A Modelling and Simulation approach to Cyber Domain

LTC Marco Biagini
NATO M&S CoE
Rome, Italy
mscoe.cde01@smd.difesa.it

Massimo Pizzi
NATO M&S CoE
Rome, Italy
pizmasio@gmail.com

LTC Jason Jones
NATO M&S CoE
Rome, Italy
mscoe.dr02@smd.difesa.it

Luc Dandurand
Guardtime
Tallinn, Estonia
luc.dandurand@guardtime.com

Andri Rebane
Kaitseministeerium
Tallinn, Estonia
Andri.Rebane@kaitseministeerium.ee

LTC Wolfhard Schmidt
NATO JFTC
Bydgoszcz, Poland
Wolfhard.Schmidt@jftc.nato.int

Marco Picollo
Leonardo
Rome, Italy
marco.picollo@leonardocompany.com

LT Sonia Forconi
Italian Army
Rome, Italy
sonia_forconi@libero.it

ABSTRACT

"*In recent events, cyber attacks have been part of hybrid warfare. NATO and its Allies rely on strong and resilient cyber defences to fulfil the Alliance's core tasks of collective defence, crisis management and cooperative security. NATO needs to be prepared to defend its networks and operations against the growing sophistication of the cyber threats and attacks it faces."* (NATO Cyber Defence, 2018)

The complexity of Cyberspace, its vast area of applications and the terminology adopted by both the Modelling and Simulation (M&S) and Cyber Community of Interest, make it difficult from both sides to achieve a comprehensive understanding on how M&S could support the Cyber Domain.

This paper proposes a holistic approach to better clarify the areas of application of state-of-the-art M&S technology in Cyberspace. Applying the NATO Concept Development & Experimentation methodology, the authors have developed a research phase, investigating possible solutions to implement a Modelling and Simulation as a Service environment to support and improve NATO's and Nations' efforts in the development of Cooperative Cyber Capabilities. In particular, this research focuses on the NATO Cyber Range Capability development and implementation, looking at improving and expanding its technical capabilities in a distributed cooperative environment through Cyber-based M&S services, namely the Cyber Synthetic Services (CyS2).

The result of this research activity is a Live-Virtual-Constructive simulation technology concept suitable to support studies and further research activities, focusing on use-cases related to the effects of Cyber threats against C2/C4ISTAR systems, Unmanned Autonomous Systems and Operational Technology like Supervisory Control and Data Acquisition systems. The CyS2 solution could potentially support any NATO or National organization dealing with the Cyberspace, and it could be considered a technical baseline for the implementation of a future NATO Cyber Synthetic Environment.

ABOUT THE AUTHORS

LTC Marco BIAGINI is the Concept Development and Experimentation Branch Chief at NATO Modelling & Simulation Centre of Excellence. He has a Ph.D. in Mathematics, Engineering, and Simulation. He has master degrees in strategic studies, peace keeping and security studies and, new media and communication. He was Battalion Commander at the Italian Army Unit for Digitization Experimentation and Section Chief in Computer Assisted Exercise and M&S Branches at the Italian Army Simulation and Validation Centre. He is visiting professor and Lecturer also at the NATO School, member of the Board of Directors of the Italian Movement for Modelling & Simulation and Chairman of the MSG 150 M&S supporting NATO CD&E.

Massimo Pizzi is an Information and Computer Engineering Master's Student at "Guglielmo Marconi" University. He is doing an internship in the Concept Development and Experimentation Branch of the NATO Modelling and Simulation Centre of Excellence of Rome, mainly focusing on Cyber Modelling and Simulation. He earned his Bachelor's Degree at "Tor Vergata" University of Rome with a thesis on Extended Queueing Networks M&S.

LTC Jason M. Jones is the Deputy Director of the NATO Modelling and Simulation Centre of Excellence in Rome, Italy. He has been a Functional Area 57 (Simulation Operations) officer since 2003 and holds a Master of Science in Modelling, Virtual Environments and Simulation from the Naval Postgraduate School in Monterey, CA.

Luc Dandurand is the Head of Cyber Operations at Guardtime, where he leads the development of new business lines for cyber ranges, exercises and advanced cyber capabilities. Prior to joining Guardtime, he was the Head of the ICT Applications and Cybersecurity Division at the ITU, directing the program to assist ITU Member States in cybersecurity and in leveraging ICTs for sustainable development. He started his career as a Signals Officer in the Canadian Forces, working mostly on advanced adversarial assessments of computer networks. After retiring from the military, he worked for Canada's Communication Security Establishment, leading a team responsible for prototyping novel cybersecurity solutions. Prior to joining the ITU, he worked at the NATO Communications and Information Agency, managing cybersecurity capability development projects for NATO and NATO Nations.

