Live, Virtual, Constructive HybrId CYBer warfarE Range (HI-CYBER)

A M&S architecture and tools for security issues analysis countering Hybrid Cyber warfare threats

Lt. Col. Marco Biagini, Lt. Col. Walter David, Capt. Fabio Corona
NATO Modelling & Simulation Centre of Excellence
piazza R. Villoresi, 1 – 00143 Roma
ITALY
mscoe.cd01@smd.difesa.it, mscoe.cd08@smd.difesa.it, mscoe.cd04@smd.difesa.it

Lt. Col. Ferdinando Battiati
Italian Army School of Transmissions and Informatics (SCUTI)
via dei Genieri, 287, 00143 Roma
ITALY
ferdinando.battiati@esercito.difesa.it

Agatino Mursia, Lucio Ganga
Leonardo Finmeccanica Spa, Land & Naval Defence Electronics
via A. Agosta snc - Zona Industriale Pantano D'Arci – 95122 Catania
ITALY
agatino.mursia@leonardocompany.com, lucio.ganga@leonardocompany.com

ABSTRACT

Recent simultaneous, evolving threats of Hybrid Warfare (HW) in all physical environments and the information space aim to target the civilian and military decision making processes and human and social behaviour to achieve (geo) strategic goals. It is crucial to protect communications and networks that support Decision Support Systems (DSS) like digitized Command and Control systems (C2).
This paper describes the concept for a Live, Virtual and Constructive Hybrid Cyber warfare Range (Hi-Cyber), to support NMSG ET-043 Hybrid Warfare Concept Development activities focussing on Cyber aspects within other threats in a HW scenario.
As a result, the paper illustrates the Hi-Cyber concept and the overarching architecture developed as a federation of systems, like a Cyber Attack Simulator, a Hybrid Warfare Scenario Generator and Animator (HW-SGA), C2 systems, Live, Virtual and Constructive tools. Furthermore exploiting heterogeneous technologies, through Systems in the loop (SITL), High Level Architecture (HLA) Run-Time Infrastructure (RTI) and gateways between different communication protocols.
In conclusion, the Hi-Cyber architecture aims to demonstrate and to provide an integrated simulation-based communication and networking environment where it is possible to investigate security issues, evaluate the level of protection, resilience and reactivity of communications and networks. In addition to test the countermeasures to cyber attacks in an Hybrid environment performed to target and to disrupt decision support systems affecting human behaviour in the decision making processes.

Keywords: Hybrid warfare, Cyber warfare, Modelling and Simulation (M&S), Communications, Networks, Human Behaviour, Decision Making Process.

1.0 INTRODUCTION

"*You might not be interested in hybrid warfare, but hybrid threats are definitely interested in you*." [1] The 'hybrid warfare' expression emerged in 2006 after the 2nd Lebanon war, when the Hezbollah used successfully a mix of tools from terrorism to conventional fight against Israeli forces and so far there is no uniform definition. Hybrid threats and tactics are as old as war (as the example of the Troy horse) [2]. Hybrid warfare exploits non-military means in close coordination with military force. [3]. The large use of Special Forces (SF) and/or conventional forces in tactical scenarios and in coordination with offensive Information and Cyber operations makes it crucial to protect our communications and networks in a virtual transversal domain. This paper describes the required properties and capabilities of a Live Virtual Constructive (LVC) Hybrid Cyber-warfare Range (Hi-Cyber) that aims to provide a credible simulation-based experimentation environment where possible Hybrid Threats scenarios will be analysed and evaluated. Those scenarios will be taken into particular consideration the Cyber domain related to communication networks, information flows and decision support systems (i.e. a C2 system) and how they could be attacked and compromised.
Decision making processes and courses of action (COA) rely on the quality (integrity) and availability of information provided by Decision Support Systems (DSS) and Command and Control Systems (C2) connected by network. A failure or corruption of information might negatively influence the decision and mission execution.
The Hi-Cyber concept developed by authors is proposed to support countering Cyber threats in a Hybrid environment by extending the Hybrid Warfare Concept Development activities under the NATO Modelling and Simulation Group (MSG) Exploratory Team (ET)-043 and capitalizing from the implementation and customization of an ongoing National (Italian) Military Research Program (PNRM), the Cyber Security Simulation Environment (CSSE). The first section of this paper illustrates the hybrid and cyber threats.
In the following section the central topic of the paper is addressed. The requirements for the development of the Hi-Cyber and the related Modelling and Simulation (M&S) tools, in terms of general properties and capabilities, are described. The Hi-Cyber concept is based on an integrated simulation environment aimed at modelling hybrid and cyber threats to networks enabled forces and to provide a simulation-based communication and networking environment for evaluating the level of protection of communication and networking solutions as well as the related counter-measures.
As a result, the section illustrates the Hi-Cyber overarching architecture and related M&S tools, focussing on a Networks and Communications Simulator (the Cyber Attack Simulator). The Hi-Cyber architecture is developed as a possible federation of systems (Fig. 3), The requirements for the development of a Hi-Cyber and the related M&S tools, in terms of properties and capabilities, are described. The Hi-Cyber concept is based on an integrated simulation environment allowing to model tactical communication systems and networks.
In the conclusions, it is stressed that the Hi-Cyber architecture aims at demonstrating how it will be possible, to investigate and to evaluate communication and networks security issues in case of cyber attacks in a Hybrid Warfare environment, both in term of resilience and reactivity in operational scenarios, as well as testing the appropriate countermeasures.

