2019 11th International Conference on Cyber Conflict:
Silent Battle
T. Minárik, S. Alatalu, S. Biondi,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2019 © NATO CCD COE Publications, Tallinn

Cyber-Physical Battlefield Platform for Large-Scale Cybersecurity Exercises

Joonsoo Kim
Senior Researcher
National Security Research Institute
Daejeon, South Korea
joonsoo@nsr.re.kr

Kyeongho Kim
Senior Researcher
National Security Research Institute
Daejeon, South Korea
lovekgh@nsr.re.kr

Moonsu Jang
Senior Researcher
National Security Research Institute
Daejeon, South Korea
moonsujang@nsr.re.kr

Abstract: In this study, we propose a platform upon which a cyber security exercise environment can be built efficiently for national critical infrastructure protection, i.e. a cyber-physical battlefield (CPB), to simulate actual ICS/SCADA systems in operation. Among various design considerations, this paper mainly discusses scalability, mobility, reality, extensibility, consideration of the domain or vendor specificities, and the visualization of physical facilities and their damage as caused by cyber attacks. The main purpose of the study was to develop a platform that can maximize the coverage that encompasses such design considerations. We discuss the construction of the platform through the final design choices.

The features of the platform that we attempt to achieve are closely related to the target cyber exercise format. Design choices were made considering the construction of a realistic ICS/SCADA exercise environment that meets the goals and matches the characteristics of the Cyber Conflict Exercise (CCE), an annual national exercise organized by the National Security Research Institute (NSR) of South Korea. CCE is a real-time attack-defense battlefield drill between 10 red teams who try to penetrate a multi-level organization network and 16 blue teams who try to defend the network. The exercise platform provides scalability and a significant degree of freedom in the

design of a very large-scale CCE environment. It also allowed us to fuse techniques such as 3D-printing and augmented reality (AR) to achieve the exercise goals.

This CPB platform can also be utilized in various ways for different types of cybersecurity exercise. The successful application of this platform in Locked Shields 2018 (LS18) is strong evidence of this; it showed the great potential of this platform to integrate high-level strategic or operational exercises effectively with low-level technical exercises. This paper also discusses several possible improvements of the platform which could be made for better integration, as well as various exercise environments that can be constructed given the scalability and extensibility of the platform.

Keywords: *cyber exercise, cyber conflict, cyber-physical systems, ICS/SCADA testbed*

1. NEED FOR A CYBER-PHYSICAL BATTLEFIELD (CPB) IN LARGE-SCALE CYBER EXERCISES

The purpose of a national cyber security exercise is to assess the national readiness with regard to cyber threats and to enhance the cyber defense capability of national cyber warriors. In cyberspace, there is no clear boundary to determine who will fight together for national security. Recent national cyber exercises currently attempt to invite as many entities as possible to participate regardless of whether they are private companies, public institutions, national critical infrastructure operators, or from the military or academia. To handle a national cyber crisis effectively, it is critical to prepare all potential players within the country so that they can become involved and effectively perform their expected roles whenever necessary. International cooperation with allied countries or international organizations also becomes more important. The capacity of national cyber security involves readiness for well-ordered cooperation or coordination between all possible cyber stakeholders. This is one of the reasons why increasing numbers of large-scale cyber exercises to cover national and international cooperation have tended to be introduced recently.

Recent cyber exercises have also attempted to integrate their technical hands-on exercises with high-level operational or strategic table-top exercises. The omnipotence of the advanced ICT technologies also defines the unlimited power of malicious cyber attacks. However, to ground the exercise scenario in reality and to keep the exercise participants immersed without questioning the authenticity of the scenario, scenario

injects[1] for operational or strategic table-top exercises should be connected to technical scenarios. This also provides an opportunity to test one of the most important cyber crisis management capabilities: cyber crisis communication to support rapid and accurate decision-making. To assess the current situation of cyber security exercises accurately, reporting to high-level decision-makers with the correct, often non-technical, terms and with succinct but sufficient information is crucial. Therefore, providing interesting and realistic scenarios to trigger the need for technical players to report to high-level table-top players is constantly being emphasized during efforts to prepare national and international cybersecurity exercises.

Not all cyber attacks should be reported to the high-level officials' table, requesting their timely decisions. What determines the need to report is the damage that the cyber attacks cause or will soon cause to organizations, a nation or to the international community. Therefore, another trend in current cyber security exercises is that they expend much more effort on exercising scenarios in which critical infrastructure must be protected. Damage to critical infrastructure through cyber-based attacks can have a significant impact on national security and on the economy and citizens' livelihoods and safety [2]–[4]. It is, therefore, important to develop a comprehensive national strategy to deal with cyber security issues. This effort should be followed by constantly testing and improving the strategy in national exercises on CPBs simulated around national critical infrastructure installations.

When developing national cyber crisis exercise scenarios, many different factors are considered, such as the objectives, participants, and target capabilities of the exercise, among others. Moreover, one of the most interesting questions when preparing national exercises at present centers on what national critical infrastructure sectors should be chosen to be simulated as a CPB for the exercise. One determining factor is how significant the physical harm to individuals or properties may be if and when the sector is compromised by cyber attacks. Efforts to answer this question can create a sense of alertness within the national cyber community and an incentive to develop true national response capabilities against future cyber threats. A system of cooperation will be established.