Andri Rebane is working in the Estonian Ministry of Defence as the Executive Project Manager for the Cyber Range and Cyber Exercises being responsible for development of the capability and integrating the Cyber Range to the day-to-day cyber operations, education and training. He is also working closely with NATO developing the military alliance's Cyber Range capability. He started his career as a conscript and IT-specialist in Estonian Defence Forces and his previous positions include Chief Information Security Officer at the Cyber Policy Department and the deputy Chief of Cyber Incident Response Capability at the Estonian Defence Forces.

LTC Wolfhard Schmidt is the Branch Head Wargaming and M&S Training Support Division at NATO Joint Force Training Centre (JFTC) in Bydgoszcz (Poland). He was also Branch Head Training Support at JFTC and Head of German Support Element Joint Headquarters Centre in Heidelberg. As commander he was the National Commander and German NBC-Kontingent CJFTF CM in KUWAIT. He was awarded of a MBA at UniBw Hamburg.

Marco Picollo has a Master's Degree in Physics and almost 15 years of experience in M&S working in the Italian Defence Industry. His expertise covers M&S standards and M&S application fields such as CD&E, distributed simulations, training and integration with real systems and command & control in air, naval and land domains. He has been participating to several initiatives and activities such as the Simulation Interoperability Standards Organization, and in various NATO working groups and activities such as the Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise. Currently, he is the Head of the Control Rooms Unit in the Engineering function of Leonardo's Land and Naval Defence Electronics Division

LT Sonia Forconi obtain a PhD in Telecommunications Engineering at "Tor Vergata" University of Rome, Italy (2016), with the thesis "Functional analysis of the Data Streaming service in 4G Long Term Evolution technology and study simulation of relations between Quality of Service and Quality of Experience". She is a Lieutenant Italian Army (OF-1) working in the Concept Development and Experimentation Branch at NATO Modelling & Simulation Centre of Excellence in Rome in the fields of Communications, Networking and Cyber Modelling and Simulation, Information Technology DefNet modelling and simulation, Cyber Defence modelling and simulation.

A Modelling and Simulation approach to Cyber Domain

LTC Marco Biagini
NATO M&S CoE
Rome, Italy
mscoe.cde01@smd.difesa.it

Massimo Pizzi
NATO M&S CoE
Rome, Italy
pizmasio@gmail.com

LTC Jason Jones
NATO M&S CoE
Rome, Italy
mscoe.dr02@smd.difesa.it

Luc Dandurand
Guardtime
Tallinn, Estonia
luc.dandurand@guardtime.com

Andri Rebane
Kaitseministeerium
Tallinn, Estonia
Andri.Rebane@kaitseministeerium.ee

LTC Wolfhard Schmidt
NATO JFTC
Bydgoszcz, Poland
Wolfhard.Schmidt@jftc.nato.int

Marco Picollo
Leonardo
Rome, Italy
marco.picollo@leonardocompany.com

LT Sonia Forconi
Italian Army
Rome, Italy
sonia_forconi@libero.it

INTRODUCTION

The Cyber Domain (or Cyberspace) has been officially recognized by NATO as a military domain of operations in which it's necessary to effectively defend, just as it happens for land, sea, air (NATO Warsav Summit Communiqué, 2016). This domain crosses over all the others, since communications and networks are ubiquitous and their impact on military operations could have significant effects.

Despite the global recognition of its importance, discussing Cyber concepts can easily cause misunderstanding issues because of the lack of standardization of Cyber terminology (Manjikian, Obstacles to the Development of a Universal Lexicon or Cyberwarfare, 2017) (CCD CoE Cyber Definitions, 2018). Speaking about M&S in a Cyber context can generate even more confusion due to some overlapping terminology which results in misinterpretations depending on the reader's background. Surprisingly, the Cyber and M&S domains seem to have evolved in isolation until now, thus leaving synergies largely unexplored, in part due to the confusion resulting from the overlapping terminology.

The NATO M&S CoE, who provided support in the development of a military research project about the use of simulation in support of Cyber, started investigating possible activities and short falls to continue to develop the topic of M&S support in Cyber focusing on two main areas: human interoperability problems between the M&S and the Cyber Community of Interest (CoI), and the investigation on possible requirements to use M&S solutions in the cyber domain looking at available capabilities in NATO and Nations, taking into consideration activities performed by different stakeholders to define requirements to support Cyber activities.

In the final chapter, to address some of the described short falls, the authors provide a description about a possible M&S-based solution, the CyS2, illustrating three use-cases, and their suitability to satisfy possible training and Concet Development and Experimentation (CD&E) requirements.

CYBER AND M&S INTEROPERABILITY

In the Cyber CoI, Cyber Security can be defined as the end state to be achieved to protect the data, the networks and the Information and Communication Technology (ICT) systems in the Cyberspace area of operations. In order to achieve the end-state it is necessary to develop a Cyber Defence capability implementing the Information Assurance components (confidentiality, availability, non-repudiation authentication and integrity) (Forconi, Biagini, & Corona, 2017) to be able to plan and execute Cyberspace Operations (COs) (US Joint Chiefs of Staff, 2013) (US Joint Chiefs of Staff, 2014) (CCD CoE Cyber Definitions, 2018). COs can be either defensive, offensive or exploitation, to discover own and adversary vulnerabilities. More recently with increased digitalization of human activities and the use of generic, highly-functional digital systems in all sorts of military equipment, the scope of cyber security has grown to encompass cyber-physical systems based on other so-called Operational Technology (OT).

