INTEROPERABLE SIMULATION AND SERIOUS GAMES FOR CREATING AN OPEN CYBER RANGE

Agostino G. Bruzzone [(a)], Riccardo Di Matteo [(b)], Marina Massei [(c)],
Enrico Russo [(d)], Mirko Cantilli [(e)], Kirill Sinelshchikov [(f)], Giovanni Luca Maglione [(g)]

[(a)] [(c)] DIME University of Genoa,
[(b)] Simulation Team SIM4Future, [(d)] DIBRIS University of Genoa,
[(e)] Liophant Simulation, [(f)] [(g)] Simulation Team

[(a)] agostino@itim.unige.it, [(b)] riccardo.dimatteo@simulationteam.com, [(c)] massei@itim.unige.it,
[(d)] enrico.russo@unige.it, [(e)] mirko.cantilli@liophant.org,
[(f)] kirill.sinelshchikov@simulationteam.com, [(g)] maglione@simulationteam.com

[(a)] [(c)] www.itim.unige.it, [(b)] www.sim4future.com, [(d)] www.dibris.unige.it,
[(e)] www.liophant.org, [(f)] [(g)] www.simulationteam.com

ABSTRACT

The paper proposes an open architecture to support the creation of a synthetic environment devoted to simulate complex scenarios related to the protection of cyber-physical systems. The proposed approach is based on applying the combination of interoperable simulation and serious games to develop a framework where different models, as well as real equipment, could interoperate based on High Level Architecture standard. By this approach, it becomes possible to create a federation reproducing a scenario including multiple physical and cyber layers interacting dynamically and reproducing complex situations. The authors propose an example of specific case study conceptually developed to apply this approach.

Keywords: Cyber Range, Multi Layer Modeling, Interoperable Simulation, Serious Games

1 INTRODUCTION

Today "Cyber" is an hot spot, as well as a buzz word, and there are many discussions about it; therefore despite the general considerations, the experienced along recent years confirm the impact of threats acting on the cyber layer and the escalation of attacks in this "space" that is constantly growing in terms of extension, impact, tactics and strategies (Wilhoit & Hara 2015; Page et al. 2017). Due to these reasons, the development of Cyber ranges as a synthetic environments devoted to address cyber defense is currently evolving quickly as a necessity (Pridmore et al. 2010; Winter 2012; Ferguson et al. 2014). In facts along last years the cyberspace impact on physical system exploded and the cyber attacks confirmed the need to develop new capabilities able to support the development of new systems and policies in this area (Cashell et al.2004; Kunder et al. 2010; Sgouras et al. 2014). A major additional issue is represented by the Education and Training, another set of activities that require a framework where to conduct test and exercises (Pham et al. 2016; Törngren et al. 2017).

In this sense a Cyber Range is expected to provide the opportunity to experience the use of tools and techniques able to improve the stability, security and performances of cyber physical systems.

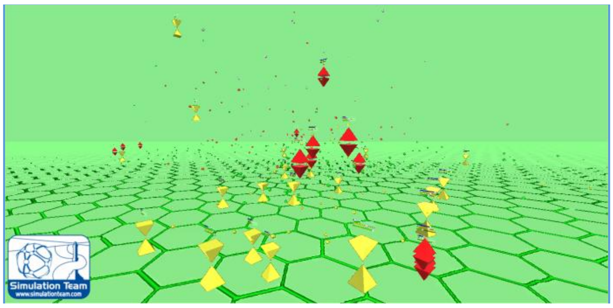


Fig.1 – Cyber Space Representation coupled with real layer within Simulation Team Synthetic Environment

The Cyber Range concept is similar to that one of the shooting and kinetic ranges, in use by military force, that allows to train warfighters in using weapons and conduct operations. In similar way, the cyberwarfare actors and players are expected to use the Cyber Range for training as well as for development and testing of new solutions and tactics in order to ensure consistent operations and readiness for real fighting. From this point of view it is evident that the cyber warfare is evolving from simple attacks to become part of more evolved and comprehensive strategies based on the use of real "cyber weapons" that could compromise critical infrastructures, society policies and endanger human life (Chakhchoukh & Ishii 2015); to face these challenges there is a growing need of Cyber Ranges able to reproduce multiple layers that are closely interconnected as it happen in the real world (Bruzzone et al.2016). Due to theses reasons and considering the complexity of the proposed scenarios, the authors suggest the adoption of an open architecture able to integrate different components including specific models, meta-models, interoperable simulators as well as real equipment. A review of the literature shows that the integration of interoperable simulators, analytical models and real equipment have been also successfully used also in the physical space in sectors like Industry, Logistics, Healthcare. Examples of review articles and applications in different areas also including security issues can be found in (Michael et al., 2014; Zhou et al., 2016; Longo, 2015; Longo 2012).

2 STATE OF ART IN MODELLING CYBER WARFARE & EXISTING CYBER RANGES

It is evident since several years that the cyber warfare is a crucial element to simulate in order to support decision makers to face challenges posed by cyber warfare itself (Stytz & Banks 2012).

