SAND2018-4836B

Applying Model-based Situational Awareness and Augmented Reality to Next-Generation Physical Security Systems

Elaine M. Raybourn, Ray Trechter

Sandia National Laboratories*, Albuquerque, New Mexico USA
{emraybo, rtrech} @sandia.gov

Mixed, augmented, and virtual reality hold promise for many security-related applications including physical security systems. When combined with models of a site, an augmented reality (AR) approach can be designed to enhance knowledge and understanding of the status of the facility. The present chapter describes how improved modeling and simulation will increase situational awareness by blurring the lines among the use of tools for analysis, rehearsal, and training—especially when coupled with immersive interaction experiences offered by augmented reality. We demonstrate how the notion of a digital twin can blur these lines. We conclude with challenges that must be overcome when applying digital twins, advanced modelling, and augmented reality to the design and development of next generation physical security systems.

Keywords. Augmented reality, digital twin, modeling, simulation, physical security systems, situational awareness, next generation

1.0 Introduction

Augmented reality (AR), mixed reality (MR), and virtual reality (VR) hold promise for many security-related applications including installation security. When combined with a virtual representation of a site created through modeling, these approaches can be designed to enhance the knowledge and understanding of the status of the facility. A user can view and interact with a 3D model of an entire facility updated with probabilistic assessments based on all current data including predictions for likely potential threats. The commander could know exactly where security personnel are at all times and the system could guide the operator's actions based on current and historical data (Trechter, 2014).

As cyber-physical security systems become model-based and leverage augmented, virtual, or mixed reality, the gaps between training, planning/analysis, and situational awareness simulations disappear. Through a model driven contextual interface, trainees have the ability to experience a virtual representation of a real-world facility and participate in realistic training. Security force leadership can similarly use this model to improve tactics or to plan upgrades. Users of these systems will be able to virtually experience a combat sequence or, in the case of actual watch standers, participate in virtual no-notice drills.

Current efforts by the authors and others include the development of flexible, powerful tools for analyzing security in operational spaces, particularly facilities, and their surrounding terrain. These physics-based, 3D, terrain-aware simulations analyze a system's performance, often including the interplay between its components (e.g. sensors, energy, cybersecurity, and personnel). The use of autonomous systems, especially Unmanned Aerial Systems (UAS), as dynamic sensors and other applications is underway. AR is being used to explore and visualize new security concepts. Simulations also often incorporate a mixture of these live and simulated assets.

A science and technology (S&T) goal for next-generation physical security facilities is to increase situational awareness with the use of new technologies such as the integration of artificial intelligence, machine learning, and software analytics with a virtual representation or model of the site (Callow et al., 2016). Professor Michael Grieves (2014, p. 1) coined the term "Digital Twin" in 2003 to refer to "a virtual, digital equivalent to a physical product." This term gained traction in the past decade and has been expanded to manufacturing enterprises, operations, and facilities. When combined with data from sensors, the devices, personnel, and other sources create a living, digital simulation model or digital twin of a site (GE Research, 2017). A facility's digital twin updates and changes as their physical counterparts change, providing understanding of each unique asset, in this case a facility, over time. In addition to real-time data feeds, a digital twin can be informed by historical data from a variety of sources. The twin is not just a generic model of a facility; it is for all intents and purposes a representation of a specific site that improves with data over time.

Ultimately, the creation of a secure site's digital twin will provide new and more versatile tools for evaluating security systems that blur the lines between activities such as real-time situation awareness/command-and-control, design, analysis, training, and various modes of exercises—be they tabletops or force-on-force rehearsals. Immersive technologies underpinning a digital twin approach will accelerate the adoption of intelligent, adaptive training ecosystems for game-based and transmedia learning (Raybourn, 2007; 2014). The twin and its data can support a virtual environment, or world, for VR training applications with multiple participants. That same digital twin can easily provide coordination of virtual assets, along with virtual features and cues for AR training applications. Physical security system designers can take advantage of a twin collecting data and learning over time to check proposed design changes, and a vulnerability analyst can use that same data to identify possible threats and a site's readiness to handle them.

Just as important as creating high-fidelity simulations with these techniques are the real-time data channels that feed real sensory data to the virtual representation and vice-versa. It is here where autonomous systems and humans with AR technology work with the virtual system to improve overall situational awareness. AR presents a compelling opportunity to improve security personnel's situational awareness by displaying elements of the virtual world's model, including entities that are not in the responder's line-of-sight, and predictive analytics based on a simulation's ability to run faster than real-time. Examples where the predictive capabilities of simulations might be quite helpful are providing security forces paths that avoid enemy fire or observation, and predicting the future positions of hostile forces based on previous observations.

However, a sobering realization is that far too many critical infrastructure systems and facilities are vulnerable to cyber and physical attack. The physical security installation community has identified several emerging scenarios which serve to update critical infrastructure defensive security countermeasures, but nevertheless there always remain a number of considerations (Clem et al., 2015). For example, modern physical security systems and facilities that rely on subsystems communicating via Internet Protocol have given rise to cyber-physical attacks. Cyber-physical system attacks can cripple a nation's critical infrastructure, energy grids, transportation, etc.

Model-based situational awareness is required for improvements in analysis, rehearsal, and training. Subsequent sections of the present chapter describe how achieving this S&T goal is addressed with tools for modeling, simulation, and current practices underway today. Simulations are enhanced especially when coupled with immersive interaction experiences offered by AR, MR, and VR (Raybourn, 2016). We discuss the notion of digital twin in the context of physical security system installations. We then apply this concept

to a hypothetical use case loosely based on actual events, in which we set the stage for the ways improved modeling and simulation may facilitate improved situational awareness. We conclude by identifying challenges and proposing recommendations for next-generation physical security systems.

2.0 Model-based Situational Awareness for Physical Security Today

A facility's physical security system is truly a system-of-systems when one considers all the elements needed to secure a location. To model a facility at the necessary level of fidelity, a site's barriers, buildings, sensors, vehicles, people, and other significant real-world objects must be presented in a model. When done well, simulations may detect vulnerabilities in tactical operations by analyzing the environment based on geography, sensing, and timing. Users can then conduct specified analyses, such as the effectiveness of observation posts in detecting targets, and exploring multiple phenomenology including physical, cyber, and human behavioral effects. These analyses may allow a user to target specific areas of concern, minimizing overall system costs (Garcia, 2008).

Many tools are used to improve the physical security of facilities today. For example, Joint Conflict and Tactical Simulation (JCATS) is a well-known human-in-the-loop simulator that allows response force effectiveness to be evaluated through live, force-on-force exercises using teams of attackers and defenders. However, these exercises can be costly and time-consuming. That said, a simulated force-on-force exercise with JCATS is a great alternative to a live exercise, as it captures the critical human dimension introduced by system operators, and provides the opportunity for participants to share knowledge and train together. Site personnel can improve site security by combining simulated exercise results with robust data analysis, the results of other modeling and simulation, and consultation with subject matter experts.

Facilities also use video game technology, such as serious games and game-based training, to facilitate cognitive training and experiential learning in situated contexts and immersive scenarios (Raybourn, 2007; 2014; 2016). The goals of these cognitive trainers for physical security system personnel are often enhanced retention of knowledge, skill development, and practice of key training objectives. When combined with analytics resulting from tools such as JCATS and game-based trainers, virtual environments become force multipliers.

Current modeling and simulation capabilities support the analytics and technology underpinning the next-generation digital twin, and as such, directly determine whether an advantage will be provided to the

Figure 1: Virtual Facility Display with Dante.

security forces. One such tool, *Dante*, develops physics-based, 3D, terrain-aware simulations that analyze a security system's performance (Trechter, 2014). Simulations include physical objects (e.g., buildings, equipment, vehicles, and weapons), people and their behaviors, communications, cyber systems, and the interplay between each of these components. Intelligent characters are driven by non-deterministic simulated behaviors. The characters are influenced by their environment *and* their perceptions. As such, they may respond differently given the same situation. An important consideration for this discussion, the simulations created with Dante may incorporate a mixture of live and simulated assets. Linkages between the virtual and physical worlds are built into this simulation framework.

Creating an accurate 3D terrain model of a facility for use in a Dante simulation is of key importance. Terrain models serve as the synthetic environment for a site's virtual world and as a vital backdrop for simulation, exploration, and visualization of security concepts and operations. These terrain models have elevation data, imagery, road data, barriers, buildings, and often building interiors. Geographic Information Systems (GIS) and 3D modeling tools are used along with tools that seek discontinuities, paths, and features to improve confidence in terrain accuracy. Fortunately, terrain data in security simulations tends to consist of static features for a site (e.g., installation features such as buildings and roads do not tend to move often). Accurate terrain supports path generation algorithms based upon multiple influences such as terrain features, sensor fields, data from imagery, and energy signatures. For example, these algorithms can plan intelligent movement around a camera's view and take threats into account when finding an optimal route. Accurate terrain is especially important for AR applications as the location of physical world features need to be mapped into the coordinates of the facility model so that virtual feature and cues generated by a simulation show up in an operator's field of view correctly (e.g., a suggested route on an operator's head mounted display shows a path around a building rather than through it).

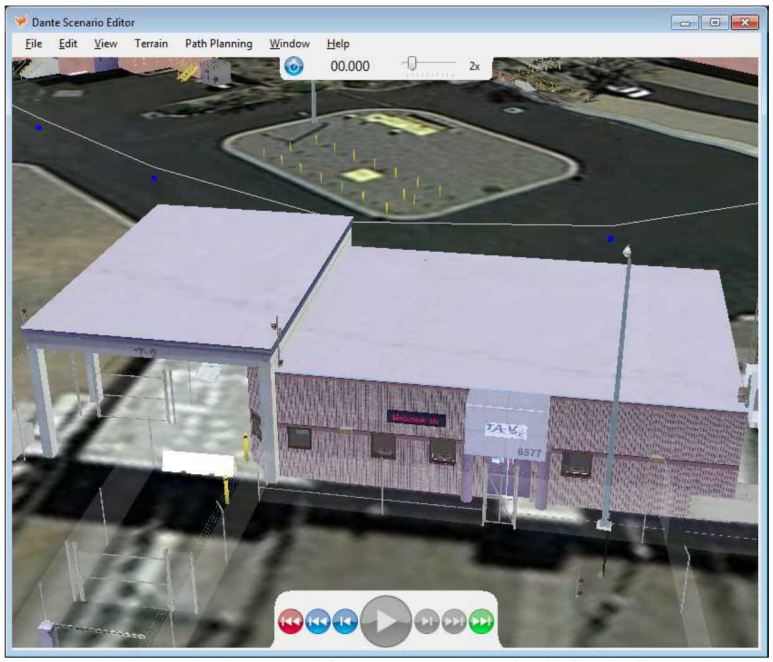

Figure 2: Dante Terrain with Features (e.g. buildings fences).

Augmented reality applications show promise for enhancing model-based situational awareness, especially when used with physics-based, 3D, terrain-aware simulations that can analyze a security system's performance. AR applications need not only enhance model-based situational awareness with visual representations or feedback. Representations may also be auditory, haptic, or olfactory. AR may also be

dynamic, adaptive, and persistent. AR can be used with physical security system models to 1) serve as cues for the existence of sensors that are not visible (blind spots), 2) provide locations of key assets, 3) recommend defensive positions, 4) locate/mark opposing forces for training and experimentation, and 5) generate avatars reflecting "patterns of life," especially those representing vulnerable populations such as children, elderly, etc. While there remain technology maturity challenges with respect to the use of outdoor AR for geolocating personnel (motion, weather, blockage, night, sensor drift, etc.) these applications can support installation design, test and evaluation, and simulation of training and rehearsal.

In summary, we briefly discussed some of the tools for modeling and simulation that are characteristic of current practices underway today as an introduction to the notions that follow. In the next section we discuss the application of a *digital twin* to the context of physical security system installations.

3.0 A Secure Facility Meets its Digital Twin

Accurate facility modeling and terrain development are needed for security simulations in general and to implement a digital twin. Data feeds must be added to reflect the current situation on the ground along with adding predictive capabilities to this adaptive model. The site's digital twin needs sufficient data updates by various means (e.g., sensor input, updates from responders) to stay synchronized with their physical counterparts, and support response force decisions with real-time status. Secure facilities usually have a variety of sensors including cameras, fence line sensors, and radars that can update the digital twin in real-time, and this information can be made immediately available to the entire response force.

The response force itself is a source of real-time information. Staff in the central alarm/control station and responders typically use radio communications to direct forces and communicate an unfolding situation with each other. Having a digital twin focused on command and control systems, and the right equipment such as a smart phone, tablet, or a head mounted display, allows communications to be relayed visually and persistently through an AR channel. A display is used in lieu of, or in conjunction with, radios. The alarm station can mark entities such as enemy forces, identify areas of relative safety, or direct responders to engagement locations. Responders, in turn, can assess and mark threats and other items of tactical significance through their smart devices, and feed these back to the twin that stitches together personnel and sensor report into an overall picture for an engagement as it unfolds. This works the same with training exercises in and around the facility as data is captured from observer notes and After Action Review (AAR) reports along with data from automated engagement systems using Multiple Integrated Laser Engagement Systems (MILES). These data sources can be used to tune a digital twin's artificial intelligence (AI) over time and, given the virtual representations' near-perfect understanding of the site terrain and pathways to target areas, the system becomes a formidable opponent that can be used to train response forces or act as an aide during actual operations.

In addition to real-time data of an operation, there are innumerable facility data sources that can be used to align a twin with its physical counterpart and improve its usefulness for decision support. A facility's badge system is a source of information of normal and possibly anomalous access to secure areas(Klinger et al., 2013)).). The electronic security system that connects various sensors and cameras can be gleaned for false alarm rates by time of day, season, and environmental conditions such as sun, rain, and wind to better discriminate among real threats and noise in the environment. Recoding the weather may be important given its impact on sensors. Along with these data sources, video captures from numerous cameras can help to establish an installation pattern of life that can be data mined for possible threats.

As it turns out, a site's digital twin may be used in part to address another bedeviling problem faced by the installations community: cyber attacks upon elements of the physical security systems itself (Dignan, 2017). Typically, the operational networks with cameras and other sensors using IP for connectivity are air gapped and have careful configuration management. However, as is the case with other control systems,

vulnerabilities may occur through improper configuration, insider attack, and covert communications links. Attacks on cyber infrastructure are hard to diagnose and may go unnoticed because it is the network itself that is used to detect and respond to cyber exploits. If the infrastructure is compromised to some degree and clever attackers cover their tracks, a digital twin can have access to the actual state of the device in the control system and not just the state reported on the network. According to Colin Parris, Vice President of Software Research for GE Global Research, "We're using physics to detect what's going on and we know what the normal state is for the machine." (Dignan, 2017). Using an industrial control system example, Parris further explained that "if a cyber attacker were to spoof a sensor it may be obvious if one sensor says it's 20 degrees and another says it's 200." (Dignan, 2017).

Extending this example to the world of physical security, installations have access to overlapping cameras or other sensors covering a particular area. By directly accessing these devices through a separate or redundant path, the signals (e.g., pixels in the case of a camera) from each can be used to update their twin image. These virtual sensor representations can then be compared and triangulated to point out a sensor that is at odds with the status reported over the network, and thus detect some types of exploits (Russel et al., 2016). For example, consensus may then be reached among different sensor types (e.g., does a fence line sensor and camera have a signal that represents an intruder in the same location?). What is perhaps even more powerful is the notion that digital twin images of sensors may be able to virtually reconstruct what *should be* seen by another device, allowing a compromised sensor or malfunctioning device to be bypassed, and allowing security staff to continue their activities without a gap in their situational awareness.

In the next section we describe a fictional scenario and fictional tools used by a team of attackers and hackers. This example attack with both a physical and cyber element is based loosely on the 2015 and 2016 attacks against the Ukraine power grid. Much of the digital twin capability described is achievable in the near-term; however, additional S&T efforts in artificial intelligence, machine learning, and software analytics are needed if we are to create living, digital simulation models that update and change as their physical counterparts change.

4.0 Scene: Sunday, 1600. Somewhere in the countryside…

A group of insurgents, traveling by van, roll through the country side on a sleepy Sunday afternoon. The attack team's assignment is straightforward: they are to breach the facility perimeter; proceed to the location of the control systems; and use their explosives charges to damage the power plant, including backup generators, beyond repair, necessitating weeks for restoration. A cyber exploit will be used in conjunction with the physical attack to compromise the site's Alarm, Communication and Display (AC&D) system and hide sensor alarms from the defenders. The attack team is armed modestly with rifles, breaching tools, and some explosive cutting charges. What the assault team lacks in materiel provisioning is made up for by intelligence along with an insider who is part of their team.

The facility, which is experiencing yet another routine day among many, is prepared. Its perimeter has a clear zone made from two parallel physical fences with sensors installed in between the fences. Access into this perimeter is controlled at vehicle and personnel access points. The facility bristles with cameras, thermal imagers, and other devices that feed into a central alarm station. Central alarm station operators monitor video stream and sensor alerts, assess potential anomalies and intrusions, and maintain contact with both forces and the watch commander via radio. Security forces patrol both outside the perimeter and within the facility, backed up by a Quick Reaction Force (QRF) on duty at security forces headquarters a few minutes away. These security elements—cameras, sensors, and the alarm station— are connected by Alarm Communications & Display (AC&D) software, isolated on its own network. Modern equipment uses the IP protocol, which makes configuration and extension of the AC&D relatively easy. The AC&D is the trusted source for status of the cameras and sensors for

the site's physical security. Unbeknownst to the facility's defenders, one of their own has been working patiently over time with a hostile information operations team to compromise the AC&D at the targeted facility. Their chosen method uses a cyber exploit similar to that of the well-known attack on the Ukrainian power grid.

A fascinating article on the subject of the Ukraine power grid attacks was published in *Wired* on June 20, 2017. Recall that on December 23, 2015, at exactly midnight, a cyber attack to the power grid resulted in 225,000 Ukrainians losing electric power. The same thing happened almost exactly to the day a year later (Greenberg, 2017). While power was lost only for a few hours on each occasion, it was enough to be noticed by the global community. Especially since it had been noted by Ukrainian officials that "there had been 6,500 cyber attacks on 36 Ukrainian targets in just the previous two months," including a cyber attack that took down two servers at the same time at StarLightMedia, the largest broadcast conglomerate in the Ukraine (Greenberg, 2017). During the forensic analysis of the SilverLightMedia cyber attack, it was discovered that "the hackers used BlackEnergy for access and reconnaissance, then KillDisk for destruction" (Greenberg, 2017). By this time, BlackEnergy and KillDisk had infected the networks of at least three Ukrainian power companies and were waiting to be deployed by the hackers at the appropriate moment (Lipovski & Cherepanov, 2016; ICS-CERT, 2016). All this was preparatory work for the main thrust of the attack, a copy of control software used by the power company had been surreptitiously obtained by the hackers and was run remotely to issue commands that shut down power generation to a large part of the country. According to Greenberg (2017), attacks of this kind are becoming more common as hackers find way to obtain copies of system control software and make their own "enhancements."

In our notional scenario, the goal for the cyber element of the attack is to hide the many alarms, video, and other information provided by the AC&D, thereby blinding the central alarm stations and providing the attackers with a tactical advantage. Preparation for this type of attack begins with the acquisition of a legitimate copy of the AC&D software (Clem et al., 2015). The software is then examined for configurations options, supporting XML definitions, and source code when available. Changes to the Human Machine Interface (HMI) to not show sensor alarms leaves the alarm station operators and watch commander in the dark about events as they unfold, and thus prevents effective response. A special command line key sequence can be added that allows the AC&D software to function normally during system checkout and mask off alarms prior to an attack. All that is needed is for an insider colluding with the attack team to load the exploited AC&D software during routinely scheduled maintenance and upgrades.

To execute the plan discussed above, the attack team stops by the road a half-mile away from the mission-critical facility, out of sight and beyond the site's sensor field coverage. Five insurgents exit the van and begin their approach to the south of the facility while those remaining in the van head north. The attack team on foot is a diversion. They plan to breach and attack the side of the facility opposite of the building housing the critical asset, so as to draw the security personnel toward the south. These attackers take a stealthy approach to the assigned breach point on the fence. They wait for an opportune time to cut the fence, and then move aggressively to a diversion target building in the facility. The team remaining in the van positioned themselves and began the main assault from the north at the sound of gunfire and communications from the diversion team leader that their breach had been successful. The main attack team hopes to win a race against the distracted security personnel to the target building, place their charges in a fashion to cut both normal and backup power, and engage security forces as they arrive. All seems normal from the display in the alarm station and will continue to appear that way even as the facility enters the fight of its life…

4.1 A Digital Twin Saves the Day

With the standard setup of cameras and sensors feeding a central AC&D, the defense of a such a facility would be in question. Lacking the situational awareness to discern the number and direction of the attacks

in a fight that lasts but a few minutes, there is a reasonable chance that the diversion will succeed, drawing security personnel away just long enough for the main assault on the critical asset building. However, this facility has a digital twin that includes not only the physical security system and its AR displays, but also other aspects of the site such as emergency services, building automation systems, and utility usage. The twin has many uses such as predictive maintenance and energy management, but in this case, it serves as secondary status or a watchdog for the electronic security system (ESS), which has virtual representations for all components, even the AC&D system itself. The digital twin is implemented in a continuous simulation with a separate path to sensors sometimes avoiding the network adapter and accessing the device's signals directly. This approach allows the output from different sensor types covering the same terrain to be compared through algorithms that look at the location, size, speed, and even the surmised intent of the entity; it also allows these virtual security system elements to watch each sensor, achieve consensus in what may be in the field of view, and detect when a device is not functioning properly due to hardware malfunction or perhaps even a cyber exploit such as the one planned in our fictitious scenario.

As the diversion attack starts, the alarm station is rightfully caught off guard, but not for long. As the attackers cross the sensing fields, the AC&D system continues to report nothing interesting; however, sensor events are relayed directly from the digital twin to secure phones carried by the security forces and to the AR-enabled, truck-mounted displays. With a heads-up on suspicious activity on the south side of the facility, security forces discover the breaching team as they cross the fence. Meanwhile, the momentarily bewildered alarm station crew also using the status updates provided by the site's twin begins to piece together the situation. The consensus mechanisms built into the twin's virtual agents quickly identify the AC&D system as "odd-man-out" by not showing an alerted state. Security forces are already executing the defense plan on the south side of the perimeter through radio communications and twin updates. By the time the main attack has initiated, the site security forces have established their response rhythm and, thanks in part to the twin, this attack is no surprise.

The site's digital twin has more than sensor data at its disposal. The terrain, buildings, fences, and other features have been recorded with a laser scanner. This information includes exact detail of the facility. Every berm, depression, and natural cover from vegetation on all pathways to and from the facility have been enumerated, along with their ease of traversal. Further, the digital twin has participated in and been informed by simulated and live training exercises, allowing its artificial intelligence to learn over time. The twin had already proven to be a formidable opponent when training security forces —all the while training its own algorithms. The security personnel have used AR and digital twin artificial intelligence to train with "what if" scenarios involving virtual assets. In this scenario the twin's knowledge was used in real-time to suggest maneuver routes and courses-of-action to the security forces. Those suggested moves were optimized to bring the breach quickly to an end, while at the same time ensuring minimal damage. The site's digital twin provided the security forces with knowledge overmatch.

5.0 Toward Digital Twin

The preceding section foot stomps how intelligent digital twin technology will ultimately provide improved model-based situational awareness for a variety of cyber-physical security systems to include facilities, military installations, mobile security command posts, and next-generation physical security incorporating AR. The digital twin, as a learning system, learns from itself—using sensor data that convey various aspects of its operating condition. Sensor data can come from 1) human experts, such as engineers with deep and relevant industry domain knowledge, 2) from other similar machines or fleets of machines, and 3) from the larger system and environment of which it may be a part. A digital twin integrates historical data from past machine usage into its digital model.

As a way of introducing how improved models via digital twins and AR representations can improve situational awareness, we embellished one of the most intriguing public hacks against a private company, and described how (an albeit futuristic) digital twin could have played a role in a provocative view of the future. While the addition of digital twin technology could greatly enhance cyber-physical security systems, it may also present significant challenges for physical security systems and personnel.

For example, a survey of different-sized companies found that many organizations are not prepared for modern technical challenges. Digital twins present unique modern, socio-technical challenges. The authors of the survey concluded that to face modern technical challenges security systems must be "supported by educated, informed, well-equipped personnel that grow their skill sets over time" (Gregory-Brown and Wylie 2017, p. 30). Additionally, according to Gregory-Brown and Wylie (2017, p.2-3) safeguarding remains an important cyber-physical security issue:

> "…reliance on control systems continues to expand across not only industrial settings, but also the operation and maintenance of our cities, our buildings and all kinds of modern smart applications. Recognition that even dedicated, special-purpose ICS components, such as intelligent embedded devices and programmable devices that are used for command and control, can carry vulnerabilities exploitable by malefactors is increasing among ICS security practitioners and the broader security community, as is concern about ransomware, which has started to invade the corners of almost any digital system."

Stamp and others (2003) echo the call for training and education of security personnel, as S&T moves toward automation and the inclusion of intelligent technologies for physical security systems and facilities. They underscore the potential for inadequately trained personnel to cause security deficiencies, especially if they interact with automation.

The Ukraine power grid hack should serve as an example of how important it is to mitigate cyber-physical security system vulnerabilities across the board. Several more recent attacks use similar tools as those on the Ukraine power grid (Higgins, 2017). Clem and others (2015) recommend utilizing LVC (live, virtual, constructive) model-based situational awareness and simulation to test cyber exploitation of control systems and physical security systems.

In addition to next generation approaches to using testbeds or LVC to validate intrusion detection systems or approaches against simulated attacks, Yang et al. (2014) proposed a multilayer approach to security that utilizes intelligent, electronic devices that initiate alerts toward self-recovery without human intervention, a part of the system's resilience. Another challenge will be keeping the security, reliability, and integrity of machine learning algorithms intact (Raybourn et al., 2015) as organizations and security personnel alike begin to trust and depend more heavily on the predictions and recommendations made by intelligent digital twin technology.

Finally, the National Academies found that the electric grid of the United States is vulnerable to a number of attacks, among them cyber (Walton, 2017). In the report, the US Departments of Energy and Homeland Security are urged to work together to address the vulnerabilities. As far as the impact—it can be far reaching—according to Morgan, a professor of engineering at Carnegie Mellon University and chair of the committee, "long-duration outages that leave millions without power could result in economic damages estimated in the billions of dollars, posing serious threats to health and public safety, and also potentially compromising national security" (Walton, 2017). Strengthening our cyber-physical security systems for U.S. critical infrastructure with cyber countermeasures remains an evolving challenge for the Federal Government, private enterprise, and the public that must be addressed collaboratively.

8.0 Conclusion

In the highly VUCA environment that constitute cyber-physical security systems and security operations, training is obsolete as soon as it is deployed. A survey of service strategy documents conducted by one of the authors highlights the shared belief of the need for training and education modernization and some congruence on how to achieve it (Raybourn et al., 2017). Modernization will require much more realistic scenarios utilizing robust models, emulated software and hardware environments, and MR/AR/VR simulations, with adaptive, persistent, and blended live, virtual, constructive, and gaming environments (Machi, 2017; Raybourn, 2007; 2014; 2016). The use of AR, model-based situational awareness, and digital twins, will greatly enhance the future of training personnel with immersive simulation. According to Machi (2017) AR/MR/VR could be combined with artificially intelligent avatars who serve as instructors to train personnel in a number of maneuvers. As cyber-physical security systems become model-based and leverage augmented, virtual, or mixed reality, the gaps between training, planning/analysis, and situational awareness simulations disappear. In the present chapter we discussed the notion of digital twin in the context of physical security system facilities. We applied this notion to a hypothetical scenario loosely based on actual events. We concluded with a discussion on the challenges that will be encountered as S&T moves toward digital twin technology and offered general recommendations for next generation physical security systems.

Acknowledgements. *Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

9.0 References

Callow, D., (2016). SAND2016-12214 Physical Security System of the Future: Vision and Roadmap, 2016 Sandia National Labs.

Clem, J., Atkins, W., Urias, V. (2015). Investigation of Cyber-Enabled Physical Attack Scenarios. SAND2015-4202C. Sandia National Laboratories, Albuquerque, NM. Retrieved March 6, 2018 from https://www.osti.gov/scitech/servlets/purl/1255768.

Dignan, L. (2017). GE aims to replicate Digital Twin success with security-focused Digital Ghost. Between the Lines, ZDNet.com. Retrieved on April 17, 2018 from https://www.zdnet.com/article/ge-aims-to-replicate-digital-twin-success-with-security-focused-digital-ghost/.

Garcia, M.L. (2007). The design and evaluation of physical protection systems, 2nd Edition. Butterworth-Heinemann Newton, MA, USA.

General Electric Research. (2017). Predix technology brief: Digital Twin, retrieved on April 17, 2018 from https://www.predix.com/sites/default/files/predix-digital-twin-technology.pdf.

Greenberg, A. (2017, June). How an entire nation became Russia's test lab for cyberwar. Wired. Retrieved March 6, 2018 from https://www.wired.com/story/russian-hackers-attack-ukraine/.

Gregory-Brown, B., Wylie, D. (2017). Securing industrial control systems – 2017: A SANS survey. SANS Institute InfoSec Reading Room. Retrieved March 6, 2018 from https://www.sans.org/reading-room/whitepapers/analyst/securing-industrial-control-systems-2017-37860.

Grieves, M.W. (2014). Digital Twin: Manufacturing excellence through virtual factory replication. Digital Twin Whitepaper. Michael W. Grieves, LLC. Retrieved April 17 from http://www.apriso.com/library/Whitepaper_Dr_Grieves_DigitalTwin_ManufacturingExcellence.php.

Higgins, K.J. (2017, January). Latest Ukraine blackout tied to 2015 cyberattackers. Dark Reading. Retrieved March 6, 2018 from https://www.darkreading.com/threat-intelligence/latest-ukraine-blackout-tied-to-2015-cyberattackers/d/d-id/1327863.

Hutchins, E. (1995). *Cognition in the wild*. The MIT Press: Cambridge, MA.

ICS-CERT (2016). Cyber attack against Ukrainian critical infrastructure. Retrieved March 6, 2018 from https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

Klinger, K., Small, D., Gottlieb, E., Whetzel, J., Gillis, H., Wharton, J. (2013). Final Report for Advanced High Security Command and Control Interface LDRD (AHSC2I). SAND2013-8249. Sandia National Laboratories, Albuquerque, NM.

Lipovski, R. & Cherepanov, A. (2016, January). BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry. WeLiveSecurity. Retrieved on March 6, 2018 from https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/.

Machi, V. (2017, November). The Future of Training and Simulation: Preparing Warfighters for Tomorrow's Battlefields. National Defense Magazine. Retrieved April 29, 2018 from http://www.nationaldefensemagazine.org/articles/2017/11/22/the-future-of-training-and-simulation-preparing-warfighters-for-tomorrows-battlefields.

Paul (2017, January). Second Ukraine power outage linked to Russian hackers. The Security Ledger. Retrieved March 6, 2018 from https://securityledger.com/2017/01/second-ukraine-power-outage-linked-to-russian-hackers/.

Raybourn, E. M. (2016). A Metaphor for immersive environments: Learning experience design challenges and opportunities. Proceedings of MODSIM. Arlington, VA: NTSA.

Raybourn, E. M. (2014). A new paradigm for serious games: Transmedia learning for more effective training & education. *Journal of Computational Science*, (5) 3, Elsevier, 471–481.

Raybourn, E. M. (2007). Applying simulation experience design methods to creating serious game-based adaptive training systems. *Interacting with Computers*, 19, Elsevier, 207-14.

Raybourn, E.M., Schatz, S., Vogel-Walcutt, J., Vierling, K. (2017). At the Tipping Point: Learning Science and Technology as Key Strategic Enablers for the Future of Defense and Security. I/ITSEC (Interservice Industry Training Simulation & Education Conference), NTSA.

Raybourn, E.M., Fabian, N., Davis, W., Parks, R.C., McClain, J., Trumbo, D., Regan, D., Durlach, P. (2015). Data privacy and security considerations for Personal Assistants for Learning (PAL). Proceedings of the 20th International Conference on Intelligent User Interfaces Companion, 69-72.

Russel, J., Andersen, J., Sterns, C. (2016). Video motion detector fused radar: The first volumetric ultra-low NAR sensor for exterior environments. SAND2016-0083. Sandia National Laboratories, Albuquerque, NM.

Stamp, J., Dillinger, J., Young, W., Depoy, J. (2003). Common vulnerabilities in critical infrastructure control systems. SAND2003-1772C. Sandia National Laboratories, Albuquerque, NM.

Trechter, R. (2014). Physical Security Simulation and Analysis Tools. Sandia National Laboratories, Albuquerque, NM. SAND 2014-3718P. Retrieved on April 17, 2018 from http://umbra.sandia.gov/pdfs/resources/danteopshed.pdf.

Walton, R. (July 24, 2017). National Academies report finds grid vulnerable to cyber physical attacks. UtilityDive. Retrieved March 6, 2018 from http://www.utilitydive.com/news/national-academies-report-finds-grid-vulnerable-to-cyber-physical-attacks/447707/.

Yang, Y., McLaughlin, K., Sezer, S., Littler, T., Im, E.G., Pranggono, B., and Wang, H.F. (2014). Multiattribute SCADA-specific intrusion detection system for power networks. IEEE Transactions on Power Delivery, 29 (3), 1092-1102. Retrieved March 6, 2018 from http://shura.shu.ac.uk/11129/.