M&S methodology, Techniques and Tools can be applied to the Cyber Domain to support and improve the effectiveness in Concept Development & Experimentation (CD&E) analysis, Education, Training and Exercise (ETE), and Operations (decision support and analysis in planning and executions phases). For all of these points, one of the common challenges to face is to find a common understanding: in the authors' experience, in fact, while there are no big issues about the "modelling" idea, the "simulation" word usually brings to mind very different interpretations of the concept behind it. To quick clarify the concept, we find it useful to compare it with its counterpart: emulation. In fact, while "Emulate" derives from *aemulus* (rival) (Castiglioni & Mariotti, 2007) and involves the process of replicating in order to reproduce a system mainly as substitution, "Simulate" derives from *similis* (similar) (Castiglioni & Mariotti, 2007) and involves the process of modelling in order to represent (rely on a proper abstraction) a system mainly for analysis. Repeatability is a key feature of simulation, while in emulation it is uncertain, and differently from a simulator, an emulator usually works close to real-time (McGregor, 2002).

In M&S terminology from the military training domain: Live simulation is defined as a simulation involving real people operating real systems; Virtual simulation is defined as a simulation involving real people operating simulated systems; Constructive simulation is defined as a simulation involving simulated people operating simulated systems and real people can be allowed to stimulate (make inputs) to such simulations (U.S. Department of Defense, 2011). In Cyber training the word "simulation" is commonly used to express a kind of Live fire activity, where roleplay factions (blue and red teams) simulate friendly and enemies parties, play with real cyber-related equipment (to include that made by Virtual Machine (VM) and virtual appliances) over real (virtual) networks producing real cyber effects.

This is actually quite far from how M&S is applied to simulation activities in support of training in the M&S CoI. In fact, the Cyber Domain's simulation exercises would be considered an emulation based on the definition of the M&S CoI. The equivalent exercise of the cyber example in the M&S domain would see echelons of your own forces deployed into a weapons range, assigned roles as friend and foe within an operational scenario, and then given live ammunition to "train" against each other. Thus most activities in the Cyber Domain are emulations in the M&S CoI terminology, with Cyber simulation rarely used because models of computer systems that can simulate the behaviour necessary to support these activities are uncommon, especially when computer system emulation via VMs is relatively trivial to do.

Terms like "VM" and "virtual networks" then have no corresponding terminology in the M&S CoI domain, while the term "virtual", related to simulation, has a totally different meaning as illustrated afore. Also the term "federation*"* means different things to the two CoIs. In Cyber terminology, "federation" is a term related to the Information Technology (IT) world that means the connection of two systems/facility via a network, adopting standard communication protocols. In the M&S CoI, "federation" is mostly related to a High Level Architecture (HLA) collection of models and simulations and supporting infrastructure that work together based on a common understanding of the objects portrayed in the system (Defense Modeling & Simulation Coordination Office, 2012).

CYBER CAPABILITIES

NATO and nations have started to develop Cyber Capabilities, moreover organizations that focus on different aspects of the Cyberspace from ETE, to CD&E and support to Operations. In some of these organizations M&S could provide a tangible support and not only for ETE.

NATO

Even though NATO relies on solid cooperation with partners and industry, there are several initiatives that NATO adopts to be more effective in the cyberspace (NATO Topic 78170, 2018).

Regarding training and education in Cyber, NATO is pooling its capabilities to provide a large offer of education and training courses. In particular the NATO Communication and Information Agency (NCIA) with its Cyber Security Service Line is responsible for planning and executing all life cycle management activities for cyber security (NCIA Cyber Security, 2017). The Cooperative Cyber Defence Centre of Excellence (CCD CoE), even if it is not belonging to the NATO Command Structure, as a multinational and interdisciplinary hub of cyber defence expertise supports NATO focussing on technology, strategy, operations, law and ET (CCD CoE Homepage, 2018).

From the NATO ET organization, the NATO Communications and Information Systems School (NCISS) mission is to provide training to personnel from Allied nations with a raising emphasis on cyber defence Education and Training (E&T) (NCISS Homepage, 2018). In addition, the NATO School Oberammergau (NSO) offers cyber defence-related ET (NATO School Homepage, 2018). Last but not least, the NATO Defence College promotes strategic thinking on political-military matters including cyber defence issues (NDC Homepage, 2018).