Therefore, constructing a realistic CPB for large-scale national or international exercises has become a critical goal. This provides a magnifying glass for exercise participants to focus on certain sectors of national critical infrastructure and to assess our preparedness, as a nation or along with our international allies. The exercise should be able to visualize the most devastating effect of cyber threats on our critical infrastructure based on realistic, but somewhat worst-case, scenarios. It can provide an opportunity to examine how well we are prepared to battle the future threats of

1 *Injects* are defined as events, typically planned through entries on the Master Scenario Events List, that controllers must simulate, including directives, instructions, and decisions [1]. Exercise controllers provide injects to exercise players to drive exercise play towards the achievement of objectives. Injects can be written, oral, televised, and/or transmitted via any means (e.g., fax, phone, email, voice, radio, or sign).

cyber attacks on our critical infrastructure. We claim that these tools are fundamental to prepare for such battles in cyberspace.

2. TOWARDS A UNIVERSAL EXERCISE PLATFORM FOR CONSTRUCTING A CPB

Good exercise scenarios should provide decision challenges based on a wide spectrum of scope, duration, and the intensity of the cyber operation consequences. Therefore, exercise preparation groups can leverage a widely known tool developed to make use-of-force assessments [5]–[9]. Known as a Schmitt analysis, it introduces different factors that can be used in the assessment of whether cyber operations violate the prohibition of the use of force; such as severity, immediacy, directness, invasiveness, the measurability of the effects and military characteristics, among others.[2] The most important scenario to cover is when national critical infrastructure is targeted by cyber operations in a manner that may have a severe impact on a State's security, economy, public health, or environment [5].

To experiment with the various criteria of a Schmitt analysis, a versatile CPB exercise environment should be developed. For example, it should be able to visualize the *severity* of physical consequences that can cause great harm to the nation and society. Different types of consequences should be representable. Regarding *immediacy*, given that the timeline of the exercise scenarios may not precisely match the actual exercise time, the time for which to visualize consequences should be controllable based on the exercise progress or the exercise scenario. If technical exercises are integrated with operational or strategic exercises, the process can be *directed* to visualize the consequences and to issue high-level table-top scenarios only when a red team (RT) successfully compromises the blue team (BT)'s network. By designing cyber systems as isolated and highly secured, or military-related, we would also like to consider the *invasiveness* or *military character* factors.

Hence, the technical means of constructing a CPB should be established. Doing so is challenging, because many requirements to support the developed technical and table-top exercise scenarios must be met. One way to tackle this problem is to run the design from scratch. This is the usual means of developing ICS/SCADA testbeds for academic research, for security validation, or for training and exercises [10]–[19]. One main problem with this approach is reusability. For every new critical infrastructure sector introduced, the entire cycle of the CPB development should be iterated with

2 It is desirable to develop exercise scenarios in which each criterion of the Schmitt analysis can be configured as an adjustable parameter and its variation can be maximized, considering the unsettled nature of the "use-of-force" or "armed attack" threshold. In an ideal situation, this tool can work as a framework in determining the next critical infrastructure target to build as a CPB. In many cases in reality, however, after a CPB is constructed based on its technical or practical availability, exercise scenarios will be developed accordingly.

nearly the same amount of resources used in the previous cycle. Another problem is that conventional testbeds are mostly developed for academic research or for the training of field experts. In many cases, they are not suitable for general cybersecurity exercises and can be leveraged only for very limited purposes, due to their lack of scalability or flexibility.

There are increasing cases of critical infrastructure simulations specifically designed for hands-on or live-fire exercises [20]–[28]. They have many different features, but they also seem to share the common philosophy of realistically emulating the actual field environment and emphasizing the visualization of the physical world as controlled by digital systems in cyberspace and the damaging effects of cyber attacks.

However, it appears that their focus has been on constructing offline cyber ranges. Even when they were intended to provide online exercises, their exercise environments were developed while assuming that the participants would connect to the cyber range network remotely, usually through a virtual private network (VPN) [21], [25]. In such a case, the scalability issue of providing the same environment to each participant is resolved by time-dividing the online access to the system and sharing the environment within the same participant group. A miniaturized diorama city composed of different cyber-physical elements, such as power stations, traffic lights, a water treatment system, military sites, and other elements is developed. The city is controlled and supervised by a realistic ICS/SCADA system and the developers incorporate interesting ideas and technologies to visualize CPBs more realistically.

These cyber ranges, however, are not designed with a view to the reproduction of the same environment to provide a separate environment simultaneously to different BT participants. The scalability issue remains in this sense when targeting large-scale exercises to provide each BT with a separate defense mission on their cyber-physical battleground.

Moreover, cyber ranges are not mobile. When cyber ranges may not be able to accommodate all exercise participants, they can only be experienced through remote video cameras.

Another important issue is extensibility. Exercise coverage is becoming more widespread, and the affiliations to which the training participants belong are becoming more diverse. There is also a growing demand for an exercise environment to cover various areas. Custom designs have limitations. It is necessary to develop a general cyber exercise platform that fosters continuous innovation with integrated knowledge and with accumulated CPB design management experience.

The exercise platform used in this paper refers to a set of technical means for establishing an exercise environment for technical hands-on and table-top exercises to simulate various types of critical infrastructure. The platform should be developed to visualize provocations and responses on the CPBs. It is designed to utilize various technical elements to express the physical properties of cyber-physical systems and the damage that may be caused by a cyber attack on them.

The platform should be capable of extensibility to represent different elements of critical infrastructure on the same platform and to enable the inter-domain integration of different infrastructure sectors seamlessly. In other words, we aim to establish a virtuous process cycle to perform system development on new areas and integrate them while reusing or improving existing systems. Thus, we sought to develop a 'platform' that could gradually encompass all areas of the infrastructure that should be considered to assess and strengthen national cybersecurity capabilities on an ongoing basis.

