[15]. It could also be construed as violation of independence and territorial sovereignty of the affected state, even if such an employment of forces was conducted in direct and immediate pursuit after perpetrators of a criminal act committed in the territory of a neighbouring state employing such forces. It is even more apparent if such an employment of regular (or clandestine) forces is conducted in order to apprehend a person suspected of having committed a crime in the territory of the state undertaking the hot pursuit[16].

Even if such actions are apparent breaches of Article 2(4) of the UN Charter, unless they cross the threshold of an armed attack, they would not justify an armed

response in self-defence under Article 51 of the UN Charter. The position of the United States, as reflected in the 2012 speech by then the Legal Adviser to the Department of State – Mr. Harold Hongju Koh[17] and restated in the U.S. DOD Law of War Manual[18] is that "[…]*the inherent right of self-defense potentially applies against any illegal use of force*[…]", which seems to contravene the essence of the ICJ ruling on merits in the Nicaragua Case, in this particular aspect favourable to the United States, as it rejected the claims by Nicaragua that certain actions perpetrated or supported by the United States amounted to armed attacks and thus merely constituted a different category of the use of force, not entitling Nicaragua to exercise its right to self-defence under Article of the UN Charter. The rationale behind such position of the United States might be related to recent practice of "targeted killings" of individuals suspected of terrorist activities against United States or its citizens, conducted within the territories of third states and justified not by extraterritorial exercise of criminal jurisdiction (terrorist acts are grave criminal offences, obviously), but by self-defence. This position, however, was contested by the International Group of Experts involved in the drafting of the *Tallinn Manual 2.0*, who in majority considered that states being affected by the use of force not amounting to an armed attack would not be entitled to respond under the self-defence paradigm and rather being obliged to respond with other measures than armed force, as an armed response might be unlawful in the absence of an armed attack[19].

Mr. Koh in his 2012 speech, while referring specifically to cyber operations that are not meant to lead to armed attacks, stated that "[…] *there is no threshold for a use of deadly force to qualify as an 'armed attack' that may warrant a forcible response. But that is not to say that any illegal use of force triggers the right to use any and all force in response—such responses must still be necessary and of course proportionate*."[20] Even though necessity and proportionality of the response were mentioned, such an assertion is at least slightly worrying, as it clearly indicates the nation's intent to reserve the right to an armed response to actions not amounting to armed attacks, while at the same time to deny similar right to other nations[21].

Before answering the question of the types of cyber activities that would constitute a use of force, let us first briefly discuss examples of cyber activities, which – although immoral and in certain instances also contrary to international law – would not amount to use of force in the meaning of UN Charter Article 2(4).

Firstly, cyberespionage conducted in peace time – not only isn't it prohibited (or even regulated) by international law *per se*, but also in general would not amount to use of force, as normally such activities are conducted clandestinely, without resort to conventional military operations and most often, without any use of physical violence or other forms of force. It should be noted, however, that peacetime espionage constitutes criminal offence under domestic criminal laws of vast majority of nations, regardless of whether it is conducted "traditionally" or with the use of cyber means or capabilities. "Attractiveness" of cyber spying tools originates from the removal of the requirement for physical presence at the source of the information.

It should be noted, however, that if:

- cyberespionage is conducted with the use of methods which themselves violate international law (e.g. tapping submarine communication cables located within territorial waters of the victim state) or
- cyberespionage operation is facilitated by an activity which would violate sovereignty of the victim state (e.g. physical intrusion into computer systems of the victim state in order to introduce spyware on a USB flash drive), or
- measures taken to gain access to computer systems which are the target of the cyberespionage operation result in unintended consequences considered unlawful (e.g. causing damage to communications infrastructure or destroying computer data),

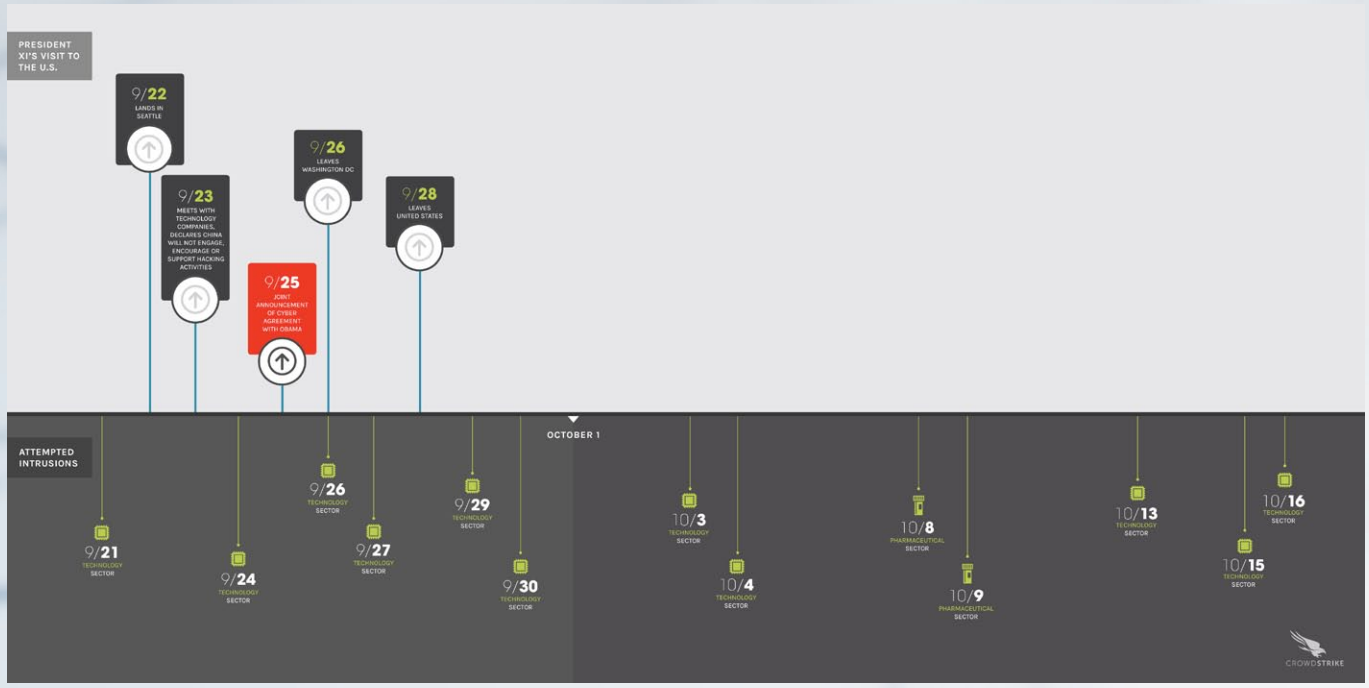
the whole cyberespionage operation (otherwise not unlawful) might be considered as violating international law and – if attributed to a state – result in that state's responsibility (liability) for violation of international law[22]. States' responsibility for unlawful cyber actions will be discussed in a slightly more detailed manner described in the following parts of this article.

The second example of cyber activities which do not constitute use of force and – in the absence of a specific bilateral or multilateral treaty – would not be a violation of international law (however could be considered a criminal offence and would definitely constitute a civil law delict) is intellectual property theft (also referred to as industrial or economic espionage). Recently, there has been a number of widely reported "hacks" against large international and U.S. corporations[23], among them in particular the "SONY Hack", allegedly attributable to North Korea. Although some investigations on the intellectual property thefts have resulted in indictments against Chinese military[24] (who could be considered state's agents if acting in their official capacity), the cyber-theft concerned has been conducted in order to give an unfair advantage to a Chinese producer of solar panels in its competition against a U.S.-based company and no substantial evidence has been found to prove the actions of the indicted personnel had been conducted on behalf of or under the direction of the Chinese authorities, thus these cyber-facilitated intellectual property thefts could not be directly attributed to China. It nevertheless gave the U.S. administration additional arguments in applying more pressure on Chinese government to commit to fighting cyber-facilitated criminal activities conducted by Chinese citizens or with the use of Chinese cyber infrastructure, which eventually resulted in the signing of the September 2015 bilateral cyber commitments to:

"(1) […] *develop constructive law enforcement cooperation on cyber-enabled crimes;*
(2) engage in high-level dialogue on cybercrime and network protection;
(3) not conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the

intent of providing competitive advantages to companies or commercial sectors; and (4) make common effort with the United States to further identify and promote appropriate norms of state behavior in cyberspace through an annual Senior Experts Group meeting led by the Department of State."[25].

The bilateral cyber commitments did not (unfortunately) stop Chinese cyberespionage activities against the U.S. Allegedly, on the very next day after the signing of the bilateral cyber commitments, China-affiliated actors committed a cyber-theft attempt[26] and similar occurrences have continued almost every day (see the figure below).



Source: https://www.crowdstrike.com/blog/wp-content/uploads/2015/10/CrowdStrike-China-Timeline.jpg

Going back to the essential question of what cyber operations would amount to use of force in the meaning of Article 2(4) of the UN Charter. An apparent conclusion is that certainly such cyber operations, the scale and effects of which are comparable to "conventional" actions amounting to use of force. Therefore, let us now examine the types of "conventional" activities that could amount to use of force without crossing the threshold of an armed attack. Once again, the ICJ ruling in the Nicaragua Case[27] becomes helpful, making use of the scarce treaty law and *opinio iuris* available and coming to a conclusion that providing support (other than merely financial aid) to armed opposition groups striving to overthrow the government is an illegal use of force and thus a violation of Article 2(4) of the UN Charter[28]. At the same time, exercising economic or political coercion, or providing sanctuary to armed groups (without directly supporting such groups) in most of the cases would not constitute use of force[29].

More specific guidance can be found in another "cornerstone" ruling by the ICJ, namely the judgement on the case of Democratic Republic of Congo vs. Uganda[30]. In Paragraph 162 of the ruling, ICJ quoted the Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations[31], in particular the following passage:

"[…] *no State shall organize, assist, foment, finance, incite or tolerate subversive, terrorist or armed activities directed towards the violent overthrow of the regime of another State, or interfere in civil strife in another State* […]".

The ICJ ruled that actions by Uganda in the territory of the Democratic Republic of Congo constituted a grave violation of the prohibition formulated in Article 2(4) of the UN Charter, even if these actions were not meant to change the political regime in Congo, but to achieve perceived Ugandan security needs and to support irregular elements engaged in civil war with the Congolese governmental forces. Uganda was found responsible for violation of sovereignty and territorial integrity of Congo[32].