From a capability perspective NATO ACT has promoted and developed the NATO Cyber Range Capability (NCRC). This is a growing capability structured with four components: the existing capability in Estonia provides an environment for training and exercises used by NATO; the NCISS; and the others two focused to provide a range in which is possible to practice different aspects of COs and testing activities (NATO investing development Estonian Cyber Range, 2016) (NATO Factsheet Cyber Defence, 2018). Regarding the simulation aspects, the NCRC shall provide a simulated environment able to interact and interoperate with other cyber ranges; integrate with emerging capabilities varying from Industrial Control Systems (ICS) and Internet of Things to special systems in different military domains; simulate the Internet and other types of networks with technical tuneable characteristics; make Communication Information System (CIS) available and provide the simulation of human users.

Taking into consideration the operational aspect, with the establishment of the NATO Computer Incident Response Capability (NCIRC) NATO provides a round-the-clock defence support handling incidents and providing specialist services to prevent, detect, respond and recover from cyber incidents (NATO Factsheet Cyber Defence, 2018). In addition the last NATO effort in the Cyber Domain aims to provide a command structure to support Cyber operations at Operational level establishing a new Cyber Operations Centre, which is still in progress (NATO Factsheet Cyber Defence, 2018).

Estonia

Estonia has recognized Cyberspace as a domain of operations and in defence this will be materialized by creating the Estonian Defence Forces Cyber Command on 1st of August 2018 (Government updated its Action Plan, 2018) (Gov approved national Def Dev Plan next Decade, 2017). The newly created Cyber Command will facilitate the Cyber Conscription (MoD Est Cyber Conscription, 2017) as one of the efforts to broaden the capability and employ new staff.

At the same time efforts continue to build up the Cyber Defence capability through several other means: including the use of volunteers to protect the e-way of living by organizing them to Estonian Defence League's Cyber Unit (Estonian Defence League's Cyber Unit, 2018); engaging young people to the cyber field through the CyberSpike event (CyberSpike, 2018); developing the NATO Cyber Range (NATO investing development Estonian Cyber Range, 2016) and integrating cybersecurity into the conventional defence exercises (Maryland Guard, Estonian Service Members Conduct Cyber Exercise, 2018).

All these efforts are targeted at attracting people to cybersecurity, educating and training existing employees to address cyber threats and building a better national Cyber Defence through competent personnel and wide national and international cooperation. The backbone of this is the Estonian Defence Forces Cyber Range that supports technically the execution of the aforementioned capabilities, events and projects.

The Cyber Range provides new techniques and measures to train cyber personnel, enables collective training to reduce the cost of the overall training curriculum, and enables separation of training from live systems within the simulated environment so day-to-day operations are not compromised.

Italy

Taking in account the challenge to raise the level of networks and systems defence from cyber threats, 2017 was a crucial year for Italian Defence in this domain. In fact, many activities were realized to give Italy the capability to respond to new challenges and threats that the nation and the Armed Forces are called to face and fight back (Ministero della Difesa, 2017). More in detail, the goals achieved in 2017 were: the update of Command and Control (C2) structure; the initial strengthening process of the Italian Cyber Defence Capability development; the implementation of Cyber Defence specialists E&T process; the development of the Army cyber defence training laboratory (Laboratorio Addestrativo Difesa Cibernetica – LADC); the delivery of specific initiatives for information campaign and education; the research of personnel to contribute to the establishment of the Italian Joint Cyber Operations Command (Comando Interforze per le Operazioni Cibernetiche – CIOC) with a reorganization of the Defence Computer Emergency Response Teams (CERT).

Regarding the operational aspect, the CERT, is now the Italian cyber defence operational core within the CIOC, often called to cooperate with the computer incidents response cores (Nuclei di Risposta agli Incidenti Informatici) and to coordinate the Computer Incident Response Teams (CIRT) activities over all defence Services networks and systems. CERT's main tasks are: to prevent computer incidents; to minimize the impact incidents have on networks and systems, to support response and restoration activities; to advise and inform about Cyber threat and risks and to contribute to ET about Cyber.

The LADC project is intended to be a complementary Army Service Cyber Lab element, with the main tasks to: educate and train personnel employed in Cyber Defence; develop and maintain a capability to study and analyse the cyber-attacks, develop technical exercises or simulations focussed on the Army Cyber Domain, integration of CIS or ICT security in the course, information activities (e.g. seminars).

The NATO M&S CoE has supported with research and study activities some of these Italians national initiatives and has developed and published a research study called Communication, Networking and Cyber (CN&C) M&S (NATO M&S annual review 2017). Applying the CN&C M&S approach to Cyber use-case aiming to evolve the military research program called Cyber Security Simulation Environment (CSSE) it was demonstrated against possible effects of COs, and in particular the effects of CNAs executed against wireless tactical networks, namely Software Defined Radio (SDR), on C2 systems.

CYBER TRAINING AND EXERCISES

Cyber training is one of the most suitable areas where M&S can provide wide support in training military personnel and leaders that work within the cyber environment. In this section the authors illustrate some of the most important initiatives related to training requirements to support different aspects of the Cyberspace and the major NATO venues to experiment and exercise M&S-based cyber related capabilities.

