



Issue 16
1st Issue 2018
ISSN: 2242-441X

nmiotc

*Maritime Interdiction Operations
Journal*

NATO MARITIME INTERDICTION OPERATIONAL
TRAINING CENTRE

**The use of Simulation in Collective Training
for Maritime Interdiction Operations**

**Clausewitz's "Wonderful Trinity" of War in
the 21st Century: A Commentary on the use
of Artificial Intelligence in Modern Warfare**

**Disaster Relief Operation and Gender
Perspectives**

**SAURON Real-life Scenario: A Terrorist
Coordinated Attack in a EU Port**

**9th NMIOTC Annual Conference
Food for Thought Paper**





NATO Maritime Interdiction Operational Training Centre

3rd Conference on Cyber Security in the Maritime Domain



10 - 11 April 2019

CONTENTS



COMMANDANT'S EDITORIAL

4

Editorial by Stelios Kostalas
Commodore GRC (N)
Commandant NMIOTC

MARITIME SECURITY

6

The use of Simulation in Collective Training for Maritime Interdiction Operations
by James Rapp, Senior Advisor, CAE Defence & Security

22

SAURON Real-life Scenario:
A Terrorist Coordinated Attack in a European Union Port
by Ph.D.(c) Eleni-Maria Kalogeraki, Dr. Spyridon Papastergiou,
Associate Professor Nineta Polemi, Professor Christos Douligeris

28

9th NMIOTC Annual Conference
Food for Thought Paper
by NMIOTC

TECHNOLOGICAL ISSUES

11

Clausewitz's "Wonderful Trinity" of War in the 21st Century:
A Commentary on the use of Artificial Intelligence in Modern Warfare
by George Kiourktsoglou
Lecturer, University of Greenwich, London

GENDER ISSUES

18

Disaster Relief Operation and Gender Perspectives
by Cdr Junko Kawashima, Japan Maritime Self Defence Force

HIGH VISIBILITY EVENTS

31

NMIOTC TRAINING

39

MARITIME INTERDICTION OPERATIONS JOURNAL

Director

Commodore S. Kostalas GRC (N)
Commandant NMIOTC

Executive Director

Captain R. Lapira ITA (N)
Director of Training Support

Editor

Commander P. Batsos GRC (N)
Head of Transformation Section

Layout Production

Lieutenant JG I. Giannelis GRC (N)
Journal Assistant Editor

The views expressed in this issue reflect the opinions of the authors, and do not necessarily represent NMIOTC's or NATO's official positions.

All content is subject to Greek Copyright Legislation.
Pictures used from the web are not subject to copyright restrictions.

You may send your comments to:
batsosp@nmioct.nato.int



NMIOTC Commandant's Editorial

This year's NMIOTC Annual Conference coincided with a very significant date, the anniversary of the World War II landing in Normandy - Operation Overlord, which was the most complex amphibious operation ever to be undertaken. The largest naval, air and land operation in history of mankind.

Seventy four years have passed since then and the security environment has fundamentally changed. The Alliance faces an arc of instability and insecurity along its periphery and beyond: challenges and threats originate from both, the east and the south. "We don't only see a more assertive Russia; we

see all the instability, the violence to the south of our Alliance: Iraq, Syria, the Middle East, North Africa". (Address by NATO Secretary General Jens Stoltenberg to the NATO Parliamentary Assembly, Warsaw, Poland, May 2018).

At this pivotal time, we need to be strong and continue to adapt our collective efforts aligning them with those of the international community's to project stability, ensuring deterrence, defense and Maritime Security. The challenge in the south provides an opportunity to enhance regional understanding and situational awareness,

aiming at creating a safer and better world.

NATO's adaptation, commitments for projection of stability, and implementation of the initiatives post Brussels (22 February 2005) and Warsaw (8-9 July 2016) Summits, call for opportunities for training for the Allies along with their five Enhanced Opportunities Partners (Georgia, Sweden, Finland, Australia and Jordan). Training is perceived as soft power, low profile, low intensity, high efficiency, long endurance engagement and under this concept will only strengthen cooperation between NATO, the European Union

and the broader international community of interest for Maritime Security Operations.

Our societies are societies of values, including individual liberty and prosperity, human rights, democracy and the rule of law. These shared values are essential to what we do. Not only we share the same principles, but we are dedicated in and unified to the common effort to stand up for those. The importance of carefully balance between East and South sets a serious burden on us, here in NMIOTC for a simple reason; we lay at the Southeast side of the Alliance's footprint and we are committed to dedicate our capacity and potential to provide training to those involved with MSO Tasks. The presence of Alliance's ships and teams here in NMIOTC, is considered by us as commitment of high impor-

tance to our values, principles and norms and transmits widely, a significant message for our contribution to the Alliance in regards to supporting security in the maritime environment.


The first article of our journal presented by Mr James Rapp CB addresses "The Use of Simulation in Collective Training for Maritime Interdiction Operations / A White Paper for the NATO Maritime Interdiction Operational Training Centre". It is followed by an interesting take of Mr George Kiourtsoglou on "Clausewitz's 'Wonderful Trinity' of War in the 21st Century: A Commentary on the use of Artificial Intelligence in Modern Warfare". Cdr Junko Kawashima of Japan Maritime Self Defence Force focuses upon the "Disaster Relief Operation and Gender Perspectives". Finally, we have a four authors' article, Ph.D.(c) Eleni-Maria

Kalogeraki, Dr. Spyridon Papastergiou, Associate Professor Nineta Polemi and Professor Christos Douligeris present the "SAURON real-life Scenario: a Terrorist Coordinated Attack in a European Union Port".

Having said that allow me to highlight the NMIOTC Cyber Security conference next April is the ongoing commitment of NMIOTC to tackle the cyber security issues in the Maritime Environment, an area and a topic that will dominate our efforts intensively, at least for the next decade. It will be another stepping stone for NMIOTC to engage with the international community to create opportunities for a better understanding and to support the cyber security at sea that will eventually reduce potential cyber threats to the international maritime community for the years to come.

Stelios Kostalas
Commodore GRC (N)
Commadant NMIOTC





The Use of Simulation in Collective Training for Maritime Interdiction Operations

by James Rapp
Senior Advisor, CAE Defence & Security

1 Introduction

As NATO acknowledged when establishing its Maritime Interdiction Operational Training Centre (NMIOTC), maritime interdiction operations (MIO) can be multifaceted and may also involve the full spectrum of maritime warfare. In many cases, there will be a complex geopolitical situation to add to the challenge confronting the command. All this adds to the importance of suitable education and training. As a training centre for MIO, the NMIOTC plays an important role in the development of doctrine and procedures and in preparing ship's teams through a mix of classroom instruction, some simulation and live training. Live training is important but has its limitations, and can also be difficult to achieve within a ship's programme. This paper considers the use of simulation in collective training for MIO, and how industry can help provide cost effective, flexible training solutions. In assessing how training is best undertaken, an integrated approach is

needed which considers how best to deliver every element of training from individual to collective. This paper does not address how industry can assist in the delivery of an Integrated Training Solution, but a summary of CAE's methodology is included as an Annex.

2 The Training Challenge

2.1 The Wider Training Challenge

Upgrading existing naval fleets with complex ships, aircraft and weapon systems brings with it the challenge of providing realistic cost-effective training, while at the same time maximizing the availability of personnel for frontline service. Added pressures arise from the increasingly intricate and uncertain nature of the operating environment, including for MIO.

Modern warships are technically complex. Some are specialized for a designated warfare role but may also have modular components to give

flexibility for multi-faceted missions. Highly automated onboard systems are also leading to smaller ships' crews. These factors are driving change in onboard routines, and demanding operational programmes are also reducing the time available for training onboard. These factors are especially significant when looking to maintain perishable skills and when scheduling collective training for disciplines that are not routinely required.

Many new warships are designed to deploy for long periods and the practice of exchanging crews in theatre rather than rotating ships is increasing. Under this operating pattern, naval training needs to provide readily available and flexible shore and ship based training media, to enable effective training and to keep the crew prepared for current and upcoming missions.

2.2 The MIO Training Challenge

Prior to entering an operational theatre to conduct MIO, most navies

recognise the benefit of undertaking focused collective training in scenarios that reflect the assigned mission. This helps to ensure a unit has the necessary knowledge and skills at every level, from the command down to individual members of the boarding team. However, there are several obstacles that may hinder delivery of effective live MIO training including:

- Operational programme pressures, driven for some by ship availability and for others by limited budgets.
- MIO sometimes being considered a low-key task, making MIO training 'nice to do' rather than 'essential'.
- Being able to assemble and maintain the infrastructure needed to deliver training that is suitably demanding to add value and instil confidence in a ship's team.
- The limitations of conducting realistic end-to-end live training involving new generation aircraft and ships, notably: complex security protocols; EMCON restrictions; the need for larger operating areas; and a red force with much more capability.

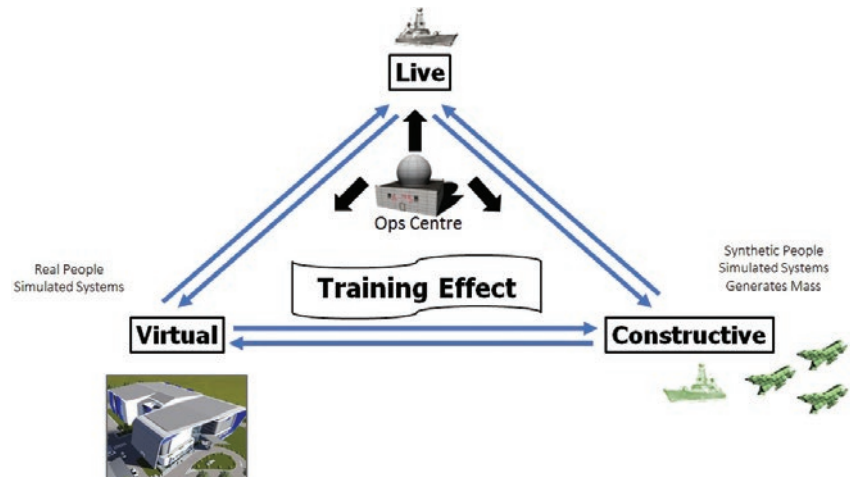
For these reasons, it is becoming more difficult to assemble a suitable force mix, both as own and as opposing forces, to create live MIO training to test every level onboard. MIO training is less than complete if it does not go beyond the procedural and tactical elements of conducting a boarding operation.

This paper will now address those aspects of MIO training that can be enhanced by greater use of synthetic training, whilst recognising that live training will always remain an essential component.

3 Live Virtual Constructive Training

There is much talk today of 'Live Virtual Constructive Training' (LVC(T)) as the optimum future training

solution. LVC(T) links live and virtual training and then adds computer generated forces (CGF) (constructive simulation) all within a common operating environment. This promises to create scale and a better setting for testing modern sensors and weapons. In doing so, it should also solve some of the scheduling and budgetary pressures confronting navies today, and help to overcome the limitations of live training for modern weapons and sensors.



The acronym 'LVC' is frequently used but not always fully understood. This Table explains its three components.

The LVC construct makes use of the following technologies:

- Embedded simulation.
- Datalinks – ship-to-ship, ship-to-aircraft, aircraft-to-aircraft, aircraft-to-surface.

- Wide area networks to allow communication between air and surface assets.
- Common database (CDB) protocols. The CDB is an open, standard database that defines a single synthetic representation of the world. It allows for a common correlated real/synthetic environment within and across each of the LVC domains. It also allows for the correlation of multiple databases in varying formats in real-time. This includes out-the-window

visual scenes in a simulator, plus all other systems in simulators, such as sensors, Computer Generated Forces (CGF) and navigation systems.