2 THE CYBER THREAT IN A HYBRID WARFARE ENVIRONMENT

2.1 Non-linear and hybrid warfare

In his short story, "Without Sky" (Bez Neba), published on March 12, 2014, President Putin's advisor Vladislav Surkov, under his pseudonym Nathan Dubovitsky, told about the "fifth world war": "*It was the first non-linear war…All against all…A few provinces would join one side a few others a different one. One town or generation or gender would join yet another. Then they could switch sides, sometimes mid-battle. Their aims were quite different. Most understood the war to be part of a process. Not necessarily its most important part."*[4].

General Valery Gerasimov, Chief of the General Staff of the Russian Armed Forces and First Deputy Minister of Defence, in his article "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations", published on Voyenno-Promyshlennyy Kurier (VPK) (Military Industrial Courier), presents the recent past present and expected future of warfare and his view on the war as much more than military conflict, now conducted by a roughly 4:1 ratio of non-military and military measures. The nature of threats is in continuous evolution and available war models are not useful to represent each war: each war represents an isolated case, requiring an understanding of its own particular logic, its own unique character and continuous adaptation. [5]

Comprehensive hybrid strategies of states and non-state actors exploit a broad, complex, adaptive integrated mix of civil or non-military measures across the full Diplomatic/Political, Information, Military, Economic, Financial, Intelligence, Legal (DIMEFIL) spectrum such as political pressure, diplomatic, informational campaigns, economic intimidation, sanctions, manipulation in combination with special and conventional military forces and unconventional means, overt and covert activities, by military, paramilitary, irregular and civilian actors. The target are adversaries' vulnerabilities but direct military conflict is kept below a threshold in order to create ambiguity and denial and avoid a strong response from the international community. The focus is on complicating decision making processes with the goal of achieving geopolitical and strategic objectives. [6]

NATO identified Hybrid threats as multimodal, low intensity, kinetic as well as non-kinetic, including asymmetric conflict scenarios, global terrorism, piracy, trans-national organized crime, demographic challenges, resources security, retrenchment from globalization and the proliferation of weapons of mass destruction, "posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives."[7]

The objective of Modelling and Simulation Group - Exploratory Team MSG-ET-043 is to assess the modelling and simulation requirements and shortfalls. The team will explore if the gaps in fulfilling the emerging requirements need to start a working group(s) on the topic. [8].

Figure 1: Adapted from a briefing given by Gen. Valery Gerasimov during the Russian Ministry of Defense's Third Conference on International Security, Moscow. [5]