Indeed, since the beginning of this decade, it has been proposed this concept as following: "a cyber range is a facility allowing a model of an IT system to run in a simulated environment to perform tests and measurements that are applicable to the real world" (Winter, 2012).

Even statistics turn to be an useful "tool" for analyzing cyber attacks along those years; for instance a pretty interesting study presents a statistical framework for investigating cyber attack data and predicting them in term of attack rate with reasonable accuracy (Zhan, Z. et al. 2013).

US DoD (United States Department of Defense) is deeply involved in cyber range investigation through the National Cyber Range (NCR) operated by the Test Resource Management Center (TRMC) and the project has been seen as a major event in this context (Pridmore et al. 2010). In facts the evolution of this program allowed to analyze the DoD PMs (program managers) necessities and to refine objectives: "Internet-like environment by employing a multitude of virtual machines and physical hardware" have to be created "to find the best approach for testing the cyberspace resiliency of the systems under development" in order to show how incorporating cyber security at early stage of the development life cycle "helps to avoid high cost integration" (Ferguson et al. 2014)

A more recent definition of cyber range in training perspective says "Cyber-Range is a vehicle used to train in offensive and defensive Information Operations and Information Warfare" (Lawless et al. 2014) In this case it is presented a modular approach to the Cyber-Range Framework development, tailored for being adaptable and to meet current and future needs.

Again, statistics play a key role: advanced forecasting technique such as Exponentially Weighted Moving Average (EWMA) are applied to investigate Distributed Denial of Service (DDoS) attacks (Olabelurin et al. 2015) and it is proposed a methodology for reducing the number of alerts and false positive alarms.

Typically, training in this context is very crucial for military personnel: an interesting work on NATO MSG-117 activities (assessing which areas of Modeling and Simulation could contribute to cyber defense) and SISO standards summarizes the current position in this sense (Croom-Johnson, S., 2015).

Obviously the personnel is a key factor in managing cyber security issues and social engineering should be properly addressed in this field (Granger 2001; Evans & Wallner 2005; Goodchild 2012). Indeed, despite a large numbers of certifications, applicants assessment is quite challenging. From this point of view gamefication is used to evaluate skills and technical abilities (Cherinka & Prezzama 2015).

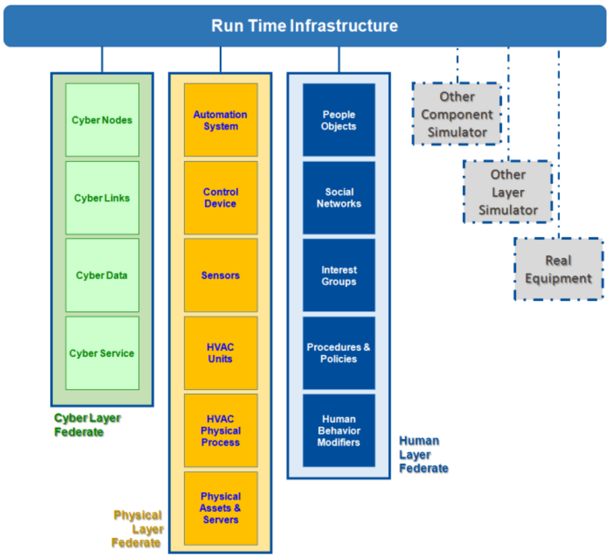


Fig.2 – Example of the Open Proposed Architecture

End users are once more involved in the process, providing an ad hoc experience of cyber threats seems to be an helpful approach in the framework of Internet of Everything (IOE) for securing resilience of devices (Lawless et al. 2015). On the same track it is possible to apply Cyber Range to Concept of Operations (CONOPS) in order to recover from a disaster affecting a large company; this approach had allowed to develop useful and realistic scenarios for disaster testing (Ali & Santos 2015; Kisekka & Baham 2015).

Testing and training are again core elements of scientific research on cyber range: "Cyber Security Training Range, a simulation infrastructure where various scenarios can be recreated and tested, to educate Mission planners, Mission engineers and System administrators on the possible attacks at the different mission phases, shall be available as daily working asset." (Mann & Zatti 2016).

In this sense the use of proper modeling techniques to reproduce heterogeneous networks incorporating multiple entities to create a realistic cyber-physical scenario is fundamental (Bruzzone et al.2013). A large number of trainees performing training activities in specific environment that contains virtual machines, network topology, security-related content etc is quite challenging, a possible solution is the use of automatic generated cyber ranges for education and training based on specifications defined by the instructors (Pham et al 2016; Bruzzone et al. 2016). DDoS are one of the most "effective" and "efficient" threat to deal with. Modeling is used to develop a model of normal user behavior with weighted fuzzy clustering (Zolotukhin et al.2016).