NCIA Cyber Security Service Line

As a consequence of the establishment of the Global Programming for E&T within NATO, a Cyber Defence (CD) Operations Training Requirements Analysis (TRA) was performed in 2014 for the whole NATO organization. The outcome of this highlighted a series of training gaps at different levels, mainly Strategic and Operational that required further analysis.

The CD Department Head (CD DH) made up a strategic plan for Training Needs Analyses (TNAs) to address and find solutions to fulfil the highlighted CD training gaps. In the last years, 4 CD TNAs have been performed on different Target Audiences (TAs) at Strategic and Operational levels in NATO, namely SHAPE JCyber and J2 divisions, NATO CIS Group, NCI Agency. NATO HQs TNA is currently in progress. TNA reports show the detailed outcomes with regards to existing or to be developed training initiatives that would fulfil the detected CD

training gaps. One of the main outcome of these TNAs was that training in support of strategic/operational planners and advisors is either it does not exist, or does not fully match the specific training needs of the Alliance's personnel.

In parallel, the Allied Command Transformation (ACT) is working on the definition and implementation of a NCRC and the concept of federation of different training capabilities offered by Allies, Partners, National military organizations or other entities from the private sector and Academia.

In light of this, the NATO M&S COE has started to explore how M&S might support the federation of Cyber training capability by providing specific M&S-based services in support of either individual or collective ETE initiatives.

International Cyberspace Operations Planning Curricula

The NATO Multinational Capability Development Campaign (MCDC) is a US-led transformation force-multiplier joined by the NATO ACT has participated in since 2002 (NATO MCDC Homepage, s.d.). MCDC is designed to develop and deliver new capabilities promoting collaborative concept focussing on coalition operations.

In 2017 the project plan for the International Cyberspace Operations Planning Curricula (ICOPC) was finalized with the purpose to provide international partners E&T and planning guidelines to effectively integrate COs as components of a multinational force operation (NATO MCDC 2017-2018 Cycle, 2017). NATO and the U.S. co-lead the project with 11 contributors and 2 observer nations. In the project, MCDC identified insufficient availability of competent planners due to the lack of unclassified/unrestricted E&T curricula for the planning and employment of COs, the fact that essential tasks related to CO planning are not routinely included in Multinational Forces (MNF) exercises and the insufficiently defined common standard for a CO's E&T framework. Often, partner nations don't have a standardized agreement, framework, C2 structures and process to collaboratively plan COs. Reaching the objectives would achieve the outcome of having an unclassified standard, and interoperable educational planning curricula to effectively build courses to train CO planners. Cyber Ops planners shall have the tasks to: conduct mission analysis, develop Courses of Action (CoA), develop CO Plans and conduct a handover to operations staff.

According to this initiative the NATO M&S CoE received by the Italian MoD the Request for Support to investigate about the use of M&S to possibly support Cyber Ops planners' courses.

Requirements for collective training of Multinational Headquarters

In general the understanding of Cyber Defence means protection of the Alliance's CIS. For this reason significant initiatives were started by NATO and the nations to fulfil Cyber Defence collective and individual education shortfalls through specific courses. All of these initiatives have in common their focus on building and improving the capabilities to defend cyber-attacks and to secure the operational networks to build-up and improve a Cyber Defence Subject matter expertise individual and team.

Commanders and Staff need to be ready to deal with the consequences of a successful executed attack. How can Headquarters on various levels ensure that they still can execute their missions with limited CIS and/or corrupted data? Currently the major Command Post eXercises (CPX) doesn't reflect this topic in their training objectives. The CIS availability for the training audience is currently more part of the exercise real life support rather that is integral part of the training goals. Standing Operating Procedures dealing with Cyber-attack based effects on CIS and data are hardly in place, and currently we cannot train in an efficient way during a Computer Assisted eXercise (CAX) or a CPX, as simulation is replacing/substituting the real operational networks for the training audience and there are no effective simulation solutions to stimulate CIS/Data in place.

To successfully train the training audience, we need to have two key factors in place: CIS availability and its "Plan B" as part of the exercise objectives and tools to stimulate cyber-attack based effects in CAX which allow effects in a controlled manner without effecting the overall exercise IT platform.

The NATO Joint Force Training Centre (JFTC) initiated a workshop in 2017 to check whether there are Commercial Off-The-Shelf tools that can simulate cyber-attack based effects in a constructive training environment as CAX.

These simulated effects can be split into two major pillars: hardware, software and network anomalies such as denial of service of a C2/FS, reduced data throughput in a network, blurring monitors, blue screens, no response of keyboard and mouse; data manipulation such as display of wrong locations of units/elements, missing or wrong air tracks in C2 and FS of the training audience.

The workshop in 2017 proved that in general technical solutions already exist. JFTC currently is preparing a second workshop, in September 2018, to further elaborate the existing possibilities with the intent to trigger a timely procurement process to close the existing training support gap.