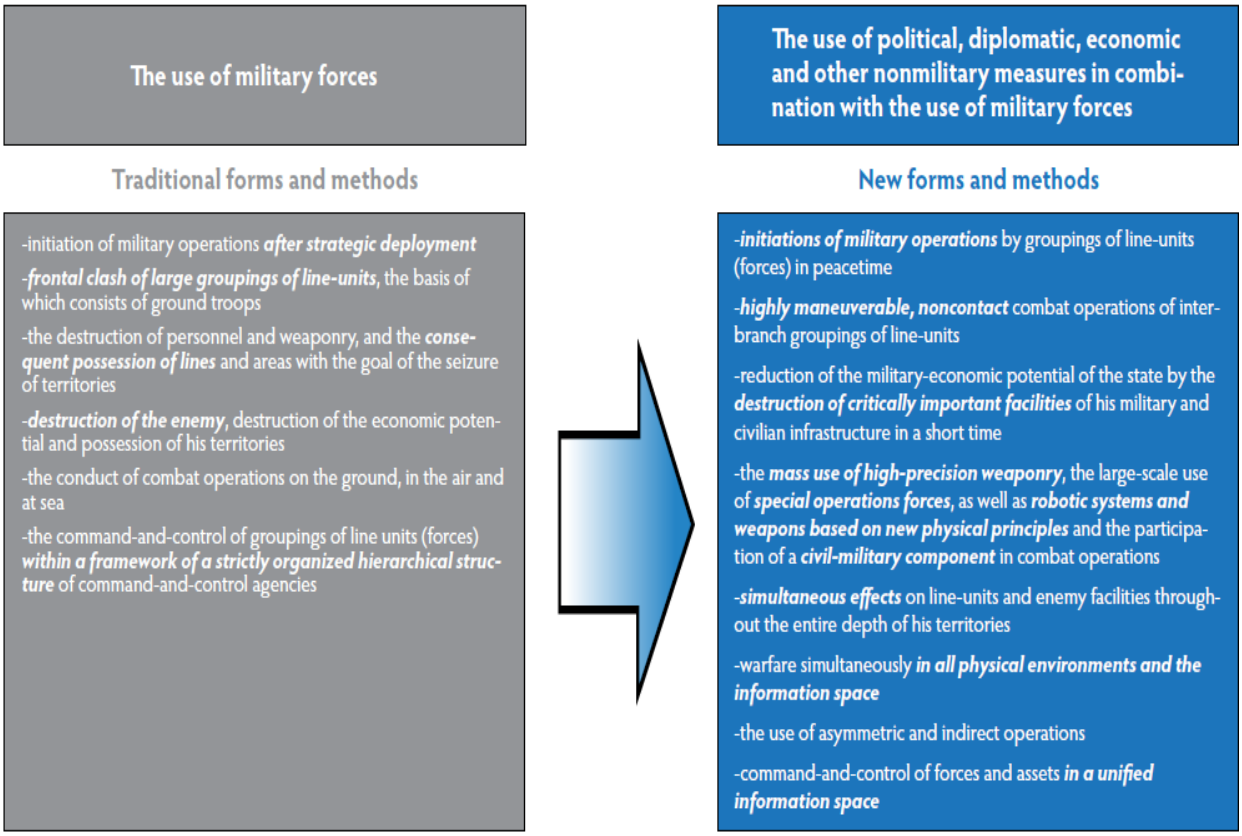

Figure 2: Graphic from Gen. Valery Gerasimov article in Voyenno-Promyshlennyy Kurier, 26 February 2013, translated by Charles Bartles. [4]

2.2 Countering Cyber warfare in a Hybrid Warfare environment

Asymmetric warfare, Information warfare and Cyber warfare are important domains of Hybrid Warfare (HW) that can be fought on three battlegrounds: within the front zone population, home front population and the international community. [10] The dual nature of HW and the Information and Cyber domain require a response using civilian and military tools and therefore coordination between NATO and EU including effective information exchange and training of police forces, border management systems, anti-corruption agencies, transparency in the energy business and in political parties funding and collaboration. Furthermore a joint approach between governments, Centres of Excellence [9] and International Organizations. EU Cyber Security Strategy [10] aims to strengthen the capacity to identify and tackle hybrid threats [11] preparing as a response the 'EU Joint Framework on countering hybrid threats' initiative, with the EU Hybrid Fusion Cell within the EU Intelligence and Situation Centre (EU INTCEN) and the Centre of Excellence for 'countering hybrid threats' that member States are invited to establish [13] and Finland is already considering [14].
Cyberspace is a virtual space built from information, not limited by time or location but limited only by hardware and software. NATO Warsaw Summit, July 2016, recognized cyberspace as a 'domain of operations' [15] and decided to expand the capabilities and scope of the NATO Cyber Range (para 71). [7] While Information warfare for the conduct of Information Operations, relies on Psychological Operations, Military Deception, Operations Security, Computer Network Operations and Electronic Warfare, [15] Cyber warfare refers to sustained, coordinated computer-based cyber-attacks by a state or non-state actors against the targeted IT infrastructure. Cyber-attacks strike at the core by affecting Command and Control (C2). [16] They are designed to affect the decision making process and therefore the human/social behaviour by disrupting or denying IT infrastructures and\or the access to information, overloading or misleading information, creating confusion, aiming at stimulating irrational behaviour and wrong decisions.
The Observe-Orient-Decide-Act (OODA) decision cycle can be affected by cyber-attacks. Observations of