Drafters of the *Tallinn Manual 2.0* have adopted a set of eight criteria meant to assist in evaluating whether a cyber operation qualifies as use of force by comparing it to a conventional action or operation that would be considered as such. The criteria are[33]:

1) Severity – the consequences of a particular cyber operation in terms of their duration, scope and intensity have to be significant enough; mere inconveniences would not suffice. The more severe consequences of a cyber operation, the more likely would such operation be considered as use of force;

2) Immediacy – the sooner the consequences of a cyber operation manifest, the more likely it is that the operation would be considered as use of force;

3) Directness – there should be a causal

link between the cyber operation and its consequences, preferably a direct one. The more direct causal link, the higher likelihood of recognition of use of force;
4) Invasiveness – the more intrusive the cyber operation is, the more likely it would be considered as use of force; the invasiveness can be assessed from a purely technical perspective (e.g. breaching a firewall vs. passive examination of vulnerabilities or APT[34] vs. DDOS[35]), based upon "target" selection criteria (publically accessible services vs. confined military domains) or take into account the assumed purpose (exfiltration of information vs. inserting malware to disrupt the functioning of the targeted system);
5) Measurability of effects – if the consequences of a cyber operation are apparent, identifiable and quantifiable (e.g. the volume of altered/corrupted/destroyed data, the number of disabled servers, percentage ratio of service degradation), such an action could more likely be construed as use of force;
6) Military character – in particular if the cyber action can be considered as either part of military operations of the adversary or in fact does facilitate a specific military operation by e.g. disabling early warning systems to cover movements of forces; directing cyber operations against military cyber infrastructure might also be considered when assessing this criterion;
7) State involvement – clearly if state involvement can be demonstrated (and – optimally – proven), the question of whether a cyber action amounts to use of force is easier to answer, especially if a given cyber operation is linked to other actions by that state. Article 2(4) of the UN Charter explicitly mentions the use of force by states, as opposed to Article 51 dealing with armed attacks. As reflected in the *Caroline* case as well as the practice of individual States and the collective actions undertaken by the UN (Resolution 1368) and NATO (12 September 2001 decision by the North Atlantic Council to invoke Article 5 of the Washington Treaty) in the aftermath of the 9/11 attacks), there seems to be an understanding that a non-state actor can be responsible for an armed attack[36].
8) Presumptive legality – acts not explicitly prohibited by international law (treaty provision, customary law rule) are generally permitted and this equally applies to cyber operations, e.g. cyber espionage, as discussed above. Cyber actions analogous to conventional ones prohibited by international law would likely be construed as uses of force.

When it comes to examples of cyber operations amounting to use of force, the Tallinn Manual 2.0 is not very generous. It does clearly state that cyber operations which result in inflicting destruction, damage, injuries or deaths (or the combination thereof) would undoubtedly be considered as uses of force, perhaps even armed attacks if certain threshold of the harm's significance is crossed. It also mentions providing an organized armed group with malware and training necessary to conduct cyber operations amounting to a use of force against another state as an example of use of force, following the logic of ICJ's rulings in Nicaragua and Congo cases. Providing malware and training necessary to conduct propaganda, disinformation activities, to spoof governmental web pages or bring them down with the use of DDOS techniques (assuming no severe consequences are caused by such actions) would not amount to use of force and neither would providing financial resources to such an armed group, even if the resources are utilized to obtain cyber capabilities or conduct cyber operations as a part of irregular warfare waged by this group.[37]

One could argue that providing an armed group with tools and training tailored to conduct a highly targeted cyber operation, meant to degrade a state's defence by e.g. disrupting early warning systems or corrupting geographical data in weapons' guidance systems, would constitute use of force even if such a cyber operation causes no physical harm or damage, as it would be more than merely electronic warfare or signal jamming. If successful, such a cyber operation might shift the balance between the state forces and irregular armed group.

Acts by a state, to include cyber operations, need not cross the threshold of use of force in order to be considered violations of international law. The following section of this article will discuss the principle of non-intervention in the context of the Nicaragua case, as well as states' sovereignty and independence.

3. THE PRINCIPLE OF NON--INTERVENTION. SOVEREIGNTY IN CYBERSPACE

In the Nicaragua case quoted above, the ICJ considered that the United States of America, by "[…]*training, arming, equipping, financing and supplying the contra forces or otherwise encouraging, supporting and aiding military and paramilitary activities in and against Nicaragua, has acted, against the Republic of Nicaragua, in breach of its obligation under customary international law not to intervene in the affairs of another State*"[38]. In two other parts of the ruling, the ICJ found the United States in violation of the sovereignty of Nicaragua[39]. Although the ICJ has separated the breaches of the principle of non-intervention and violation of Nicaraguan sovereignty, in the author's view *any* forcible intervention in a foreign country would constitute a breach of that country's sovereignty.

Currently, the principle of non-intervention is understood as the obligation of states to refrain from interfering with "[…]*matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State*."[40]

Intervention can be defined as interference by one state in external or

internal matters of another state, such as political, social, economic systems or foreign policy, be it directly or indirectly. Mere criticism cannot be regarded as intervention – there has to be an intent and attempt to impose changes. The interference has to be "*coercive or dictatorial*" in order to be considered an intervention, thus sanctions or unilateral discontinuation of diplomatic relationships cannot be regarded as interventions, whereas providing support to armed opposition or – in particular – direct military involvement in support of armed opposition's operations undoubtedly constitute an intervention. U.S. Activities in Nicaragua were considered by the ICJ as unlawful, even if certain forms of support rendered to the *Contra* forces were not military in nature (e.g. financial support) and even if the U.S. did not (officially) share the political objectives of the *Contras*, i.e. to overthrow the government of Nicaragua. Falling short of the use of force (or the threat thereof), certain forms of support to armed opposition may nevertheless constitute intervention, as ruled by the ICJ in the Nicaragua Case[41].

There are situations, in which intervention can be legally justified, to include:

1) Protection of citizens abroad, although nowadays it is considered that such justification exists only in the face of an immediate threat to the lives of the citizens and the unwillingness or inability of the territorial state to protect the persons at risk;
2) Humanitarian intervention (responsibility to protect) – one of the most controversial bases for the use of force in general and intervention in particular; not universally accepted and – in order to be justifiable – would have to either be authorised by the UN Security Council or – in the absence of the Security Council's mandate – occur in response to an overwhelming, urgent and extreme humanitarian distress[42];
3) In the exercise of individual or collective self-defence, where the intervention is both proportionate and necessary to repel an armed attack;
4) Under the authorisation of the UN Security Council in accordance with Chapter VII of the UN Charter, although from a doctrinal perspective, use of force under Chapter VII does not constitute an intervention *per se*[43].

Since – as proposed above – any intervention (as defined by the ICJ in the ruling on the Nicaragua case) would also constitute violation of the sovereignty of the "victim" state and the main purpose of this article is to discuss cyber operations in this context, the following few paragraphs will touch upon the concept of sovereignty as applicable in the cyber domain.

Sovereignty is one of the founding aspects of the existence of a state and its relations with other states and comprises of three main features:

1) jurisdiction, generally exclusive, over a territory and population permanently present in this territory;
2) obligation not to intervene in the areas of exclusive jurisdiction of other states;
3) respect to obligations under customary international law and treaties, which the state consented to enter into.

Sovereignty equals states' freedom to exercise discretionary powers within the limits of international law.[44]

Nowadays, however, sovereignty of states is to a large extent limited by international law, both customary and treaty, by mutual interdependence of states, in particular economic interdependence, as well as membership in international organisations, taking over parts of what used to be the sovereign competences of states. Sovereignty is also challenged by technological developments, globalisation and tendency to remove legal constraints on international trade, which all may lead towards a '*post-territorial world*'[45].

Challenged doesn't mean obsolete, though, and in the author's view sovereignty emanates outside the physical or geographical territories of states into – among others – cyberspace. This does not only imply that a state may exercise its sovereignty with regard to cyber infrastructure and persons located or activities conducted within the territory of that state, but also exercise the functions of a state in external relations, to include lawful activities in cyberspace.

Sovereignty in the cyber context means – in the view of the author – the ability of a state to perform its inherent, sovereign functions in cyberspace without interference from other states. The manner in which such functions are performed is not absolutely free – international law does apply to cyberspace and thus may restrict the discretion and freedom of state's organs in cyberspace.

Internationally lawful activities of a state should be unimpeded by other states, regardless of whether they occur solely in cyberspace, or they actually emanate into physical domains. Nowadays a state cannot properly function without being able to operate in cyberspace and even certain aspects of states' foreign policies are performed in the cyber domain, e.g. via strategic communications conducted on electronic media. Sovereignty encompasses the freedom to formulate foreign policy[46] – there is no controversy in this statement. Therefore, if a state decides to formulate elements of its foreign policy via activities conducted in cyberspace, it should be free to do so, as long as these activities do not constitute violations of international law.

Of course, freedom to formulate foreign policy incudes the freedom to enter into any treaties or other international agreements, to include those governing the conduct in cyberspace, however no state can be obliged to agree to a certain cyber-related treaty. The situation will differ in the presence of an international agreement, which would restrict state's sovereignty in cyberspace by e.g. making elements of "territorial" cyberinfrastructure available to another state. In accordance with the *pacta sunt servanda* rule, such a restriction is to be respected and observed.

In the era of cloud computing, traditional territorial approach to sovereignty in the aspect of jurisdiction is complicated. Customary international law recognises state's exclusive jurisdiction over its own territory and activities conducted therein. Generally, states cannot exercise their jurisdiction extraterritorially

without the consent of the territorial state concerned[47]. Minority of the experts involved in the *Tallinn Manual 2.0* project suggested that states can exercise sovereign rights over governmental data transmitted outside their own territory or governmental cyber infrastructure. Majority of the experts disagreed, stating that data stored abroad cannot be subject to the sovereignty of the state which originated the data, unless international law so provides.[48]

In the author's view, an alternative approach might be proposed. Assuming that State A agrees to host websites or data of State B (as it was the case in 2008 when Poland offered to host Georgian governmental websites brought down in Georgia by DDOS campaign allegedly launched from Russia). Should it mean that State A now exercises sovereign rights over such websites or data? Should State A be free to modify the content? In the author's view, State B retains certain sovereign rights over such data or websites, to include the right to modify content, add or remove information, etc., as long as when exercising these sovereign rights, State B does not violate international law and sovereignty of State A in particular. Of course, such rights to modify, add, remove etc. might be secured in an international agreement between States A and B regarding hosting of websites and data originated by State B.

On the other hand, let's consider a modification of the aforementioned scenario. State A hosts websites and data of State B. Individuals (or groups) whose IP addresses indicate their location in State A conduct a cyber operation aimed at defaming the website and exfiltration of data. Should State B be authorised to implement the measures to repel the interference? If so, is State B authorised to exercise jurisdiction in the territory of State A?

The answers are not easy. In the author's view, State B would only be authorised to implement passive defence measures, "hardening" the security of the servers and perhaps passively collect data of the perpetrators. Without explicit consent of State B, State A would not be authorised to conduct active defence or "hacking-back" activities to stop the intrusion, just as in the case of providing external security to a diplomatic mission, where the Host Nation would be responsible for it. And again, State B would have to request State A to prosecute the perpetrators who were within the exclusive territorial jurisdiction of State A and eventually perhaps request their extradition. Once again, specific rights of State B could be secured in an agreement with State A, regarding hosting of websites and data originated by State B.

States are generally prohibited from violating other states' sovereignty (except for cases of self-defence and authorisations of the UN Security Council) and from that perspective it is irrelevant whether such violation occurs in physical domains or in cyberspace. The obligation to respect states' sovereignty does not bind non-state actors, as they are not subjects of international law, however – as it will be discussed – if actions by a non-state actor are attributable to a state, that state may bear liability for such actions. The fact that non-state actors cannot be held liable for violation of sovereignty, does not render their actions lawful – in fact in most cases such actions would violate domestic laws of the victim state[49].