- Synthetic environment databases built to the CDB specification allow multiple synthetic training devices to draw from a single central database, ensuring correlation and enabling quick database modifications when required. The

Table 1. Description of LVC Components

Item	Price
Live Training	Real people operating real systems in operational units. Live participants operate live systems and platforms (including their full range of mobility) in the physical environment. In this case, real people using real equipment are required to conduct training with and against notional forces. The realism of such training can be enhanced using embedded simulation, and by connecting to a constructive simulation environment in real time.
Virtual Training	Real people operating simulated systems. Live participants operate an operational system, such as a radar or weapons platform, in a synthetic environment, including distributed mission operations. In this case, real people interact with simulations and computer-generated forces.
Constructive Training	Virtual forces operating virtual systems (controlled by real people). Those forces can be controlled by live participants, typically command and staff trainees, or have their own artificial intelligence and behaviour. The trainees provide stimulus to simulated forces at all levels and act upon the consequences generated by the simulation.
LVC Training (LVC(T))	Training that blends all three components above in a common operating environment, with the operational picture shared through fixed networks or data links.

CDB promotes interoperable training and mission rehearsal while reducing database development, configuration control and publication time and cost.

- Ground mission coordination, record and playback briefing centre.
- Instrumented training ranges with time and space positioning information to allow the monitoring of flight and ship operations and the gathering/recording of flight data.

Integrating these LVC technologies is expected to bring real benefit to navies who can afford to invest in such training infrastructure. It creates a demanding environment for the full range of units, including 5th Generation aircraft and modern ship sensors, and would also enhance MIO training, particularly in scenarios involving other warfare disciplines.

4 Graduated Team Training

However, before being able to exploit

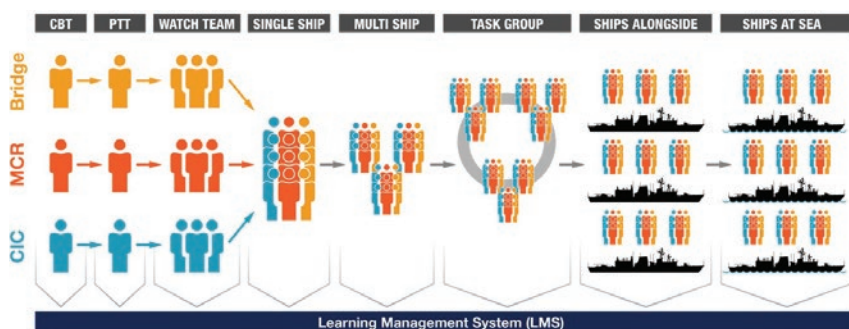


Figure 2: Graduated Team Training

the training benefits of LVC(T), success in MIO will continue to depend on having well trained personnel who have undertaken focused collective MIO training. Unless these building blocks are in place investing in complex LVC(T) architectures are unlikely to be cost-effective. Training must be integrated, starting with the individual, and then graduating upwards to full team training, whole ship training, task group, joint and then coalition training.

5 The Use of Simulation for Collective Training for MIO

Short of full LVC(T) and all it has

to offer, the two key 'teams' where collective training for MIO can be enhanced using simulation are the Command Team and the Boarding Team.

For the Command Team, the greater complexities associated with the Command and Control of MIO may best be addressed and then practised using constructive simulation, with virtual units having the right characteristics being directed by the Command Team and then responding as they would for real. Role players representing other authorities, such as higher command, NGOs, and the Press can add to the realism of the scenario. For the Boarding Team, virtual reality training can augment but should not replace live training. In both cases, in-built after action review processes support objective assessment of performance and allow scenarios to be re-run to allow a different courses of action to be taken.

6 Boarding Team Training

Boarding Teams will always need live collective training but there are significant benefits if augmented by virtual reality simulation. Virtual training can improve operator skills and teamwork and potentially allows training to be completed more rapidly. Using a virtual reality immersive trainer, a boarding party can be trained in a practically unlimited number of situations. One solution presented to the NMIOTC previously by CAE in conjunction with Re-liON is the Re-liON Small Unit Immersive Trainer. The wider benefits of this type of training

were described in a past journal by Chris Haarmeijer, Re-liON's CEO . This training system creates a virtual network by having individuals use lightweight equipment that includes:

- a full-body smart vest with wearable sensor system,
- a headset with head or helmet mounted visual system and
- replica weapons.

Each member of the Boarding Party wears a set of this equipment and a combination of up to sixteen individuals and instructors may be wirelessly networked together for training. The wearable system is synchronized with central simulation control (EXCON) to ensure that each boarding party member shares the same view of the digital battlespace.

Virtual training effectively compresses training time: instead of travelling to different training locations, each can be simulated in one physical location. This frees up time to rehearse a larger variety of scenarios and assess actions taken by full debriefing using the inbuilt after-action review system.

Another important benefit is that this virtual training system is easily transportable; and if so desired, multiple systems can be networked to support multiple-unit training in a common scenario in different locations.

7 Command Team Training

Modern simulation offers realistic MIO training and rehearsal for commanders in realistic scenarios. The NMIOTC already reinforces its courses for Command Teams with training in its MIO Simulator using a network of PCs. These can potentially be enhanced using a network of reconfigurable tactical mission training systems (TMT) or through constructive simulation using PCs; the latter is used extensively by land force commanders but is also suitable in a naval setting. In either case, computer generated forces are used to simulate

<p>1. High learning value Scientifically validated Rapidly exercise complex scenarios After Action Review Fully Immersive</p>	<p>3. Cost Effective Train any situation in any culture Rapid scenario generation Easy to operate and maintain Safe, zero risk</p>
<p>2. Train as you operate Team based Natural locomotion and arm gestures No mouse and keyboard required Scales in floor coverage Wireless weapons</p>	<p>4. Flexible Mobile system Train anywhere anytime No travel time to specialist ranges Create your own scenario Interoperable</p>

Table 2. Advantages of Virtual Training

various entities: warships, merchant ships, submarines, aircraft, and other offshore installations. An exercise controller defines the synthetic training area and scenario, leading to command teams being trained on the application of MIO doctrine (such as legal considerations, Rules of Engagement (ROE), intelligence support, media operations) and most importantly effective communication. Often in a coalition of the willing, data links and other data transfer processes will not be compatible.

7.1 Providing Command Team training using a Tactical Mission Trainer (TMT)

CAE has developed a TMT using commercial-off-the-shelf (COTS) software and CAE's synthetic environments. It has been designed for complete flexibility and supports multiple roles and ships, and can provide individual, team, and collective training. For Command Team Training for MIO, a single console could be used by a ship's command team to represent their 'own ship' within a force and for interaction with other units and commands, within a network, or just to role players. More consoles would be needed if the scenario were to include other warfare disciplines at an operator level but with the emphasis here on training the command team this should not be necessary.

7.2 Providing Training using Constructive Simulation (a Maritime Command and Staff Training System)

An alternative approach could be to train using PC based constructive simulation. CAE's system provides:

- Interaction of entities (i.e. vehicles, aircraft, ships, individuals such as soldiers, groups, humans) operating in a simulated environment
- Interactive (driven by operator inputs) high resolution simulation, no aggregated models but some automatism and
- Displays a realistic mission environment (tactical and logistical situation, topography, weather) in real time

In a naval context, entities can be: all types of platforms from minor war vessels to frigates to auxiliaries to aircraft carriers, rotary and fixed wing aircraft, manned and unmanned. Simulation includes information operations, logistic constraints (fuel remaining etc.), and weapon system fidelity according to the complexity of scenario.

The benefits of CAE's Constructive Simulation include

- Comprehensive exercise editor and exercise directing functions
- Creating a training environment that simulates the wide range of external factors that a Command Team must be able to address
- Comprehensive After Action Review (AAR) - capability manual and automatic bookmarks
- Replay of any situation, seen from the point of view of any party, or as an overview over all parties involved in the exercise
- Fully customisable by the user

8 Conclusions

With increasing pressures on operational programmes, finite budgets and less uniformed manpower available to deliver training, the case for increasing the use of simulation for MIO training has grown stronger. Live training remains essential but simulation can reduce the overall collective training burden.

Used correctly, within an integrated approach to training, simulation offers major benefits, and at a lower total cost.

An integrated approach to training, along the lines outlined at the Annex, is recommended to gain maximum benefit from industry.

9 Providing an integrated naval training solution

9.1 The Challenge

Most Navies are facing an increased



operational tempo, with limited numbers of service personnel and ships, and restricted budgets. Yet high quality training remains critical to maintaining operational capability. Furthermore, the sophistication of modern systems, the cyber and security threats to those systems plus EMCON restrictions, is constraining their peacetime use and reducing the effectiveness of live training.

9.2 The Solution

Navies around the world are therefore seeking help from industry to develop, manage and deliver the training required to support today's complex platforms and operations. They are also recognising the benefits of having an industry partner to assist in the design and management of a total training enterprise that adopts an integrated and 'holistic' approach to training.

A training systems integrator (TSI) acts as a partner throughout the training lifecycle, beginning with requirements definition and an analysis of alternative training approaches through to design and delivery of a training solution to meet the navy's operational requirements. To meet the full range of future missions, a TSI must be equipped to deliver comprehensive training for individuals, teams, units and task forces so they are suitably

prepared for joint and coalition operations. Use of networked, modular and configurable training systems within a 'system of systems' provides flexibility and cost-effectiveness. Looking ahead, inclusion of a live-virtual-constructive (LVC) training environment will enhance the resultant integrated naval training solution.

A series of business models are possible ranging from full military design and ownership, with industry in support, to industry delivering a training solution and using industry capital investment to fund training equipment and instructors. In both models, the naval customer approves the training design and sets training standards; in the second he simply pays for the services required.

9.3 The Benefits

The industry partner manages all training tasks except those that cannot be delegated, freeing Navy personnel for operational assignments. The industry partner hires top-of-their-class ex-military instructors with the required subject matter expertise and

military ethos to deliver the training. Enhancing simulated training in a synthetic environment will free up people and reduce the demand on operational units.

Industry will become a risk-sharing partner with its measure of success dependent upon the effectiveness of its elements of the training programme. Industry will guarantee availability of training and address potential obsolescence issues that may arise. An experienced Training Supplier will manage the entire industry team and have access to a global network of suppliers and partners. This obviates the need for the Navy to devote extra resources to managing multiple contracts. Engaging with a single industry partner maximises commonality across the training systems in areas such as management information, synthetic environment, databases and courseware. It also helps make the overall training system more scalable for the inevitable changes and evolving requirements that will arise over the long life of a training system.

Rear Admiral James Rapp CB Senior Naval Advisor, CAE Defence & Security

James Rapp has been Senior Naval Advisor to CAE since January 2015. CAE is the world's most experienced training systems integrator, and he assists the company with its business development in the naval domain.



In his last appointment in the Royal Navy, he was Director General for the spectacular programme of events to mark the 200th anniversary of the Battle of Trafalgar. Before that, he was Flag Officer Sea Training and responsible for the operational sea training of all the Royal Navy's ships, submarines and auxiliaries, and ships from 19 other foreign navies.

Earlier in his career, he served in the Fleet Air Arm, spending 6 years flying as an Observer in anti-submarine Sea King helicopters. He commanded four ships including three Type 22 frigates: HMS BRAZEN, during the first Gulf War; HMS BRILLIANT, when undertaking UN embargo operations against the former Yugoslavia, and HMS CORNWALL, as Captain of the Second Frigate Squadron. He also served twice in the Ministry of Defence in the Directorate of Navy Plans and twice on the staff of the Commander in Chief Fleet.

List of Acronyms and Abbreviations

Abbreviation	Description
AAR	After Action Review
COTS	Commercial-off-the-shelf
CDB	Common Database
CGF	Computer Generated Forces
EMCON	Electromagnetic Emission Control
EXCON	Exercise Control
NMIOTC	NATO Maritime Interdiction Operational Training Centre
MIO	Maritime Interdiction Operations
LVC	Live Virtual Constructive
LVC(T)	Live Virtual Constructive Training
ROE	Rules of Engagement
TMT	Tactical Mission Trainer
TSI	Training Systems Integrator

CLAUSEWITZ'S "WONDERFUL TRINITY" OF WAR IN THE 21ST CENTURY: A COMMENTARY ON THE USE OF ARTIFICIAL INTELLIGENCE IN MODERN WARFARE



by George Kiourktsoglou
Lecturer, University of Greenwich, London

Abstract

Carl von Clausewitz conceptualized war as a 'wonderful trinity' between 1816 and 1830, during the exceptionally tumultuous period that followed the rise and fall of Napoleon Bonaparte. Since then, warfare has been broadly defined as a blind instinct, an activity of the soul and a political instrument, with all three attributes merging into one continuum similar to human genome. In a different vein, the dawn of the 21st century saw the emergence of the fourth industrial revolution with disruptive innovation as its poster child. New technologies came to the fore, with applications ranging from fracking, 3D printing and robotics to artificial intel-

ligence (A.I.) and its crown jewel, deep learning. Slowly and mostly away from the dazzling spotlights of the media-loving publicity, modern warfare joined the rising number of human activities incorporating the latest technological breakthroughs in their DNA, causing an ineluctable mutation. Against this landscape, the following commentary is an effort to fleetingly touch upon the mutations to which Clausewitz's warfare is being subjected due to the latest wave of disruptive innovation. Up to a certain degree, it is also an educated guess at the new landscape which is emerging in national defence worldwide. At the dawn of a new technological era, artificial intelligence is shaping up as the key com-

ponent of military prowess.

