The 12th International Defense and Homeland Security Simulation Workshop (DHSS), 006
19th International Multidisciplinary Modeling & Simulation Multiconference

2724-0037 © 2022 The Authors.
doi: doi.org/10.46354/i3m.2022.dhss.006

Hybrid and Cyber Threats in Towns, Critical Infrastructures and Industrial Plants

Agostino G. Bruzzone[1,2*], Marina Massei[1,2], Antonio Giovannetti[1]

[1]Simulation Team, via Magliotto2 , Savona, 17100, Italy
[2]SIM4 Future, via Trento 34, Genova, 16145, Italy

*Corresponding author. Email address: agostino.bruzzone@simulationteam.com

Abstract

The abstract proposes an innovative model to assess combined Hybrid and Cyber Threat in Towns, Critical Infrastructures and Industrial Facilities; the approach use innovative MS2G (Modeling, interoperable Simulation and Serious Game) paradigm in combination with AI to support risk assessment as well as design and reengineering of architecture and procedures to enhance resilience of complex systems.

Keywords: Cyber Security, InfoSec, Simulation, AI, Hybrid Threats, Strategic Engineering, MS2G

1. Introduction

Design of critical infrastructure is one of the best examples to illustrate advantages of interdisciplinary approach. Indeed, in such cases it is essential not only to guarantee proper operation but to ensure that it is sufficiently resistant to changes in boundary conditions and is capable to continue to operate even in case of various possible problems. Furthermore, apart from accidents and natural disasters, it is necessary to guarantee also sufficient protection against hostile actions (Bruzzone et al., 2016). Indeed, critical infrastructures as well as Industrial Plants, such as seaports, were one of most attractive targets in hostilities since millennia; often these elements are bordering Town further reinforcing the strategic importance to protect them and to avoid vulnerabilities that could promote domino effect; this requires to create resilience that it is often based on use of innovative models and approaches. indeed, in the past these aspects were mostly related to physical interference and required such measures as control of access of personnel and vehicles, nowadays it is more common to be subjected to various kinds of cyber-threats (Bruzzone et al., 2015). Since a decade it is always more common to see cyber-attacks which lead to disruption in various services. In particular, since the beginning of Ukraine crisis the country was subjected to blackouts caused by cyber-attacks (Sullivan 2017). In last years, there have been many cases of attacks on IT (Information Technologies) platforms of the infrastructures. Among numerous notable cases, it is possible to highlight Stuxnet virus, which, in its variations, was used against nuclear program of Iran as well as other SCADA-governed (Supervisory Control And Data Acquisition) facilities (Karnouskos, 2011). Other more common cases are related to utilization of crypto-lockers to take in "hostage" target IT platform and unlock it only if ransom is paid. Furthermore, different coordinated cyber-attacks were organized recently against power grids in order to cause blackouts. Another important factor is that nowadays, cyber-attacks became also actively used in political, military and economical conflicts.

Indeed, in case of this kind of aggression it could be very difficult to identify the attacker, even harder to acquire sufficient evidence in order to proceed with legal actions. Considering this, attacks on IT platform became one of most common tools of so-called Hybrid warfare, in which it is often desirable to cause damage while hiding real identity (Bruzzone & Di Bella, 2018).

In order to analyze better what and how must be protected, it is essential first to understand better the nature of attacks. Obviously, from point of view of the attacker, this kind of actions leads to best results when causes as much of troubles to the adversary for as long time as possible. Considering this, ideal target must affect as many persons as possible and be easy to damage and/or difficult and expensive to repair. Considering that in case of cyber threats it is extremely difficult to cause physical damage, it is much more common to disrupt services and block operation of certain infrastructures or plants, whenever is possible. Obviously, among most attractive targets it is easy to imagine power grids, transportation networks, critical infrastructures, industrial plants, etc.

Another important consideration is related to the sequence of operations required to achieve the desired for attacker results. For example, it is practically impossible to brute-force properly done passwords, hence, other techniques are usually used (Ferguson et al., 2011).

In particular, previously mentioned Stuxnet virus is believed to be deployed in the target system by means of infected USB drive. Hence, someone was tricked in trying an unknown device using computer belonging to a protected network.

Indeed, it is much more common to start such attacks using social engineering, rather than blindly trying all possible attack vectors, which would also cause undesired attention from the potential victim. Another approach is based on utilization of unknown or not-yet-patched vulnerabilities, as was used with SolarWinds IT management platform, known to be one of biggest and massive series of cyber-attacks as of 2022; fortunately, attacks of this scale are very rare (Willett, 2021).