Miming the real systems is another M&S application "mimetic environments, which mimic actual networks including personal computers, network assets, etc., are required for cyber range or malware analysis" (Yasuda,

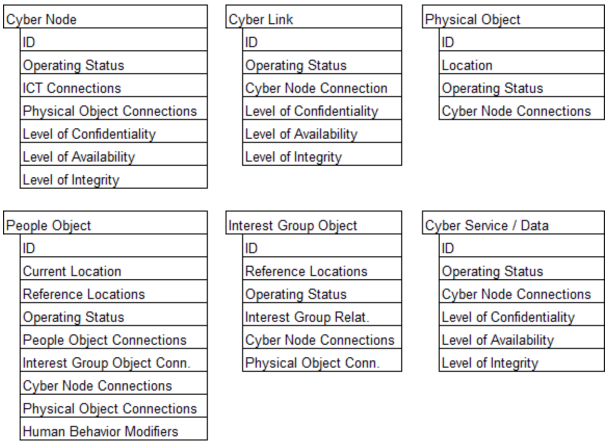
S. 2016; Yasuda et al. 2017). In facts decision makers face cyber attacks and military commanders (as decision makers themselves) need models able to improve awareness of threats development; from this point of view interoperability is a major issues as suggested by recent works from NATO MSG-117 (Modelling and Simulation to Support Cyber Defence) that address, as anticipated, this aspect with special focus on standardization process (Croom-Johnson & Couretas 2016). It is important to outline that, from this point of view, time-cost reduction is always a goal to be reached while developing cyber range environments through avoidance of errors in its configuration (Damodaran & Tidmarsh 2016). Again, cyber range and test at low cost are heavily involved while analyzing threats of actual automated systems, such as SCADA (Supervisory control and data acquisition), along with related potential issues and criticalities (Hallaq et al. 2016). Lately, research is being even more focused on education issues; for instance, in order to evaluate the success rate of cyber security students, especially while performing lab activities in their master classes, have been identified “metrics, like the number of IDS alerts, network sessions, or top destination IP addresses, …, indicators of success or failure for final grade” (Caliskan et al. 2017). This is expected to be helpful to manage the growing number of cyber security exercises and evaluate students across different institutions and academic years.

3 SIMULACRA ARCHITECTURE

SIMULACRA (Simulation Multi Layer Architecture for Cyber Range) is an open interoperable architecture based on HLA, designed by authors, that is allowing to combining different simulators, models and real systems in order to create a common synthetic environment. The approach is based on MS2G (Modeling, interoperable Simulation and Serious Games) paradigm and emphasize the importance to be able to combine together multi resolution models and to cover specific layers also by metamodels when more high fidelity solutions are not available or usable (Bruzzone et al.2014). In this case, the development process should be strongly integrated with VV&A (Verification, Validation and Accreditation) in order to guarantee a constant control of the simulation confidence bands and fidelity even in relaxed conditions devoted to investigate complex scenarios.

Indeed the use of engagement techniques and immersive solutions common in Serious Games are considered fundamental due to their capability to provide an intuitive environment where the players could quickly understand the situation evolution and consequences of different operations in a scenario where the dimension and complexity is very hard. In facts, today, it could be interesting to evolve in this framework from the traditional man-in-the-loop approach, often based often in using hackers as players in the cyber defense training, to condition where it is applied the concept of man-on-the-loop supervising several assets and driving the operations at high level while low level actions are simulated by agents reproducing humans or artificial intelligences (Magrassi 2013; Bruzzone et al.2015). In this sense the authors have already experienced several applications and developed solutions such as in the case of T-REX or JESSI, an agent driven stochastic simulation able to combine real and cyber components of a multidimensional space that include air, land, sea, underwater, space and cyberspace (Bruzzone et al.2016); this framework includes population, legacy and autonomous assets as well critical infrastructures to develop complex scenarios and it is able to cover social engineering, human behaviors and ICT network simulation (see figure 1). In this case it is proposed an architecture able to incorporate some of the capabilities addressed by T-REX with others provided by other federates as proposed in following figure 2.

The proposed architecture deals to the use of specific objects within the Federation Object Model devoted to share the entities, attributes and interaction among the different simulators as proposed in figure 2. The objects and attributes include among the others:



Cyber Node
- ID
- Operating Status
- ICT Connections
- Physical Object Connections
- Level of Confidentiality
- Level of Availability
- Level of Integrity

Cyber Link
- ID
- Operating Status
- Cyber Node Connection
- Level of Confidentiality
- Level of Availability
- Level of Integrity

Physical Object
- ID
- Location
- Operating Status
- Cyber Node Connections

People Object
- ID
- Current Location
- Reference Locations
- Operating Status
- People Object Connections
- Interest Group Object Conn.
- Cyber Node Connections
- Physical Object Connections
- Human Behavior Modifiers

Interest Group Object
- ID
- Reference Locations
- Operating Status
- Interest Group Relat.
- Cyber Node Connections
- Physical Object Conn.