1. Carl von Clausewitz's view of war as a 'wonderful trinity'

Mankind has fought countless wars for thousands of years. 'Blood has turned into the currency of war' as the maxim goes. Wars have claimed millions of lives, while at the same time they have left their indelible stamp on history. Along this timeline of blood, which lasts longer than five millennia, the salient feature of warfare has been the monopoly - to an absolute degree - imposed on it by humans (Singer, 1999 I). No other species on the planet has managed to come even close to the structured way humans fight wars. Fast-forwarding slightly closer to the present time, a defining characteristic of warfare in the last four centuries has been the fact that it has mainly taken place

among sovereigns and their coalitions.

1.1 What is War?

Clausewitz defines war as: '[...] not only chameleon like in character, because it changes its color in some degree in each particular case, but it is also, as a whole, in relation to the predominant tendencies which are in it, a wonderful trinity, composed of the original violence of its elements, hatred and animosity, which may be looked upon as blind instinct; of the play of probabilities and chance, which make it a free activity of the soul; and of the subordinate nature of a political nature by which it belongs purely to the reason' (von Clausewitz, 1873 I). These three components - instinct, soul, politics - fused into a continuum humans perceive as war, are closely weaved into each other. However, they manifest themselves via different actors in the theater of war. The blind instincts of hatred and animosity apply to the people who support violence in the form of war; the play of probabilities and chance applies to the practitioners of war, the military; finally, the political nature of war applies to the leaders who wage war by instigating the passions and the blunt animosity of their citizens towards the other side, the enemy.

1.2 What is War made of?

When Clausewitz authored his treatise 'on War' in the late 19th century following the rise and fall of Napoleon Bonaparte, Europe was still reeling out of a particularly tumultuous period of its history. In the previous decades millions of human lives had perished in the fields of combat along and across the continent. With the privilege of hindsight and using his particularly penetrating and well-honed military thought, he managed to break down war into its four constituent elements (von Clausewitz, 1873 II), in effect describing its substance, which had previously remained untouched over 5,000 years. The four elements were:

- Danger;
- Physical Effort;

- Uncertainty
- Chance;

However, in the late 20th century and at the dawn of the 21st, war started mutating. Although it still remains of the same nature - as described in paragraph 1.1 - its substance is undergoing a phase of profound changes. In the following paragraphs, an effort is undertaken with the aim to touch upon the gist of the ongoing and deep mutation.

2. Disambiguation: Systems' Spectrum of Complexity and Sophistication

From the very beginning, it must be made clear that there is a non-linear

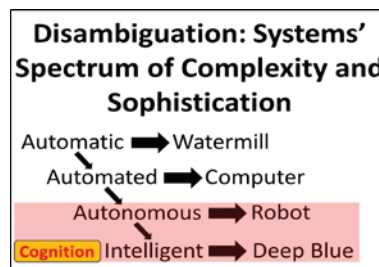


Image 1: Systems' Spectrum of Complexity and Sophistication (Source: Author, 2018)

and highly convoluted relation between a system's sophistication and the degree of human intervention during its operation. This is the so-called concept of 'sliding intervention', which implies that human involvement can 'slide' back and forth depending on operational needs. In the examples that follow, one will easily realize that a simple mechanical contraption, like for instance the watermill, needs remarkably limited human intervention during its operation. The same low human intervention is required by a high-tech system featuring cognitive ability – a so-called 'learning machine' – which can operate on its own, while teaching and improving itself in the execution of a highly complicated task

with minimum human involvement. The full spectrum of systems' sophistication features four categories of differing complexity (Image 1). Mov-

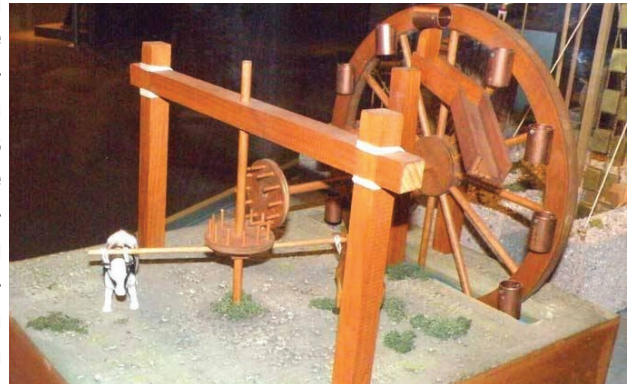


Image 2: Hydraulic wheel of Perachora (Source: Hellenica World, 2018)

ing from the least towards the most sophisticated systems, these are:

- Automatic;
- Automated;
- Autonomous;
- Intelligent;

To better understand the categorization, in the paragraphs immediately below, one characteristic example is given for each category of sophistication.

2.1 Automatic: the Watermill

The watermill (Image 2) was invented in the 3rd century BC in ancient Greece. It was a simple automatic system that turned kinetic energy into mechanical one. The input of energy could take place naturally via for example a waterfall or could include the use of a domestic animal like a horse or an ox. The transformed energy could then be used in a variety of daily human activities like for instance the milling of corn. Human intervention was kept to an absolute minimum.

2.2 Automated: the ENIAC

The Electronic Numerical Integrator and Computer (Image 3), which was completed in 1945, was the first general-purpose electronic computer. Originally the ENIAC was designed to assist in the study of thermonuclear weapons (Rhodes, 1995). At a later stage, it was also used by the U.S. Army as a computational tool in the calculations

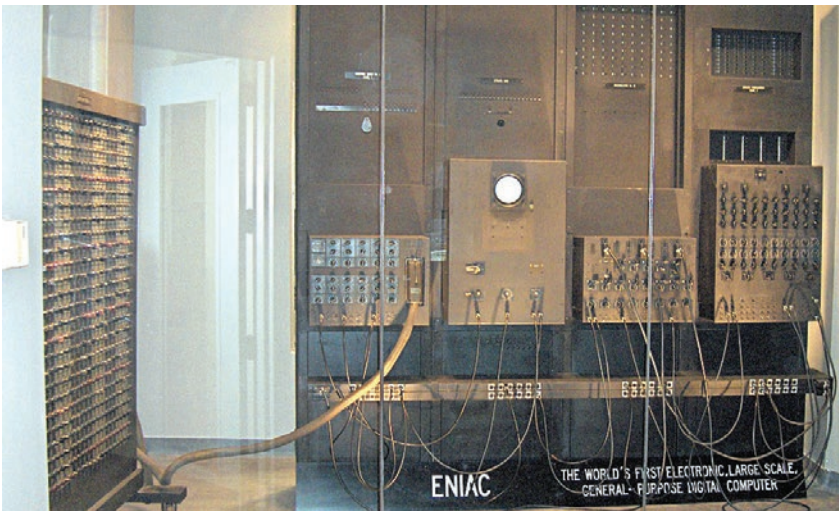


Image 3: The ENIAC (Source: PENN Engineering, 2018)

of artillery firing tables (Moye, 1996). The ENIAC was at least 1,000 times faster than any other computational machine of the same period (Dalakov, 2016). It was also the signature-manifestation of a new era in the application of algorithmic mathematics, since it combined speed and user-friendly ease of programmability. Human intervention was indispensable to the programming/preparatory stages of operations, but it was kept – just like the watermill in the previous example – to a minimum, while the machine was running complex calculations.

2.3 Autonomous: the Robot

While the watermill and the ENIAC embodied to different degrees the concept of automation, the first industrial robot was a rather hybrid manifestation of both automation and autonomy. It was given the name Unimate (Peters, D'Aluisio, 2000) and it was invented by George Devol. The Unimate (Image 4) had a mechanical arm and was commissioned on a General Motors assembly line at the Inland Fisher Guide Plant in New



Image 4: The Unimate (Source: Robotics Industry Association, 2018)

Jersey's Ewing Township in 1961. The patent filed by Devol in 1954 and granted in 1961 starts with the following: 'The present invention relates to the automatic operation of machinery, particularly the handling apparatus, and to the automatic control apparatus suited for such machinery' (Rosen R. J., 2011).



Image 5: Deep Blue (Source: The Computer History Museum, 2018)

2.4 Intelligent: Deep Blue

Deep Blue (Image 5) was the first computer that won both a chess-game and a match against a grandmaster like Gary Kasparov. The development of the machine began in 1985 by IBM and eleven years later, in 1996, it was put into its first test against Kasparov.

3. Types of Weapons' Autonomy

Autonomy is defined in the Oxford dictionary as 'freedom from external control or influence, independence' (Oxford dictionary, 2018 I). In the same vein, a system's autonomy is its ability to carry out a task, or tasks, without human intervention. The system can be run by either a pre-installed software program or a platform of artificial intelligence, a feature that implies cognitive ability and interaction with the environment. Weapon's autonomy can be broken down in five functional areas (Boulain, Verbruggen, 2017 I):

- mobility;
- targeting;
- intelligence;
- interoperability; and
- health management

It must be mentioned that a system can feature differing degrees of autonomy depending on the function. For instance, a weapon's system can be semi-autonomous in targeting but fully autonomous in its movements. In the same vein, the autonomy of a system for a given function can change depending on the nature of the task. This is the concept of the so-called 'sliding autonomy'. The typology of human-weapon command-and-control interface can be summed-up as (Boulain, Verbruggen, 2017 II):

- Human-in-the-loop weapons: robots that can select and deliver force only with a human command;
 - Human-on-the-loop weapons: robots that can select and deliver force under the oversight of a human operator who can override the robot's actions.
 - Human-out-of-the-loop weapons: robots which can select targets and delivering force without any human input or interaction.
- To better understand the previous two categorizations, three examples are given of weapons' systems of differing degrees of autonomy.

3.1. Semi Autonomy (Human in the Loop): Robotic sentry weapons (Image 6)

Based on the existing known technology, a robotic sentry weapon is a typical example of a system that features different degrees of autonomy depending on the underlying function. Such systems are usually fully autonomous in the detection of targets. However, as soon as the function of targeting is complete, the system comes to a halt, waiting for a human to intervene and make a call of judgment. More specifically, the human operator has to make up his mind, whether the

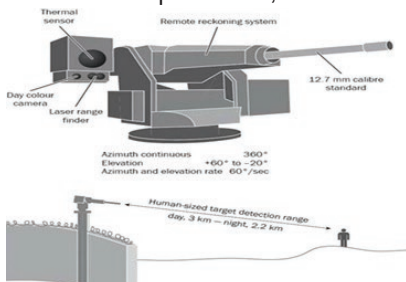


Image 6: Robotic sentry weapons: DODAAM's Super Aegis II (Source: Boulanin, Verbruggen, 2017 III)

detected target is indeed an enemy or just a civilian. It is easily understood, that robotic sentries may potentially raise legal questions which are not the subject of the present analysis. However, the problematic of fully autonomous targeting and subsequent target-engagement seems to be a problem that can be easily tackled using artificial intelligence, and more specifically machine learning.

3.2 Supervised Autonomy (Human on the Loop): Short-range air defence systems (Image 7)

As a general comment, all air defence systems operate under some kind of human supervision. Although information on the use of such a system is not always prompt, it is understood that a Phalanx system most frequently works in a human-on-the-loop mode. A Patriot system's or Israel's Iron Dome's degree of autonomy depends, as explained previously, on the nature of the threat. By the same logic, the Aegis system features 'sliding autonomy', depending on the nature of the task.