Undoubtedly, physical intrusion into the territory of a state (including its territorial waters, seabed underneath territorial waters and national airspace) in order to conduct a cyber operation would constitute violation of sovereignty. This is equally true with regards to physical intrusion into cyber infrastructure of the victim state (the physical layer of cyberspace).

There should be also not much discussion with regards to cyber operations which result in physical damage or injuries – as discussed in the first version of the Tallinn Manual, such cyber operations may even be construed as amounting to armed attacks[50], thus they would also clearly constitute violations of sovereignty of the victim state. Also, significant and lasting degradation or loss of functionality (mere inconveniences would not suffice) – in particular of critical infrastructure located in a state's territory as a result of a cyber operation would be considered as violation of sovereignty of the affected state. In this case, it should not matter whether the critical infrastructure is owned or operated by the state or a private entity and this would also be applicable to critical cyber infrastructure.

Controversies do arise in the case of cyber operations which result in no manifested physical consequences, merely cause degradation or loss of functionality of certain systems or alteration or destruction (erasure) of data. The eight criteria proposed in the Tallinn Manual 2.0 for assessment of whether a cyber operation amounted to use of force may become useful also in the assessment of possible violation of sovereignty. The immediate consequences of a cyber operation might cause no physical harm, however indirect consequences might be severe. As an example, a cyber operation is conducted by intelligence service of State A in order to erase metadata collected by prosecution of State B as forensic evidence in an investigation against citizens of State B suspected of espionage in favour of State A. The immediate consequence – deletion of computer data – is unlikely to be considered as violation of sovereignty of State B. However, the second-order effect and the intended outcome of the cyber operation is to prevent State B from prosecuting suspected spies, thus State B is restricted from exercising one of the fundamental attributes of sovereignty, namely jurisdiction over its citizens. The causal link between the cyber operation and eventual inability to exercise jurisdiction clearly exists, even if it is not absolutely direct.

A second example might be less controversial, as even the drafters of the Tallinn Manual 2.0 seemed to have agreed that interference with or usurpation of inherently governmental function of a state with cyber means would constitute violation of sovereignty, regardless of whether such function is actually performed by a governmental institution or has been privatised.[51]

Examples of interference with or usurpation of inherently governmental functions include denying the state the ability to pay its officials their salaries, interfering with official intergovernmental communications, degrading key national defence activities (systems)[52] or – of significant importance recently – disrupting interrupting the conduct of elections.

Let us develop a bit on the conduct of elections, as recent events (in particular those surrounding the last U.S. presidential elections) have raised important questions on third states' involvement in the election process and influence on the results. To what degree would a state have to interfere with the conduct of elections in order to be in breach of the principle of non-intervention or the sovereignty of the affected state?

Although probably the expectations would be different, in the author's view, mere exfiltration and publicising of information undermining the reputation of a candidate (or political party) would – in most of the cases – not constitute an intervention or violation of sovereignty of a state, even if the action is in fact intended to influence the public opinion to change its perception of the candidate or party and eventually cast a different vote than initially intended.

The situation would be different if a cyber operation was used in order to interfere with an electronic (on-line) voting system or systems used to count votes and results of the elections. Such interference, if conducted by a state in order to pursue the results of elections that would be favourable to the perpetrating state, undoubtedly would constitute an infringement of sovereignty of the affected state and – most likely – amount to an intervention. Let us consider the following scenario: State A conducts cyber operation meant to alter the contents of the official communiques issued by the Ministry of Foreign Affairs of State B condemning unlawful conduct of naval vessels of State A in the territorial waters of State B. The communiques are published on the official websites of the Ministry of Foreign Affairs of State B and broadcasted on the Internet via the official YouTube Channel of the Ministry of Foreign Affairs pf State B. With the use of sophisticated cyber means, the communiques published in writing are replaced with their forged versions and video broadcasts appropriately cut in order to create the impression that State B is merely "concerned" with the conduct of naval vessels of State B and does not actually condemn them.

As stated above[53], sovereignty encompasses, among others, the freedom of a state to formulate its foreign policy. Any restrictions on this freedom would constitute infringement of sovereignty, therefore – as described in the scenario – cyber operations resulting in interference with a state's formulation of foreign policy would also constitute violation of sovereignty, even without physical intrusion or emanation in the territory of the affected state. Arguably, a cyber operation meant to spread disinformation or in other manner influence a state's foreign policy might amount to infringement of sovereignty, if attributable to another state, vitally interested in achieving such an effect on an adversary.

Since it has been identified that only states or state actors can violate sovereignty of another state and similar actions conducted by a non-state actor (in the absence of attribution to a state) could not be considered as infringing sovereignty (although will most likely constitute a criminal offence under the criminal laws of the affected state), let us now briefly examine the principles of state responsibility.

4. STATES' RESPONSIBILITY FOR INTERNATIONALLY UNLAWFUL ACTS

This section will briefly discuss aspects of state responsibility for internationally unlawful actions, in particular with regard to cyber operations amounting to interventions or otherwise infringing the sovereignty of the affected state and thus violating international law. The deliberations below will be mainly based on the Draft Articles on State Responsibility for Internationally Wrongful Acts[54] hereinafter referred to as the "Draft Articles".

It is a universally accepted principle of customary international law, as codified in Article 1 of the Draft Articles that states bear responsibility for the violation of their international obligations. Article 2 provides that in order to be internationally wrongful, an act has to encompass two constitutive elements: be attributable to a state and constitute a breach of international obligations of that state.

The key element of attribution can be fulfilled by satisfying one of the conditions laid down in Chapter II of the Draft Articles:

1) Conduct of state organ "[…] *whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central government or of a territorial unit of the State*." (Art. 4);
2) Conduct of persons or entities exercising elements of governmental authority (Art. 5);
3) Conduct of organs placed at the disposal of a State by another State (Art. 6);
4) Excess of authority or contravention of instructions by a person or entity empowered to exercise elements of governmental authority (Art. 7);
5) Conduct directed or controlled by a State (Art. 8);
6) Conduct carried out in the absence or default of the official authorities (Art. 9);
7) Conduct of an insurrectional or other movement which becomes the new government of a State or succeeds in establishing a new State in part of the territory of a pre-existing State (Art. 10);
8) Conduct acknowledged and adopted by a State as its own (Art. 11).

Actions by other individuals acting within the authorisation of the state or under its command, to the extent the individuals concerned are subject to international duties will also be internationally wrongful[55]. Examples of international law breaches resulting in individual responsibility include "*offences against the peace and security of mankind*", as stipulated in the *Draft Code* of Crimes against the Peace and Security of Mankind (hereinafter referred to as the "Draft Code")[56]. The draft Code lists the following crimes: aggression (Article 16), genocide (Article 17), crimes against humanity (Article 18), crimes against United Nations and associated personnel (Article 19) and war crimes (Article 20). With regard to the crime of aggression (of particular interest here, given the topic of this article), the commentary to the Draft Code stipulates:

"*The action of a State entails individual responsibility for a crime of aggression only if the conduct of the State is a sufficiently serious violation of the prohibition contained in Article 2, paragraph 4, of the Charter of the United Nations. In this regard, the competent court may have to consider* […] *whether the conduct of the State constitutes a violation of Article 2, paragraph 4, of the Charter and whether such conduct constitutes a sufficiently serious violation of an international obligation to qualify as aggression entailing individual criminal responsibility. The Charter and the Judgment of the Nurnberg Tribunal are the main sources of authority with regard to individual criminal responsibility for acts of aggression*."[57]

The Nurnberg Tribunal clearly recognized the roles of States and individuals in stating that:

"*Crimes against international law are committed by men, not by abstract entities, and only by punishing individuals who commit such crimes can the provisions of international law be enforced*."[58]

It has to be underlined that breaches of international law by individuals acting in their capacity as state organs incline the responsibility of the state for such breaches and the attribution of the act of an individual to a state for the purposes of state responsibility is a matter of international law, not domestic law of the state. There might also be cases where a state becomes responsible for acts of private persons, in particular when the state concerned fails to exercise due diligence to prevent individuals being citizens of that state (or present within its territory.) from committing internationally wrongful acts. While with regard to administrative officials and members of the armed forces states (normally) possess disciplinary powers and mechanisms to either prevent or enforce breaches, the exercise of due diligence with regards to private persons will be subject to certain limitations, i.e. to mainly prevent possible wrongful acts within means and capabilities as well as to prosecute offenders, should a violation occur, and compel them to compensate for the damages. Failure to prosecute would equal failure to exercise due diligence and might result in international responsibility of the state. [59]

The paradigm would shift if private individuals, despite not being state officials, are prompted, encouraged or instigated to conduct internationally wrongful acts *de facto* on behalf of the state. In such a case, which has to be assessed on a factual basis, individuals might be considered as so closely associated with the state's organ, that the act committed by a private individual would be regarded as committed by the state. To certain extent this might pertain to activities of corporations, which although having separate legal personality may be considered as agents of the state, in particular when they are under a governmental contract or have been outsourced to perform certain governmental functions. The state concerned might then be liable for the actions of private actors conducted by the order of state authorities, in accordance with instructions of the state bodies, under the direction or control of the State (criterion of effective control as in the case of de facto commanders)[60].

Similarly, a state may be held accountable for actions of private persons forming an insurgent group in another state, provided that – as ruled in the Nicaragua Case – the insurgents remain under effective control of that state[61].

As provided for in Chapter IV of the Draft Articles, a state may be held accountable for internationally wrongful acts of another state, when acting "[…] *with knowledge of the circumstances of the internationally wrongful act* […]":

1) Aids or assists in the commission of such act (Art. 16);
2) Exercises direction and control over the commission of such act;
3) Coerces another state to commit such act.

It is irrelevant, whether an internationally wrongful act has been committed in a physical domain or in cyberspace; if the act is attributable to the state under international law and constitutes a breach of an international obligation of the state, it entails the responsibility of the state even if the act itself or its consequences emanate only in cyberspace[62]. A state can be held liable for cyber operations which violate any kind of international obligation of that state, e.g. conducting a cyber operation from a naval vessel passing through territorial waters of another state, thus in breach of the innocent passage regime as regulated by Art. 20 of the United Nations Convention on the Law of the Sea.

As proposed above, providing an insurgent group with cyber tools necessary to conduct a cyber operation intended to inflict damage or cause casualties in the state struggling with insurgency, might amount to an unlawful intervention, which is apparently an internationally wrongful act.

Equally, instigating a hacker group to conduct cyber operations against another state, which would result in damage, harm or significant degradation of the functioning of critical infrastructure in the victim state, if attributable (in any of the manners proposed by Chapter II of the Draft Articles) to a state, would constitute an internationally wrongful act. If such a hacker group is provided with guidance as to the objects, nodes or elements of infrastructure to be targeted and complies with the guidance, such a situation might satisfy the effective control test[63].