Cyber Service / Data
- ID
- Operating Status
- Cyber Node Connections
- Level of Confidentiality
- Level of Availability
- Level of Integrity

The interactions in this case address issues such as:

○ Cyber Attack Action against a Target
○ Cyber Defensive Action on a Target
○ Routing for accessing a Cyber Service
○ Sending / Receiving Data from a Cyber Service

Indeed it is important to define also performance indexes to evaluate the pending potential of cyber threats on physical systems; for instance respect an comprised information shared between *A* and *B* as proposed below:

$$OL^{c}_{G,A,B}(t) = [1 - \prod_{i=1}^{n} Mn(i,G,A,B,t)]\left[1 - \prod_{j=1}^{m} Ml(j,G,A,B,t)\right] \quad (1)$$

$$Mn(i,G,A,B,t) = \begin{cases} i \in G & Ln^{c}_{i}(t) \cdot (1 - P(t,G,A,B)) - 1 \\ & i \notin G \quad 1 \end{cases} \quad (2)$$

$$Ml(j,G,A,B,t) = \begin{cases} j \in G & Ll^{c}_{i}(t) \cdot (1 - P(t,G,A,B)) - 1 \\ & j \notin G \quad 1 \end{cases} \quad (3)$$

$$OLg^{A}_{B}(t) = \max\,(OL^{c}_{G} \;\; \forall G \in Path(A,B,t) \quad (4)$$

$OL^{C}_{G}(t)$	Confidentiality Level on the G-th Path a t-time
$OLg^{A}_{B}(t)$	Global Confidentiality between A & B at t time.

n	number of cyber nodes
m	number of cyber links
G	path among two cyber assets
Path(A,B)	Set including all alternative path between A and B at t time
P(t,G,A,B)	Probability to use G-th Path from *A* to *B* at t time

Ln^C_i	Level of confidentiality of the i-th node
Ll^C_j	Level of confidentiality of the j-th link

The authors are currently working in adapting previous simulator for this purposes in order to extend their capabilities for addressing the specific new scenario proposed in the following.

4 GRID ATTACK AND AUTOMATION

One of the critical factors is the presence of nodes of different independent networks in the same geographic locations, for instance an office could have its own cable network with or without connection to the internet, while in the same time there are several mobile and WiFi networks covering the same area. Obviously, a bridge between them could be created; indeed this could happen occasionally or purposely, in the first case, for example the cause could an employee that could decide to use internet on a work place by activating a 3G modem or WiFi hotspot on a phone, connecting internal and external networks. In the second case, depending of available resources and intruder background and skills, there are different types of communication channels that could be established, starting from that ones mentioned before up to data transmission techniques which could allow to communicate even with air gaped devices, for example using PC speakers (Lazic & Aarabi 2006), noise of fan changing its rpm (Guri et al. 2016), transmitting RF (radio frequency) signals using memory data bus (Guri et al. 2015a) and even regulating thermal pattern of a PC (Guri et al. 2015b). Obviously all these techniques could be used not only separately, but also in combination to create mesh network of compromised systems, containing even air gaped devices in the case they are already infected. It is important to mention also that growing amount of IoT (Internet of Things) devices that introduce often insecure and outdated software, creating additional vulnerabilities and vectors of attack (Barcena & Wueest 2015). From the point of view of creating a cyber range, it is convenient to simulate several independent networks, not originally connected, as well as the establishment of occasional temporary or permanent link between them. In facts, for instance a possible targets of hackers is a very critical network: power grid (Adams, 2015); in this sense a very notable case of cyber blackout happened at the end of 2015 in Ukraine (Sullivan 2017). Obviously these facts create a lot of concerns about reliability of perspective smart electric grid; for example as consequence of an attack the power could be simply switched off as well as reprogrammed and invalid switching of electric devices could result in unsafe connections which may lead to fire in the target place (Mo et al. 2012).

There are even some other vectors of attacks which have theoretical foundation, but, fortunately, limited experimental exploitation; for instance it's possible to 'brick' or even explode the battery of an Apple's laptop flashing microcontroller's firmware (Miller 2011). So it is evident that several different kinds of interactions could affect physical and cyber systems and assets.

5 SCENARIO & EXERCISE ON THE SYNTHETIC ENVIRONMENT

It is currently possible to define a testing scenario covering multiple layers including among the others:

- ICT Infrastructures
- Business Processes & Real Operations
- Facilities
- Entity & Units
- Population & Users

To create this reliable and useful scenario, it is proposed to define a specific case to be investigated in relation to an infrastructure providing business services. Obviously, it is useful to finalize the case in order to be realistic and easily extendable to a wide range of applications; in the paper the mission environment suggested is related to a College/University Department facing different kind of internal and external threats as well as malfunctions.

In facts, a University Department represents a good example of a division within a larger organization. While the Department shares a different number of units, services and procedures coordinated centrally, it may decide to adopt or extend its own. For this reason, the Department depends also on internal administrative or technical employees who shall assist its Academic staff. Employees belong to internal units according to their functions, namely, if they work for accounting, research and teaching support or for the IT and technical field support.