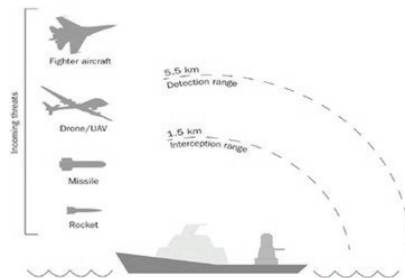


Image 7: Short-range air defence systems: Phalanx close in weapon system (Source: Boulanin, Verbruggen, 2017 IV) tic sentry weapons: DODAAM's Super Aegis II (Source: Boulanin, Verbruggen, 2017 III)

3.3 Full Autonomy (Human out of the Loop): Loitering Weapons (Image 8)

Loitering weapons are systems that usually operate on 'sliding autonomy', depending on the environment they are launched within. Once they become airborne, they seek their target, either based on a pre-installed software code or operating on a platform of artificial intelligence. If potential targets are of high value, like for instance manned

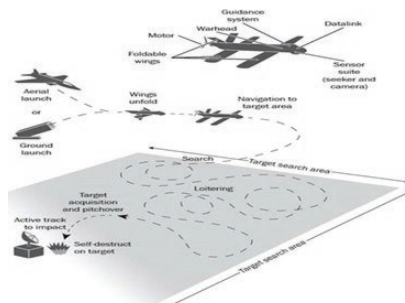


Image 8: Loitering weapons: (Source:Source: Boulanin, Verbruggen, 2017 V)

armored vehicles, then as soon as a target is detected, the loitering weapon flags it up to the operator and then it goes into 'stand-by' mode, awaiting human intervention. Otherwise – this is its most frequent mode of operation – it engages its target(s) without human intervention, although there is always the choice for a human operator to intervene, up until a few seconds ahead of the engagement of the target.

4. Artificial intelligence is changing the DNA of conflict and imparts irreversible mutations

The Oxford dictionary defines intelligence as 'the ability to acquire and apply knowledge and skills' (Oxford dictionary, 2018 II). In a similar vein, the artificial intelligence laboratory at Stanford University defines A.I. as 'the ability of a machine to perceive something complex and make appropriate decisions' (Stanford Artificial Intelligence Laboratory, 2018). The three weapons' systems described in the previous paragraphs can all be fitted with an A.I. platform, which as already discussed, can give the system full autonomy. However, before such a mutation takes place, the platform upon which the system operates has to evolve to a point capable of supporting decision making without human intervention. The attribute of decision-making can be imparted on the machine via traditional software programming or via 'teaching', which implies cognitive ability on the part of the machine. In either case, it can be easily understood that the DNA of conflict is changed permanently because once a weapons' system becomes fully autonomous, human supervision cannot exercise any control due to the complexity of the task – analysis and synthesis of number of parameters in a time horizon so short that renders effective intervention beyond human reach.

4.1 Types of Artificial Intelligence

Broadly speaking there are three types of artificial intelligence (Singer, 1999 II).

- The reactive one, when the machine reacts following interaction with its environment. As an example of reactive intelligence, one can easily think of the sentry system in paragraph 3.1 as soon as it detects a target;
- The predictive one, when the machine runs ahead of time and 'predicts' the future, taking subsequently the necessary steps to alter it. In this case, one can visualize

a patrol on foot doing reconnaissance in enemy territory, while using a robot supported by an A.I. platform as an escort with the aim to identify improvised explosive devices;

- The creative one, which corresponds to what engineers call scenario analysis. The only difference is that in this case, it is not based on software programming but the cognitive ability of the machine;

4.2 Case Study I: the 3rd offset strategy

The 3rd Offset Strategy was presented on the 15th of November 2014 by the then U.S. Secretary of Defense Chuck Hagel. The strategy was a collection of four disruptive technological innovations whose aim was to ensure that the U.S. and its armed forces retain military supremacy against all potential contenders well into the 21st century (Breaking Defence, 2018).

The four disruptive innovations were:

- Robotics and Autonomous Systems;
- Miniaturization;
- Big Data;
- 3D Printing

More specifically, the big data component of the strategy had among its implicit aims the gradual replacement by 'smart systems' of a large part of the military personnel who were tasked with the analysis of the raw intelligence collected by humans and/or machines – aerial or underwater drones for instance. At present, there is the impression – not far from the truth on the ground – that at times of conflict, humans can be overwhelmed by a tsunami of raw data to be analyzed. At the same time, efforts to better understand the battlefield and all parameters related to it, can be promptly frustrated by the lack of time. As such, big data supported by the necessary programming code or by artificial intelligence platforms can enhance the processing capacity of existing weapons' systems, while simultaneously, they can reduce the processing time of massive quantities of data at different

stages of military operations.

4.3 Major A.I. Techniques and Big Data

Artificial intelligence is any programming – in the broader sense – technique that apes human intelligence and renders a machine 'smart' in terms of making decisions. As examples, one can mention the two prevailing ways of imparting intelligence on a machine, either traditional, but highly complex, programming leveraging decision trees, or neural networks – systems that try to mimic the human brain in its functions. Machine learning is a subset in the continuum of artificial intelligence, comprising techniques that render a machine 'smart' by developing its cognition. In other words, a machine can be taught to perform a specific task or tasks, like for instance the instant recognition of a terrorist. Deep machine learning is the latest development in A.I. techniques and refers to a machine that not only is 'smart' featuring cognitive abilities, but it can actually teach itself. A prominent example in this case is the Alpha Go, an A.I. platform

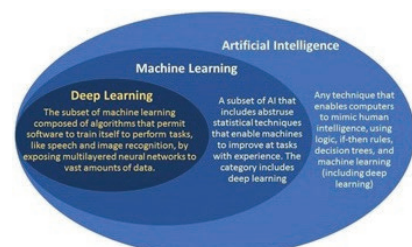


Image 9: Artificial Intelligence Techniques (Source: Geospatial World, 2018)

developed by Alpha, Google's parent company. Alpha Go managed to beat a human grandmaster in Go, an ancient Chinese strategy game. Deep learning machine specialists managed to 'educate' Alpha Go on the game by having it play against itself. Finally, to 'teach' a machine, A.I. experts need massive quantities of data in the form of images or sounds or even bank transactions. The salient feature of these sets of data is that they cannot be realistically

processed via traditional programming methods due to their sheer size. This is the concept of big data.

5. The Trade-off: Open-Source Warfare

As already discussed in the present analysis, autonomous weapons are changing the DNA of war by leveraging artificial intelligence and more specifically machine learning. This developing wave of technological disruption is omnipresent in weapons' technology, from land-warfare, to sea and air. Manifestations of the U.S. 3rd Offset Strategy have already brought down the costs of weapons' systems – in some cases by an order of magnitude. Above all, weapons' autonomy has in numerous cases taken soldiers off the theatre of action and placed them in the safety of a control room, thus reducing the cost of war in human lives. However, there is a price to pay for such a unique technological advancement and it is not of a monetary nature. Warfare in the 21st century is open-source, meaning its technology can be leveraged not only by state actors in the form of structured and well regimented military bodies, but also by insurgents and even terrorists



Image 10: Drones built by Daesh terrorists in Syria (Source: Sputnik, 2018)

like the ones of Daesh in Iraq and Syria. Image 10 shows a drone made with off-the-shelf components, built to a potential cost of no more than \$2,000. Although the specific swarm of similar drones was not supported by an artificial intelligence platform, it was GPS based and Daesh terrorists launched it to overwhelm Russian army and airforce units in Hmeymim and Tartus in Syria. According to the Russian Ministry of Defence the attacks were successfully repelled, but

the incident graphically proves in the most blatant of ways that warfare in the 21st century is not only asymmetric in its nature, but it is being progressively commoditized in its resources.

5.1 Case Study II: Fighting Terror and its Asymmetry

By 2040, two thirds of the world population will be living in cities. Today there are 29 megacities as they are called. These are ultra-sized urban centres with population of more than ten million people. Twenty years ago, their number was thirty percent lower, but it has come up following a massive tsunami of formerly farming populations – to the degree of eighty million people a year – which has flooded megacities worldwide (Economist, 2018). Whether law enforcement is dealing with a string of terrorist atrocities like 7/7 downtown London, or a national military is fighting a war like the ‘surge’ the U.S. forces fought in 2007 Fallujah Iraq, conflict in the 21st is morphing into something more and more urban. Just in the United Kingdom, there are 4.6 million C.C.T.Vs. Statistically, the average Briton gets picked up by a close circuit camera approximately 300 times a day. It is easily understood that within the context of counter-terrorism, no clandestine agency can analyse such a massive amount of data produced incessantly on a daily basis. However, artificial intelligence can ‘identify that a needle has to be found in haystack and then go ahead and find it’ (Singer, 1999 III). Disruptive innovation in the form of machine learning platforms underpinning weapons and

surveillance systems is the answer to the asymmetric warfare that national militaries have fought repeatedly since 9/11. The same family of technologies can also enhance law enforcement and render it more potent and more efficient in urban counter-terrorism. However as mentioned in paragraph five, one should not forget that these technological luxuries come at the price of open warfare, which means that it is just a matter of time – if it has not already happened – before a terrorist cell wakes up to the use of the innumerable A.I. applications.

6. Conclusion: The Name of the ongoing Mutation

Danger	➡	Ethical Trap
Physical effort	➡	Hyperspeed
Uncertainty	➡	Fidelity
Chance	➡	‘Fog of War’ lifted

Image 11: The ongoing mutation
(Source: Author)

Going back to the point from which this analysis started – paragraph 1.2–, war as described by Clausewitz is mutating due to disruptive innovation. Based on the discussion in this commentary, its constituent elements are being progressively replaced by a ‘mix of new substances’, which are still in the making given the breakneck pace of technological advancement. More specifically, the salient feature of the danger to life is being replaced by an ethical trap which relates to the use of advanced technology in the place of human assets. The physical

effort that has been since the dawn of history deeply embedded in the core of war is mutating into hyper-speed on the battlefield. This is the signature characteristic of advanced weapons’ systems supported by software and A.I. platforms. The uncertainty that defined the outcome of innumerable battles throughout history gives now its place to robust fidelity supported by the accuracy of machines deployed to the theater of action. Above all, the element of chance, described by Clausewitz as the ‘fog of war’ (von Clausewitz, 1873 III) is being lifted due to the gradual substitution of the human element, which is volatile in its nature, by ‘smart machines’ in the form of advanced weapon systems (Image 11). For militaries around the world, this set of ongoing mutations is of an evolutionary nature, similar to the concept of the survival of the fittest (Spencer, 1865). As such, national defences will have to be kept up-to-date on an ongoing basis, while tuning up to the disruptive innovation of artificial intelligence. The alternative is technological obsolescence, which mathematically will set militaries on a path of irrelevance. Nations shunning the transformative trends in the defence industry will risk their national security and find themselves seriously challenged by potentially asymmetric enemies, who at the end of the day may very well turn out to be more technologically advanced. To summarise, war in the future will be defined more by technological prowess and less by military virtue as described by general Carl von Clausewitz.

References

- Boulanin V., Verbuggen Maaïke, (2017) I. ‘Mapping the Development of Autonomy on Weapons Systems. Existing functions and capabilities.’, SIPRI Report. p. 20. Viewed on the 31st of July 2018, accessed via <https://goo.gl/QAJSxv>
- Boulanin V., Verbuggen Maaïke, (2017) II. ‘Mapping the Development of Autonomy on Weapons Systems. Typology of the human–weapon command-and-control relationship according to Human Rights Watch.’, SIPRI Report. p. 26. Viewed on the 31st of July 2018, accessed via <https://goo.gl/QAJSxv>
- Boulanin V., Verbuggen Maaïke, (2017) III. ‘Mapping the Development of Autonomy on Weapons Systems. Robotic Sentry Weapons.’, SIPRI Report. p. 45. Viewed on the 31st of July 2018, accessed via <https://goo.gl/QAJSxv>
- Boulanin V., Verbuggen Maaïke, (2017) IV. ‘Mapping the Development of Autonomy on Weapons Systems. Robotic Sentry Weapons.’, SIPRI Report. p. 38. Viewed on the 31st of July 2018, accessed via <https://goo.gl/QAJSxv>

Boulanin V., Verbuggen Maaïke, (2017) V. 'Mapping the Development of Autonomy on Weapons Systems. Robotic Sentry Weapons.', SIPRI Report. p. 51. Viewed on the 31st of July 2018, accessed via <https://goo.gl/QAJSxv>
 Peters M., D'Aluisio F., (2000). 'Robo sapiens: evolution of a new species'. The MIT Press. pp. 186–189. ISBN 0-262-13382-2
 Rhodes, R., (1995). 'Dark Sun: The Making of the Hydrogen Bomb'. First Simon and Schuster 2005. p. 251
 Singer, P. W., (2009) I. 'Wired for War'. Penguin Books. p. 267

Singer, P. W., (2009) II. 'Wired for War'. Penguin Books. p. 77

Singer, P. W., (2009) III. 'Wired for War'. Penguin Books. pp. 273-6

Spencer, H, (1865). 'Principles of Biology'.

Von Clausewitz C., (1873) I. 'On War'. Enhanced Media Publishing 2017. p. 25

Von Clausewitz C., (1873) II. 'On War'. Enhanced Media Publishing 2017. p. 41

Von Clausewitz C., (1873) III. 'On War'. Enhanced Media Publishing 2017. p. 73

Web Document: Breaking Defense, Article by Freedberg S. J. Jr., (2014). 'Hagel Lists Key Technologies For US Military; Launches 'Offset Strategy''. Viewed on the 31st of July 2018, accessed via <https://goo.gl/VdgyB>

Web Document: Dalakov, Georgi, (1996). 'ENIAC. History of Computers'. Viewed on the 31st of July 2018, accessed via <https://goo.gl/G1kdEL>

Web Document: Economist, Article, (2018). 'The future of war'. Viewed on the 31st of July 2018, accessed via <https://goo.gl/wHm8df>

Web Document: Geospatial World, Article by Datta A., (2018). 'Top eight disruptive technologies and how they are relevant to geospatial'. Viewed on the 31st of July 2018, accessed via <https://goo.gl/Pg9gGk>

Web Document: Moye, William T., (1996). 'ENIAC: The Army-Sponsored Revolution'. Viewed on the 31st of July 2018, accessed via <https://goo.gl/LbEvf2>

Web Document: Rosen, R. T., (2011). 'Unimate: The Story of George Devol and the First Robotic Arm'. The Atlantic. Viewed on the 31st of July 2018, accessed via <https://goo.gl/AZK9hG>

Web Document: Sputnik, Article, (2018). 'Drones That Attacked Russian Bases in Syria Resemble US Military UAVs'. Viewed on the 31st of July 2018, accessed via <https://goo.gl/2V9hri>

Web Portal: Hellenica World, 'Greece, Ancient Greek Technology: Hydraulic wheel of Perachora'. Viewed on the 31st of July 2018, accessed via <https://goo.gl/gqcWxf>

Web Portal: Oxford Dictionary I, 'Definition of Autonomy'. Viewed on the 31st of July 2018, accessed via <https://goo.gl/NZ7QBG>

Web Portal: Oxford Dictionary II, 'Definition of Intelligence'. Viewed on the 31st of July 2018, accessed via <https://goo.gl/205kLC>

Web Portal: Penn Engineering, 'ENIAC: Celebrating Penn Engineering History'. Viewed on the 31st of July 2018, accessed via <https://goo.gl/89DMBZ>

Web Portal: Robotics Association, 'UNIMATE: The first industrial robot'. Viewed on the 31st of July 2018, accessed via <https://goo.gl/h1DLeH>

Web Portal: Stanford Artificial Intelligence Laboratory, 'Definition of Artificial Intelligence'. Viewed on the 31st of July 2018, accessed via <https://goo.gl/cnHARX>

Web Portal: The Computer History Museum, 'Deep Blue II'. Viewed on the 31st of July 2018, accessed via <https://goo.gl/DzNAK6>

Bionote

George Kiourtsoglou is a senior lecturer at the University of Greenwich in London, U.K.. He lectures on Maritime Security, Maritime Economics as well as Strategy and Management.

As an intern, he worked for the Israeli Public Corporation of Electricity and from 1996 until 2009 for Royal Dutch Shell.

George is a fellow of the British Higher Education Academy and a member of the American Nuclear Society, the Chartered Management Institute and the Institute of Marine Engineering, Science and Technology in London.

He speaks Greek, English, German, Japanese and French.





Disaster Relief Operation and Gender Perspectives

by Cdr Junko Kawashima
Japan Maritime Self Defence Force

Traditional notions of security and safety have changed because of an increased understanding that many humanitarian crises are multicausal. Complex emergencies can only be resolved by a comprehensive approach to crisis management

Japan has learned what is 'Gender Perspective' and its importance through the experience of participating in Peace Keeping Operations. Under UNSCR1325, the importance of gender perspective is slowly but gradually being accepted in Japan Self Defense Force (JSDF) especially in Japan Ground Self Defense Force. How about in Japan Maritime Self Defense Force (JMSDF)?

Why so many natural disasters occur in Japan?

To answer this question, I have to mention the geographical characteristics of Japan and it strongly influences missions

and operations of JSDF.

Japan is surrounded by the sea and there are four plates connected around it (the Eurasian Plate, the North American, the Pacific and the Philippine Plate) and this accounts for the frequent earthquakes and active volcanic activities. As Japan belongs to the Asia-Monsoon area and also as there are typhoon tracks passing over Japan, localized torrential rain frequently occurs. One more unique characteristics is that Japan has steep slopes and rivers are short and rapid and that cities and farms are

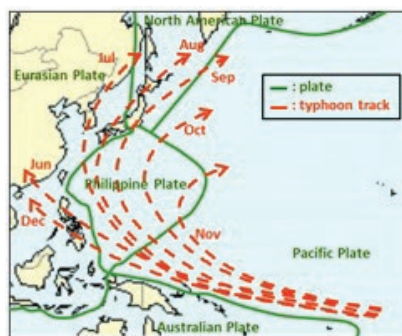


Figure 1: Plate and Typhoon Tracks around Japan

located close to rivers, sea sides and volcanos. These features are at the

	2011	2012	2013	2014	2015	2016
Response to Natural Disasters	7	6	23	13	13	10
Transporting Emergency patients	444	410	401	407	419	409
Search and Rescue	31	26	25	17	22	25
Firefighting	60	62	93	73	61	57
Other	44	16	13	11	26	14

Figure 2: Record of Disaster Relief Dispatches of JSDF(2011-2016)²

root of many kinds of natural disasters such as earthquakes, Tsunamis, floods, landslides and in the worst case nuclear reactors were damaged.

According to the records from 1900 to 2015 ¹, more than 14 percent of the big earthquakes and Tsunami in the world had hit Japan. Due to frequent and large scale natural disasters, JSDF has many Disaster Relief (DR) missions.

What kinds of damages occurred in such catastrophic disaster? I would like to go over the Great East Japan Earthquake in 2011 as

¹ White paper on Disaster Management 2017, Cabinet office, Government of Japan

² White Paper, Ministry of Defence of Japan, 2012 to 2017

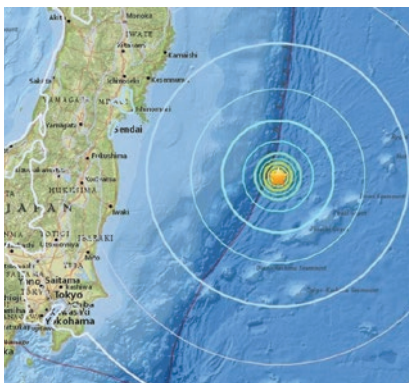


Figure 3: Tsunami hit the eastern part of Japan

casualties, loss of government function and absence of rule of law, damage to infrastructure, shortage of water and food, people are displaced and forced to live in shelters, worsening hygiene environment, epidemics and so on. Natural disasters impact the daily lives of people in many aspects; physically, socially, politically economically and so on. In

this is one of the recent and worst disasters in the country's history.

The Great East Japan Earthquake 2011



On 11th March 2011, at 14h46m, Japan was hit by a 9.0 magnitude earthquake that caused widespread damage to Japanese eastern coastal region. It lasted approximately six minutes and occurred at a depth of approximately 24.5 kilometers with an epicenter of approximately 130 kilometers of east of Sendai City. Within the first day following the earthquake, more than 50 aftershocks happened, some of them were measured at least 6.3 on the Richter scale. The tsunami that followed the earthquake devastated the coastal

areas of Tohoku area and southern Hokkaido. The first tsunami wave reached the coast only 15 minutes after the earthquake. It was reported that the maximum height of the wave was at approximately 40.5 meters and more than 500 kilometer in length in coastal areas was directly impacted.

The earthquake and tsunami claimed the majority of the 19,630 lives and 2,600 missing and the injured 6,230 as of 1st March 2018 . Approximately 121,800 houses were completely destroyed, 281,000 half destroyed and 744,500 partly destroyed, also more than 14,500 public buildings were damaged . This disaster displaced approximately 340,000 people.

Three nuclear power plants operated in that area and Fukushima No.1 nuclear power plant was damaged, it lost electricity following the earthquake and tsunami. In time, the International Nuclear Event Scale was raised to Level 7, the highest level. The widespread damage has been referred to as the worst natural disaster in the recorded history of Japan.

Natural disaster causes mass

short, it causes 'chaotic situation'/civil emergency situations.

In the Great East Japan Earthquake 2011, there were some reports that women and girls were raped in the chaotic situation.

In terms of security and safety of civilians, armed conflict and natural disaster share similar conditions.

Natural disasters are one of the human security issues.

And from the point of view of the maritime security, Disaster Relief is one of the stability operations on the same level as piracy, terrorist challenges, illegal activities, migration, human trafficking and so on.

Gender Perspectives in Disaster Relief operations of JMSDF in the Great East Japan Earthquake

What kind of gender perspectives we can pinpoint in JMSDF operations?

Researching the past operations of JMSDF, I came to the realization that

³ Report of overview of the Great East Japan Earthquake 5th March 2018, Disaster Response Headquarter, Cabinet office

⁴ White paper on Disaster Management 2017, Cabinet office, Government of Japan

⁵ Report of overview of the Great East Japan Earthquake 5th March 2018, Disaster Response Headquarter, Cabinet office



Figure 4



Figure 5



Figure 6



Figure 7

Transport ships and Supply ships performed to full their ability and capacity, transport ships made one package of these supports for half a day and they provided the support package moving around several positions in their operation area. Data showed that approximately 60% of the people who used the support were women.

Some of the officers mentioned, after the operation, that one of the most effective role

gender perspective worked effectively in some kinds of operations in which JMSDF faced to civilian population especially vulnerable people like women, children, aged people, sick people and disabled persons, as they are easily affected in chaotic situation.

In the Great East Japan Earthquake, JMSDF's mission was Search and

in life support operations in the Great East Japan Earthquake:

1. Some ships provided hygiene facilities for victims and sheltered people and all bath/shower rooms were separated by gender. (See Figure 4)
2. Laundry support was provided in ships and was supported by male and female crew separately. (See Figure 5)

of women in that operation was that women could gather information, on questions such as 'Are there any isolated areas and people who remained without support?' 'What supplies and services women need?' 'Where were the people who need particular help, such as pregnant woman, children, and elderly people who need nursing and disabled people?'



Figure 8: Women listen to requests

JMSDF could share such information with other government agencies; police, fire service, local government, NGOs, International Organization and so on.

Rescue, transportation of relief supplies/medical teams, information gathering to locate isolated area and people who remained without support, support for victims in shelters mainly

water, foods, hygiene, medical/psychological check and response to the damage of Fukushima nuclear power plant. JMSDF deployed more than 60 ships and about 100 aircrafts and helicopters to the disaster area.

I will attempt to give a brief description of some of the gender perspectives

3. Ships quartered women and provided them with spaces to socialize, take a nap, look after babies, relax.
4. Medical care was important. Many women, including pregnant women, preferred female surgeons/hospital corpsmen. Women were treated and got medical examinations in separate space. (See Figure 6)

5. Some destroyers provided temporary shelter in the ships for evacuated children. (See Figure 7)
6. Supplies for women and babies were sorted by women according to their specific needs.

Moreover, women played an important role as a kind of adviser to male commanders.