The NATO CWIX 2018 Cyber Focus Area

The Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise (CWIX) is an annual event designed to improve interoperability in NATO. One of the activities planned and executed for this edition, in June 2018, was to investigate interoperability and service resiliency between cyber ranges. The NATO M&S CoE, in collaboration with Leonardo Company, provided a Modelling and Simulation as a Service (MSaaS) Cloud Solution, the Open Cloud Environment ApplicatioN (OCEAN), partnering with the Estonian Cyber Range to perform the required tests. In this context, OCEAN aimed to provide a remotely access cloud-based virtual environment to enable cyber services redundancy and cyber resilience testing.

Other exercise venues regarding Cyber aspects are: Locked Shield, Cyber Coalition, Trident Series, Viking, CyCon, and EuroCyber, I/ITSEC, ITEC, NMSG BM and RTGs/ETs, TIDE Sprint, CAX Forum, CD&E Conference.

M&S CYBER SERVICES

M&S, as discussed above, can support several activities in the Cyber Domain also in terms of supporting NATO's and Nations' capabilities and training centres like the JFTC. In particular, the emerging technologies and innovative approaches in applying an "as a service" paradigm offer new opportunities in the M&S application areas to Cyber.

Modelling and Simulation as a Service

Recent developments in computing and networking are making possible to benefit from the products of computing without the full investment in hardware, software, personnel and infrastructure. This happens thanks to the cloud computing paradigm. It is essential that M&S tools are made conveniently accessible to a large number of users, as often as possible. To achieve widespread accessibility, a new M&S framework is required, whose M&S tools can be accessed simultaneously and spontaneously by a large number of users for their individual purposes. This "as a service" paradigm has to support stand-alone use as well as integration of multiple simulated and real systems into a unified simulation environment, whenever the need arises.

The adoption of M&S over a cloud architecture has defined as MSaaS. More precisely, the NATO Science and Technology Organization (STO) has defined MSaaS as *"the combination of service-based approaches with ideas taken from cloud computing"* (NATO STO MSG 136, 2016). The MSaaS architecture development is based on a standard methodology called the NATO Architecture Framework (NAF) (NATO Architecture Framework v4.0 Documentation, 2018). The NATO STO MSG-164, building upon the Allied Framework for MSaaS developed by NATO STO MSG-136, has been tasked to advance and promote the operational readiness and establishment of an MSaaS infrastructure that is available for use in operationally relevant environments supporting continued MSaaS experimentation and evaluation efforts.

The Cyber Synthetic Services

The CSSE project demonstrated how M&S could be implemented to support Cyber Domain CD&E activities. The CSSE project implemented a Live-Constructive simulation architecture to develop a testbed environment developing functions to design, develop and execute tactical communication network scenarios (mission threads) to analyse possible cyber threats and related countermeasures on real C2 systems. In particular the execution of COs against a SDR connected to a wireless tactical network.

From the CSSE demonstrator it was developed a functional concept for the study of an approach to wireless networks based on the Software Defined Network technology, demonstrating the capability to provide to Cyber/IT operators a Decisional Support System that helps to identify, isolate and eventually neutralize potential network's threats (Cyber Security Simulation Service, POLARIS Innovation Journal). This concept according to the application of the MSaaS paradigm has suggested to the authors further research and study activities to define other possible interesting areas of application and in particular a set of possible M&S-based core services related to the Cyber environment, the CyS2.

The idea supporting the CyS2 solution is based on Live-Virtual-Constructive (LVC) MSaaS technology and focuses on three initial use-cases, not still implemented, to demonstrate and evaluate COs effects against NATO and Nationals C2 and C4ISTAR systems, Military communication networks and data exchange affecting multi-domain Unmanned Autonomous Systems (UAxS) and robot swarms, OT used in society to the extent relevant to the military domain like ICS and in particular related to Supervisory Control And Data Acquisition (SCADA) architectures in critical infrastructures.

CyS2 to support C2 and C4ISTAR M&S Cyber use-case

The COs applied to military tactical, operational and strategic networks can help to demonstrate and evaluate the effects on C2/C4ISTAR systems with a special focus on the effects of cyber threats.
This use-case was demonstrated by the CSSE prototype. Further developments were made to deploy components of the CSSE prototype in a cloud environment (i.e. OCEAN), providing Scenario Generator and Animator services and Communication and Networking Simulation (i.e. SVC) services under the MSaaS paradigm.
The proposed solution has the potential to match with requirements for collective training of Multinational Headquarters currently under development by JFTC. Furthermore the same solution could be adopted to support with M&S the International Cyberspace Operations Planning Curricula (ICOPC) Courses for Cyber Ops planners.