As an example of an internal administrative process, we could consider a “purchase request” concerning acquisition of material for a “research project”. The accounting staff of the Department applies internal arrangements on everything related to the tender specifications, the choice of potential suppliers; in this way the staff is supposed to record and verify all the support documentation. When the procurement process is finalized in terms of purchase request and winner selection, it is created and added the final order to the central accounting software, managed by the central University Informatics Centre. At the time of ordered goods arrival at the destination (the Department), it is conducted an acceptance check respect original requirements; in positive case, the administrative staff confirms the invoice receipt and authorize the payment through the accounting software.

The internal IT staff also supports this process by making available different tools that they implement and manage locally. Among these tools, a file server allows the administrative staff to save and share, with the correct authorization rights, all the necessary documentation. Moreover, a calendar system helps in maintaining the deadlines of procurements processes and a ticketing system helps in keeping tracks of their status and of all the related communications.

In our case, as it happen commonly, the Academic staff also access the file server and is enabled to use it to save all the data belonging to research and teaching activity.

Considering the importance of mentioned services and of the saved data, the IT staff should also implement a reliable backup system and related procedures that could ensure business continuity in the event of problems. In order to keep these IT services active internally, the Department is expected to be equipped with a server room that is powered and equipped by air conditioning through a central power grid and a central HVAC (Heating, ventilation and air conditioning) system supporting all the buildings of the campus were is located the Department. In the proposed case, an external provider is currently responsible for maintenance of these facilities and it mainly operates using the Internet connection to access the control units of such installations. The Department has also a computer lab where students are able to follow lectures, conduct exercises and/or access Internet. A dedicated network segment of the infrastructure of the Department enables desktop computer and students' laptops to access the campus network as well as Internet.

In terms of threats, it is decided to focus on the following aspects:

- Social Engineering: invoice with cryptolocker
- Denial of Service (DoS): Students in the Laboratories (voluntarily/accidentally) block access to the campus network for the whole Department, so it turns impossible to access accounting program; this event could be coordinated in case of voluntary action with some other attack initiative carried out locally
- Hacking of the Service Provider Network resulting in enabling access to infrastructure services

It is identified a set of possible alternative in terms of ICT configurations in order to check vulnerabilities and impacts, for instance between on-premises vs cloud solutions (So 2011).

5.1 Social Engineering Attacks

Social Engineering typically involve human factors; usually psychological manipulation is used to fool users or employees into handing over access privileges, confidential and/or sensitive data (Lord 2017). In facts, the social engineering techniques are often based on simple email or other kind of communication distributed over a wide number of users that devoted to cheat on them; sometime reference to general issues and urgency are used to solicit emotions in the potential victims that often react instinctively or superficially by clicking over malicious links and/or malicious files. In facts social engineering also use the weakness in the processes related to human elements (e.g. password recording or selection), in general it is evident that it is pretty challenging to defend large organizations and enterprises from these threats (Granger 2001; Evans & Wallner 2005; Goodchild 2012).

As anticipated, often social engineering attacks are based on email specifically designed to look like a communication from a contact or a reliable organization (e.g. service messages, bank communication, request for information about some public work); in case the user clicks on these malicious attachments, usually, he install, unconsciously, some malware or ransomware (Abraham et al.2010); in facts, in general these email are pretty generic and include even errors and mistakes in order to discriminate smart and aware employers from superficial ones in order to maximize the penetration capability; however sometime the emails are tailored for specific users, just to look like originated from someone inside their organization or in their contact list. In facts often for most attackers is more easy to rely on social engineering respect to work hard in vulnerabilities of the Operating Systems (O.S.): in facts this approach address temporal weakness or superficial attitude of users and does not require much lower skills and efforts as well as not need to deal with the continuous advances and upgrades of the security systems (Mitnick 2001; Pettey & Goasduff 2010). Based on some statistics it is noted that technical weakness are addressed just by a small percentageof the cyber attacks while the remaining large majority uses social engineering methods; due to these reasons it is evident that the different O.S. does not guarantee too much respect these aspects (Saini et al. 2012). A very common social engineering attack adopts the phishing (statistically around 91% of data breaches) therefore currently ransomware is beginning to turning very popular in this area. In facts, it is not possible to define a single line of defense against social engineering, but education and training are important, in facts there are also solution to address specific typologies, such as ransomware. In general a good practice is to use reliable antivirus software, to make regular backups, to update software and to make sure that email attachments are scanned (especially compressed files and all document formats that support macros); it is also useful to disable the possibility to install unnecessary browser plugins and to teach personnel to pay attention before to click. It is evident that in our case study the Social Engineering represents a fundamental layer to be simulated.

5.2 Denial of Services

DoS attacks accomplish this by flooding the target with traffic, or sending them information that causes an accident. In facts the denial of Service (DoS) is very popular and aims to block a machine, or network, making it inaccessible to its users through saturation.

These attack are usually focusing on denying the service for the legitimate users (employees, members, or account holders). DoS attack victims often are subjects used to manage web services for different organizations, private or public as well as to internal different divisions. Practically the DoS attacks block temporary the services and the server access, so in general they does not cause loss of information nor theft of sensible data, however the service deny could generate extended damages in terms of time delays and costs and could even be a vector to coordinate other cyber attacks (Peng et al. 2007; Gupta & Badve 2016).