However, lower scale attacks on typically vulnerable IoT (Internet of Things) devices are much more common; indeed, this kind of equipment is systematically rarely updated, while numerous devices keep default combination of login and password for authentication, which make them almost completely exposed to anyone (Barcena & Wueest 2015).

Considering this, it is more probable that an intrusion would start with infection of a single device connected to the target network, either because of vulnerability, open access or human error.

Considering this, it is possible to develop a case study related to analysis, prevention and remediation of cyber-attacks, taking seaports as example. In addition, the cyber layer is strongly related to communications and socials that nowadays are related to STRATCOM and Media Attacks that are another critical aspect in relation to modern Hybrid Threats.

2. Scenario Definition

At this point it is possible to identify a scenario, effective in improvement of handling of cyber-threats. In particular, it should have following principal characteristics:

- Address critical infrastructure.
- Include realistic representation of relative IT infrastructure.
- Have possibility to reproduce various hypothetical threats and tactics.
- Be capable to employ different countermeasures.
- Address mutual influence of events occurring in real world and in cyber-space.

Considering this, possible advantages of utilization of simulation are evident. Indeed, it would allow to test various combinations of attack and defense techniques, hence, to improve efficiency of protection as well as to provide to relative authorities a better vision of possible scenarios. Furthermore, properly developed model would be relatively easy to adapt to other situations.

3. State of the art

In the past there were developed several models capable to address highlighted issues. In particular, T-Rex simulator is focused on analysis of combined attacks on physical and IT infrastructures of the target; indeed, it simulates diffusion of a virus capable to potentially disrupt operation of physical defense of a seaport, while contemporary a UAV (Unmanned Airborne Vehicle) attack is deployed to physically damage the target (Bruzzone et al., 2013; 2018). One of interesting aspects of this simulation is that the very similar situation occurred in attack on Aramco oil processing plant. Despite this consideration, T-Rex model required redesign according to recently discovered threats, vectors of attacks and real-life examples. In some cases, it is used a simulation of computer networks, created ad-hoc to study processes related to cyber-security, however, these models are less connected to the "physical" world as would be preferable for more detailed evaluation (Bruzzone et al., 2017). Indeed, T-Rex represents a very good example of MS2G paradigm use that is suggested also in this case to reinforce interoperability within an immersive intuitive environment.

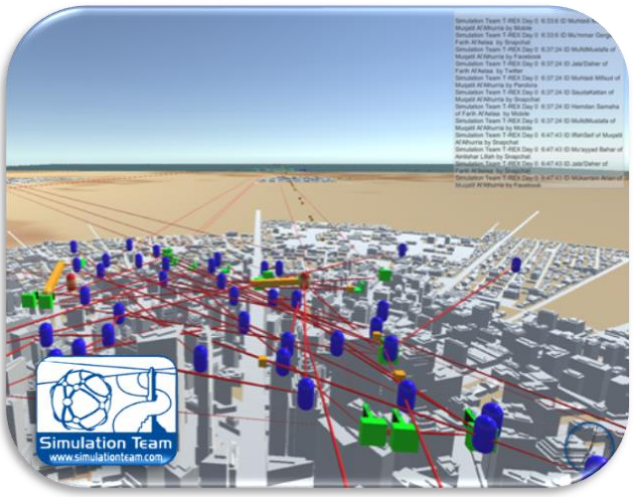

Figure 1. T-Rex simulation of cyber-physical assets Nowadays the Hybrid Threats together with Cyber represent a major risk for complex systems that impact on multiple layers; the impact on population should be obviously consider crucial as well as their beliefs and consensus, considering that compromising services and diffusing fake news promote mistrust and fear, potentially at very high levels able to lead to major emotional crisis on economic and political aspects as well as up to civil disorders. A screenshot of T-Rex with relative representation of a city in combined cyber-physical way is present on the figure 1.

4. The Proposed Model

The developed simulator handles the proposed scenario using 2 level model: it includes a real world representation of a seaport as well as corresponding virtual counterpart. In particular, the real world level represents activities, common for a container terminal of a seaport: loading and unloading of ships, handling of containers on yard, including dangerous goods, loading and unloading of trucks, movements of personnel and of the equipment etc. Vice versa, the cyber-space reflects configuration and behavior of relative IT infrastructure. For example, it handles different kinds of connection, such as LAN (Local Area Network) and WLAN (Wireless LAN), includes dynamic connection and re-configuration of network, based on availability of wireless base stations (WiFi, Mobile, Long-Range wireless), handling of access policies, tweaking of protection level of network nodes, modeling of the data exchange etc. Hence, the network is conveniently modeled as mathematical graph (Van Steen, 2010).

At the same time, the model omits purely theoretical attacks and data breaches, such as extraction of data from air-gapped systems by using speakers, cooling fan rotation speed, signals from memory data buses etc (Guri et al. 2015).

Figure 2. Data exchange representation in the simulator Is overlapped with the physical world

Visual representation of the data exchange in the simulation Is present in the figure 2, with highlight in traffic and band saturation as well as on the status of the cyber physical elements present within the scenario that could be attacked and/or compromised.

In the simulation, it is possible to assign to any realistic asset of simulated seaport its virtual counterpart, as well as to add completely new virtual entities. For example, it is possible to attach to a crane respective communication and telemetry modules operating in LoRa (Long-Range radio) connection, mobile terminals of yard operators connected through WIFi, create routers (including wireless ones) and signal repeaters, introduce servers, workstations and backup units. Once started, the model automatically identifies suitable network configuration based on types of devices, hence, connects them in a network. During scenario evolution, the WiFi and mobile network devices could switch between different base stations. Apart from normal configuration, the model handles also improper from point of view of InfoSec yet realistic scenarios; for example, a workstation could be connected simultaneously to the protected network and, to a mobile network, e.g. when an employee connects his or her smartphone to the computer, for instance simply to charge it but activating tethering of the connection. The complete visual representation of cyber-physical simulation is shown in the figure 3. In particular, In the Illustration It Is possible to see how different cranes, machines workstations, smartphones, network equipment and even cellular base station have their virtual counterpart.

The user is enabled to configure levels of protection of the infrastructure, for example, to enable or disable access control to the protected network, tune level of antivirus & firewall protection etc. Similarly, it is possible to define how advanced is the attacker, which would influence probability to breach certain components of the protected network. The model is focused mostly on diffusion of a virus in the network, hence, during the run it evaluates possibilities related to infection of new assets as well as chances to detect the intrusion and counteract.

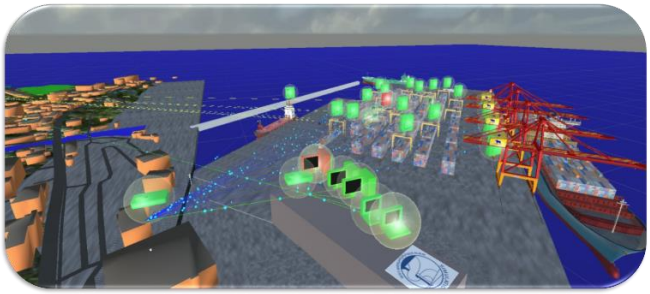

Figure 3. Cyber-physical view of a seaport

Similarly, the next figure shows presence of an Infected device in the simulated network. In particular, it was compromised an on-board computer of one of port machines. Consequently, based on boundary conditions, it is possible that the attack will proceed affecting other machines and nodes or that It could be Identified and Isolated. In any case, the simulation allows evaluation of both scenarios, as well as some intermediate possibilities.

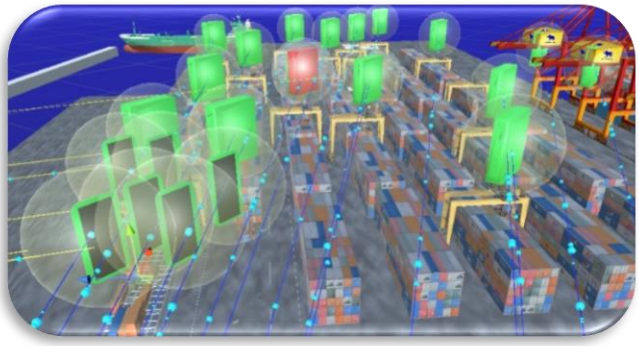

Figure 4. Infected device

While being developed for the seaport scenario, the model of IT infrastructure is completely independent from it and could be used in other simulations. In particular, the scenario of interest is implemented in Unity engine, hence, the model could be adapted to operate in various possible simulated scenarios.