Cyber M&S supporting UAxS CD&E, the Robotic Research and Concept Development (R2CD2) project

UAxS are systems with features that make them autonomous/intelligent, according to different levels of autonomy (NATO ACT CEI CAPDEV, 2016), in different tactical and operational scenarios (e.g. UAVs for air, UGVs for land, etc.). Their continuous evolution and use in tactical scenarios makes them vulnerable to possible cyber threats, particularly the communication infrastructure these systems use for information exchange. A holistic approach is necessary to identify software and hardware components that compose UAxS infrastructures to be protected (Madan, Banik, & Bein, 2016). Furthermore, Cyber risk analysis should be used to prioritize identified threats and COs should be modelled and simulated to provide support to risk analysis activities.
The objective is to create a simulation environment, called UAxS Cyberspace Arena (UCA) (Biagini, et al., 2016), and dedicated to the implementation of the UAxS communication infrastructure, capable of implementing countermeasures in the case of COs. The UCA is based on an integrated simulation environment able to provide capabilities to support the evaluation and experimentation of UAxS tactical telecommunication networks. The designed architecture and the simulation environment can be reused for developing related CyS2.
The R2CD2 project, developed by the NATO M&S CoE with the support of the industry, is a first embryonic implementation of the UCA architecture without the communication and networking simulation. The project allows to model and to simulate UAxS ground and air platforms and to exchange information between the simulated entities and a C2 systems, using the C2SIM standard extension for UAxS developed by the M&S CoE. Next project step will be the integration/federation of communication and networking simulation and cyber component of the CSSE, possibly within a CyS2 approach, to make this use-case demonstrable.

Operational Technology and SCADA Modelling and Simulation

A SCADA system is a distributed computer system for electronic monitoring of physical systems. The three basic functions performed by the SCADA system are data acquisition, monitoring and control. SCADA systems, widely distributed for the critical infrastructure management, are a key component of energy management structures. The need to study their vulnerabilities and build their resilience is, undoubtedly, of strategic interest for the Defence. In fact, SCADA systems are used extensively for traffic control (air, rail, automotive) management of fluid transport systems (water supply, gas pipelines, and oil pipelines), energy distribution (electricity transmission networks), management of production lines for industrial processes and environmental remote sensing.
In the OT area, the CSSE prototype demonstrated a potential application of M&S to support cyber M&S-based experimentation activities not only on tactical networks but in general on communication networks and complex systems like SCADA systems controlling critical infrastructures (Sadi, Ali, Dasgupta, & Abercrombie, 2015). In line

with the approach of Defence, performing M&S of vulnerabilities in a SCADA system it's possible show the effects of cyber threats and help to develop the related countermeasures. In fact, it is also possible to interface real network traffic with simulated traffic available with OPNET's system-in-the-loop (SITL) capability with simulated SCADA devices (Colbert & Kott, 2016).
Regarding SCADA systems no core CyS2 have been yet developed, nor were they designed. The research and study activity status in this area is still at the level of a feasibility study, investigating the state-of-the-art.

CONCLUSIONS AND WAY AHEAD

In conclusion the M&S approach to Cyber domain foresees the development of CyS2 as a solution to create simulations of large-scale cyber effects through the use of realistic models that can help military staff to better predict possible outcomes, analysing and assessing various courses of action, in particular thinking about possible effects against C2/C4ISTAR and SCADA systems. In addition, requirements for collective training of Multinational Headquarters have started to be developed collaborating with JFTC. Furthermore, requirements to support with M&S tools the Cyber Ops planners' courses are going to be developed within the NATO M&S CoE and ITA MOD, as contribution to the ICOPC MCDC initiative.

The CyS2 seems to be promising as a possible solution which will help to strike a better balance between simulation and emulation, and may facilitate the integration of real-life systems into exercise and training scenarios. At this stage the CyS2 solution needs to be better defined and developed under the MSaaS paradigm and implemented within a cloud infrastructure.

The NATO M&S CoE has started at the end of 2017 an initiative to promote to interested nations and to NATO an initial concept proposal for the development of what the authors named the NATO Cyber Synthetic Environment (CySE). One aspect of this concept is to address the identified short falls within a comprehensive approach, improving interoperability by pooling a common base of resources of Subject Matter Experts in M&S and Cyber, M&S Cloud environments (i.e. MSaaS), Models and LVC Simulators, gateways and interfaces, and experimentation venues. The CyS2 could be considered one of the possible technical solutions for the future NATO CySE concept implementation. The CySE aims to define, design and develop a M&S environment to be used to support and extend Nations and NATO Cyber Ranges, Labs, schools and training centres with an approach based on the MSaaS paradigm.

ACKNOWLEDGEMENTS

A special thank for the kind and professional collaboration goes to: Rita Russo and Saverio Di Marco from NCIA; William Severin from NATO MCDC; Fabio Corona from NATO M&S CoE; Agatino Mursia and Lucio Ganga from Leonardo; Prof. Giacomo Morabito from University of Catania; Giuseppe Pennisi from "Scuola Telecomunicazioni Forze Armate" of Chiavari.