From a viewpoint of the four pillars of UNSCR 1325 (Participation, Protection, Prevention, Relief and Recovery), JMSDF operations in the Great East Japan Earthquake were particularly related to the following three pillars.

1. Protection. To protect women and girls in emergency/humanitarian situations.

2. Participation. The participation of women at all levels of decision-making in operations, in military capacity
3. Relief and Recovery. To provide relief and recovery through a gendered lens by respecting the civilian and considering the needs of women and girls.

Incorporate Gender Perspectives into higher level

As evidenced above the JMSDF applied gender perspectives to their operations at field level. However, admittedly the ‘gender perspective’ is not still systematically established in JMSDF.

Through the experience of the Great East Japan Earthquake, I come to the realization that commanders serve an important role to accomplish the operation/mission more smoothly and effectively also from gender point of view.

Reviewing this operation, I would like to highlight some of most important points to incorporate gender perspective

within operational and strategic level.

At Operational level

- Staffing
Officers / crews who are familiar with Civil affairs/Civil-Military cooperation is required.

- Planning
It is necessary to pay attention to the vulnerable; women, children, the sick, the elderly, people with disabilities. Gender analysis is included in the operation plan.

- Training/Education
This is most important. The training related to gender issues should be provided as a basic knowledge in HA/DR operation.

At Strategic level

-Staffing
Officers/Staffs who know Civil affairs/Civil-Military cooperation is required.

- Planning
Officers/Staffs with Civil affairs/Civil-Military cooperation expertise are required.

- Training/Education
The opportunities should be offered to Commanders to deepen their knowledge of gender issues. (e.g. Share best practices,

lessons learned, human rights)

Navy operations and Gender Perspectives

An important aspect of Navy’s role in Disaster Relief operations is to provide well-organized support soon after the disaster occurred when there are few governmental and non-governmental groups commencing their activities in devastated areas; demonstrating the Navy’s characteristics, quick response, maneuverability, capacity, self-contained, flexibility etc.

Every country is in different maritime security environment and every Navy has different missions according to the security environment. Some conduct many Disaster Relief operations, some are facing migrants, human trafficking, boarder control and terrorist attacks.

Emergency situations in every country are different, however, whatever the situation Navies can be called to respond to such an emergency situation in which they have to engage and treat civilian, therefore we should prepare for it.

Junko KAWASHIMA

Embassy of Japan in Belgium - First Secretary and Commander
Aide to the Special Representative for the NATO Secretary General (Charged with: Women, Peace and Security)

1997, Graduated from Dokkyo University, Joined Maritime Self-Defense Force JMSDF Officer Candidate School Training Squadron Headquarters, JS Kashima, JS Asuka etc., Command and Staff course, JS Mashu, JS Asagiri etc, Commanding Officer of JS Setoyuki.

At present post after working at the Maritime Staff Office and JMSDF Officer Candidate School.





SAURON Real-life Scenario: A Terrorist Coordinated Attack in a European Union Port

by Ph.D.(c) Eleni-Maria Kalogeraki, Dr. Spyridon Papastergiou,
Associate Professor Nineta Polemi, Professor Christos Douligeris

Abstract

Ports are the cornerstone of Maritime Supply Chain operations becoming a target for hackers, who are increasingly evolving their skills launching cyber, physical or combined sophisticated attacks on ports' infrastructures and facilities, including global navigation satellite systems, Information and Communication Technology devices (ICTs) and surveillance networks. Such attacks can disable a vessel, hijack, divert or steal cargo or cause disruption of a greater value; ports' operations interruption and environmental harm with devastating effects on humans' life. This article presents a real-life terrorist-attack scenario that will be utilized as a pilot use-case to demonstrate and

evaluate the operations of a holistic Situational Awareness (SA) platform, which is under development in the context of the EU research ongoing project "SAURON". The proposed platform targets at protecting ports' infrastructure, goods and people located within and its surroundings against physical, cyber and combined threats. The scenario analysis aims to conceptualize terrorists' activity and the extent of loss and casualty that they may cause.

Keywords

Terrorist-attack, cyberphysical threats, holistic Situational Awareness, port Critical Infrastructures, cyberterrorists.

1. Introduction

Maritime transport has been a catalyst for European economic growth over its

history. Despite the crisis that hit the global economy in 2009, it still plays a vital role in the EU's trade. To consider the high value of Maritime transport in the EU economy, according to recent statistical metrics [1]: (i) almost 90% of the European Union (EU) external freight trade is seaborne, (ii) short sea shipping facilitates nearly the one third of all the EU internal market exchanges in terms of ton-kilometers and (iii) approximately 400 million passengers embark and disembark at European ports annually. Consequently, EU ports are considered one of the main Critical Infrastructures (CIs) in Europe [2]. During the last decade, coordinated and composite terrorist attacks impinge on the global welfare. New alarming scenarios are causing mass atrocities and severe repercussions to the EU Member States' regions, such as the November's 2015 coordinated Paris attacks, 2016 Berlin Christmas market attack, June 2017 London Bridge

attack and August 2017 Barcelona attacks [3]. Taking into account the most recent EU TE-SAT [4] regarding 2017 annual terrorist activity: (i) 68 people died and approximately 844 people were injured from terrorist incidents throughout the EU and (ii) 205 terrorist attacks were either failed or thwarted or completed in nine Member States. Similar attacks could be staged in the EU Maritime sector in the near future. Due to the rapid growth of complex and heterogeneous interconnected ICTs in the shipping sector, Maritime Industry is currently subjected to cyberphysical attacks. A genuine danger of maritime physical attacks is piracy, such as the Somali piracy, which has reached its peak from 2000 to 2009 and it still threatens the international Shipping Industry. Concerning the maritime cyber-threat emerging landscape, after the 2017 ransomware cyberattacks, WannaCry, WanaCrypt0r 2.0 and Petya, which resulted in shutting down terminal activities in some commercial ports causing economic loss in leading shipping and oil companies worldwide, such as AP Moller-Maersk, new ransomware cyber-attacks have been identified during 2018. Moreover, in March 2018, the Svitzer shipping company has suffered a significant data breach where sensitive individual information of nearly 500 Australian employees was exposed as a result of an 11-month active cyber-attack [5]. On the 24th July 2018, American shoreside operations of Cosco Chinese shipping giant were hit by a ransomware cyber-attack, affecting telecommunication with vessels,

customers and port terminals including the Pier J terminal at the Port of Long Beach [6].

Consequently, the potential of a coordinated physical or cyber and/or combined attack in a large EU port could have a dramatic impact on the European maritime transport affecting the economy and social well-being on a global scale. Therefore, the fight against terrorism and the protection from cyberphysical criminal activity have become a top priority for the EU maritime security policy [4]. Coherent plans are implemented to reinforce maritime security against illegal shipping and fraudulent operations in ports. For example, on the 26th June 2018 European ministers have realized a revised action plan in collaboration with partner countries and global organizations (i.e. NATO, United Nations) that concerns current and future challenges according to the following parameters that put Maritime EU security at major risk: terrorism, cyber and hybrid, chemical, biological, radiological and nuclear threats [7]. Additionally, the European Commission supports research projects that are in line with EU Innovation Actions (IA) for CIs Protection (CIP). According to the Council Directive 2008/114/EC [2], protecting port EU infra-structures against physical, cyber and/or combined threats is a key issue. SAURON (Scalable multidimensional Situation Awareness Solution for protecting European ports) is an EU H2020 ongoing research project <https://www.sauronproject.eu/> [8] addressing the CIP-01-2016-2017

topic: Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe.

SAURON main purpose is to provide a multidimensional yet installation-specific Situational Awareness (SA) concept to help port operators anticipate and withstand potential cyber, physical or combined threats to their freight and cargo business and to the safety of their employees, visitors, passengers and citizens in the vicinity.

This work presents a real-life complex terrorist cyberphysical attack scenario which will be used as a pilot use-case to demonstrate and evaluate the project SAURON results of the proposed holistic SA concept. To better comprehend the main points of the scenario, that triggers a series of cyber and physical attacks, business workflows and diagrams are carried out.

2. A quick glance at the SAURON project's content

The SAURON project puts the focus on the protection of EU Ports under Transport Infrastructure and means of transportation type of CIs. SAURON is an easily deployable SA holistic platform for EU ports and comprises the following applications: (i) the Physical Situation Awareness (PSA) application to estimate the physical risks of the port and their impact, (ii) the Cyber Situation Awareness (CSA) application to assess cyber-risks, CIs vulnerabilities and the propagated effects, (iii) the Hybrid Situation Awareness (HSA) application, that fuses the physical environment and cyberspace to support the prevention, detection or response and mitigation of any physical, cyber or combined threat and (iv) the Emergency Population Warning System (EPWS) that aims to inform and protect both, the inhabitants in the vicinity of the ports and the emergency teams in charge of intervening in case of attack.



A detailed description of the SAURON concept together with its applications has been presented in [9].

3. Selection criteria for the SAURON use-case

SAURON analyses the potential of launching sophisticated coordinated terrorist attacks on EU ports via a complex real-life terrorist attack scenario that consists of both physical and cyber attacks on a port's Critical Service: the Cruise Service. To this extent, the scenario will be carried out under real conditions [9]. The selected Cruise Service is significant and satisfies the prerequisites below: (i) it addresses the European scale/nature; large, European cruise and commercial ports are involved, (ii) it is an economic enabler with high economic impact across the entire EU Maritime Industry and Economy, (iii) it meets the EU environmental requirements and standards.

4. SAURON real-life terrorist-attack scenario in an EU Port

This section analyses in detail the SAURON real-life terrorist-attack scenario. The demonstrated scenario illustrates how a terrorist group can attack a cruise ship berthed at the port's premises. The scenario includes a set of complex threat scenarios, both physical and cyber, that are capable of causing human casualties and serious damage in the Port's vicinity. Furthermore, the scenario

will describe a fusion of port security deficiencies and emergencies that have been stated, recorded, implied or suspected. The preferred scenario is described as follows:

A terrorist group aims to launch an attack on a cruise ship during its visit to the Port, causing serious human casualties and destruction of the Port's premises.

Before performing the violent physical attack, a series of specific cyber-attacks is planned for creating a limited disruption inside the port facilities (i.e. false perimeter intrusions, false fire alarms, surveillance system shut down), in order to occupy the majority of the security personnel in addressing these false problems and confuse them, causing chaos. Consequently, normal activity and transport inside the port will be interrupted. This situation will facilitate terrorists' entrance to the cruise terminal without being noticed and allow them to attack the berthed Cruise ship killing and injuring people and damaging the port's facilities. Terrorists' highlighted actions for realizing the coordinated cyber and physical attacks are depicted in Figure 1 using the business process diagram of BPMN 2.0 modeling notation [10] and they are presented in the following:

- Terrorists intend to gather information about the Port Authority organization (i.e. identify port's cruise primary operations, personnel involved and key employees etc.) To achieve this, ter-

rorist hackers begin to survey the targeted Port Authority by looking through public documentation or relevant news articles avoiding exposing themselves by carrying out physical reconnaissance. Depending on the imagery available one can see information, such as perimeter fences, lighting port facility, some of the CCTV cameras, etc. As a result, they get familiar with important cruise line information, such as the arrival-departure time of the targeted cruise ship to the Port (from the Port's interactive map). This could take a six-month effort.

- Their survey, allows them to detect a number of key-employees suspected to have some kind of access to relevant systems at the port. Thus, they conduct phishing attacks targeting these key-employees at the Cruise Terminal to the exploitation of more sophisticated, remote malware affecting the onboard communication interfaces and units of the cruise ship in question. Furthermore, by composing a series of cyber attacks, they manage to compromise a few computers and critical elements of the Port's Cruise terminal. As a result, the cyber-terrorists gain unauthorized remote access to the port system. They also succeed in compromising the email account

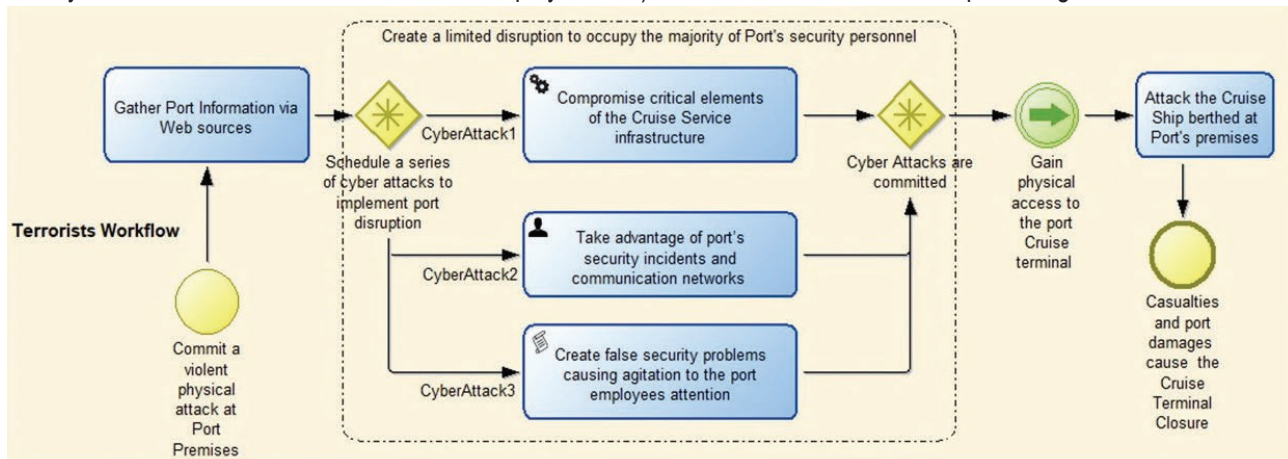


Fig. 1: Terrorist activity workflow of the combined attacks visualized using BPMN 2.0 modeling specification.

of a key-employee. Hence, they can identify the employee's communications with ship agents and port internal colleagues regarding the targeted cruise ship arrangements. During the survey, terrorists have noticed that the Port's premises are protected by a technology surveillance (CCTV) system. Additionally, they have identified that the CCTV system covers only partially the berth entrance of the cruise port's terminal. The CCTV camera system and monitors are situated in an access control room sustaining records

- The Port's targeted key-employee sends via his compromised email account a message to the security guard who is responsible for the cruise passenger terminal entrance, to inform him about the food supplier's arrangement regarding the targeted cruise ship. Now terrorists are aware of the exact timetable of the transfer of supplies from the pier to the cruise ship and the specific information regarding the supplier truck's license plate and driver's personal data (i.e name, ID number). Then, the skilled cyber-terrorists, alter

vessel is planning to make a six-hour stop. Once the cruise vessel is docked, passengers get out from the vessel, following the ISPS security protocol procedures to ensure port's security protection. Passengers who successfully complete the security control can take the shuttle bus that links the quay to the port's terminal. The cruise ship captain has invited all passengers to join a cocktail party onboard with a live concert starting a few hours before the ship departs from the Port. Hence, most passengers are waiting to embark on the cruise ship to join the cocktail party. Terrorists take advantage of their access to the port's closed-circuit television cameras, gained through cyber-attacks realized by the cyber-terrorist group. They replace the web camera's live video streaming with their stored videos of port security alerts, in order to create a limited disruption inside the port facilities to occupy the majority of the security personnel in addressing these false problems. Moreover, terrorists freeze the frames of the video camera showing the cruise passenger terminal entrance area without anything happening. Though, cameras have an internal storage recoding mechanism. Once, this storage is full, the CCTV will start to overwrite what is recorded deleting evidence of the actual terrorist attack. Then, terrorists are disguised as cruise ship's caterers and drive a fake supplier's truck full of sophisticated weapons aiming to enter into the cruise passenger terminal. As they reach the terminal, the security guard has retained the fraudulent information verifying the driver's name, ID and truck license plate. Thus, terrorists can successfully pass the security inspection. The port's false problems have caused confusion and nobody notices the fake supplier's truck approaching the berth of the targeted cruise

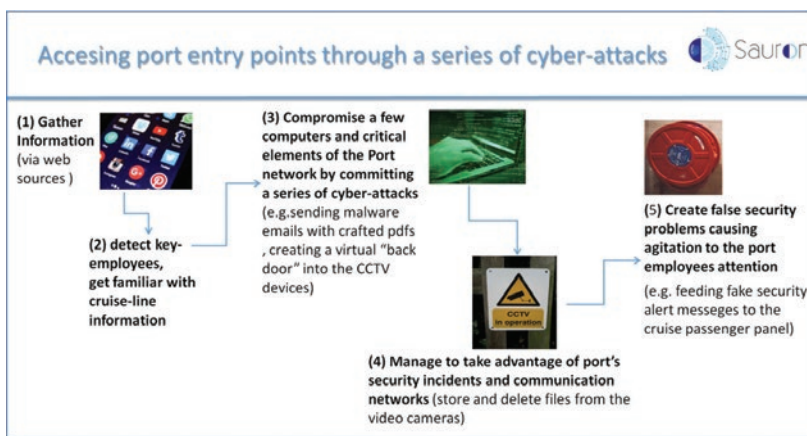


Fig. 2: Terrorists launch a series of cyber-attacks to gain physical access to the Port Cruise Terminal.

on a monthly basis. Hence, the adversaries exploit vulnerabilities of the Port's CCTV system and succeed to gain access to the Port's surveillance network. They may log keystrokes, take screenshots, identify GPS locations, store and delete files from the video cameras. Thus, they can take advantage of the port's security incidents (i.e. reported fire alarms, surveillance system shutdown events, etc.). Additionally, they search for limited security coverage entry points of the cruise passenger terminal by observing the port's video camera. Information generated from these actions (i.e. video files with the port's security incidents stored and kept to the hacker's devices) will help Terrorists to organize accurately and thoroughly their upcoming terror attack within three months.

the information regarding the food arrangements according to their requirements and send a new spoofing email notification from the port employee's email account to the corresponding security guard of the cruise terminal. Moreover, the arrival time of the catering truck has been rescheduled and set two hours before the actual time. At this new time settings, terrorists will reach the same terminal in a fake food truck pretending to be the cruise ship's caterer. As cruise ships' catering arrangements shift frequently, the security guard has not verified the change with the internal port employee. This activity is carried out a day before the armed intrusion.

- By the day the cruise ship is approaching the Port, the armed intrusion is arranged from the terrorists to occur. The cruise

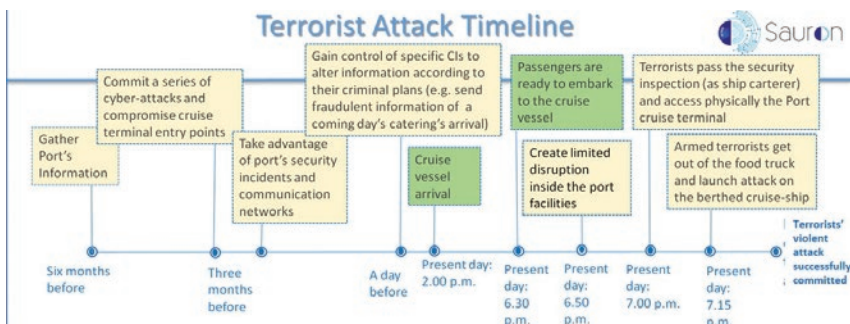


Fig. 3: The timeline of the combined terrorist attacks.

ship. Then, the small heavily armed terrorists launch an attack on the passengers of the targeted cruise ship from the cruise ship berth. Unfortunately, the cruise vessel contains a large number of tourists. As the authorities have not arrived yet to prevent the attack, terrorists are shooting ceaselessly onto the vessel while they are simultaneously running to the east-side of the berth. When the Coast Guard arrives at the Cruise Ship berth and tries to chase the attackers the terrorists have caught up a motorboat appeared from the east coast and thus they manage to decamp. The terrorist coordinated attack has been successfully realized resulting in multiple fatalities and hundreds of wounded people. In this situation, the port's premises shall be evacuated and closed for a long period due to the security breach. Terrorists have carried out successfully the attack at the EU port and inflicted widespread death and destruction. Figure 2 illustrates terrorists' goal of organizing a series of cyber-attacks. Figure 3 shows the current real-life terrorist attack scenario in a timeline row.

To prevent or eliminate the damage, SAURON will indicate proposed strategies to the EU Ports. For example:

- (i) Prevent adversaries from gathering port internal information, check on a frequent basis and give a report for unusual external technical activity that might be testing the port Firewall. (ii) Encounter phishing attacks control, personnel's behavior and unusual IT

system activity to guard against insider and external threats: (a) Regarding administrative access and use of credentials, provide a forensic trail that can be monitored and questioned, (b) check the data flow for anomalies in traffic (i.e. from RAT activity and inform the security staff whether there are anomalies, (c) identify individual activity taken place while the individual is not physically present (i.e. monitoring log-on, recognizing individuals on CCTV screens).

5. Conclusions

The analysed terrorist-attack scenario is a conjunction of coordinated sophisticated cyber and violent physical attacks at the port cruise terminal premises aiming to inflict widespread death and destruction and cause the evacuation and closure of an EU port for a long period due to the occurred security breach. The presented scenario intends to describe a fusion of port security vulnerabilities that have been identified



or reported. The BPMN 2.0 business workflow visualization [10] depicts a sequential timeline row presentation of the attackers' records that allows port analysts to better comprehend what triggers the attackers' activity and help them realize under which circumstances they are able to succeed their goal. SAURON aims to provide a holistic Situation Awareness (SA) concept for protecting EU ports and their surroundings. It has the purpose to ensure an adequate level of both physical and cyber security for European ports and to limit, as far as possible, the detrimental effects of combined physical and cyber-attacks. As soon as SAURON SA platform is completed, it will be tested in line with the real port systems trying to prevent the coordinated attacks of the presented use-case or eliminating its consequences.

6. Acknowledgements

The authors are grateful to the European Commission for supporting the SAURON project (<http://sauronproject.eu/>) under grant agreement No. 740477 addressing the topic CIP-01-2016-2017. The authors would like to thank all project members for their valuable insights. Finally, special thanks to the University of Piraeus, Research Centre for its continuous support.

References

- [1] European Commission. Mobility and Transport. Maritime: What do we want to achieve? https://ec.europa.eu/transport/modes/maritime_en, last accessed 2018-08-07
- [2] Council Directive 2008/114/EC on the identification and designation of Euro-pean critical infrastructures and the as-sessment of the need to improve their protection, Official Journal of the Euro-pean Union, L 345/75-82
- [3] The Economist, Terrorism Timeline, Terrorist atrocities in western Europe. <https://www.economist.com/graphic-detail/2017/03/23/terrorist-atrocities-in-Western-europe>, last accessed 18-8-07
- [4] European Union Agency for Law En-forcement Cooperation, Europol report, Terrorism: the overall terrorist threat to the security of the EU remains acute. last accessed 2018-07-30 <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/terrorism>.
- [5] Ariel Bogle, ABC news, Svitzer employ-ee details stolen in data breach affect-ing almost half of its Australian employ-ees, 15th March 2018, <http://www.abc.net.au/news/2018-03-15/sensitive-data-stolen-from-global-shipping-company-svitzer/9552600>, last ac-cessed 2018-08-07
- [6] The Maritime Executive. Cosco Re-ports Cyberattack at its U.S. Operations, <https://maritime-executive.com/article/cosco-reports-cyberattack-at-its-u-s-operations#gs.OGIgtYc> last accessed 2018-08-07
- [7] European External Action Service, Maritime security: EU adopts new ac-tion plan for more secure seas and oceans https://eeas.europa.eu/headquarters/headquarters-homepage/47365/maritime-security-eu-adopts-new-action-plan-more-secure-seas-and-oceans_hr, last accessed 2018/08/07
- [8] SAURON Homepage, <https://www.sauronproject.eu/>, last ac-cessed 2018/07/30
- [9] Rafael Company, Gimenez Pablo, Car-vajal Federico, Llopis Pérez Israel, Pa-pastergiou Spyridon, Polemi Nineta, "Multidimen-sional Solution for Protect-ing European Ports", NATO Maritime Interdiction Operations Journal, Pro-ceedings of the 2nd Conference of Cyber Security, "Maritime Cyber Securi-ty and Cyber Defense: NATO-EU co-operation implementing the outcomes of the Warsaw Summit. Recent interna-tional evolutions in the environment, 2017, Issue 14, ISSN:2242-441X
- [10] OMG Group, BPMN 2.0 Specification, <https://www.omg.org/spec/BPMN/2.0/>, last accessed 2018/08/07

AUTHORS

Eleni Maria Kalogeraki, PhD(c)
Dept. of Informatics, University of Pireaus,
Karaoli & Dimitriou 80, 18534 Pireaus, Greece, elmaklg@unipi.gr, elmaklg1@gmail.com

Dr. Spyridon Papastergiou
Dept. of Informatics, University of Pireaus,
Karaoli & Dimitriou 80, 18534 Pireaus, Greece, paps@unipi.gr

Associate Professor Nineta Polemi
Director of UNIPi Security Lab, Department of Informatics, University of Piraeus,
Karaoli & Dimitriou 80, 18534 Pireaus, Greece, dpolemi@unipi.gr, dpolemi@gmail.com

Professor Christos Douligeris
Dept. of Informatics, University of Pireaus,
Karaoli & Dimitriou 80, 18534 Pireaus, Greece, cdoulig@unipi.gr

9th NMIOTC Annual Conference

FOOD FOR THOUGHT PAPER

“Fostering Projection of Stability through Maritime Security: Achieving Enhanced Capabilities and Operational Effectiveness”

1. GENERAL

a. The security environment facing the Allies in Europe is changing in fundamental ways, including a steady growth of security challenges emanating from Europe's southern periphery, around the Mediterranean and beyond. The Alliance's maritime security challenges in the south east region include destabilization, terrorism, radicalization, migration, and environmental concerns. The complexity and the dynamic strategic environment along with the plethora of issues Allies will face in the future are fundamentally transnational and require international cooperation and partnerships to address.

b. The current increasingly diverse, unpredictable, and demanding maritime security environment in the southern periphery and beyond, requires actions in order to reinforce Alliance's collective defence, enhance operational capabilities and effectiveness, and strengthen of forces resilience. Further to the main responsibility and mission of NATO to protect and defence its territory and populations against attack, NATO must retain its ability to respond to crises beyond its borders, and remain actively engaged in projecting stability and enhancing international security.

c. It is a continuous effort of the Alliance to respond to security challenges, based on its recognized experience, its crisis management and cooperative security capabilities. Emerging security challenges poses further amplification of Alliance's strategic anticipation to enhance the ability to understand, track and ultimately, anticipate the actions of potential adversaries. Deterrence and defence policy, based on an adaptive mix of conventional and non conventional means is a core element of the overall strategy.

d. Credible, flexible, resilient, and adaptable steps have been taken by the Allies in order to improve its capacity on non conventional threats. Cyber attacks pose an emerging challenge for the security of the Alliance and could be as harmful to modern societies as a conventional one. Cyber defence was decided to be one of the core tasks of Allies collective defence and a reaffirmation on NATO's defensive mandate came out, in both recent Warsaw and Brussels Summit. Cyberspace was recognized as a domain of future operations.

e. In the same context, hybrid warfare has been addressed by NATO as an adversary designed to exploit national and international vulnerabilities across the political, military, economic, social, informational and infrastructure spectrum. Hybrid threats are an international issue but a multinational framework is needed to be developed to facilitate cooperation and collaboration across borders further to a resilient and credible national governance. The Alliance having adopted a strategy and actionable implementation plans, is committed to effective cooperation and coordination with partners and relevant international organizations, in efforts to counter hybrid threats.

f. Facing long-term challenges, NATO will continue to enhance its role in projecting stability and in strengthening security beyond its borders, and to pursue cooperative security through partnership with relevant countries and other international organizations.

2. CONFERENCE TOPICS

The Conference focused on the following five main topics covering military, commercial and legal perspectives:

- a. The emerging security challenges in Central and East Mediterranean. Countering terrorism and deterring transnational criminal activity along with illegal migration.

- b. NATO - EU cooperation on issues of common interest. Strengthening and ensuring the coherence and mutual reinforcement of NATO and EU Capability Development efforts.
- c. The developments of Maritime Security Operations (MSO) Tasks and their implication on capability development and operational effectiveness.
- d. MSO and the latest Technological Developments / Innovations.
- e. Gender perspective in Maritime Operations.

3. OUTCOMES

a. Emerging Security Challenges

The Mediterranean region is facing an unprecedented multiplication of regional crises and unpredictable changes, creating a fundamentally unstable maritime environment affecting individual countries and Trans-Atlantic stakes in these region as well as NATO as an Alliance. The result of this instability is a variety of threats, above all terrorism and the Proliferation of Weapons of Mass Destruction along with transnational criminal activities and irregular migration. Regional maritime security challenges impose substantial human, economic and energy costs with far-reaching security implications beyond the specific geographical area. A holistic and comprehensive approach is needed in order to respond to the multifaceted challenges of the Mediterranean region and to strengthen Collective Defense.

b. New Threats in the Maritime Domain

Last decades great emphases have been given in countering challenges derived from the sea for a more secure environment. Analyses have shown that while governments as individuals or under the auspices of bilateral, multinational and international cooperation fight against existing threats, new ones arise in a constantly manner. In the modern battlefield, the West defines the "Hybrid Warfare" as an emerging threat for the overall security, coming mainly from non-state actors often associated with terrorist groups and organizations. Despite the fact that the term "Hybrid War" is recently appeared in the scene, it is the continuation and the escalation of the existing asymmetric threat. It combines conventional and non-conventional warfare, derived from both state and non-state actors. Hybrid warfare actually is much broader and more complex, requiring a whole-of-government and whole-of-society approach to access the necessary means and authorities to address them. A resilient, credible, and capable governance along with deeper cooperation and collaboration among public, private, and international organizational entities is the path for a credible deterrence against Hybrid threats.

A critical factor while addressing new threats in the maritime domain includes, but not limited, to new technological developments and innovations. The technological achievements combined with the significant increase of a numerous weapon's autonomy increase the weapons effectiveness and consequently our ability to cope with. In conjunction with the above, the appearance of a combination of autonomy and cognition creates a more complex environment and introduce Artificial Intelligence in the field of asymmetric warfare. Artificial Intelligence is a new challenge with potential devastating influence and affects in maritime security in the long term. Deep knowledge, limitations on machine autonomy, identification of autonomous systems vulnerabilities is the path to mitigate the malicious use and the risks from technological developments.

c. Instability of Mediterranean Region

Last decade the Mediterranean region faces serious challenges on multiple fronts. Illicit trade in narcotics, goods and weapons, large movements of refugees and migrants, the majority of them preyed upon by human smugglers and traffickers, illegal cross borders activities, terrorist activities and more. The unstable political environment of the countries of North Africa, the continuity of the war conflicts in Syria along with the involvement of regional power states creates a complex geopolitical environment to the area. The intervention of regional power actors in many cases have an increased present to the area. Russian Federation is one of the key actors in the vicinity of East Mediterranean with a continuously, increasing and strong intervene in Syria. This intervention and military influence strengthen Russia's presence in the region protects its own geopolitical interests in the Middle East. The Instability in the Central and East Mediterranean not only affects regional states but also extends to the Black Sea, the Gulf periphery and to the rest of the states in the Middle East. Interagency approach, interoperability and cooperation enhancing, and in general a greater regional integration is the path for a sufficient governance at sea in order to

increase the stability in the Mediterranean region.

d. NATO – EU Cooperation

Facing common challenges and strategic interests, NATO and the European Union (EU) cooperate on issues of common interest. A cooperation, which is more important than ever, in order to cope with the unprecedented challenges emanating from the East and South. The NATO-EU Joint Declaration from Warsaw Summit verified the substantial relations between the two organizations and outlined areas for strengthened cooperation in the light of common challenges from the East and South, including countering hybrid threats, enhancing resilience, defence capacity building, cyber defence, maritime security, and exercises. NATO and EU are the most prominent regional security providers in deterrence and their cooperation should be further deepened. The expansion of the cooperation and the enhancement of their strategic cooperation at every field are important elements in the development of an international “comprehensive approach” to crisis management and it will be the key in their joint efforts to make the Euro-Atlantic area safer.

e. Gender Perspective in Maritime Operations

Military operations in today’s world require a diversity of qualifications and resources to ensure that peace and security are achieved and maintained. The complementary skills of both male and female personnel are essential for the effectiveness of NATO operations. In this regard a clear understanding of gender issues and awareness at all levels is needed along with gender equality in order to better implement Women Peace and Security Policy into maritime operations and planning. Gender perspectives should be integrated at all levels and in all phases of the planning, execution, assessment and evaluation of operations in order to improve operational effectiveness and strengthening maritime capability.

4. CONCLUSION

The conference participants strongly agreed that all the above are issues, which are important to maintain open for continue confront and for sharing experiences. These are also issues to which maintain high the awareness in order to not lose the knowledge for the overall benefit of NATO and in the same way to better understand how to cope with for the purpose of improving the effectiveness of the connected maritime security tasks.

The Keynote speakers emphasized the need for better capability in the maritime; the need for rapid deployment capability in order to get soon on target and to always maintain high the awareness in the complexity in all the areas we are working and the essential importance of partnership and networking. Operations at sea are not enough without a broader engagement of all the involved actors in the related region; in particular, if we try to project stability. In this contest it was also highlighted the strategic importance of the Black Sea that tends to be in tension or stable together with the Mediterranean Sea.

During the discussions, inside the specific panels, the attention was driven to the link between illegal and criminal activities in one hand and hybrid strategy on the other. Then it was driven to the energy issue, which is a substantial one that does affect the global geopolitics area because of the related economic impact and the need of maritime security in order to ensure the ability, of the navies and coast guards, to effectively protect the infrastructures and the lines of communication.

The issues related to the gender perspective and artificial intelligence were of very interest to the participants. On the gender perspective the discussion brought the attention to maintain high the awareness on this area and that there is the need for continuing the efforts in further development in doctrine and training. The discussion was also very interesting on the artificial intelligence and autonomy and the cyber threat for their huge impact on merchant ship operations and maritime security in general. About artificial intelligence and gender perspective awareness there is really room for much more involvement on both those areas for NATO and NMIOTC that furthermore goes for procedure/guidelines and training needs. Finally, there is the need for closer partnership between commercial shipping industry and NATO in the area of safety of shipping.



*Visit of Diplomatic Academy of
Ministry of Foreign Affairs, January 23, 2018*



*Visit of CAPSTONE, General and Flag Officer Course,
February 21, 2018*



Visit of H. E. the Ambassador of the Republic of Poland in Greece and Polish flag hoist ceremony after the assignment of a Polish Officer in NMIOTC March 16, 2018



Visit of the Commandant & Rector of Bulgarian Navy Academy, Commodore Boyan Kirilov Mednikarov March 23, 2018



Advance Research WS and International Partners' Outreach Event, supported by Science for Peace and Security Programme May 15-17, 2018



9th NMIOTC ANNUAL CONFERENCE June 5-7, 2018



Change of Command. Commodore Charalampos Zisimopoulos GRC (N) handed over to Commodore Stelios Kostalas GRC (N), June 18, 2018



Change of Command Group Photo, June 18, 2018



*Visit of Military Partnerships Directorate (MPD) Director,
Major General Odd Egil Pedersen
June 19, 2018*



*Visit of Emmanouelle College
June 28, 2018*



*Training of ITS MARGOTTINI
February 22-23, 2018*



*NMIOTC Trial Course 20000
February 26 - March 2, 2018*



*Training of US 26th Marine Expeditionary Unit
February 22-23, 2018*



*In Port Phase Training during Exercise NOBLE DINA 2018
March 15, 2018*



*NMIOTC Course 2000-3000
March 19-23, 2018*



*Training of USS CARNEY
March 19-21, 2018*



*Training of GRC SOF Team
June 18 - 22, 2018*



*Training of Jordanian Boarding Team
June 18 - July 2, 2018*



NMIOTC
Souda Bay 732 00 Chania
Crete, GREECE

Phone: +30 28210 85710

Email: studentadmin@nmiotc.nato.int
nmiotc_studentadmin@navy.mil.gr

Webpage: www.nmiotc.nato.int