Most popular DoS methods deals with flood and crash services. In case of flood attacks the target system receives too much traffic for a server buffer, causing it to saturate, slow down and eventually stop. Examples of flood attacks include among the others: buffer overflow attacks, ICMP Flood, SYN flood; other DoS attacks simply exploit the technical vulnerabilities that cause a system, a server or target service blocking. A specific and popular alternative type of DoS attack is defined Distributed Denial of Service (DDoS). In facts the DDoS attacks are carried out by multiple systems that conduct synchronized DoS attacks against a single target. DDoS main difference is that uses distributed resources to carry out the attack, instead of being originated by a single location. In general, the identification of attack source is pretty challenging considering that often it is carried out by a *botnet*: compromised systems that have been already corrupted and that serve as operative support for the attackers (Abu Rajab et al. 2006). Today there are several solutions devoted to defend against most traditional forms of DoS attacks, however DDoS are still one of the major threats for many organizations even if usually require strong capabilities by the attackers. Cyber offensive actions are currently very effective and limited capabilities are available for the defenders; in general it is not possible to share resources over the web being attack proof, therefore it is evident that training and experimentation allows to develop technological and procedural solutions as well as cyber defense tactics that could reduce the cyber vulnerability. Some of these methods are simple such as to install and maintain valid antivirus and keep them updated, or to install personal/centralized firewalls and configure it properly to limit outbound and inbound traffic to the desired traffic. In our case study the DoS is expected to be used at different levels: as a standalone attack by students for fun, as well as coordinated attack to block administration processes and controls.

5.3 Hacking

Hacking exploiting the gaps in the service providers network is a consolidated approach by hackers, therefore usually, these shortfalls are quickly solved directly by ISP technicians (Internet Service Providers).

Therefore the web services based on MSPs (managed services provider) introduce specific vulnerabilities considering that these subjects are often responsible for remotely accessing and managing their ICT resources and user systems of their customers; these capability relies usually on direct and privileged accesses to the customer networks; the case of recent Teamviewer hacking is a very good example (Dunn 2017). In facts, when MSPs are based on cloud or hosting solutions they hold a very large amount of data, often sensitive and/or confidential. So by targeting just a single MSP an hacker could obtain several accesses to different networks and organizations. In many cases, often the most popular methodology to conduct the attack is based on phishing emails containing executable attachments. In facts it is common for the hacker to register spoofed domains in order to send emails from them pretending to belong to reliable organizations (e.g. academic organizations, charity, etc.). In case the malicious link is clicked the attachment delivers its payload to access to target network. In general, the stolen MSP credentials usually could provide administrator or domain administrator privileges to the hackers; in addition the attackers trades and shares often accesses and credentials to move through different MSP networks and their users. Major issues to defend MSP networks and services against attackers are based on several main principia such as to avoid that users share single account credential to access the services, two factor authentication, conducting continuous security tests, adopt endpoint security approach. MSP in our case represent a potential source for obtaining credential and accesses to the services for the attackers even if it is not hypothesized to organize a specific hacking of the MSP just for planning an offensive action against the Department.

CONCLUSIONS

The SIMULACRA architecture presented in this paper is inspired by the synthetic environments developed by Simulation Team for different applications and it is very promising to create an interoperable Cyber Range open to be integrated with different models. In facts the authors are currently finalizing the *Academic Department Scenario* in order to conduct dynamic experimentations and to test the interaction of IA with both University and High School Students during the simulation. The following step is to integrate some automation system to verify the interoperability of plant control within the proposed federation of simulators.

REFERENCES

Abraham, S., & Chengalur-Smith, I. (2010) "An overview of social engineering malware: Trends, tactics, and implications", Technology in Society, 32(3), 183-196

Abu Rajab, M., Zarfoss, J., Monrose, F., & Terzis, A. (2006) “A multifaceted approach to understanding the Botnet Phenomenon”, Proc. of the 6th ACM SIGCOMM Conference on Internet Measurement, October, pp. 41-52

Adams Jr, J. A. (2015) “Cyber Blackout: When the Lights Go Out--Nation at Risk”, Friesen Press, Altona, Canada

Ali, J., & Santos, J. R. (2015) “Modeling the Ripple Effects of IT-Based Incidents on Interdependent Economic Systems” Systems Engineering, 18(2), 146-161

Barcena, M., Wueest, C. (2015) “Insecurity in the Internet of Things”, Security Response Symantec Tech Report, Mountain View, CA

Bruzzone A.G., Massei M., Longo F., Cayirci E., di Bella P., Maglione G.L., Di Matteo R. (2016) “Simulation Models for Hybrid Warfare and Population Simulation”, Proc. of NATO Symposium on Ready for the Predictable, Prepared for the Unexpected, M&S for Collective Defence in Hybrid Environments and Conflicts, Bucharest, Romania, Oct.17-21

Bruzzone A.G., Massei M., Longo F., Nicoletti L., Di Matteo R., Maglione G., Agresta M. (2015)“Intelligent Agents & Interoperable Simulation for Strategic Decision Making on Multicoalition Joint Operations”, Proc.of DHSS, Bergeggi, Sept.