REFERENCES

Biagini, M., Forconi, S., Corona, F., Mursia, A., Ganga, L., & Battiati, F. (2016). *The Unmanned Autonomous Systems Cyberspace Arena (UCA). A M&S architecture and relevant tools for security issues analysis of autonomous system networks.*

Castiglioni, L., & Mariotti, S. (2007). *Vocabolario della lingua latina.*

CCD CoE Cyber Definitions. (2018). Tratto da CCD CoE Website: https://ccdcoe.org/cyber-definitions.html

CCD CoE Homepage. (2018). Tratto da CCD CoE: https://ccdcoe.org/

Colbert, E. J., & Kott, A. (2016). *Cyber-security of SCADA and Other Industrial Control Systems.* Springer.

CyberSpike. (2018). Tratto da sites.google.com: https://sites.google.com/view/kyberolympia/eng

Defense Modeling & Simulation Coordination Office. (2012). *Documentation of Verification, Validation, and Accreditation (VV&A) for Models and Simulations.*

Estonian Defence League's Cyber Unit. (2018). Tratto da kaitseliit.ee: http://www.kaitseliit.ee/en/cyber-unit

Forconi, S., Biagini, M., & Corona, F. (2017). Communication, Networking and Cyber Modelling and Simulation Support Defence. *I/ITSEC*.

Gov approved national Def Dev Plan next Decade. (2017). Tratto da valitsus.ee: https://www.valitsus.ee/en/news/government-approved-national-defence-development-plan-next-decade

Government updated its Action Plan. (2018). Tratto da valitsus.ee: https://www.valitsus.ee/en/news/government-updated-its-action-plan

Italia - Ministero della Difesa. (2012). *Direttiva interforze di policy sull'ambiente cibernetico.*

Madan, B., Banik, M., & Bein, D. (2016). Securing unmanned autonomous systems from cyber threats. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*.

Manjikian, M. (2017). Obstacles to the Development of a Universal Lexicon or Cyberwarfare. *European Conference on Cyber Warfare and Security*.

Maryland Guard, Estonian Service Members Conduct Cyber Exercise. (2018). Tratto da defence.gov: https://www.defense.gov/News/Article/Article/1526872/maryland-guard-estonian-service-members-conduct-cyber-exercise/

McGregor, I. (2002). The relationship between simulation and emulation. Tratto da https://ieeexplore.ieee.org/document/1166451/

Ministero della Difesa. (2017). Cyber Defence. *Rapporto Esercito 2017*.

MoD Est Cyber Conscription. (2017). Tratto da twitter.com: https://twitter.com/MoD_Estonia/status/824537838586916865

NATO ACT CEI CAPDEV. (2016). *Autonomous Systems Countermeasures.*

NATO Architecture Framework v4.0 Documentation. (2018). Tratto da nafdocs.org: http://nafdocs.org/

NATO Cyber Defence. (2018). Tratto da NATO Website: https://www.nato.int/cps/en/natohq/topics_78170.htm

NATO Factsheet Cyber Defence. (2018). Tratto da NATO Website: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/20180213_1802-factsheet-cyber-defence-en.pdf

NATO investing development Estonian Cyber Range. (2016). Tratto da kmin.ee: http://www.kmin.ee/en/news/nato-investing-development-estonian-cyber-range

NATO MCDC 2017-2018 Cycle. (2017). *International Cyberspace Operations Planning Curricula (ICOPC) - Final Project Plan.* Multinational Capability Development Campaign.

NATO MCDC Homepage. (s.d.). Tratto da NATO ACT: http://www.act.nato.int/mcdc

NATO School Homepage. (2018). Tratto da natoschool.nato.int: http://www.natoschool.nato.int/

NATO STO MSG 136. (2016). *Modelling and Simulation as a Service*. Tratto il giorno May 2016 da STO CSO - STO activities: http://www.cso.nato.int/activities.aspx?RestrictPanel=5

NATO Topic 78170. (2018). Tratto da NATO Website: https://www.nato.int/cps/en/natohq/topics_78170.htm

NATO Warsav Summit Communiqué. (2016). Tratto da NATO Website: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

NCIA Cyber Security. (2017). Tratto da NCIA Website: https://www.ncia.nato.int/Our-Work/Pages/Cyber-Security.aspx

NCISS Homepage. (2018). Tratto da NCISS: https://www.nciss.nato.int/

NDC Homepage. (2018). Tratto da NATO Defence College: http://www.ndc.nato.int/

Sadi, M. A., Ali, M. H., Dasgupta, D., & Abercrombie, R. K. (2015). OPNET/Simulink Based Testbed for Disturbance Detection in the Smart Grid. *Proceedings of the 10th Annual Cyber and Information Security Research Conference*.

U.S. Department of Defense. (2011). *Modeling and Simulation Glossary.*

US Joint Chiefs of Staff. (2013). *Cyberspace Operations.* Tratto da Joint Publication 3-12 (R): http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf

US Joint Chiefs of Staff. (2014). *Information Operations.* Tratto da JCS Joint Publication 3-13: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf