Washington, We Have a Problem: The Foundation for Live Virtual Constructive (LVC) Exercises Requires Fixing!

John M. Kent Gritton,
David M. Kotick
Naval Air Warfare Center,
Training Systems Division
Orlando, FL
john.gritton@navy.mil;
david.kotick@navy.mil

Gary R. Fraas
M&S Strategic Partners, LLC
Maitland, FL
gfraas@cfl.rr.com

Courtney Dean
Aptima, Inc
Woburn, MA
cdean@aptima.com

ABSTRACT

While not as serious as the issue prompting Apollo 13's famous quote, the challenges with LVC's foundation are solvable with equal resolve. Specifically, the problems with the foundation stem from stagnation to process improvements, time, costs, and personnel required to establish and execute LVC events in common virtual environments (VE's). The fundamental causal issues are varied, but include technical, procedural, and policy aspects; not to mention emerging operational requirements such as cyber warfare.

Events that connect multiple virtual, constructive and live assets with a diverse topology into a single structured environment have been conducted since at least 1992. While individual technologies within these LVC environments have dramatically improved over the past 23 years, the team processes and level of effort to establish and execute the LVC environment have not. Operation Blended Warrior (OBW) was established as a Special Event at Interservice/Industry, Training, Simulation, and Education Conference (I/ITSEC) 2015 for the purpose of identifying, documenting, and understanding the challenges faced in creating and implementing a large-scale, interoperable LVC environment, as well as for suggesting and advocating specific actions and overall solutions for the issues encountered.

This paper will discuss the development of the 2015 OBW LVC effort, the challenges uncovered during its conception and implementation, and a process for advocating solutions that leverage the I/ITSEC intellectual capital and National Training and Simulation Association (NTSA) advocacy experience. Key areas of discussion will include standards, technical integration, Information Assurance (IA)/Cybersecurity, International Traffic in Arms (ITAR)/Export Administration Regulations (EAR), integration and testing processes, and resources required.

ABOUT THE AUTHORS

Kent Gritton: Mr. Kent Gritton has been supporting Team Orlando as the Director, Joint Training Integration and Evaluation Center (JTIEC) for the past 9 years, and a member of the Acquisition Workforce supporting Navy training for 15 years. Kent is also the LVC lead for Program Management at NAWCTSD, Orlando FL. In this capacity, he led the Navy's efforts to establish the inaugural Operation Blended Warrior (OBW) at I/ITSEC, and remains involved in all aspects of future OBW events.

David Kotick - NAVAIR Esteemed Fellow: Mr. Dave Kotick is a nationally recognized expert in the field of Modeling and Simulation (M&S). He currently serves as the Principal Modeling and Simulation Engineer, NAWCTSD, Advanced Simulation, Visual and Software Systems Division. He has over 30 years of experience in the Navy M&S Research and Development arena. His works have been published in technical journals, conference proceedings and NAVAIR technical and special reports. He currently holds multiple patents (pending and granted) in the fields of digital communications and simulation technology. Mr. Kotick holds B.S. and M.S. degrees in Electrical Engineering from the University of Central Florida.

Gary Fraas: Mr. Gary Fraas presently serves the M&S community as an independent consultant specializing in engineering, program planning & management, and business development and represents the National Training and

Simulation Association as the lead for Operation Blended Warrior. Previously, Mr. Fraas was a career Navy civilian for 39 years and most recently served as the Advanced Simulation, Visual & Software Systems Division Head at NAWCTSD. Mr. Fraas has a M.S. in Computer Engineering from UCF, and a B.S. Electrical Engineering from Michigan State University.

Courtney Dean: Courtney Dean is a Senior Scientist with Aptima, Inc. He has experience in survey development, job analysis, and test construction and validation, with a focus on rating convergence in assessment centers. He is also the A-Measure(r) Product Manager where his responsibilities include leading the development of customized performance measurement tools to support warfighters' assessment of live and simulation-based training. He holds an MA in Applied Psychology from the University of West Florida.

Washington, We Have a Problem: The Foundation for Live Virtual Constructive (LVC) Exercises Requires Fixing!

John M. Kent Gritton,
David M. Kotick
Naval Air Warfare Center,
Training Systems Division
Orlando, FL
john.gritton@navy.mil;
david.kotick@navy.mil

Gary R. Fraas
M&S Strategic Partners, LLC
Maitland, FL
gfraas@cfl.rr.com

Courtney Dean
Aptima, Inc
Woburn, MA
cdean@aptima.com

BACKGROUND

Operation Blended Warrior (OBW) was conceived as a multi-year, Live-Virtual-Constructive (LVC)-focused special event for I/ITSEC 2015. The premise for the event is that the level of effort (time and personnel) to develop LVC virtual environments, and the subsequent integration of disparate systems within, has only slightly improved since the first integrated event in 1992. Loper, M., Goldiez, B., and Smith, S. (1993) describe similar challenges for the first I/ITSEC integration event with a comparable number of participants, systems integrated, and time required (Table 1). While individual capabilities used with and within these virtual environments have improved, the foundational development and integration efforts have not. Stated another way, despite the clarity in the LVC Architecture Roadmap (Henninger et al, 2008), why has LVC not progressed further toward the "plug 'n play" paradigm?

Table 1. 1992 v 2015 I/ITSEC Event Comparison

	1992	2015
Preparation time	8 months	9 months
Number of participants	28	31
Number of systems	41	47
Number of pre-I/ITSEC test weeks	1	3
Number of vignettes	2	15

Three overarching objectives were developed as a result of OBW concept analysis:

1) Document activity and challenges uncovered to the extent possible. Use data to inform potential solutions that would improve the ratio of time and effort to create an integrated LVC environment to the time and effort spent in LVC environment execution.
2) Leverage the collective LVC intellectual capital at I/ITSEC to help determine potential solutions to uncovered challenges. Create OBW working groups and establish a multi-disciplinary Integrated Product Team (IPT) to accomplish same. Create an organizational construct that provides NTSA data to actively advocate for newly identified potential LVC solutions.
3) Ensure that the NTSA/IITSEC organizational constructs created are scalable beyond initial targeted LVC challenges (construct should support other M&S community challenges such as cyber warfare, unmanned vehicles, and robotics, to name a few).

OBW was born out of a directive to invite conference attendees (government, industry, and academia) to interconnect on the show floor using a government supplied network infrastructure. The concept of OBW grew from some basic precepts: participants are limited to US persons only during the first year; participants must have a presence on the exhibit floor; the network infrastructure must be representative of real world capabilities; and, no limits on simulations or capabilities to be integrated within OBW. An overarching scenario of a contested Humanitarian Assistance (HA)/Disaster Relief (DR) in support of a friendly nation was developed. The scenario involved insurgents with hostile nation support taking advantage of a friendly nation's natural disaster as the result of a Black Swan event. The vignettes employed were crafted to showcase participant capabilities and arranged timewise to be chronologically logical. HA/DR was selected as the overarching scenario to enable creation of vignettes that complemented whatever simulation or capability a participant desired to integrate and showcase. While the network was representative of real life LVC architecture (albeit limited to the I/ITSEC locale), and representative platform and weapon capabilities were employed in the vignettes, OBW departed from the norm by not creating the vignettes from a pre-determined training objective, nor dictating/pre-selecting the systems to be employed.

While the as yet undetermined LVC event at I/ITSEC was announced 4 Dec 2014, the development team and OBW concept was not approved until 16 Jan 2015. Integral to the approved concept were focus areas deemed worthy of concentration when uncovering the challenges to LVC development/execution. A four year plan (Table 2) was established whereby a set of the focus areas would be addressed each year; each succeeding year would add to the previous year's focus areas. OBW 2015's focus areas were standards, after-action review, and cyber. The fourth year was designed to measure our advancement to a Plug 'n Play environment and use of enterprise solutions.

Table 2. Planned OBW Focus Areas

Focus Area	I/ITSEC 2015	I/ITSEC 2016	I/ITSEC 2017	I/ITSEC 2018
Baseline	X	X	X	X
Common protocol standard (common data standards) / SAF	X	X	X	X
Distributed debrief / AAR	X	X	X	X
Ops in a contested environment / Cyber	X	X	X	X
Performance measurements (How / What)		X	X	X
Multi-level security / Cross-domain solution		X	X	X
Distributed exercise planning		X	X	X
Exercise, network, comms management (coalition incl)			X	X
Presentation environment (control / mgt / debrief)			X	X
Role players / event based control			X	X
Persistent, consistent, rapid turn, plug 'n play Enterprise solutions (guards, gateways, etc)				X

From 16 Jan to 30 Nov 2015 (317 days), the design, organization, creation, and development of the OBW concept took place. The formal announcement of the special event and call for participants took place 4 Mar 2016. After 39 submissions by interested organizations, OBW 2015 supported 31 participants and integrated 47 unique systems. Reasons cited for the ~20% de-commitment to OBW include: time and expense of participation; timing of event within an organizations' fiscal year (available resources already obligated); and internal reorganization of priorities.

The first of three participant planning meetings took place 2-4 June 2015 (181 days prior to OBW execution). The result of these planning meetings, and 17 ensuing participant conference calls, was the creation of 15 unique 30-minute vignettes that were executed during the week of I/ITSEC in five 90-minute blocks. Vignettes focused on showcasing participant capabilities and included operations around the following disciplines: emergency management, command and control, convoy, cyber, medevac, air to air combat, remotely piloted aircraft, close air support, amphibious assault, and strike.

ISSUES / LESSONS LEARNED

The challenges encountered and lessons learned span a variety of areas which will be addressed in the following categories: LVC Interoperability Standards, Network Analysis, Policy, Integration Testing, Terrain and Virtual Model Databases, Trainee Human Performance, Cyber, and I/ITSEC.

LVC Interoperability Standards

Within the M&S training domain, there are two principle standards from which to choose to allow simulation interoperability within LVC events: High Level Architecture (HLA) and Distributed Interactive Simulation (DIS). Both are IEEE standards (IEEE Std 1278™ and IEEE Std 1516™) but approach data interoperability differently. HLA manages data through a Run Time Infrastructure (RTI) using a federation-specific choice of a data exchange model (Federation Object Model or FOM) while DIS does so through strictly defined data packets. Even though HLA was mandated by the Under Secretary of Defense for Acquisition and Technology as the standard technical architecture for all U.S. DoD simulations on 10 September 1996, DIS is still widely used. Further, there are multiple RTI's (which don't interoperate) and FOM's from which to choose if pursuing an HLA solution. Once HLA users agree upon the data to be passed between simulations, different implementations of the RTI's by different manufacturers have resulted in significant incompatibilities because they write to the network differently (Ross, 2012). This has then resulted in the need for additional gateway and bridging technologies.

Without revisiting the pros and cons of HLA vs. DIS, the existence of and widespread use of both creates difficulties in integration/interoperability. OBW 2015 initially planned to use HLA 1.3 with the NGPro RTI and Naval Aviation Simulation Master Plan (NASMP) 1.4.15 FOM. The rationale for this choice was based on a number of factors, however there were immediate challenges and lobbying efforts to consider alternative RTI's and FOM's. Perhaps these efforts were amplified by the volunteer nature of OBW participation. Regardless, the lesson learned from this is that there is not a uniformly employed RTI nor FOM – all are optimized for specific applications.

After significant discussion during the first OBW planning meeting, the DIS 6.0 standard was uniformly accepted and implemented by all participants. This decision proved beneficial from two perspectives: 1) the relative degree of complexity of integration/interoperability within the OBW networked environment was reduced; and, 2) using data collected from DIS integration/interoperability provides a baseline of comparison from which to evaluate future OBW iterations employing HLA or other standards with higher degrees of complexity. Two different gateways (JBUS and AMIE) were employed to support simulations needing translation from HLA or TENA to DIS. Only one system using HLA was integrated into the network; no system using TENA was integrated.

The primary challenge OBW 2015 experienced with implementation of DIS 6.0 was in the interpretation of the standard. A small group of participants (2 of 31) relied on past experience within LVC events and they implemented what they anticipated vice what was requested. Another group of participants (7 of 31) encountered integration challenges with the network mode: they attempted to network in broadcast mode when multicast was the published approach. Both sets of challenges were readily and easily rectified, but indicative of the types of challenges that cause a spike in resources during LVC integration.

<u>Finding</u>: Interpretation of selected interoperability standard caused problems for at least 22% of participants.

Network Analysis

The OBW special event network was representative of various DoD LVC distributed training architectures. As in most LVC operations, data types and protocols are varied. In support of this large scale integration effort, several OBW VLANs and Ports were established to transport and route OBW information. (These included support for DIS, HLA, Cyber, Video, HTTP, TENA, and Management network segments/functions). The DTC also provided core and resource allocations for common LVC functionality (such as protocol bridging, SAF, Audio and Video routing, and Network management). This provided the DTC full Mission Control capabilities (central control for all vignettes, role playing, exercise control and coordination, technical oversight and a configurable viewing area).

Network data was captured by both industry and government partners during various phases of OBW testing and vignette executions. After all the OBW vignettes were executed, a data analysis phase provided the team insight as to the type of data being passed as well as error conditions that may have occurred. Below is a summary of data taken from OBW M&S segments utilizing network capture utilities and vendor supplied log analysis tools. Data is divided into two major categories: that captured during the actual demonstration events, and that captured during integration periods. Data is also subdivided into types of data (Entity (Air, Subsurface and Surface), Radio, EM, Underwater acoustics, Weapons, etc) within the variant collection periods. Non M&S data is also flagged with regard to type and possible contamination of the M&S VLAN segments.

Data was collected in an ad-hoc fashion i.e,, not all collected the same data nor for pre-set specific times. Because no specific structure was put in place for network data collection, not all performance periods were covered. However, enough data was collected and analyzed to give a representative traffic summary of the primary M&S VLANS during the special event. Using a variety of industry and government developed analysis tools, a characterization of the OBW networks primary VLANs are provided. The collected data spanned all five integration periods and five days of execution as follows:

1) Vignette 3 – Approx 26 min – Convoy
2) Integration Period 1 – Approx 8 min
3) Integration Period 2 – Approx 16 min
4) Integration Period 3 – Approx 30 min
5) Integration Period 4 – Approx 22 min
6) Vignette 7/8 – Approx 57 min – Fallon/Cyber
7) Integration Period 5 – Approx 31 min
8) Vignettes 13/14/15 – Approx 116 min – Landing/Assault/Strike

Prior to the start of OBW, a challenge predicted by many was that OBW would stress the bandwidth for the network, and potentially cause data transfer problems, if it was rated at 1Gb or less. The fiber optic network backbone selected for OBW was rated at 1Gb with each VLAN allocated 100 Mb of network bandwidth. Despite the moderate to heavy volume of traffic, M&S VLAN (DIS/HLA and other traffic) data consumed no more than 10% (peak) of the allocated VLAN band-width with an average of around 7% of the allocated amount. Accordingly, this sample of data analysis suggests that DIS network traffic is more efficient than anticipated.

Protocol data units within the OBW M&S space (Ports 6993/6996 and 6994) can be generally characterized and summarized as follows: 1) Entity, 2) Communication (Transmitter/Receiver), 3) Weapon (Fire/Detonate), 4) Emitter, 5) Acoustic, 6) Data (Set Data), 7) IFF, and 8) Other. Table 3 represents OBW M&S element distributions over the eight collected data sets/periods (vignettes are in bold).

Table 3. Collected OBW Data – M&S Element Distribution

	Entity	Comms	Weapon	Emitter	Acoustic	Data	IFF	Other
Vignette #3	92 %	3%	< 1 %	1 %	2 %	2 %	< 1 %	< 1 %
Integration Period #1	51 %	45 %	< 1 %	2 %	0 %	1 %	1 %	< 1 %
Integration Period #2	49 %	45 %	< 1 %	2 %	0 %	1 %	1 %	< 1 %
Integration Period #3	87 %	10 %	< 1 %	2 %	0 %	< 1 %	1 %	< 1 %
Integration Period #4	87 %	7 %	< 1 %	3 %	1 %	< 1 %	2 %	< 1 %
Vignettes #7/8	54 %	44 %	< 1 %	1 %	0 %	< 1 %	1 %	< 1 %
Integration Period #5	98 %	< 1 %	1 %	< 1 %	0 %	< 1 %	< 1 %	0 %
Vignettes #13/14/15	71 %	18 %	9 %	1 %	< 1 %	< 1 %	< 1 %	< 1 %

The OBW ‘Entities’ may be further subdivided as follows: Entity ‘Kind’ – Air, Surface, Land, Lifeform, Munition, and Other (Cultural, Environmental, Supply etc). As expected, this data varies with vignette type. Table 4 represents the percentage (and total packet count) of entity types out of the total number of entities per data collection period.

The data shown in Table 4 reveals a couple of large data anomalies worth addressing (highlighted in red). The root cause was traced to a non-consistent adherence to M&S standards. This data was traced to two OBW participants that published non-valid Entity type data packets (Entity-0). In both cases, the network policy (network VLAN and Port usage) was followed correctly, but a violation of the interoperability standard occurred. It is believed that a single application utilized in two exhibit floor locations may have caused the problem. While not readily apparent that malformed packets caused issues within OBW, malformed packets are known to have caused various errors on ‘other’ connected systems, and could have caused problems to OBW.

Table 4. Collected OBW Data – Entity Type Percentages

	Air	Surface	Land	Subsurface	Lifeform	Munition	Other	Number of Entity Packets
Vignette #3	53 %	2 %	1 %	0 %	37 %	4 %	3 %	614,198
Integration Period #1	85 %	3 %	7 %	0 %	2 %	2 %	1 %	137,531
Integration Period #2	90 %	2 %	6 %	0 %	0 %	1 %	1 %	245,589
Integration Period #3	89 %	2 %	7 %	0 %	0 %	1 %	1 %	425,167
Integration Period #4	85 %	1 %	1 %	3 %	0 %	8 %	2 %	239,765
Vignettes #7/8	90 %	4 %	1 %	0 %	0 %	5 %	< 1 %	527,288
Integration Period #5	16 %	< 1 %	9 %	0 %	7 %	< 1 %	**66 %**	563,998
Vignettes #13/14/15	35 %	1 %	40 %	0 %	15 %	4 %	**5 %**	1.394,985

As in most semi-constrained networks that are controlled by policy, violations will occur. The anomalies described above address situations where the policy was correctly followed, but an incorrect interpretation and implementation of the standard occurred. A number of different policy violations occurred during the OBW event when viewing the network from a global perspective. Looking at the similar VLANS described above from a network level, a total of 28,158,264 packets were captured across 306 minutes of recording time (yielding an average packet rate of 1534 packets / sec).

Of significance in the analysis of this data is that two thirds (67%) of the observed network traffic was unknown data, and thus, in some way, policy violations were occurring. The total M&S VLAN captured packets resolved to only one third of the total network traffic.

These 'unknown' data communications can be further divided into two categories: known communication messages and unknown communication messages. Only 2 % of the unknown data communications were comprised of known or valid formats and can be traced to typical Operating Systems (OS), user initiated applications, and other common/related communications placed on the 'wrong' VLAN (eg, Skype, Network Errors and Warnings, ARP, IPV6, and HTTP traffic). An amazing 98% of the unknown data communications were comprised of unknown formats. Further, almost two thirds of this network traffic (65%) used 10 different non-provisioned ports. Non-adherence to communications policy of this magnitude, coupled with previously identified policy violations, indicate a high potential for network / system errors to occur at the enterprise level.

It is outside the scope of this paper to further analyze policy issues surrounding data transfers. The identification of the scope of this challenge however, provides a valuable lesson learned to designers of OBW 2016 and other LVC events. A refinement to policy (to include vetting of additional protocols), and mechanisms required to help adjudicate a better network implementation, are planned for OBW 2016 in hopes of leading to a more robust integrated and distributed environment.

<u>Finding</u>: Bandwidth was not a limiting factor – only 10% of M&S VLAN segment was used. Participant non-adherence to published network policy resulted in 67% non-DIS data on M&S VLANs, and 65% of communications network traffic on ports not authorized for use during OBW'15?

Policy: Information Assurance

Information Assurance (IA) has become a necessary but burdensome schedule driver for LVC events. Platform capabilities and operational tactics, techniques and procedures are typically represented within LVC events; the protection of this information is critical. With the growing complexity and interconnectedness of the technologies employed in LVC events, the time it takes to review the architecture and processes employed have similarly increased. While OBW 2015 was conducted solely at the UNCLASS level, the need to follow IA processes was imperative for protection against malicious code, and other vulnerabilities and possible threats. Adhering to a formal IA process revealed a better understanding of the associated challenges. Baseline planning numbers for obtaining a 60 day Interim Authorization to Test (IATT) from the Naval Air Systems Command (NAVAIR) approval authority were 180 days for a closed network, and between 270 to 360 days for more complex networks that would include outside connectivity (internet, etc) and coalition members. The level of acceptable risk and degree of testing and documentation drives these planning numbers. Planning time for an Authority to Operate (ATO) requires in excess of one year. These planning numbers drove OBW 2015 to a very conservative closed network at I/ITSEC, but also highlighted the difficulties for future OBW events (IA participants for one OBW would need to be identified and a package prepared/submitted prior to completion of the preceding OBW).