Bruzzone A.G., Massei M., Tremori A., Longo F., Nicoletti L., Poggi S., Bartolucci C., Picco E., Poggio G. (2014) "MS2G: simulation as a service for data mining and crowd sourcing in vulnerability reduction", Proc. of WAMS, Istanbul, September

Bruzzone A.G., Merani D., Massei M., Tremori A., Bartolucci C., Ferrando A. (2013) “Modeling Cyber Warfare in Heterogeneous Networks for Protection of Infrastructures and Operations”, Proc.of I3M2013, Athens, Greece, September

Caliskan, E., Tatar, U., Bahsi, H., Ottis, R., Vaarandi, R. (2017) “Capability detection and evaluation metrics for cyber security lab exercises”, Proceedings of the 12th International Conference on Cyber Warfare and Security, ICCWS, pp. 407-414

Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004) “The economic impact of cyber-attacks”, Congressional Research Service Documents, CRS, Washington DC

Chakhchoukh, Y., & Ishii, H. (2015) “Coordinated cyber-attacks on the measurement function in hybrid state estimation”, IEEE Transactions on Power Systems, 30(5), 2487-2497

Cherinka, R., Prezzama, J. (2015) “A model for building a cyber security talent pipeline”, Proc. of 19th WMSCI, Vol.1

Croom-Johnson, S. (2015) “Cyber in simulation - Modelling the invisible threat”, Fall Simulation Interoperability Workshop, SIW, Orlando, August-September

Croom-Johnson, S., Couretas, J.M. (2016) “Cyber tools and standards to improve Situational Awareness”, Simulation Innovation Workshop, SIW, Orlando, September

Damodaran, S.K., Tidmarsh, D. (2016) “Model based verification of cyber range event environments”, Simulation Series, 48 (5)

Dunn J.E. (2017) "Questions linger after ISP blocks Team Viewer over fraud fears", Naked Security, Sophos, March 14

Evans, S., & Wallner, J. (2005) “Risk-based security engineering through the eyes of the adversary”, Proc. of 6th Annual IEEE SMC Information Assurance Workshop, June, pp. 158-165

Ferguson, B., Tall, A., & Olsen, D. (2014) “National cyber range overview” Proc. of IEEE Military Communications Conference (MILCOM), October, pp. 123-128

Goodchild, J. (2012) “Social engineering: The basics”, CSO Online, IDG, August 3

Granger, S. (2001) “Social engineering fundamentals, part I: hacker tactics” Security Focus, December, 18

Gupta, B. B., & Badve, O. P. (2016) “Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment”, Neural Computing and Applications, 1-28

Guri, M., Kachlon, A., Hasson, O., Kedma, G., Mirsky, Y., & Elovici, Y. (2015a) “GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies”, Proc. of USENIX Security Symposium, pp. 849-864

Guri, M., Monitz, M., Mirski, Y., & Elovici, Y. (2015b) “Bitwhisper: Covert signaling channel between air-gapped computers using thermal manipulations”, Proc. of IEEE 28th Computer Security Foundations Symposium (CSF), July, pp. 276-289

Guri, M., Solewicz, Y., Daidakulov, A., & Elovici, Y. (2016) “Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-Gapped Computers”, arXiv preprint arXiv:1606.05915

Hallaq, B., Nicholson, A., Smith, R., Maglaras, L., Janicke, H., Jones, K. (2016) “CYRAN: A hybrid cyber range for testing security on ICS/SCADA systems, Security Solutions and Applied Cryptography in Smart Grid Communications, pp. 226-241

Kisekka, V., Baham, C. (2015) “Applying cyber range concepts of operation to disaster recovery testing: A case study” SIGSAND AIS Electronic Library from Proc. of ACIS , Puerto Rico

Kundur, D., Feng, X., Liu, S., Zourntos, T., & Butler-Purry, K. L. (2010) “Towards a framework for cyber attack impact analysis of the electric smart grid”, Proc. of 1st IEEE Int.Conf on Smart Grid Communications (SmartGridComm), October, pp. 244-249

Lawless, B., Flood, J., Keane, A. (2014) “A framework to address challenges encountered when designing a cyber-range”, Proc. of European Conference on Information Warfare and Security, ECCWS, January, pp. 258-263

Lawless, B., Flood, J., Keane, A. (2015) “Analysis of the implementation of an interactive kinetic cyber range component”, Proc. of European Conference on Information Warfare and Security, ECCWS, January, pp. 389-394

Lazic, N., & Aarabi, P. (2006) “Communication over an acoustic channel using data hiding techniques”, IEEE transactions on multimedia, 8(5), 918-924

Lord N. (2017)"Social Engineering Attacks: Common Techniques & How to Prevent an Attack", Digital Guardian, August 29

Longo F., Chiurco A., Musmanno R., Nicoletti L., (2015). Operative and procedural cooperative training in marine ports, Journal of Computational Science, vol. 10, pp. 97-107.