the environment relies on information contained in information systems and communication networks but it may be compromised. In the Orientation phase, the trust to the integrity of information is very important in addition to other parameters (cultural traditions, experience, etc.), low levels of available information and trust to the information will increase the risk of irrational decisions. [18]

3 CYBER SECURITY SIMULATION ENVIRONMENT (CSSE)

The CSSE project is a National (Italian) Military Research Program (PNRM). It is an open and non-classified environment, it is configurable and capable to create and/or modify scenarios, equipment models, protocols, cyber threats and related countermeasures. It is a versatile tool that will be used for its institutional activities by the Italian Army School of Transmissions and Informatics (SCUTI).
The Cyber Security Simulation Environment (CSSE) project aims at delivering a demonstrator that, through the use of advanced simulation tools and techniques, is capable of defining, analysing and evaluating scenarios related to communications networks (tactical or infrastructural) of military units facing cyber threats. CSSE project has been based on two phases. The first one posed the theory foundations of the demonstrator using also as reference the outcomes provided by some NATO working groups in the international arena such as:

- SAS-065 (NATO C2 Maturity Model),
- SAS-085(C2 Agility)
- MSG-117 (M&S in support of Cyber Defence)

Those working groups have explored new C2 (Command and Control) approaches to address operational scenarios in which military forces are required to operate with a strong presence of Non-Governmental Organizations (NGO) and of local military forces and paramilitary organizations (i.e. police and similar). This environment requires a stronger coordination and collaboration (see NATO SAS-065 and SAS-085 Research activities [19]) that should be possible to achieve only through an extensive and a broad exchange of data and information and eventually through the creation of a specific Close Cyber Security Support (CCSS) capability [20]. All the information flows and data exchanges are essential and have to be protected by the cyber-attacks to preserve the information awareness superiority.
In the second phase, the CSSE project objectives were developed to:

- analyse the state of art in the fields of Modelling and Simulation and Cyber Security and put them in synergy with a detailed focus on military networks and cyber threats;
- define and describe operational scenarios, making also reference to the outcome of NATO SAS-065 and NATO SAS-085 in terms of possible scenarios, in which operate military tactical networks and also civil NGO networks subjected to cyber-attacks;
- define and develop ad-hoc models [21] [22] and a simulation architecture that will allow for building a test bed environment (demonstrator) in which attackers and defenders can exercise the scenarios, cyber threats and related countermeasures previously identified without disturbing and affecting the real operational network;
- evaluate, on the demonstrator, different situations, building a repository of reference scenarios to be used for cyber operators training;
- disseminate the results obtained from the campaign of experiments

The demonstrator architecture is capable of experimenting cyber issues not only related to tactical networks but in general on communication networks and is making use of advanced simulation techniques as the Live - Constructive simulation used to evaluate state-of-the-art live cyber threats and countermeasures. The environment is so capable of mixing real live and simulated objects to increase flexibility and to offer a higher number of possible combinations (simulated against real, real against real, etc.).

The demonstrator can be seen also as a first step of a future integrated system (Cyber Trainer) in which

exercises are performed by several groups that operate in Red versus Blue Forces type scenarios.

4 THE HI-CYBER CONCEPT

The LVC (Live Virtual Constructive) Hi-Cyber has been developed by authors and proposed as an emerging concept to support countering Hybrid Cyber-warfare extending the Hybrid Warfare Concept Development activities under the NMSG ET-043. Hi-Cyber originates from the implementation and customization of National (Italian) Military Research Program (PNRM) CSSE that, for the characteristics and functionalities described before, represents a good starting point for the creation of a more complex prototype where the Cyber threats are one of the many dimensions within the Hybrid Warfare, and where the Constructive simulation capabilities can be able to represent some of those other dimensions and their effects at tactical and operational levels.
The proposed architecture of the LVC Hi-Cyber environment is following described in any of its components: The Cyber Attack Simulator, the Hybrid Warfare Scenario Generator and Animator (HW-SGA), C2 systems, Live, Virtual and Constructive tools, exploiting heterogeneous technologies, through Systems in the loop (SITL), High Level Architecture (HLA) Run-Time Infrastructure (RTI), gateways between different communication protocols.
The following figure depicts any of the elements and their relationship:

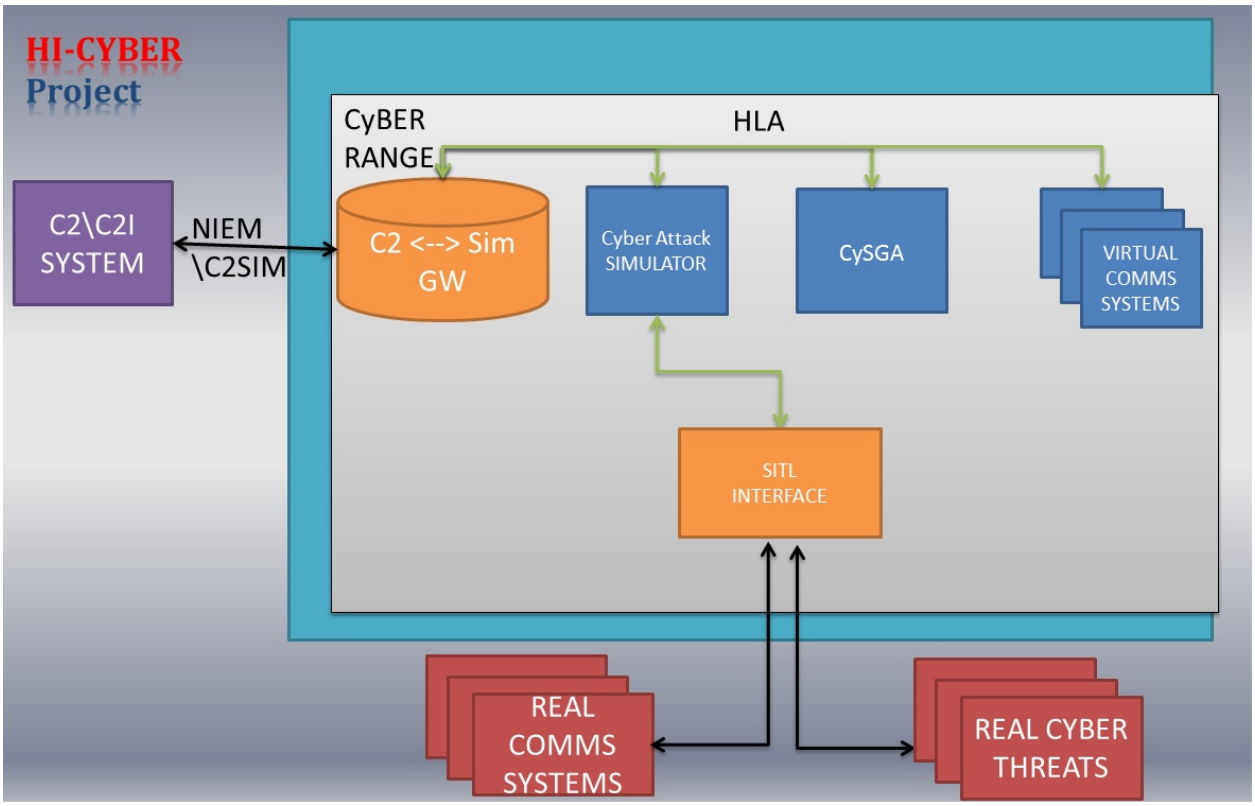

Figure 3: Proposed architecture of the LVC Hi-Cyber environment.

4.1 CYBER ATTACK SIMULATOR

The Cyber Attack Simulator represents one of the Constructive components of the LVC architecture and the core of the Hi-Cyber concept. It derives from the CSSE project mentioned before and provides the simulation of the communication network under attack. The type of cyber attacks are related to all the different layers of the communication protocol stack ranging from physical to the application ones. So it is possible to evaluate the effects of a simple radio jamming or of a more complex Denial of Service attack

[23,24,25,26].
Through its SITL (System In The Loop) interface the CSSE is capable of handling real data coming from Live components and mixing them with simulated ones. The SITL interface forces the simulator time to run at 1/1 with the real one. This means that the real equipments are not aware of exchanging data with simulated ones but seamlessly they interoperate creating a single unified environment.
In particular, Real Cyber Threats can be injected into LVC Hi-Cyber environment without compromising a real operational network but at the same time using its last up-to-date version. In the simulator a mix of real type of attacks [27] and real countermeasure or simulated improved versions that have been modelled in the Hi-Cyber environment, could be used together to test and evaluate system reliability and survivability with new approaches and solutions.