3. PLATFORM DESIGN CONSIDERATIONS

In this chapter, we describe the design considerations when developing a CPB for the large-scale national or international cybersecurity exercises.

A. Target Exercises

We had two main target exercises, the Cyber Conflict Exercise (CCE)[29] and Locked Shields (LS)[30], [31]. The main development phase lasted approximately one year, from March of 2017 (CCE 2017 planning phase) to March of 2018 (before the LS18 test-run).

1) CCE 2017

Since November of 2017, CCE has been held as an annual national live-fire attack-defense exercise, organized by the National Security Research Institute (NSR) of South Korea. CCE is a real-time battlefield drill between 10 RTs who try to penetrate a multi-level organization network on a virtualized platform and 16 BTs who try to defend the network. The maximum number of people per team is limited to five, and all participants gather at an offline venue for this event. CCE can attract the interest of young national cyber security talents or experienced pen-testers to join the RT and to practice their knowledge and skills. BT participants have included many cyber security specialists working in different public sector areas, including those in the military, government, or who work with critical infrastructure, as well as those from the major private industries, including ISPs, banks, major game companies, and other

sectors. Online preliminary competition rounds for RTs and BTs are held one month before the final exercise execution to select finalists from all the applicants.

Each BT is presented with a realistic virtualized network composed of four different zones, in this case a DMZ, an internet-connectable work zone, an intranet zone, and an ICS/SCADA zone. As usual, vulnerabilities and misconfigurations have been pre-built into this game network. Each RT should engage in step-by-step intrusion activities to access this hierarchically constructed network, pivoting through compromised machines. The ICS/SCADA Zone has served as the core element of the exercise network. It is the main cyber-physical battlefield and the final destination of the RTs. There will be significant damage if RTs succeed in penetrating this layer and committing a successful cyber attack.

One of the main exercise objectives was to provide interesting challenges which demonstrate realistic cyber incident challenges in the realistically complex full-network environment for each BT. Therefore, the highest priority is to build a realistic ICS/SCADA zone with a realistic implementation of all of the core elements included.

We also wanted to provide the participants with a dramatic visualization of their defense target, our CPB or our society, and the consequences of failures to defend these targets. Though CCE is still a highly technical live-fire attack-defense exercise, some 'soft' skills are also tested through some injects to request accurate, succinct and prompt situational reports to be sent to decision-makers and to provide sensitive and time-critical media interview questions. Here, visualization will serve a critical function by providing situational awareness on the progress of the exercise overall. This will also help high-level decision-makers who are observing the exercise to raise their cyber security awareness.

2) LS18

Locked Shields is the world's largest and most advanced international technical live-fire cyber defense exercise, as described by the NATO-affiliated Cooperative Cyber Defence Centre of Excellence (CCDCOE), which has run it since 2010 in Tallinn, Estonia. During the design of this platform, cooperation between NSR and CCDCOE for LS18 was underway.

Because the goal of LS is to offer a full-stack exercise that integrates LS technical hands-on exercises with operational or strategic/policy/media table-top exercises, there has been a long-standing desire to experiment with various scenarios covering more critical infrastructure sectors. However, another important principle of the LS team is that the technical game and the table-top exercise must constantly be integrated. Therefore, exercise scenarios could be introduced only when the technical

implementation of a new CPB is possible and the scalability issues are resolved. Therefore, our platform should have very flexible options to adapt based on changing LS demands, and it must have distinct features for specializing in large-scale cyber exercises.

B. Scalability

Originally, CCE 2017 targeted 20 BTs. For LS, the number of participating BTs has been growing rapidly, such that LS18 was expected to host more than 20 BTs. Our objective was to provide an identical and complete ICS/SCADA zone for each participating team. This means that we need to develop up to 30 sets, considering the backups and demos for the observers.

However, the costs of the specialized hardware elements, such as PLC (programmable logic controllers), actuators, and other electronic and physical devices, as well as software elements, such as an HMI (human-machine interface), historian DB, PMS (patch management system), are very high and open-source alternatives may not be available. Building scalable systems for large-scale national or international exercises was the most important goal of the project, and this goal needed to be considered in all of the design considerations listed below.

C. Mobility and Ease of Deployment

In most cases, mobility and ease of deployment are essential when considering a situation in which work cannot always be done because a venue is rented and a remote exercise site must be constructed within a limited time immediately before the event. The goals are to design and construct an environment that minimizes unnecessary annoyances which arise when moving the platform, to ensure ease of moving the platform, to establish a remote exercise site, and to establish a connection with the main server hosting the virtualized exercise network.

D. Reality or Similarity to the Field Environment

It is fairly odd to emphasize this because it is the most important consideration when building a critical infrastructure simulation system and must always be considered. Ironically, in reality, most of the ICS/SCADA simulation systems tend to be criticized for not being realistic, for many different reasons. This may be unavoidable unless the original systems and network are identically copied. For security reasons, it is often not possible or even desirable to have a complete copy of an actual operating network. Performing cyber attack-defense exercises on actual networks has many risk factors.

The basic principles for developing this platform are as follows. First, we conduct on-site visits to understand the actual network, security threats, and actual working environment of each field and design the exercise environment after consistent and

in-depth discussions with operational experts and cyber security experts in each field. Second, the key to reality concerning the exercise goals is whether the cyber crisis scenarios offered during the exercise are based on real-life cases or highly probable future threats. To maximize the exercise effect given to the BT and to ensure the immersive participation of all on this team, we strive not to compromise practicality, completeness or complexity with the technical implementation of the essential elements of the scenario.

E. Extensibility, Flexibility, and Reusability

When selecting the target critical infrastructure sector to represent the damage situation of major national infrastructure elements caused by a cyber attack, it is necessary to consider the following factors comprehensively: the exercise objective; the exercise participants; the accessibility of the technical information of the sector; the extent of the effect of damage; recent actual cyber accident cases; the cost of system and software development; LS strategy game scenario concerns; interdependency between critical infrastructure sectors; and other related factors. The coverage of the target sectors should be gradually expandable based on these criteria.

One of the most important effects of the platform is the accumulation of knowledge. Providing a shared framework of thinking that facilitates continuous innovation and improvement should be a key function of the platform. When we develop one critical infrastructure simulation system from scratch, the result will be very different from another, depending on the design choices, i.e. the system size, the implementation scope or level, the visualization concept of the simulated physical world, among other considerations. This heterogeneous collection of knowledge cannot be combined naturally. It is not cumulative. Therefore, it is necessary to develop a universal cyber exercise platform that will foster continuous innovation by providing a well-established framework when developing exercise scenarios, creating technical measures when developing new CPB designs that will enable a rich set of challenging and interesting exercise scenarios and integrating them with the existing exercise environment seamlessly.

F. Domain-Independency and Vendor-Independency

There are various types of ICS communication protocols [32], [33]. Depending on the practices or main suppliers in each sector, organization or site, the operating communication protocols differ. The characteristics of the communication subjects, organizations, sites, and the construction completion year can all make a difference as well. It is not uncommon for decades-old legacy systems to continue to operate with multiple security vulnerabilities and without major software or security updates. Depending on the vendor or contractor, the system architecture can also differ greatly.

Many major vendors often use their proprietary communication protocols instead of standard open-source protocols.

The point is that supporting all possible implementation scenarios is not possible. The platform was designed to support as many protocols as possible under the given set-up. PLC models were chosen considering the ease of recreating various cybersecurity threat scenarios. For example, to reproduce many types of cyber attack, PLC models that support multiple protocols which are compatible with Internet protocols are considered, such as Modbus TCP, CIP Ethernet/IP, Profinet, OPC, or ICCP. The platform is designed to support two or more PLC models so as not to be dependent on specific vendors. If a new protocol requirement arises, certain elements such as PLCs, SWs or APIs should be replaceable with existing ones to support them. The platform should enable a modular design in this sense.

G. Visualization

The goal was to develop a platform with a visualization layer that represents physical facilities and the damage caused by cyber attacks. As noted above, this is one of the main differences between the exercise platform and typical ICS/SCADA testbeds. Considering scalability, extensibility, and reality, it was determined early on that 3D-printing technology would be used to design and produce the diorama city in a more cost-effective and modular approach. This platform can best utilize the advantages of small-volume production of various designs of 3D printing.

The established design principles are as follows. In the center of the visualization layer, symbolic structures that represent each critical infrastructure sector are located. The surrounding area, which includes the residential, commercial and/or industrial districts, represents the physical world we live in and will show the spreading damage when needed. City districts should be designed to connect and expand with adjacent districts.

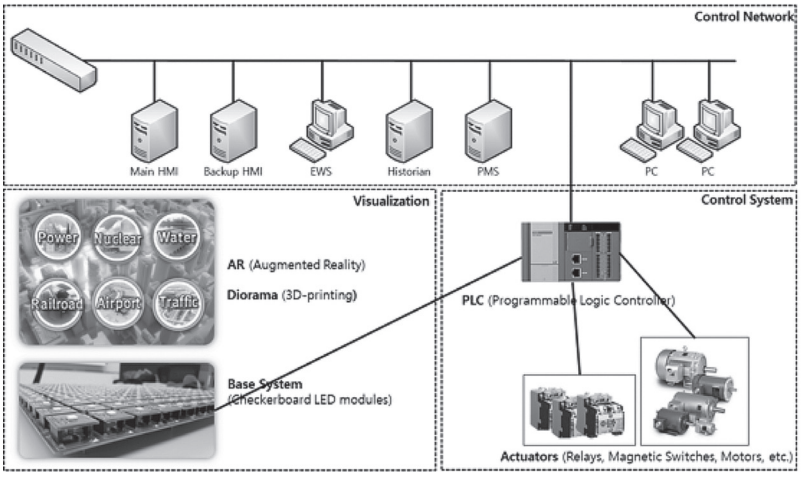
There should also be a way to provide situational awareness on top of the created cyber-physical world. At the very least, there should be a technical means of representing the normal state and the level of the damage caused by a massive cyber attack. Though there is a vast range of options from which to choose, scalability and extensibility are the top priorities. In relation to this, a basic system that uses different colors of RGB (tri-color) LED (light-emitting diode) lights is introduced first, while more dramatic and physical representation techniques could be used. It is simple but effective, with little risk of physical failure. We also devised a method to utilize AR (augmented reality) visualization technology in the 3D-printed diorama city to maximize this effect.

4. ARCHITECTURE OF THE EXERCISE PLATFORM

Based on the design considerations discussed in the previous chapter, we created the basic architecture of the exercise platform, developed a prototype, validated it, produced a modified version by fixing its faults, and used it for two major target exercises, CCE 2017 and LS18. It satisfied most of the considerations in the original design phase and contributed greatly to the success of the exercises. The platform is a system with scalability and extensibility, which were most important, and has thus far shown remarkably different concepts and possibilities compared to those of existing systems. Its visualization showed great potential and it received numerous favorable reviews, along with some criticism, as might be expected.