5. Results

The proposed model was applied to a previously developed virtual port environment and allowed preliminary assessment of risks related to cyber-protection. While the model is still in validation phase, it already allowed to improve awareness of decision makers operating in the field of interest. Furthermore, the authors testing application of development software solution to other simulators, such as supply chain models (Bruzzone et al., 2011) or air transportation (Piera, 2014). Particularly interesting would be utilization of the model with simulation based on intelligent agents (Bruzzone et al., 2009). Finally, considering always more complex situation including provocations and cyber-attacks, the framework could be helpful in order to protect towns, critical infrastructures and industrial plants from possible interferences from government-backed hacker groups and organizations and especially from combined cyber-physical threats (Mazal et al., 2019).

Proposed case study illustrates also a good example of necessity of application of strategic engineering approach to model complex systems and systems of systems (Bruzzone et al., 2021; 2022).

6. Conclusions

This paper introduces the potential of using modern MS2G paradigm and Strategic Engineering in application to address Hybrid and Cyber Threats. The protection of Town, Critical Infrastructure and Industrial Plants nowadays is strongly related to cyber-security and Hybrid vulnerabilities and relative ICT infrastructure with special attention to the consequence on the operational and physical layers. Considering this, the authors proposed a model, capable for reconstruction of typical network configurations and of simulation of different cyber-threats. The model could be embedded in other simulation-based solutions and could allow extension of their functionality in order to cover aspects related to modern threats.

References

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

Bruzzone, A., Tremori, A., & Massei, M. (2009). Serious games for training and education on defense against terrorism. GENOA UNIV (ITALY).

Bruzzone, A., Fadda, P., Fancello, G., Massei, M., Bocca, E., Tremori, A. & D'Errico, G. (2011). Logistics node simulator as an enabler for supply chain development: innovative portainer simulator as the assessment tool for human factors in port cranes. Simulation, 87(10), 857-874.

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. Proceedings of I3M2013, Athens, Greece.

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 DHSS2015, Bergeggi, Italy, September.

Bruzzone, A. G., Massei, M., Maglione, G. L., Di Matteo, R. & Franzinetti, G. (2016). Simulation of manned & autonomous systems for critical infrastructure protection. Proceedings of I3 M, Larnaca, Cyprus.

Bruzzone, A.G., Di Matteo, R., Massei, M., Russo, E. & Maglione G.L. (2017). Interoperable Simulation and Serious Games for creating an Open Cyber Range. In Proceedings of 18th conference DHSS.

Bruzzone, A., Massei, M., Longo, F. & Di Matteo, R. (2018). Learning decision making processes at strategic level based on VR & augmented reality. In Proceedings of Workshop on Applied Modelling & Simulation (p. 56).

Bruzzone, A. G. & Di Bella, P. (2018). Tempus Fugit: Time as the main parameter for the Strategic Engineering of MOOTW. Proceedings of WAMS.

Bruzzone, A. G., Massei, M., Sinelshchikov, K., Giovannetti, A., & Gadupuri, B. K. (2021). Strategic Engineering Applied to Complex Systems within Marine Environment. In *2021 Annual Modeling and Simulation Conference (ANNSIM)* (pp. 1-10). IEEE.

Bruzzone, A. G., Massei, M., & Frosolini, M. (2022). Redesign of Supply Chain in Fashion Industry based on Strategic Engineering. Procedia Computer Science, 200, 1913-1918.

Ferguson, N., Schneier, B. & Kohno, T. (2011). Cryptography engineering: design principles and practical applications. John Wiley & Sons.

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

Karnouskos, S. (2011). Stuxnet worm impact on industrial cyber-physical system security. In IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society (pp. 4490-4494). IEEE.

Mazal, J., Bruzzone, A., Turi, M., Biagini, M., Corona, F., & Jones, J. (2019). NATO use of modelling and simulation to evolve autonomous systems. Complexity Challenges in Cyber Physical Systems: Using Modeling and Simulation (M&S) to Support Intelligence, Adaptation and Autonomy, 53-80.

Piera, M. A., Ramos, J. J., Moreno, R. & Narciso, M. (2014). Causal simulation models for facing third millennium air transport sustainability. Simulation, 90(2), 162-170.

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

Van Steen, M. (2010). Graph theory and complex networks. An introduction, 144.

Willett, M. (2021). Lessons of the SolarWinds hack. Survival, 63(2), 7-26.