4.2 HWSGA

HWSGA represents another part of the Constructive components of the LVC architecture. It generates the overall Hybrid Warfare (HW) scenarios. The HWSGA allows for creating the three conditions that are used to evaluate threats and countermeasures in an HW environment (scenario).
First an ideal condition is created (no attacks), then an attack is performed and the resulting effects on the overall scenarios are evaluated, finally an attack is conducted, assuming the adequate countermeasures are in place, in order to estimate the reduced damages. The Constructive environment is able to simulate other HW threats other than the cyber to provide a credible wide spectrum of possible threats, executed in a combined way, as properly described and expected to have from an HW environment.

4.3 VIRTUAL COMMS SYSTEMS

The Virtual Comms Systems represents the Virtual component of the LVC architecture. It will allow operators to interact in a virtual 3D environment with some of the communication devices making part of the overall communication network. In the following picture, just as an example, a 3D virtualization of a radio is shown inside a vehicle.
A real operator can interact runtime with the simulation in progress and see the effects of any of his actions on the overall scenario. This will allow for advanced training operations (setting of the radios, changing frequencies, etc.) and maintenance.

Figure 4: Virtual Comms Systems.

4.4 REAL SYSTEMS, COMMS AND C2.

The Real Systems represent the Live component of the LVC architecture.

4.4.1 COMMS SYSTEM

Just as an example, a SDR Radio that, through SITL Interface, exchanges data with the Hi-Cyber

environment . In this way a real data flow (video streams, GPS data, etc.) could be injected into the Constructive component creating a mixed Live-Constructive SDR Radio Network. This will allow for the simulation of very complex scenarios where few real radios can operate with many others simulated ones. Hi-Cyber actually takes into account the orography of the land, the specific propagation model used and the multi-hop path that follow the real data information to reach the destination. Data degradation and delay, just to make an example, can in this way be fully analyzed in a configuration not easily reproducible from real.

Figure 5: Real Comms Systems.

4.4.2 C2 SYSTEMS

Real C2 to Systems represent the decision support systems that could be affected by cyber-attacks directly or indirectly. The C2 system adopted for the experimentation and demonstration purposes was the NATO ICC, using a gateway (the MDLP) able to provide simulated entities tracks from the simulation federation (HLA) to a link 16 format in order to populate the Common Operational Picture (COP) and to show the effects of possible cyber-attacks (spoofing).

Figure 6: C2 System (ICC) and Gateway (MDLP).

5 CONCLUSIONS

The paper illustrated the Hi-Cyber emerging concept developed to support the NATO Modelling and

Simulation Group (NMSG) Exploratory Team ET-43 working group concept regarding M&S Hybrid Warfare. The concept was developed taking into consideration a possible Hybrid Warfare scenario where different hybrid threats could be simulated in a Constructive simulator and executed in combination with simulated/real cyber attacks within a LVC federation.

Even if the development of the Hi-Cyber concept seems promising in fulfilling requirements for a Hybrid Cyber Range, further development is required to properly run the experimentation phase to support the proof of concept regarding the adoption of M&S tools to support and address Cyber Attacks in a Hybrid Warfare Environment. For concept development, training and exercises purposes, hybrid threats ad-hoc scenarios and tactical vignettes should be developed within the Virtual and Constructive simulation. It will be also interesting to investigate regarding possible Hybrid Warfare behavior models, affecting humans and also Communication and Network systems in relationship with cyber and other hybrid threats.