The platform consists of three main components: a visualization layer, a control system layer, and a control network layer, as shown in Figure 1. The visualization layer allows the LED modules to be placed by default on the base system in a 15x15 checkerboard pattern. A four-layer PCB (printed circuit board) was designed to control a total of 255 (LED or other digital) modules. On top of this, the 3D-printed diorama is positioned, and LEDs are used to represent a normal state and an abnormal state in different color schemes. As an option, AR technology was used to express this effect more vividly.

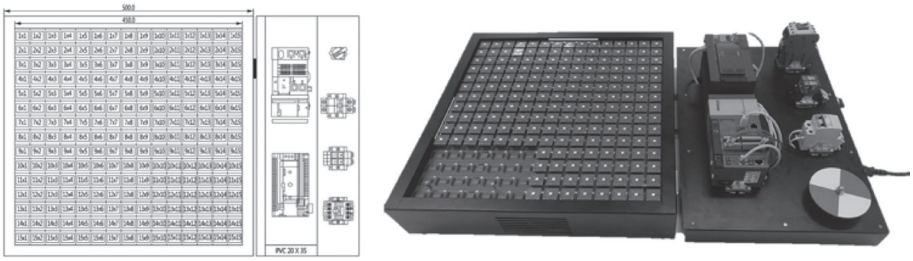
FIGURE 1. THREE MAIN COMPONENTS OF THE EXERCISE PLATFORM



To design the control system layer, six critical infrastructure sectors (a power grid, a nuclear power plant, a water purification plant, railroad control, airport control, and traffic light control) were selected and implemented among the major national critical information infrastructure sectors designated by the Korean government. After an in-

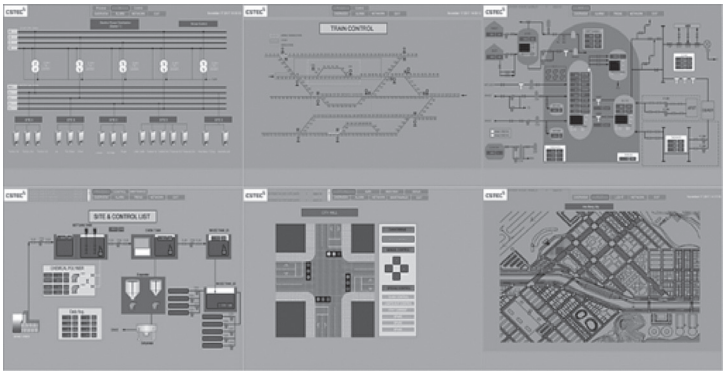
depth analysis of the control networks of each field, we derived common elements to be the focus of the development. Two PLC models from two different PLC vendors (one from a local Korean vendor and the other from a European global vendor, considering the geographic locations at which the target exercises take place) were chosen to meet several requirements, such as supported network protocols, power supply voltage, device size, usability in the actual field, and budget limitations, among others. In order to add reality by performing the actual physical operations, some typical actuators, such as a mechanical relay, a magnetic switch, and a motor with a turning plate, were connected to and controlled by the PLCs, making physical sound or moving effects. There is one master switch with which to select the operating PLC. The visualization layer unit and the control system layer unit are designed so that they can be connected and separated easily and stably through the D-sub connector for power supply and communication (see Figure 2).

FIGURE 2. DIAGRAM AND IMPLEMENTATION OF THE VISUALIZATION LAYER AND CONTROL SYSTEM LAYER



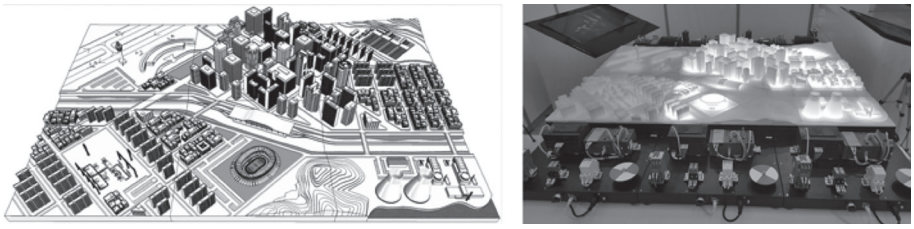
The control network layer is not a visible part of the platform, given its implementation in the virtualized game network hosted by remote cloud exercise servers. Connecting the platform to the game server was designed simply and easily as the plug-and-play level with one Ethernet interface. The control network is configured to provide a virtual environment that includes common control system components such as an HMI, an engineering workstation, a historian DB, a patch management system (PMS), and office computers. After conducting multiple on-site visits and an in-depth analysis, and consulting with field experts, we developed a highly advanced exercise environment and realistic cybersecurity incident scenarios so that the exercise participants can experience situations very similar to those in the real world. We made every effort to achieve high-quality results in all six selected fields. Common software or functionalities are shared and reusable code is recycled as much as possible. However, the PLC logic and HMI design that characterize each field are implemented independently to ensure a high degree of similarity to actual systems in the field (see Figure 3).

FIGURE 3. THE HMIS OF SIX DIFFERENT CRITICAL INFRASTRUCTURE SECTORS



A 3D-printed diorama is designed and produced for a private residential area and a commercial area in which people live, centering on a base site symbolizing each field. Completing these six sectors and integrating them into one large city naturally alludes to the extensibility of the system across critical infrastructure sectors (see Figure 4).

FIGURE 4. THE PROTOTYPE DESIGN AND THE FINAL 3D-PRINTED RESULT OF A SMART CITY DIORAMA COMPOSED OF SIX SECTORS



To make the visualization more dramatic, an additional feature is developed to automatically recognize the six critical infrastructure sectors and launch real-time live graphics using AR technology on the diorama. As shown in Figure 5, we designed the AR visual effects to show a normal state of each sector, its damaged state, and the state transition between them (due to RT's successful attack or BT's successful restoration of the damaged system) for each sector.[3]

3 Initially, showing the exercise progress using the AR was considered. However, there was also a concern that more than necessary information for RTs or BTs can be provided for them to experience a realistic cyber conflict during the exercise. Therefore, AR was designed to provide only the amount of information that can be experienced and obtained in reality. A situational awareness tool was developed independently for exercise operators or observers.

FIGURE 5. AR VISUAL EFFECT DESIGN ON THE 3D-PRINTED DIORAMA OF THE PLATFORM

Based on this platform design, CCE 2017 deployed three smart cities (for a total of 18 simulation systems in six areas) to serve as the core network which must be defended by the BT against the RT's campaigns. In LS18, considering fairness across the BTs, 24 complete sets of water treatment plant systems were developed and given to each BT. In addition, one smart city, composed of six different areas, is constructed to provide a demo for the observers (see Figure 6).[4]

FIGURE 6. LS18 SET-UP OF THE WATER TREATMENT PLANTS FOR 22 BTS AND THE LS18 SMART CITY DEMO

During both events, the exercise platform attracted attention as the highlight and it was evaluated to have contributed greatly to the success of both events. Most importantly, we provided each BT with a separate, advanced and realistic ICS/SCADA network environment in which technical hands-on exercises could be conducted. It also enabled the running of a new strategic game scenario of drinking water pollution during a cyber warfare situation. We demonstrated the platform's easy deployment and good mobility during all the processes of preparing and conducting the three exercises of CCE 2017, the LS18 test-run, and the LS18 main execution. Before and after the LS18 events, all systems required long-haul shipping between Estonia and South Korea, but no durability issues arose.

4 One of the practical but important goals of hosting a large-scale cyber exercise is to raise the cyber security awareness of high-level decision-makers and to increase their interest and investment in cyber security. The enhanced visualization feature of the platform is effective in providing such an impact to achieve the goal.

5. DISCUSSION OF POSSIBILITIES, LIMITATIONS, AND FUTURE IMPROVEMENTS

The platform can revolutionize the national-level cyber exercise process. It is difficult to provide exercise scenarios and environments that are tailored to the needs and tastes of everyone because there are many organizations participating in large-scale national-level exercises and their situations are all different. Generalization is widely used to resolve this issue. Hence, there may be criticism that the scenarios are not specific and do not reflect reality. Customized exercises are great, but can be very costly and may not be suitable for large-scale exercises.

A recent report [34] regarding the Grid Security Exercise (GridEx) IV in the United States highlights an attempt to develop a new exercise process. Six months before the main execution, basic scenarios were given to participating national institutions. Each institution developed its own exercise scenario following the needs of the field and carried out a local exercise in synch with the overall exercise plan. This represents a highly desirable approach, and the question arises whether the proposed platform could be introduced to a similar process. It may be possible for customized exercise environments based on the direct needs and reality from the field to be designed and developed in a distributed manner.

As discussed earlier, one of the most important characteristics of the platform is the accumulation of knowledge. Due to the existence of the exercise platform, knowledge can accumulate around the common elements of the cyber-threat environment of each institution. Through the platform, a portfolio of various national cyber-physical battlefields can be built.

There were some critical reviews of the platform by those who felt that it might oversimplify reality. Reality is a highly relative concept. The concepts of 'verisimilitude' or 'suspension of disbelief' must be considered.[5] When planning and preparing the exercise, it is necessary to provide trainees with elements that make the exercise situation appear real; if this is done, trainees will be willing to suspend their disbelief within the framework of the narrative provided and accept an impossible mission to protect society. Therefore, having the actual systems used in the field environment, apart from its possibility, does not guarantee a realistic exercise experience. The trainees can feel a greater sense of reality in a simple world that is seamlessly connected. Though there will always be aspects to be improved, we feel that the proposed platform was sufficiently detailed and complete, while implementing the critical elements of a CPB to provide practical real-life experience to the trainees.

5 *Verisimilitude* has its roots in both the Platonic and Aristotelian dramatic theory of *mimesis*, the imitation or representation of nature [35]. This leads to the idea of '*(willing) suspension of disbelief*', a term coined by Samuel Taylor Coleridge [36]. Although these concepts are originally developed for literary work, they are widely used in any kind of storytelling, including (serious) game design [37], [38].

The future plan is to build a specific and interesting portfolio that will demonstrate the potential of the developed platform. Without becoming mired in unproductive discussions focusing on technical implementation issues, we will select any areas that meet the exercise goals and create the best cyber-threat scenarios in the future. We will secure a variety of interesting CPB deployments.

One possibility is the logical implementation of cross-sector dependencies between multiple critical infrastructure sectors [33], [39]–[41]. Another possibility is to include electronic warfare with cyber exercises [42]–[44]. This will be more appropriate for high-level wargame-like table-top exercises and the use case of the platform may be limited to visualization effects of electronic warfare impacts. Whether it is possible or desirable to integrate cyber warfare and electronic warfare scenarios with very different attributes into one exercise depends on the choices made by exercise planners. Nonetheless, it is clear is that there is a demand for this type of exercise and that this platform has the potential to be used even in these extreme cases. Another possibility is to use sensor modules to construct an IoT-enabled cyber-physical system, such as an IoT-enabled smart grid [45]–[48] or an industrial IoT system [49]–[51]. The possibilities are endless. This platform will provide a basis for accumulated knowledge and technologies as long as we continuously innovate.

6. CONCLUSION

In this study, we proposed a means by which to construct a cyber-physical battlefield platform for large-scale cyber exercises. The main goal is to develop a platform that maximizes the coverage to encompass various design considerations, such as the target exercises, scalability, mobility, reality, extensibility, domain or vendor independency, and visualization technologies of physical facilities and their damage as caused by cyber attacks. The three main components of the platform are the control system layer, the virtual control network layer, and the visualization layer. The HW-based control system layer and the virtualized control network layer are used to simulate the control system operating in the actual field realistically, based on an in-depth analysis of the field. A checkerboard-shaped visualization layer created for a modular design is one of the most noticeable differences of this ICS/SCADA platform.

This platform played a significant role in enhancing the effectiveness of the exercises at the two events of CCE 2017 and LS18. In particular, it was demonstrated that the platform has scalability and extensibility in that a complete CPB was provided to each participating BT and six different critical infrastructure sectors were simulated based on the same platform. These were a power grid system, a nuclear power plant, a water treatment plant, a railroad control system, a traffic light control system, and an airport

control system. The goals of developing a practically complex ICS/SCADA security exercise environment that can integrate technical hands-on missions successfully with high-level table-top exercise scenarios and challenge each trainee with a real-life cyber crisis experience that will check their readiness and strengthen their capability were all achieved. We claim that this platform can be a fundamental tool that can foster continuous innovation and the accumulation of knowledge pertaining to national cybersecurity readiness assessment and capability-building activities.

Acknowledgments

The authors would like to thank Dr. Rain Ottis and Dr. Adrian Venables from TalTech and Raimo Peterson from NATO CCD COE for their valuable comments and interesting discussions on topics covered in this paper.

REFERENCES

[1] FEMA, "Program Manual: Radiological Emergency Preparedness (REP)," The Federal Emergency Management Agency (FEMA), USA, FEMA P-1028, 2016.

[2] R. M. Clark and S. Hakim, *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level*, vol. 3. Springer, 2016.

[3] Kate O'Flaherty, "Cyber Warfare: The Threat From Nation States," 03-May-2018. .

[4] Tim Johnson, "The Battlefields of Cyberwarfare Include Infrastructure and Industry, and May Become Deadly," 02-Jul-2018. .

[5] M. N. Schmitt, *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press, 2017.

[6] M. N. Schmitt, "Computer network attack and the use of force in international law: thoughts on a normative framework," *Colum J Transnatl L*, vol. 37, p. 885, 1998.

[7] M. N. Schmitt, "Cyber Operations and the Jus in Bello: Key Issues," *Intl Stud Ser US Nav. War Col*, vol. 87, p. 89, 2011.

[8] E. T. Jensen, "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense," *Stan J Intl L*, vol. 38, p. 207, 2002.

[9] A. C. Foltz, "Stuxnet, Schmitt Analysis, and the Cyber Use of Force Debate," Air War College Maxwell Air Force Base United States, 2012.

[10] H. Holm, M. Karresand, A. Vidström, and E. Westring, "A survey of industrial control system testbeds," in *Secure IT Systems*, Springer, 2015, pp. 11–26.

[11] B. Green, A. Lee, R. Antrobus, U. Roedig, D. Hutchison, and A. Rashid, "Pains, gains and PLCs: ten lessons from building an industrial control systems testbed for security research," in *10th {USENIX} Workshop on Cyber Security Experimentation and Test ({CSET} 17)*, 2017.

[12] H. Gao, Y. Peng, K. Jia, Z. Dai, and T. Wang, "The design of ics testbed based on emulation, physical, and simulation (eps-ics testbed)," in *2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2013, pp. 420–423.

[13] R. Candell, K. Stouffer, and D. Anand, "A cybersecurity testbed for industrial control systems," in *Proceedings of the 2014 Process Control and Safety Symposium*, 2014.

[14] A. P. Mathur and N. O. Tippenhauer, "SWaT: A water treatment testbed for research and training on ICS security," in *Cyber-physical Systems for Smart Water Networks (CySWater), 2016 International Workshop on*, 2016, pp. 31–36.

[15] E. Korkmaz, A. Dolgikh, M. Davis, and V. Skormin, "Industrial control systems security testbed," in *11th Annual Symposium on Information Assurance*, 2016.

[16] I. Ahmed, V. Roussev, and G. Richard III, "SCADA Testbed for Security and Forensics Research," University of New Orleans, New Orleans, United States, 2017.

[17] M. Almgren et al., "RICS-el: Building a National Testbed for Research and Training on SCADA Security (Short Paper)," in *International Conference on Critical Information Infrastructures Security*, 2018, pp. 219–225.
[18] S. Adepu, N. K. Kandasamy, and A. Mathur, "EPIC: An Electric Power Testbed for Research and Training in Cyber Physical Systems Security," in *Computer Security*, Springer, 2018, pp. 37–52.
[19] Q. Qassim *et al*., "A survey of scada testbed implementation approaches," *Indian J. Sci. Technol*., vol. 10, no. 26, 2017.
[20] E. Skoudis, "How to build a completely hackable city in five steps: And why you should build your skills in this arena," *Pen Test Hackfest*, 2013.
[21] E. Skoudis, "NetWars: CyberCity." [Online]. Available: https://www.sans.org/netwars/cybercity. [Accessed: 01-Jan-2019].
[22] CYBERGYM, "Cyber Training and Technologies Arena as a Solution." [Online]. Available: https://www.cybergym.com/arena-as-a-solution/. [Accessed: 01-Jan-2019].
[23] US ICS-CERT and Idaho National Lab., "ICS Cybersecurity (301) Course." [Online]. Available: https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT.
[24] J. K. Daoud, "Multi-PLC Exercise Environments for Training ICS First Responders," Air Force Institute of Technology, 2017.
[25] Cyber Security Training and Exercise Center, "Cyber Crisis Defense Training." [Online]. Available: http://www.cstec.kr/cstec/eng/. [Accessed: 01-Jan-2019].
[26] J. Davis and S. Magrath, "A survey of cyber ranges and testbeds," Defence Science and Technology Organisation Edinburgh (Australia) Cyber and Electronic Warfare Div, 2013.
[27] B. Hallaq, A. Nicholson, R. Smith, L. Maglaras, H. Janicke, and K. Jones, "CYRAN: a hybrid cyber range for testing security on ICS/SCADA systems," in *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*, IGI Global, 2018, pp. 622–637.
[28] Department of Homeland Security, "Cyber Storm: Securing Cyber Space." [Online]. Available: https://www.dhs.gov/cyber-storm. [Accessed: 01-Jan-2019].
[29] National Security Research Institute, "Cyber Conflict Exercise 2018." [Online]. Available: http://www.cstec.kr/cce2018/eng.html. [Accessed: 01-Jan-2018].
[30] NATO CCDCOE, "NATO Won Cyber Defence Exercise Locked Shields 2018," 27-Apr-2018. [Online]. Available: https://ccdcoe.org/nato-won-cyber-defence-exercise-locked-shields-2018.html. [Accessed: 01-Jan-2019].
[31] NATO CCDCOE, "Cyber Defence Exercise Locked Shields 2013: After Action Report," 2013.
[32] E. D. Knapp and J. T. Langill, Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems. Syngress, 2014.
[33] ENISA, "Communication network dependencies for ICS/SCADA Systems," TP-06-16-344-EN-N, Dec. 2016.
[34] North American Electric Reliability Corporation, "Grid Security Exercise GridEx IV: Lessons Learned," Mar. 2018.
[35] Wikipedia.org, "Verisimilitude (fiction)." [Online]. Available: https://en.wikipedia.org/wiki/Verisimilitude_(fiction).
[36] Wikipedia.org, "Suspension of disbelief." [Online]. Available: https://en.wikipedia.org/wiki/Suspension_of_disbelief.
[37] J. Thompson, B. Berbank-Green, and N. Cusworth, *Game design: Principles, practice, and techniques-the ultimate guide for the aspiring game designer*. John Wiley & Sons, 2007.
[38] S. De Castell and J. Jenson, "OP-ED serious play," *J Curric. Stud*., vol. 35, no. 6, pp. 649–665, 2003.
[39] P. Pederson, D. Dudenhoeffer, S. Hartley, and M. Permann, "Critical infrastructure interdependency modeling: a survey of US and international research," *Ida. Natl. Lab*., vol. 25, p. 27, 2006.
[40] F. Petit *et al*., "Analysis of critical infrastructure dependencies and interdependencies," Argonne National Lab.(ANL), Argonne, IL (United States), 2015.
[41] EPSA Analysis: J. Phillips, M. Finster, J. Pillon, F. Petit, and J. Trail, "State Energy Resilience Framework (Argonne, IL: Argonne National Laboratory, December 2016)," ANL/GSS-16/4.
[42] D. C. Schleher, *Electronic warfare in the information age*. Artech House, Inc., 1999.
[43] C. Wilson, "Information operations, electronic warfare, and cyberwar: Capabilities and related policy issues," 2007.
[44] M. C. Libicki, "The convergence of information warfare," *Strateg. Stud. Q*., vol. 11, no. 1, pp. 49–66, 2017.
[45] C. Bekara, "Security issues and challenges for the IoT-based smart grid," *Procedia Comput. Sci*., vol. 34, pp. 532–537, 2014.

[46] S. Tonyali, K. Akkaya, N. Saputro, A. S. Uluagac, and M. Nojoumian, “Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled Smart Metering systems,” *Future Gener. Comput. Syst.*, vol. 78, pp. 547–557, 2018.
[47] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, *Internet of Things security and forensics: Challenges and opportunities*. Elsevier, 2018.
[48] M. A. Ferrag, L. A. Maglaras, H. Janicke, and J. Jiang, “A survey on privacy-preserving schemes for smart grid communications,” *ArXiv Prepr. ArXiv161107722*, 2016.
[49] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, “Security and privacy challenges in industrial internet of things,” in *Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE*, 2015, pp. 1–6.
[50] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu, “Security and privacy in cyber-physical systems: A survey of surveys,” *IEEE Des. Test*, vol. 34, no. 4, pp. 7–17, 2017.
[51] C. Alcaraz, R. Roman, P. Najera, and J. Lopez, “Security of industrial sensor network-based remote substations in the context of the internet of things,” *Ad Hoc Netw.*, vol. 11, no. 3, pp. 1091–1104, 2013.