Failure to prevent misuse of national cyber infrastructure made available to another state and subsequently utilised to conduct cyberattacks against a third state could be construed as non-compliance with the requirement of due diligence and result in responsibility of the state owning the cyber infrastructure. As it will be pointed out in the following (and final) section of this article, states and non-state actors may utilise third-states' cyber infrastructure to hide or disguise their engagement in cyber operation and thus complicate identification of the actual perpetrator and proper attribution of the act. If the state, the cyber infrastructure of which is utilised to convey such a cyber operation is unaware of the fact, such state could not be considered internationally responsible. However, should the state be made aware of the misuse of its cyber infrastructure and fail to undertake respective preventive measures, it might

be considered as non-compliance with the obligation to exercise due diligence.

Given that attribution is a key prerequisite of state responsibility for breaches of international obligations, the final part of this article will address the question of why cyber tools can be highly efficient in the so called hybrid operations.

5. CONCLUSIONS: AMBIGUITY AND COMPLICATED ATTRIBUTION – USEFUL FEATURES OF CYBER ACTIONS IN HYBRID OPERATIONS.

Recently the term "hybrid warfare" has been used in so many different contexts, to include statements by high-ranking officials on NATO, to describe the ambiguous and unorthodox approach to operations aimed at achieving strategic and political goals while maintaining relatively low level of violence. In the author's view, the term "hybrid warfare" is itself ambiguous and self-contradicting, as the whole purpose of hybrid operations is to maintain the violence below the threshold of an armed conflict (be it international or non-international), thus "warfare" *de iure* would not even occur.

Hybrid operations could be characterised as the use of the whole spectrum of means, methods and capabilities: military, economic, political and technological in pursuit of strategic and political objectives. Such an approach is sometimes referred to as the DIMEFIL: Diplomatic, Information, Military, Economic, Financial, Intelligence and Legal (Lawfare[64]).

Employment of hybrid methods is aimed at confusing the adversaries as well as the broad international community as to the intents and actual conduct of the perpetrator, eroding the legitimacy of the adversary while creating the false perception of the legitimacy of the actions taken by the perpetrator and ending the hostilities before proper reaction of the international community can even occur[65].

NATO has defined hybrid operations as those, "[…] *where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design*."[66]

The whole purpose of hybrid operations is to enable the perpetrating state to utilise the so called "plausible deniability". Resorting to covert rather than over military operations, utilising proxies, misusing humanitarian convoys to provide cover for shipping military supplies to rebel forces (organised armed groups) – all these activities serve one purpose: making attribution of an internationally wrongful act at least extremely difficult, if not impossible at all. Without attribution – as stated in the previous section of this article – there is no state responsibility.

Within the DIMEFIL approach, the information domain is key, particularly apparent in the Russian hybrid operations in Crimea and eastern Ukraine, where the 'information war" doctrine by Gen. Gerasimov has been put to test. Russia disseminated misinformation to distract, confuse and degrade the opponent's capabilities and counter a threat, with large parts of the disinformation distributed over the Internet. Cyber operations have also been used in support of conventional campaign in Georgia.

The ability to deny engagement by the perpetrating state is the ultimate goal of the information campaign supporting or constituting part of hybrid operation. Utilisation of cyber means and capabilities in this regard enhances the deniability, because properly used cyber means allow to disguise the actual actors behind the cyber operation, thus complicating or even eliminating the attribution, while making it easier to infringe the sovereignty of other states and remain immune to allegations of the use of force.

States may decide to utilise specialised tools to cover their engagement in particular cyber operations. This may include spoofing, i.e. replicating existing and lawful website or IP address with a copy indicating some other nation was behind this particular cyber operation or relying upon botnets comprising of thousands of infected workstations (sometimes spread across the whole world) to conduct the cyber operation. States may also turn to hacker or hacktivist groups to conduct cyber operations in pursuit of the state's objectives and – unless it is proven that the group was under effective control of the state or its organs, there is no possibility to attribute such actions to the state. As stated by the former Legal Adviser to the U.S. Department of State, "*States are legally responsible for activities undertaken through "proxy actors," who act on the state's instructions or under its direction or control. The ability to mask one's identity and geography in cyberspace and the resulting difficulties of timely, high-confidence attribution can create significant challenges for states in identifying, evaluating, and accurately responding to threats.* […] *Established international law does address the question of proxy actors. States are legally responsible for activities undertaken through putatively private actors, who act on the state's instructions or under its direction or control. If a state exercises a sufficient degree of control over an ostensibly private person or group of persons committing an internationally wrongful act, the state assumes responsibility for the act, just as if official agents of the state itself had committed it*."[67] And even if attribution is eventually confirmed, such as in the case of the hacker group called "the dukes" which has been linked to Russian authorities[68], the forensic examination of a case sometimes takes years, during which the whole geopolitical setting might change.

Cyber tools may be highly efficient in supporting the hybrid operations of a state, alongside other areas of influence/coercion. Not only can they influence the public opinion, but – if used properly – can degrade the defences of the victim state or impact the results of elections. They might also be used by terrorist organisations, whether acting independently or as state's proxies, to inflict significant damage at a relatively low cost by targeting critical infrastructure or simply to spread psychological terror or propaganda in support of the terrorist organisations, as we have seen recently in the case of ISIS.

Most importantly, cyber tools as significant component of hybrid operations, facilitate the plausible deniability and

complicate the attribution of wrongful acts to the state actually responsible. From that perspective, it is highly likely that cyber operations or cyber-enabled operations will be increasingly utilised in the currently on-going and upcoming crises.

It should be underlined, nevertheless, that cyber means and capabilities may be used lawfully, becoming then a significant extension of conventional defence capabilities and a true force multiplier. They can be used to effectively deny or degrade the adversaries C4ISR (Command, Control, Communications, Computer, Intelligence, Surveillance, Reconnaissance) capabilities, both as part of a broader military operation[69] or independently, eg. blocking of ISIS-related social media accounts in order to degrade the terrorist organisation's communications capabilities[70]. In the Cyber Defence Pledge the Allies confirmed their commitment to develop cyber defence capabilities, recognising the importance of the cyber component in contemporary military operations. Simultaneously, NATO reiterated the intent to operate in cyberspace with respect to international law, to include the Charter of the United Nations, which is a clear indication that cyber operations can and should be conducted lawfully. ■

---

[1] Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, Adopted by Heads of State and Government at the NATO Summit in Lisbon 19-20 November 2010, http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf (access: 11.03.2017), p. 11.

[2] Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 5 September 2014, http://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease (access: 11.03.2017).

[3] Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016, http://www.nato.int/cps/en/natohq/official_texts_133169.htm (access 11.03.2017).

[4] http://www.nato.int/cps/en/natohq/official_texts_133177.htm, paragraphs 70-71, (access 11.03.2017).

[5] See for instance Paragraph 71 of the Warsaw Summit Communique.

[6] See e.g. Mamiit, Aaron (October 30, 2014). "Meet APT28, Russian-backed malware for gathering intelligence from governments, militaries: Report". Tech Times, online, http://www.techtimes.com/articles/18995/20141030/meet-apt28-russian-backed-malware-for-gathering-intelligence-from-governments-militaries-report.htm, (access 15.05.2017)

[7] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) (merits), 1984 ICJ REP. 392 June 27, 1986, http://www.icj-cij.org/docket/index.php?sum=367&code=nus&p1=3&p2=3&case=70&k=66&p3=5 (access 12 March 2017).

[8] Responsibility of States for internationally wrongful acts, as annexed to Resolution No. 56/83 adopted by the General Assembly of the United Nations on 12 December 2001, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/56/83 (access 12 March 2017).

[9] Christine Gray, International Law and the Use of Force, Oxford University Press 2009, p. 7;

[10] Ibidem, p. 30

[11] A. Mark Weisburd, Use of Force. The Practice of States since World War II, The Pennsylvania State University Press 1997, pp.3-13, 22-25

[12] C. Gray, op. cit., pp. 21-23, 25-29

[13] General Assembly resolution 2625 (XXV), 1970

[14] A. M. Weisburd, op. cit, pp. 209-242

[15] Noam Lubell, Extraterritorial Use of Force against Non-State Actors, Oxford University Press 2011,
p. 69

[16] Oppenheim's International Law, Volume 1, Peace, edited by Sir Robert Jennings and Sir Arthur Watts, Oxford University Press 2008, pp. 385-390

[17] Harold Hongju Koh, Legal Adviser, Department of State, International Law in Cyberspace: Remarks as
Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), reprinted in 54
HARVARD INTERNATIONAL LAW JOURNAL ONLINE, (Dec. 2012), http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf (access 11 March 2017)

[18] Department of Defence Law of War Manual, Office of the General Counsel, Department of Defence, June 2015, pp. 47-48, 1000.

[19] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, edited by Michael N. Schmitt, Cambridge University Press 2017, p. 337.

[20] H.H. Koh, op. cit., p. 7

[21] C. Gray, International Law and the Use of Force, op. cit., pp.228-231.

[22] Ibidem, pp. 168-174

[23] See e.g. Shane Harris, Inside the FBI's Fight Against Chinese Cyber-Espionage, posted in foreignpolicy.com on 27 May 2014, http://foreignpolicy.com/2014/05/27/exclusive-inside-the-fbis-fight-against-chinese-cyber-espionage/ (access 13 March 2017); Scott Warren Harold, Martin C. Libicki, Astrid Stuth Cevallos, Getting to Yes with China in Cyberspace, published by the RAND Corporation, Santa Monica, Calif., 2016, http://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1335/RAND_RR1335.pdf (access 13 March 2017); Cyber Espionage And the Theft of U.S. Intellectual Property and Technology, a Statement Before the House Energy and Commerce Committee, Subcommittee on Oversight and Investigations by James A. Lewis, Director and Senior Fellow, Technology and Public Policy Program Center for Strategic and International Studies (CSIS), Center for Strategic and International Studies, Washington D.C. 2013, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/ts130709_lewis.pdf (access 13 March 2017).

[24] Shane Harris, Inside the FBI's Fight…, supra note 19

[25] Department of State International Cyberspace Policy Strategy, Public Law 114-113, Division N, Title IV, Section 402, March 2016, p. 11, https://www.state.gov/documents/organization/255732.pdf

(access 13.03.2017)

[26] Dmitri Alperovitch, The Latest on Chinese-affiliated Intrusions into Commercial Companies, 19 October 2015, https://www.crowdstrike.com/blog/the-latest-on-chinese-affiliated-intrusions-into-commercial-companies/ (access 14 March 2017).

[27] Military and Paramilitary Activities…, supra note 6, Paragraphs 202-205

[28] C. Gray, International Law and the Use of Force, op. cit., pp. 75-78

[29] Tallinn Manual 2.0, op. cit., pp. 331-332.

[30] Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, I.C.J. Reports 2005, p. 168, http://www.icj-cij.org/docket/files/116/10455.pdf (access 15 March 2017)

[31] Supra note 12

[32] Armed Activities on the Territory of the Congo, paragraphs 163-164.

[33] Tallinn Manual 2.0, op. cit., pp.334-336.

[34] Advanced Persistent Threat – a type of sophisticated and usually precisely targeted cyber operation.

[35] Distributed Denial of Service – relatively unsophisticated method of shutting down servers by overwhelming them with vast numbers of internet queries.

[36] N. Lubell, Extraterritorial Use of Force..., op. cit., pp. 30-36

[37] Tallinn Manual 2.0, op. cit., pp. 331-333

[38] Military and Paramilitary Activities…, supra note 6, paragraph 292(3).

[39] Ibidem, paragraphs 292(5) and 292(6).

[40] Military and Paramilitary Activities…, supra note 6, Paragraph 205.

[41] Oppenheim's International Law…, op. cit., pp. 430-434.

[42] Alfred van Staden and Hans Vollaard, The Erosion of State Soevereignty, in: State, Sovereignty and International Governance, edited by Gerard Kreijen, Oxford University Press 2004, p. 172; Oppenheim's International Law…, op. cit., pp.442-444; For more thorough overview of the concept of Humanitarian Intervention, see Humanitarian Intervention. Legal and Political Aspects. Danish Institute of International Affairs, Copenhagen, 1999; Humaniterian Intervention and International Relations, edited by Jennifer M Welsh, Oxford University Press 2004;Nicholas J. Wheeler, Saving Strangers. Humanitarian Intervention in International Society, Oxford University Press 2003

[43] Oppenheim's International Law…, op. cit., pp. 439-447

[44] Ian Brownlie, Principles of Public International Law, Seventh Edition, Oxford University Press 2008, pp. 289-290.

[45] Alfred van Staden and Hans Vollaard, The Erosion of State Sovereignty: Towards a Post-Territorial World? In: State, Sovereignty, and International Governance, edited by Gerard Kreijen, Oxford University Press 2004, pp. 165-184.

[46] Military and Paramilitary Activities…, supra note 6, Paragraph 205.

[47] Rick Lawson, The Concept of Jurisdiction and Extraterritorial Acts of State, in: State, Sovereignty and International Governance, op. cit., pp. 281-283, see also supra note 15.

[48] The matter of sovereignty in the cyber context is discussed in Tallinn Manual 2.0, op. cit., pp 11-16.

[49] Tallinn Manual 2.0, op. cit., pp. 17-18

[50] Tallinn Manual on the International Law Applicable to Cyber Warfare, edited by Michael N. Schmitt, Oxford University Press 2013, p. 48

[51] Tallinn Manual 2.0, op. cit., pp. 22-23

[52] See the examples of disabling early warning systems or altering geographical data in weapons' guidance systems offered above.

[53] See supra note 44

[54] See supra note 7

[55] Oppenheim's International Law…, op. cit., pp. 505-508.

[56] Adopted by the International Law Commission in 1996, Yearbook of the International Law
Commission, 1996, vol. II, Part Two

[57] Draft Code of Crimes against the Peace and Security of Mankind with commentaries, adopted by the International Law Commission at its forty-eighth session, in, 1996, Yearbook of the International Law
Commission, 1996, vol. II, Part Two, paragraph 5 of the commentary to Article 16, p. 43.

[58] Nazi Conspiracy and Aggression: Opinion and Judgment, Office of United States Chief of Counsel for Prosecution of Axis Criminality, United States Government Printing Office 1947, p.53.

[59] Oppenheim's International Law…, op. cit., pp. 549-550. On due diligence, see also Tallinn Manual 2.0, op.cit., pp. 30-43

[60] Guenael Mettraux, The Law of Command Reposnsibility, Oxford University Press 2009, pp. 100-102, 110-113, 122-123

[61] Oppenheim's International Law…, op. cit., pp. 541, 553; Military and Paramilitary Activities…, supra note 6, Paragraph 115.

[62] Draft Articles…, supra note 7, Art. 1 and 2; Tallinn Manual 2.0, op. cit., p. 84

[63] See supra note 59

[64] Term developed by Col. (ret.) Prof. Charles Dunlap in his speech Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts (2001) Humanitarian Challenges in Military Intervention Conference, November 2001,Harvard University.

[65] Andrés B. Muñoz Mosquera and Sascha Dov Bachmann, Understanding Lawfare in a Hybrid Warfare Context, in NATO Legal Gazette Issue 37 (October 2016) Articles on NATO Current Challenges,

[66] Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 5 September 2014, Paragraph 13, http://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease
(access: 23.03.2017)

[67] H.H. Koh, op. cit., supra note 16, pp. 6-7

[68] The Dukes. Seven Years of Russian cyberespionage, F-Secure Threat Intelligence White Paper, F-Secure 2015

[69] E.g. Operation 'Orchard' conducted by the Israeli Defence Forces; the cyber aspect of it was in detaile described in: Sally Adee, The Hunt for the Kill Switch. Are chip makers building electronic trapdoors in key military hardware? The Pentagon is making its biggest effort yet to find out, posted 1 May 2008, http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch/0, (access 15.05.2017)

[70] See e.g. Islamic State web accounts to be blocked by new police team, posted 22 June 2015, http://www.bbc.com/news/world-europe-33220037 (access 15.05.2017)

NATO Spouses Club's Corner

International Women's Day at Kancelaria Club

8th of March, the International Women's Day, is an important holiday in Eastern Europe and some other countries. This day commemorates the movement for women's rights. It is not an official holiday in Poland, but is still celebrated by giving women flowers and small gifts.

For the NATO Spouses Club it was a perfect occasion for an international celebration at Kancelaria Club. The members of the Club enjoyed food, drinks, dancing and the show, but most of all they enjoyed each other's company. With around 22 nationalities presented in the Spouses Club, it was a truly International Women's Day. ■

Charity Bake Sale

On March 21st and 22nd, several members of the NATO Spouses Club held a bake sale and raised money for the two charities that the Club supports: the Bydgoszcz Orphanage and Szlachetna Paczka. In addition to baked goods, the ladies sold coffee mugs, beer steins and aprons. The sale was a great success. It generated over 1600 zlotys. All the money raised will be used to help the children in the Bydgoszcz Orphanage. ■

EVENTS In Retrospect
Life at JFTC

2016

JFTC at the Grand Rowing Competition of Bydgoszcz

For the third year in a row the Joint Force Training Centre's crew entered the Dragon Boats Race – an integral part of the annual Grand Rowing Competition of Bydgoszcz. The event took place on 24 September and, as every year, drew attention of thousands of Bydgoszcz citizens.

Thirteen JFTC members took the challenge and crossed swords with the team representing the Regional Police – the Centre's traditional rival in this competition. After 2 races, many liters of sweat and a great dose of fun the rivalry came to an end. Again the JFTC oponents turned out to be better, although this time the race was more matched.

Congratulations to the winners!

Strategic Foresight and Framework for Future Alliance Operations Workshop at JFTC

Finalization of defence and security implications for the Strategic Foresight Analysis (SFA) 2017 as well as description of challenges and opportunities in the security environment till 2035 and beyond for the Framework for Future Alliance Operations (FFAO) 2018 were the main topics of a workshop held at the Joint Force Training Centre (JFTC) in September. Major General Wilhelm Grün, the Centre's Commander, welcomed participants of the SFA and FFAO joint meeting on 26 September.

More than 100 representatives from 25 NATO and Partner Nations (22 NATO, 3 Partners), NATO command structures (ACO, LCC) and agencies, NATO Defence College, 15 Centres of Excellence, European Defence Agency, think tanks, academia and industry arrived in Bydgoszcz to participate in the workshop. They met in the JFTC state-of-the-art training facility to exchange their ideas and insights, and to ensure professional development of final products.

Branch Head of SACT's Strategic Analysis Branch, Colonel Tibor Szabo, expressed his gratitude for the excellent support and warm hospitality of the JFTC Staff. "JFTC has provided us a fantastic venue to continue this important work for the future plans of the Alliance."

Resolute Support Training Event 16-4 Successfully Completed

Another group of NATO soldiers got ready for their deployment to Afghanistan. The Joint Force Training Centre (JFTC) conducted its fourth 2016 Resolute Support training event between 18 and 27 October.

More than 150 soldiers from 17 NATO and partner nations gathered in Bydgoszcz to participate in 2016 last pre-deployment training executed by JFTC – half of them to get ready for their future assignment, the other half to support the preparation process.

The RS TE, designed and delivered by JFTC, has been prepared in close cooperation with the Joint Force Command Brunssum (JFCBS). The event aimed at educating the training audience in the specifics of the mission, at training personnel assigned to advisory roles and at creating conditions for team building. It consisted of both an academic part and practical exercises. Such a design of the event allowed the Bydgoszcz NATO training centre to provide the Commander of the Resolute Support mission with uniformly trained staff, fully ready to fulfill their role within a NATO-led operation.

Already on the first day of the event the participants received a broad spectrum of in-depth information about the environment they were going to be deployed to and their future work. It was possible thanks to the presence of two generals representing the RS Headquarters - Major General Paul Brier, the Deputy Commander Civil Outreach, and Major General Martin Smith MBE, the Deputy Advisor to the Afghan Ministry of Interior. They both provided the training audience with key facts and figures on RS and shared their experience which gave future members of the mission a solid background they would need during their deployment.

"Regard your future assignment as a relay race." – said Major General Wilhelm Grün, the JFTC Commander, during his closing remarks. He encouraged the Training Audience not to focus on their time in Afghanistan only. "Make use of accomplishments of your predecessors and pass the knowledge, with a little bit more from you, to your successors." The JFTC Commander emphasized that pre-deployment training delivered by JFTC created a perfect opportunity to learn from experience of former members of the mission, who augmented the events as Subject Matter Experts (SMEs). "The fresh memory can only come from those who have just returned from Afghanistan or from those who are still there" – General Grün highlighted and invited the Training Audience to come back to Bydgoszcz as SMEs to support their successors in the future.

Major General Hans van Griensven, the Deputy Chief of Staff Plans of the Joint Force Command Brunssum (JFCBS) also thanked SMEs for their devotion and assistance. "Some of you have already started your hand over/take over with your predecessors who were here during the training" – the JFCBS Chief of Staff Plans turned to the Training Audience underlining the value of support provided to the event by current members of the Resolute Support mission.

Focusing on soldiers' future deployment, General Griensven stressed the need to change the way of thinking while fulfilling the train, advise and assist mission. "Your biggest enemy is your reference – we all think in a western way. Start thinking in the Afghan way" – the JFCBS Chief of Staff encouraged the soldiers.

Yet again JFTC used its vast experience in pre-deployment training, its modern facility and tools to prove the Centre's key role in supporting NATO missions. The future Resolute Support members gained better situational awareness and understanding of Afghan Security Institutions' as well as Afghan National Defence and Security Forces' structures and processes. They received a high level preparation that would allow them fulfill their mission professionally and successfully from the very beginning.

2017

New Year's Reception at JFTC

Continuation of the Resolute Support training program and increasing involvement in exercises for multinational corps were presented as the Joint Force Training Centre's (JFTC) main plans for 2017. Major General Wilhelm Grün opened another busy year of training for JFTC during the annual New Year's Reception. The event took place on 12 January and gathered close to 80 JFTC partners and friends.

"Our training calendar is full throughout the year, and we will very quickly find ourselves heavily engaged in critical planning efforts for all the training events" – said General Grün. As the event was held two weeks before the start of the first 2017 training for future members of the Resolute Support mission in Afghanistan, the General added: "Resolute Support will continue throughout the year preparing more than 1000 staff members for their deployment (…) I expect us to provide our best professional training during each iteration" – the JFTC Commander underlined.

General Grün also emphasized JFTC's role in building interoperability of the Alliance by continuation of hosting and engaging in the Coalition Warrior Interoperability Exercise. He also marked that the Centre

would focus on deepening its relations with multi-national corps. "I envision an increasing involvement in exercises for multinational corps such as the Multinational Corps Northeast, the German Netherlands Corps and the French Rapid Reaction Corps, and further engagement in high-level readiness exercises such as Trident Joust in September this year" - said General Grün, announcing one of NATO's biggest readiness exercises with Joint Force Command Naples and approximately 700 participants to be trained at JFTC.

To achieve all goals and future plans, the Centre has already intensified efforts in developing its capabilities and capacities.

"We are building a new training area for larger NATO military organizations up to the corps level with the ability to train up to 1000 individuals here at the JFTC" – General Grün highlighted pointing out at construction works initiated within the Centre's compound.

The JFTC Commander also underlined that the Centre's everyday work and continuous development would not be possible without the outstanding support from the regional and local authorities, partners and community. "We owe a lot to the Voivodship of Kujawsko-Pomorskie and the City of Bydgoszcz, as well as to local services such as the Military Hospital, the University and all the other authorities in town" – General Grün expressed his gratitude addressing the New Year's Reception's distinguished guests, including the Mayor of Bydgoszcz, Mr. Rafał Bruski, the Deputy Voivode of Kujawsko-Pomorskie Region, Mr. Józef Ramlau, the Deputy Marshal of the Kujawsko-Pomorskie Region, Mr. Zbigniew Ostrowski and the Deputy Chairman of the City Council of Bydgoszcz, Mr. Jan Szopiński.

"Personally, I feel at home here in Bydgoszcz and I am happy to stay until 2019" – JFTC Commander admitted and wished the guests all the best for the year 2017.

Ready to Train, Advise and Assist in Afghanistan

More than 200 future advisors and staff members of the allied mission in Afghanistan participated in the first 2017 Resolute Support training conducted by the Joint Force Training Centre in Bydgoszcz. The event took place between 24 January and 2 February.

"The whole JFTC staff was committed to offer you the best possible training" – said Major General Wilhelm Grün, the Centre's Commander. In his closing remarks he stressed high value of pre-deployment preparation process and thanked the participants for their devotion during the event.

The event aimed at preparing soldiers for their roles in both executing and supporting the main effort of the mission – training, assisting and advising Afghan counterparts. Its program consisted of two phases. The first focused on delivering information and knowledge on key aspects of the mission, operational environment and on respective positions, roles, functions and responsibilities the soldiers were going to take over in Afghanistan. Phase two allowed for putting theory into practice - with emphasis on processes and procedures within respective headquarters.

"During recent days, you got a picture of your future tasks in Afghanistan. This was done as realistic as possible under given conditions" - said Lieutenant General Erich Pfeffer, the Commander of the Bundeswehr Joint Forces Operations Command. He arrived in Bydgoszcz to address soldiers before their deployment. "I am convinced that you are well prepared to quickly orientate yourself, when you get boots on the ground in Mazar-e-Sharif within the next few weeks or months."

Altogether more than 400 soldiers and civilians representing 27 NATO and partner nations worked hand in hand for the future success of the Allied mission. Half of them received their final preparation before deployment to the RS Headquarters, Train Advise Assist Command-North (TAAC-N) as well as to numerous advisory teams. The other half supported the training with their expertise, in-theatre knowledge and experience.

Among the trainers and Subject Matter Experts (SME) supporting the exercise, there were JFTC members, representatives of various NATO units and agencies, representatives of NGOs but most of all soldiers with relevant theatre experience from Afghanistan, who provided the up-to-date knowledge and information on the Resolute Support mission and Afghanistan. Lieutenant General Salvatore Alejandre, the Deputy Commander of the Allied Joint Force Command Brunssum, who also met with the trainees,

highlighted the utmost importance of SMEs's assistance: "The Subject Matter Experts provided you with the latest information available and now you are well prepared". Nevertheless, he encouraged the participants "to keep an eye on events in Afghanistan" as the country is a very dynamic place.

The need for self-education was also stressed by Lieutenant General Sandy Storrie, the Deputy Commander of the Resolute Support Headquarters. In his address not only did he provide the audience with key information on the situation in Afghanistan and the mission itself, but also gave some personal advice on how to prepare for the deployment.

As for many soldiers the training in Bydgoszcz was the first occasion to meet with their future partners, it also created a perfect opportunity for team building. And good teams are essential for success of the mission. "You should understand yourself as a 'spoke in the wheel' – said General Pfeffer. "Only when you really learn to know each other by heart, when you know your own and your buddies' strength, capabilities and limitations, will you be the team the Commander can rely on."

Graduated Readiness Force (Land) Lessons Learned Working Group Meets at JFTC

Last year's experience with focus on Major Joint Operations (+) and Land Component Command's (LCC) role were main topics of discussions held during the Graduated Readiness Force (Land) Lessons Learned Working Group (GRF3LWG) meeting. The event took place between 28 February and 2 March. For the first time the Group gathered at the Joint Force Training Centre (JFTC).

"Networking, introducing new members and, most of all, discussions on lessons learned from the past year, are key elements in the agenda of every Graduated Readiness Force (Land) Lessons Learned Working Group's meeting" – said Lieutenant Colonel Steffen Röchow, the Chairman of the Working Group. He also underlined the importance of those annual gatherings for strengthening cooperation between different NATO component commands and headquarters. "We receive information from our partner HQs, gain better understanding of processes important to coordination between us, and we share experience and best practices to develop our capacities for the future."

To maximize output and enhance discussions, the Allied Land Command Headquarters invited the Allied Command Operations, Joint Force Commands, Allied Air Command, Allied Maritime Command, Joint Analysis and Lessons Learned Centre, Joint Warfare Centre and JFTC to participate in the GRF3LWG meeting. This was also the first time when NATO Force Integration Units attended the event.

The participants worked during plenary sessions and also within syndicates. Additionally, they received in-depth information about JFTC's capabilities and capacities in support of training, its recent experience and plans for the nearest future.

"It was one of our Working Group's best meetings, also in terms of logistics. Support we received from JFTC was outstanding" – said LTC Röchow at the end of the event.

JFTC Expands Its Activities. Advisory Training in Kosovo

Preparing advisors deployed to support the NATO mission in Kosovo was the main goal of the first training for NATO Advisory and Liaison Team (NALT). The event, conducted by the Joint Force Training Centre's (JFTC) team, took place between 27 and 31 March in Pristina, the capital of Kosovo.

The approximately 40-strong NALT was established in August 2016. It focuses on advising and assisting the Kosovo Security Forces (KSF) and the Ministry of KSF. JFTC, with its vast experience in pre-deployment preparation for advisors going to Afghanistan, was a natural choice to play the leading role in developing the training for members of the new team.

The training program consisted of two modules. The first was dedicated to delivering information on key aspects of the mission and the specifics of the operational environment. The second focused on practical activities and provided opportunities for the trainees to put theory into a practical context.

A small team from the Joint Force Training Centre, acting as the Officer Directing the Exercise, supported this event with its expertise and methodology developed for the Resolute Support Mission pre-deployment training. The concept successfully used in preparing soldiers deploying to Afghanistan was adjusted and tailored to meet the NATO Advisory and Liaison Team requirements. It provided the NALT advisors with the best conditions for learning more about specifics of their mission in Kosovo and allowed them to improve their advisory skills in a safe and controlled environment.

The mission of the NATO Advisory and Liaison Team is to enable NATO to support further development of the Security Institutions in Kosovo by providing advice and support focused on capacity building, education and training coordination.

Preparation for Resolute Support Mission Completed

Between 25 April and 4 May, the Joint Force Training Centre (JFTC) was a magnet for future members of the allied mission in Afghanistan. Approximately 120 soldiers gathered in Bydgoszcz to participate in the Resolute Support training and to get ready for deployment.

During the training event, future advisors as well as soldiers who were going to fill-in various staff positions in the Resolute Support Headquarters (RS HQ) in Kabul and the Train Advise Assist Command-West (TAAC-W) in Herat, received first-hand knowledge related to their anticipated work in Afghanistan. They were provided with in-depth information on key aspects of the mission, operational environment, political, cultural and social situation in Afghanistan as well as on respective positions, roles and responsibilities they would assume upon deployment. The last phase of the exercise allowed the soldiers to examine their ability to put the knowledge into practice.

"This training is a very good mix of theory and practice (…) It gave you a very good grounding and understanding of the mission" – said Rear Admiral Simon Hardern, the Deputy Chief of Staff at the Allied Joint Force Command Brunssum, during the closing ceremony. Admiral Hardern underlined that training in Bydgoszcz gave soldiers a good start for their time in the theatre.

Also Brigadier General Massimo Biagini, the designated Commander of TAAC-W, who participated in the pre-deployment preparation together with his future staff, highlighted the relevance of the training: "It was an important opportunity to increase our knowledge about the mission and its processes, and also very important time for team-building".

Execution of the pre-deployment training would not have been possible without Subject Matter Experts (SME) – especially those with experience from the theatre. Brigadier General Ladislav Jung, the JFTC Deputy Commander/ Chief of Staff, who was also the Exercise Director, recognized efforts of the SMEs: "Predecessors training their successors – it is the most effective way of passing the knowledge (…) Thank you all for your outstanding performance and contribution to the success of this event" – said General Jung. He also passed special words of gratitude to Command Sergeant Major Daniel Hendrex from the Combined Security Transition Command-Afghanistan and Command Sergeant Major David Clark, the Resolute Support/ United States Forces – Afghanistan Command Senior Enlisted Leader. They provided a strong support to the event by delivering yet another portion of up-to-date information related to the situation in Afghanistan and the allied mission.

Chiefs of CIS Support Units Meet in Bydgoszcz

Chiefs of NATO CIS Support Units (CSU) met in Bydgoszcz on 9 and 10 May 2017. The CSU Commanders Conference, organized by the NATO Communications and Information Agency's (NCIA) Directorate of Service Operations and the local CSU, was held at the Joint Force Training Centre (JFTC).

Approximately 40 participants, including Mr. Koen Gijsbers, the NCIA General Manager, and Brigadier General Luigi Tomaiuolo, the Director Service Operations, met in Bydgoszcz to discuss NCIA's current activities and future challenges. This was the first of two conferences of this type planned for 2017.

The NCIA General Manager's visit to JFTC also created a perfect opportunity for discussing cooperation between the Bydgoszcz NATO training centre and the Agency. The NCIA is one of the JFTC's closest partners. It supports the Centre's everyday business and most of all, training events, exercises, workshops and courses conducted in Bydgoszcz. Common JFTC and Agency efforts, as well as possible ways of their further development, were main topics of the meeting held between Brigadier General Ladislav Jung, the Centre's Deputy Commander/ Chief of Staff, Mr. Gijsbers and General Tomaiuolo.

Bi-Strategic Commands IKM Working Group Meets at JFTC

Close to 30 NATO Information & Knowledge Management Officers (IKMO) gathered in Bydgoszcz to discuss ongoing projects and ways ahead. Between 9 and 11 May the Joint Force Training Centre (JFTC) hosted the first 2017 Bi-Strategic Command IKM Working Group.

Representatives of the Allied Command Operations, the Allied Command Transformation as well as IKM experts from their subcommands and associated agencies - including Land, Air and Maritime Commands, Joint Force Command Brunssum, Joint Force Command Naples, Multinational Division Southeast, Combined Air Operation Centre, JFTC, Joint Warfare Centre, Joint Analysis and Lessons Learned Centre, NATO CIS Group and NATO Communications and Information Agency – meet on a regular basis (twice a year) to enhance and streamline the information and knowledge management processes developed and used within the Alliance. This time was no exception.

Discussions between IKM experts touched upon progress and challenges related to implementation of the unified NATO Information Portal, development of new electronic document management and workflow systems. Two companies presented beta versions of software of this type which was a highlight of the event.

The JFTC team's added value to the meeting was presentation of sophisticated IKM solutions applied by the Centre within recent years. Electronic workflows and management tools used by JFTC may become a good example for other NATO commands and units.

JFTC Ball Charity Lottery Supports Residential School in Bydgoszcz

New educational supplies and training tools for physiotherapy will enhance capabilities of the Residential School and Vocational Training Centre Number 3 in Bydgoszcz. The Joint Force Training Centre (JFTC) has equipped the school with didactic and rehabilitation accessories worth more than 6,000 PLN. The money was collected during the JFTC Ball charity lottery.

On 8 June, Colonel Wojciech Czerwiński, the JFTC Headquarters Support Division Head, met with the school leadership, teachers and most of all with pupils to hand over the presents.

"This equipment will support your educational efforts when you are back after the summer break" – said COL Czerwiński addressing the students. "Now, it is time to relax after a very busy school year. But once you are back to school, make good use of the new tools."

As in the past, the school presented a beautiful music and dance performance to thank JFTC for the support. "We think that is the right way of showing how we appreciate all you do for us" – said Mrs. Alicja Kruzel, the Headmistress, "Thank you for remembering about our school and for being there for us."

Resolute Support Commander at JFTC Pre-deployment Training

Another group of future members of the Resolute Support (RS) mission arrived in Bydgoszcz to receive their final preparation before deployment. On 25 July, the Joint Force Training Centre (JFTC) opened the third 2017 iteration of its flagship training. The second day of the event was marked by the visit of General John W. Nicholson, the Resolute Support Commander. In his address to the participants he shared his thoughts and current information on situation in Afghanistan.

"This region is very important for global stability" – stressed General Nicholson and underlined the key role of NATO troops in positive changes observed in Afghanistan. "We have accomplished a lot. Our nations have. You have". The Resolute Support Commander also quoted words of Mr. Ashraf Ghani, the President of Afghanistan, showing the meaning of the allied mission to the country: "The Resolute Support legacy to Afghanistan will not be guns and ammo (…) but the systems and processes that you leave behind".

To make the Resolute Support mission successful, close to 400 soldiers and civilian experts representing various nations and institutions are now working hand in hand in Bydgoszcz during the Resolute Support pre-deployment training.

"Use this training event and a very realistic environment we replicated here for you to get acquainted with the situation you will find once in Afghanistan" – said Major General Wilhem Grün, the JFTC Commander, during the opening ceremony. The General, who is also the Exercise Director, emphasized the importance of the pre-deployment training, its theoretical and practical parts and also its teambuilding aspect: "Use time spent in Bydgoszcz also to build 'esprit de corps' that will help you in supporting your commanders and in completing your mission successfully."

By implementing the most current expertise, the training responds to the requirements of Resolute Support commanders and to the needs of the allied advisors in Afghanistan. During the event, the trainees achieve a high level of proficiency, and NATO headquarters gain readiness to train, advise and assist their Afghan counterparts.

General Salvatore Farina, the Commander of Joint Force Command Brunssum (JFCBS), who addressed the Training Audience via video teleconference, underlined significant progress in Afghanistan and its citizens' well-being that has been made throughout the recent years. "You will witness many changes and also challenges in Afghanistan. But I am confident that with your effort we will go along with the progress (…) 'More together!'" – said General Farina recalling the JFCBS's motto.

Also the representative of the Commander of the Bundeswehr Joint Forces Operation Command, Colonel Leonhard Hirschmann, put emphasis on positive changes in Afghanistan. He mentioned progress in the field of economy, anti-corruption processes and education for girls, and thus underlined the importance of the Resolute Support mission and its pre-deployment training. "The Resolute Support training event (…) is a unique opportunity for a common, yet individually shaped training throughout all tiers of the mission to create mutual understanding for each other and to form a team" – said Colonel Hirschmann. He added: "For this ambitious project, I could not imagine a better training environment than the Joint Force Training Centre."

The JFTC role in the pre-deployment training for Resolute Support mission was also recognized by General Nicholson. "I appreciate all the work you do to prepare my staff for the mission" – said the Resolute Support Commander during discussions on the future of the training and opportunities offered by the Joint Force Training Centre.

VISITS In Retrospect
Life at JFTC

2016

JFTC Hosted the German Ambassador

His Excellency Mr. Rolf Nikel, the Ambassador of the Federal Republic of Germany to the Republic of Poland, paid a visit to the Joint Force Training Centre (JFTC). On 22 September he met with the Centre's Commander, Major General Wilhelm Grün.

The JFTC as the focal point for NATO joint and combined training and German soldiers' life in Poland – these were some of the main topics of discussions between the Ambassador and the Commander.

The distinguished guest, accompanied by the Honorary Consul of the Federal Republic of Germany in Bydgoszcz, Dr. Jarosław Kuropatwiński, PhD, was briefed on the JFTC mission and its main activities. He also had a chance to see the state-of-the-art training facility, where every year thousands of soldiers train before their deployment to Afghanistan, where commanders and their staffs achieve full readiness or where interoperability between various systems used by NATO nations and agencies as well as new solutions improving the Alliance's performance are tested.

At the end of the visit, General Grün invited Ambassador Nikel to a meeting with German personnel of the Bydgoszcz NATO training centre. This created a platform for exchange of experience related to their service in Poland and for broader fruitful discussions.

Maintaining Good Relations with Regional Authorities. Major General Wilhelm Grün Pays Courtesy Visits

Photo: Andrzej Goiński, Courtesy of the Marshal's Office of the Kujawsko-Pomorskie Region

Meetings with regional authorities opened a series of Major General Wilhem Grün's courtesy visits. On 26 September, the new Joint Force Training Centre (JFTC) Commander met with Mr. Mikołaj Bogdanowicz, the Voivode of Kujawsko-Pomorskie Province. The day after, he was hosted by the Region's Marshal, Mr. Piotr Całbecki, in Touń.

The discussions focused on possible ways of developing good relations between the parties, common efforts, programs and promotion of the region. Also the situation of the Bydgoszcz airport, education, the International School of Bydgoszcz and cooperation with universities were touched upon as key topics for the international community living in Bydgoszcz.

The first and very fruitful meetings pave the way for maintaining and enhancing effective collaboration as well as partnership between JFTC and regional authorities.

Head of the Polish National Security Bureau at JFTC

Mr. Paweł Soloch, the Head of the Polish National Security Bureau, visited the Joint Force Training Centre (JFTC) on 29 September. During his meeting with the Centre's Commander, Major General Wilhelm Grün, and Deputy Commander/ Chief of Staff, Brigadier General Ladislav Jung, he was accompanied by Brigadier General Jarosław Kraszewski, the Director of the Armed Forces Supervision Department.

As this was Minister Soloch's first visit at the Bydgoszcz NATO training centre, he received much of information about the JFTC, its mission, structure, main areas of focus and activities. The discussions also touched upon the JFTC support to current operations as well as its key role in building NATO's future.

To give Minister Soloch and General Kraszewski a better overview of JFTC as a flagship of NATO training, General Grün invited his guests for a walk through the facility. This part of the visit was combined with a demonstration of simulation tools that enable JFTC to provide a state-of-the-art training support to setting the stage for exercises reflecting the operational reality.

"Thank you for fulfilling this very important allied mission" – Minister Soloch wrote in the JFTC guestbook and expressed his wishes of further success for the Centre.

Future Vice Chief of Staff at SHAPE Visits JFTC

Lieutenant General Hugues Delort-Laval, the designated Supreme Headquarters Allied Power Europe's (SHAPE) Vice Chief of Staff, visited the Joint Force Training Centre (JFTC) on 10 October. He met with Major General Wilhelm Grün, the Centre's Commander, and his Deputy, Brigadier General Ladislav Jung.

The JFTC's key role in NATO training and thus in shaping the future of the Alliance was the main topic of discussions held during the visit. General Delort-Laval received comprehensive information on the Centre's mission, structure, current activities as well as plans for future development. This, together with a walk through the facility, gave the JFTC guest a broad understanding of the Centre as a flagship of NATO training dedicated to Connected Forces Initiative's principles and as the state-of-the-art platform for experimentation.

"I know the importance of the Centre and I am determined to help SHAPE support to the greatest possible extent" – wrote General Delort-Laval in the JFTC guestbook.

Photos: Robert Sawicki, Courtesy of the City Hall of Bydgoszcz

General Grün Meets with Local Authorities and Explores Military Installations

Meetings with Mr. Rafał Bruski, the Mayor of Bydgoszcz, Mr. Zbigniew Sobociński, the Chairman of the City Council, as well as with Colonel Grzegorz Wasielewski, the Director of the NATO Military Police Centre of Excellence and Major Paweł Szymański, the Deputy Commander of the 3rd NATO Signal Battalion, marked the second part of courtesy visits Major General Wilhem Grün paid to local authorities and institutions. The visits took place between 12 and 17 October.

After meetings on a regional level, held in September, the Joint Force Training Centre (JFTC) Commander focused on discussions with the highest representatives of Bydgoszcz municipality. On 12 October General Grün met with the Mayor of Bydgoszcz and five days later he visited the Chairman of the Bydgoszcz City Council. Both meetings were devoted to current cooperation between JFTC and the City of Bydgoszcz, and to possible ways of maintaining and deepening close relations with the local community.

On 13 and 17 October, JFTC Commander visited two NATO entities based in Bydgoszcz – respectively the 3rd NATO Signal Battalion (3NSB) and the NATO Military Police Centre of Excellence (MP COE). Discussions with their leadership touched upon missions, capabilities and main activities of both institutions. As 3NSB hosted General Grün during one of its internal evaluation exercises, the JFTC Commander had an opportunity to observe the unit working at full speed. The two fruitful meetings provided General Grün with a better picture of 3NSB and MP COE, and thus paved the way for future development of cooperation between these institutions and JFTC.

Visegrad Group Directors Visit JFTC

The Joint Force Training Centre (JFTC), its mission and role in NATO transformation were main topics of the visit Visegrad Group Directors paid to the Bydgoszcz NATO Training Centre. They met with Major General Wilhelm Grün, the Centre's Commander, and his Deputy, Brigadier General Ladislav Jung, on 18 October.

Representatives of Czech, Hungarian, Slovak and Polish delegations arrived in Bydgoszcz on the first day of the Resolute Support Training Event, which gave them an opportunity to observe soldiers from various NATO and partner nations working hand in hand for a success of the allied mission in Afghanistan. This was a perfect illustration of all the information the guests received during briefings that introduced them to JFTC, its tasks and main activities.

Discussions with the Centre's leadership and key staff provided the Visegrad Group Directors with broad understanding of JFTC vital position within the Alliance and also with information about capabilities used in shaping NATO's future by delivering professional and up-to-date training for NATO forces. The demonstration of modelling and simulation tools used by the Centre in support of training completed the picture, showing JFTC as a modern institution able to fulfill NATO's evolving requirements.

Resolute Support Deputy Commander Mentors Participants of JFTC Pre-deployment Training

Lieutenant General Sandy Storrie CBE, the Deputy Commander of the Resolute Support Headquarters (RS HQ), arrived at the Joint Force Training Centre (JFTC) to observe and support the 2016 last pre-deployment training for the RS mission. He met with Major General Wilhelm Grün, the JFTC Commander, and the Exercise Director, as well as with participants of the training on 21 October.

As experience and knowledge shared by current or former members of the mission are important assets in soldiers' pre-deployment preparation process, visits of RS HQ leaders are always key moments of training events for future allied staff going to Afghanistan. General Storrie, the RS HQ Deputy Commander, provided participants of the training with yet another portion of up-to-date information related to the situation in Afghanistan and their future assignment.

Thanks to the visit, the Training Audience had an opportunity to interact with the RS HQ leadership, which was of utmost importance right before their deployment. On the other hand, General Storrie and also Command Sergeant Major Clark, the Resolute Support/ United States Forces – Afghanistan Command Senior Enlisted Leader, who visited the training area at the same time, had a chance to engage in the training, observe the participants, both Exercise Control and Training Audience, working hand in hand for future success of the mission and to learn more about JFTC as the flagship of NATO pre-deployment training.

Talks with LANDCOM Commander on Mutual Reinforcement

The Joint Force Training Centre's (JFTC) capabilities and development of Centre's cooperation with the Allied Land Command (LC) Izmir were main topics of discussions held in Bydgoszcz between Commanders of these two headquarters. Lieutenant General Darryl Williams, the LC Izmir Commander, met with Major General Wilhelm Grün and observed the JFTC training capabilities on 28 November.

General Williams met with the JFTC Commander and his key staff to explore the Bydgoszcz NATO training centre. This was his first visit to Bydgoszcz since he assumed the position of the LC Izmir Commander.

Detailed briefings explaining the Centre's role in NATO training process, presentations of divisions and interactions with JFTC key officers provided the LC Commander with a broad picture of the Centre's capabilities and what its aspirations and plans for future development were. It also revealed certain areas where common efforts of both headquarters could be initiated or intensified and also where JFTC expertise, know-how and infrastructure could serve best in support of the Allied Land Command training requirements. General Williams marked that the meeting was a good step towards mutual reinforcement and tightening partnership between JFTC and LC Izmir.

The visit took place during Citadel Bonus 2016. It created an excellent opportunity for the JFTC guest to observe the Centre hosting a large and very complex exercise. It was a perfect illustration of JFTC capacities.

2017

On Innovations at JFTC with Air Marshal Stacey

The Joint Force Training Centre's (JFTC) expansion, future development of training capacities and pre-deployment preparation for the Resolute Support mission were main topics of discussions between Air Marshal Sir Graham Stacey, the Allied Command Transformation (ACT) Chief of Staff (COS) and JFTC leadership. The ACT COS visited the Centre on 1 February.

The areas, often highlighted by Major General Wilhelm Grün, the JFTC Commander, as the Centre's focal points for the near future, predominated meetings arranged between the JFTC key personnel and the distinguished guest. Changes in the Centre's structure, planned to be implemented later this year, as well as current development of the compound created a platform for discussions on new opportunities for JFTC and its training offer. A vision of increased involvement in exercises for multinational corps and broader engagement in high-level readiness exercises was brought to the ACT COS's attention. These new fields of expertise are opening thanks to the ongoing evolution of the Centre. Stressing the JFTC's key role in NATO training, Air Marshal Stacey assured Major General Grün of his support for the Centre's efforts.

As the visit took place during the first 2017 edition of the Resolute Support training, the ACT COS had a chance to explore the event. He received in-depth information on the training from both JFTC personnel executing the exercise and future advisors undergoing their final preparation before deployment to Afghanistan. Air Marshal Stacey met with the trainees and underlined the importance of their future role. He also emphasized the significance of pre-deployment training and thanked the "fantastic team at JFTC" for their professionalism and dedication in supporting the Resolute Support mission.

Major General Sanz Explores JFTC

The Joint Force Training Centre's (JFTC) development dominated discussions between the centre's leadership and Major General Alfredo Sanz, the Supreme Headquarters Allied Powers Europe's Deputy Chief of Staff for Resources. General Sanz met with Major General Wilhelm Grün, the JFTC Commander, and his key staff on 6 April.

General Sanz was briefly introduced to the JFTC and its ongoing efforts aiming at increasing the centre's capacities in support of training. The new Command Post Training Area construction works within the JFTC compound, as well as testing innovative solutions in the centre's Peacetime Establishment were discussed first. The JFTC Commander presented his vision of JFTC as a unique training facility within NATO where training headquarters could deploy elements of their Command Post structures. At the same time, the centre will be capable of conducting exercises up to Joint Force Command level with up to 1000 soldiers involved. All this falls in line with the current training needs and requirements of the Alliance, expressed by two strategic commanders - the Supreme Allied Commander Transformation and Supreme Allied Commander Europe.

As this was General Sanz's first visit to the Joint Force Training Centre, he also received in-depth information on the centre's current activities and training capabilities. Presentations prepared by the JFTC divisions heads as well as a walk through the centre's compound gave him a broad picture of JFTC as the flagship of NATO training and state-of-the-art platform for experimentation and testing.

The Supreme Headquarters Allied Powers Europe's Deputy Chief of Staff for Resources used his stay in Bydgoszcz also to explore other allied units based in this NATO Capital of Poland. On the last day of his visit, General Sanz met with the Commanders of the 3rd NATO Signal Battalion and the NATO Force Integration Unit.

High Ranking Visitors Explore JFTC

On 4 May, the Joint Force Training Centre (JFTC) finalized its second 2017 training for Resolute Support mission. Traditionally, a JFTC flag event drew attention of numerous visitors, who used this opportunity to see the centre working at full speed and to discuss future cooperation with JFTC leaders.

Brigadier General Jürgen von Sandrart, Asistant Chief of Staff at the Supreme Headquarters Allied Powers Europe, visited JFTC on 27 and 28 April. He arrived in Bydgoszcz to explore possible ways of future cooperation. General von Sandrart, accompanied by General (ret'd) Egon Ramms, met with JFTC Commander, Major General Wilhelm Grün, and his key staff. During long and vivid discussions, the parties identified common goals that will become a basis for further engagements.

A walk through the JFTC training area and observation of the Resolute Support event were a perfect summary of the visit. They provided the guests with a broad illustration of centre's abilities and capacity.

Also Major General Ian Cave, the Deputy Chief of Staff for Plans at the Joint Force Command Naples, used the opportunity created by the Resolute Support training event to see the JFTC staff working hand in hand for success of the allied mission. He visited the centre on 2 and 3 May to talk through ways ahead related to the Trident Joust 17 Exercise.

Meeting with the JFTC Deputy Commander/ Chief of Staff, Brigadier General Ladislav Jung, and personnel responsible for the exercise, allowed the JFTC guest to discuss the progress of preparations and scenario development.

On 3 May, JFTC also hosted a visit of Brigadier General Henrik Lyhne, the Commander of the 1st Danish Brigade. He arrived in Bydgoszcz to explore the Resolute Support training event and to meet with Danish soldiers receiving their final preparation before deployment to Afghanistan.

Commander of the Multinational Division Southeast Explores JFTC

Possible ways of support and future cooperation dominated discussions between leaders of the Joint Force Training Centre (JFTC) and the Multinational Division Southeast (MND SE). Major General Wilhelm Grün, the JFTC Commander, met with Brigadier General Ovidiu Uifaleanu (ROU A), the MND SE Commander, on 16 May. The Romanian General's visit took place during a scripting event for the Trident Joust Exercise 17.

General Grün, supported by his key staff, introduced the guest to JFTC and presented its current shape and priorities. The talks also touched upon ongoing processes with the aim of increasing the Centre's capacities in support of NATO training. In-depth information about infrastructure expansion, efforts related to optimization of the Centre's Peacetime Establishment or CIS capabilities development, gave the MND SE Commander a broad picture of JFTC, its training capabilities and ambitions. This, combined with observation of the currently ongoing workshop focused on tailoring Exercise Trident Joust 17, laid foundation for discussions on future cooperation.

MND SE is currently preparing for Dacian Lancer - a certification exercise planned for spring next year. The closer look at the scripting event and links established during the visit will let the Division take advantage of JFTC experience, know-how and work – including the development of the scenario that will be used during both Trident Joust 17 and Dacian Lancer 18 exercises.

"Thank you for what you are doing for the soldiers" – General Uifaleanu addressed the JFTC Commander and his staff. "I cannot find a more important endeavor than keeping the institutional memory alive and passing all the military knowledge to new generations."

National Liaison Representatives to HQ SACT in Bydgoszcz

Fifteen National Liaison Representatives (NLR) to the Supreme Allied Commander Transformation Headquarters (HQ SACT) visited the Joint Force Training Centre (JFTC). On 17 May, the group met with Major General Wilhelm Grün, the Centre's Commander, and his key staff.

The guests, led by Danish NLR, Brigadier General Steen Hartov, arrived in Bydgoszcz to learn more about the Centre and also to see its expanding facilities. The development of JFTC capacity in support of NATO training was one of the main topics of discussions.

JFTC leaders provided the NLRs with a broad overview of JFTC current priorities, future plans and ongoing efforts that aim at rising to evolving training requirements. The guests were especially interested in the Centre's infrastructure expansion, optimization of the Peacetime Establishment, CIS capabilities development and their influence on the existing training potential. During a walk around the Centre they had a chance to see the progress of construction works throughout the compound.

The discussions also touched upon JFTC's ability to execute training in remote locations as well as cooperation with Centres of Excellence, NGOs and nations. As NLRs serve as links between their capitals and the HQ SACT, the JFTC Commander highlighted the key role of close and effective cooperation with nations as the basis of success of the Alliance and its respective headquarters.

TRANSFORMATION THROUGH TRAINING