REFERENCES

[1] A. Butenschön, EDA Project Officer, European Defence Matters, Cyber threats: are you ready? EDA 2015 Issue 09.
[2] N. Popescu, Hybrid tactics: neither New nor only Russian, European Union Institute for Security Studies, Januaury 2015.
[3] NATO Parliamentary Assembly Defence And Security Committee, Julio Miranda Calha, General Rapporteur, Hybrid Warfare: NATO's New Strategic Challenge? - Draft General Report .
[4] P. Pomerantsev, How Putin is Reinventing Warfare, May 5, 2014 available on http://foreignpolicy.com/2014/05/05/how-putin-is-reinventing-warfare/ [visited on 08 Sept 2016].
[5] C. K. Bartles, Getting Gerasimov Right, Military Review, available on http://fmso.leavenworth.army.mil/documents/Regional%20security%20europe/MilitaryReview_20160228_art009.pdf [visited on 08 Sept 2016].
[6] ACT's M&S Gap Analysis. MSG-ET-043 Hybrid Warfare Modelling and Simulation (HWMS).
[7] NATO's Bi-Strategic Command Capstone Concept NATO's Bi-Strategic Command Capstone Concept, 5000 FXX/0100/TT-0651/SER: NU0040 Dated 25 August 2010: BI-SC Input for a new Capstone Concept for The Military Contribution to Countering Hybrid Threats (MCCHT)).
[8] MSG-ET-043 Hybrid Warfare Modelling and Simulation (HWMS) Technical Activity Proposal (TAP)
[9] V. R. Morris, Connecting Allied Hybrid Networks through NATO Centers of Excellence, "Raptor 14" Multinational Training Team Approach, U.S. Army Europe's Joint Multinational Readiness Center (JMRC), Germany.
[10] NATO Modelling and Simulation Exploratory Team ET-043 Quadchart.
[11] M. Sieber, European Defence Matters, Cyber threats: are you ready?, EDA 2015 Issue 09.
[12] J. Demecq, EDA Chief Executive, in Hybrid Warfare: the future of warfare? EDA European Defence Matters, Issue 9 2015.
[13] European Commission, Joint Communication to the European Parliament and the Council, Joint Framework on Countering Hybrid Threats. A European Union Response, Brussels, 6.4.2016, Join (2016) 18 Final.
[14] Prime Minister's Office Finland, Government Report on Finnish Foreign and Security Policy Prime Minister's Office Publications 9/2016.
[15] NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html.
[16] F. Schreier, On Cyberwarfare, DCAF Horizon 2015 Working Paper No. 7.
[17] S. D. Bachmann, H. Gunneriusson, Russia's Hybrid Warfare in the East: Using the Information Sphere as Integral to Hybrid Warfare, October 7, 2015, Georgetown Journal of International Affairs - International Engagement on Cyber V: Securing Critical Infrastructure, Online, Forthcoming.
[18] E. Cayirci, R. Ghergherehchi, Modeling Cyber attacks and their effects on decision process, Published

in Proceeding WSC '11 Proceedings of the Winter Simulation Conference Pages 2632-2641 Winter Simulation Conference ©2011.

[19] NATO STO SAS-065 Final Report: NATO NEC C2 Maturity Model; NATO STO SAS-085 Final Report: C2 Agility.

[20] A. Bruzzone, A. Mursia, M. Turi, G. Giannandrea. Cyber Security: CCDS – Close Cyber Defence Support. 18th ICCRTS. June 2013.

[21] E. Guardo, G. Morabito, G. Catania, A. Mursia, F. Battiati. BRAVO: A Black-hole Resilient Ad-hoc on demand distance Vector rOuting for tactical communications. 2014 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)

[22] A. Mursia, L. Ganga, A. Leonardi, G. Morabito, C. Rametta, L. Wihl. A Simulation study of C4I Communications network under cyber-attacks. DHSS 2011. September 2011.

[23] I. F. Akyildiz, X. Wang, and W. Wang, Wireless mesh networks: a survey, Computer networks, vol. 47, no. 4, pp. 445-487, March 2005.

[24] R. Poisel, Modern communications jamming: principles and techniques, 2nd ed. Artech House, Boston/London 2011.

[25] J.-F. Raymond, Traffic analysis: Protocols, attacks, design issues, and open problems. Designing Privacy Enhancing Technologies, Springer, Berlin Heidelberg, 2001

[26] V. Gupta, S. Krishnamurthy, and M. Faloutsos, Denial of service attacks at the MAC layer in wireless ad hoc networks, in proc. of IEEE MILCOM, 2002.

[27] M. Al-Shurman, S.-M. Yoo, and S. Park, Black hole attack in mobile Ad Hoc networks, in proc. of the 42nd annual Southeast regional conference, April 2004.