Longo F. 2012. Supply chain security: An integrated framework for container terminal facilities. International Journal of Simulation and Process Modelling, vol. 7, no. 3, pp. 159-167.

Magrassi C. (2013) “Education and Training: Delivering Cost Effective Readiness for Tomorrow's Operations", Keynote Speech at ITEC2013, Rome, May 22-24

Mann, A., Zatti, S. (2016) "The ESA cyber security training range", Proceedings of the International Astronautical Congress, IAC.

Michael M., Abboudi H., Ker J., Khan M.S., Dasgupta P., Ahmed K. (2014). Performance of technology-driven simulators for medical students - A systematic review. Journal of Surgical Research, vol. 192, no. 2, pp. 531-543.

Miller, C. (2011) "Battery Firmware Hacking", Black Hat, Accuvant Labs Technical Report, USA, June 12

Mitnick, K. (2001) "My first RSA conference" Security Focus, April

Mo, Y., Kim, T. H. J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2012) "Cyber–Physical Security of a Smart Grid Infrastructure", Proc. of the IEEE, vol. 100 (1), 195-209

Olabelurin, A., Kallos, G., Veluru, S., Rajarajan, M. attacks (2015) "Multi-agent based framework for time-correlated alert detection of volume", Lecture Notes in Electrical Eng., 499-507

Page, J., Kaur, M., & Waters, E. (2017) "Directors' liability survey: Cyber attacks and data loss—a growing concern", Journal of Data Protection & Privacy, 1(2), 173-182

Peng, T., Leckie, C., & Ramamohanarao, K. (2007) "Survey of network-based Defense Mechanisms countering the DoS and DDoS Problems", ACM Computing Surveys (CSUR), 39(1), 3

Pettey C., Goasduff L. (2010) "Top Predictions for IT Organizations and Users", Gartner Newsroomm, November 30

Pham, C., Tang, D., Chinen, K. I., & Beuran, R. (2016) "CyRIS: a Cyber Range Instantiation System for facilitating Security Training", Proc. of the 7th ACM Symposium on Information & Communication Technology, Dec., pp. 251-258

Pridmore, L., Lardieri, P., & Hollister, R. (2010) "National Cyber Range (NCR) automated test tools: Implications and application to Network-Centric Support Tools", Proc. of IEEE Autotestcon, September, pp. 1-4

Saini, H., Rao, Y. S., & Panda, T. C. (2012) "Cyber-crimes and their impacts: A review. International", Journal of Engineering Research and Applications, 2(2), 202-9

Sgouras, K. I., Birda, A. D., & Labridis, D. P. (2014). "Cyber Attack Impact on critical Smart Grid infrastructures", Proc. of IEEE Innovative Smart Grid Technologies Conference, Feb., pp. 1-5

So, K. (2011) "Cloud computing security issues and challenges", International Journal of Computer Networks, 3(5), 247-55

Stytz, M. R., & Banks, S. B. (2012) "Information Value Assessment Modeling In Cyber Warfare Simulation", Proc. of Spring Simulation Interoperability Workshop, Orlando, 90-101

Sullivan, J. E., & Kamensky, D. (2017) "How cyber-attacks in Ukraine show the vulnerability of the US power grid", the Electricity Journal, 30(3), 30-35

Törngren, M., Grimheden, M. E., Gustafsson, J., & Birk, W. (2017) "Strategies and considerations in shaping Cyber-Physical Systems education", ACM SIGBED Review, 14(1), 53-60

Winter H. (2012) "System security assessment using a Cyber Range", 7th IET International Conference on System Safety, incorporating the Cyber Security Conference, Edinburgh, Uk, October 15-18

Wilhoit, K., & Hara, S. (2015) "The real World Evaluation of Cyber-attacks against ICS System", Proc. of the 54th IEEE Annual Conference of Society of Instrument and Control Engineers of Japan (SICE), July, pp. 977-979

Yasuda, S. (2016) "4-4 the Design and Application of a Mimetic Network Environment Construction System", Journal of the National Institute of Information & Communications Technology, 63 (2), pp. 93-101

Yasuda, S., Miura, R., Ohta, S., Takano, Y., Miyach, T. Alfons: (2017) "A mimetic network environment construction system Lecture", Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, pp. 59-69

Zhan, Z., Xu, M., & Xu, S. (2013) "Characterizing honeypot-captured cyber attacks: Statistical framework and case study", IEEE Transactions on Information Forensics and Security, 8(11), 1775-1789.

Zhou C., Wang J., Tang G., Moreland J., Fu D., Wu B., (2016). Integration of Advanced Simulation and Visualization for Manufacturing Process Optimization. JOM, vol. 68, no. 5, pp. 1363-1369.

Zolotukhin, M., Kokkonen, T., Hämäläinen, T., Siltanen, J. (2016) "Weighted fuzzy clustering for online detection of application DDoS attacks in encrypted network traffic", Lecture Notes in Computer Science including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, 9870 LNCS, pp. 326-338