Working with the NAVAIR approval authority (following DoDI 8510.01 among other guidelines), a process was implemented and actions taken that would better ensure IATT approval within the I/ITSEC planning cycle. Key risk reduction efforts included: maintaining a closed loop network; removing / destroying computer hard-drives after conclusion of the OBW 2015 event; and aggressive use of firewalls and tightly controlled network switches. In conjunction with these actions, the approval authority worked various aspects of the IATT package in parallel with mixed results. On the positive side, because of the parallel efforts, the total IATT timeline was 130 days (or ~72% of the overall planning cycle) – a 76 day savings. On the negative side, "locking down" the network architecture and design for an event this early in the planning cycle puts stresses on the management and engineering teams. Fully understanding all system capabilities and requirements prior to IA package submittal, which concomitantly impacts adjustments to those emergent requirements after package submittal, is difficult in a time constrained environment.

<u>Finding</u>: Early identification of key risk reduction efforts benefitted the IATT timeline.

Policy: International Traffic in Arms Regulations (ITAR)/Export Administration Regulations (EAR)

ITAR/EAR was the most surprising policy challenge of Operation Blended Warrior. International Traffic in Arms Regulations (ITAR) controls the export and import of defense-related articles and services on the United States Munitions List (USML). These regulations implement the provisions of the Arms Export Control Act (AECA), and are described in Title 22 (Foreign Relations), Chapter I (Department of State), Subchapter M of the Code of Federal Regulations.

While aware of the US State and Commerce Department's respective regulations, the inclusion of controlled items (e.g., systems, software applications, data and services as defined by the Secretary of State for purposes of export and temporary import control and identified by the U.S. Munitions List specified in part 121) connected to the OBW network created a potential situation whereby a "deemed export" could occur. The obligation to obtain an export license from the Dept. of Commerce Bureau of Industry and Security (BIS) before releasing controlled technology to a foreign person is informally referred to as a deemed export. Release of controlled technology to foreign persons in the U.S. are "deemed" to be an export to the person's country or countries of nationality and is found in 734.2(b) of the EAR. To prevent "deemed exports" (US Department of Commerce, Bureau of Industry and Security website germane), a number of provisions were put in place, and each participating company and military organization's empowered export control official signed a formal Participation Agreement by certifying the following:

- All personnel associated with OBW had up to date ITAR training
- Access to the OBW network and systems on the network was limited to US citizens
- All controlled items that were to be connected to the OBW network were identified
- ITAR controlled items would not display controlled data, would not transmit controlled data across the network, and would not be accessible by other participants connected to the OBW network

- Navy pre-configured network switches and connected to the OBW network by the participant would be protected from tampering and isolated within their booth to prevent unauthorized access

Two of the 31 participants in OBW 2015 were international companies. They were determined to be eligible to participate while operating under the following constraints: one was connected only to monitors in the Distributed Training Center (did not connect to the network); the software of the other participant was provided to the other US participating organizations, was only operated by US citizens, and operated on a segmented VLAN. Fifteen of the 47 systems connected to the OBW 2015 network had ITAR controlled components embedded. As a result of the aforementioned stringent OBW policies, and because the ITAR controlled items were under their close control, no "deemed export" was known to have occurred.

A separate lesson learned involved the need for a process within US government entities to approve security actions relative to ITAR controlled components within a networked environment. US companies have "ITAR empowered officials" to approve initiatives relative to ITAR. A similar construct does not exist within US government entities; the closest approximation is ITAR approvals for Foreign Military Sales (FMS). A networked environment like OBW 2015, however, requires protection of (not sale of) ITAR controlled components. With no "ITAR empowered official" or existing process tailored to US government organizations, a hybrid public release process was developed for Naval Air Warfare Center Training Systems Division (NAWCTSD). For OBW 2015, the NAWCTSD's "ITAR empowered official" was the NAWCTSD Commanding Officer. Upon the advice of the entity's legal counsel, which was informed by an assessment of the protection of the ITAR controlled component from the Engineering Director, Security Director, and Public Affairs Officer, the Commanding Office approved OBW ITAR actions to prevent a "deemed export" of controlled components.

<u>Finding</u>: Integrated events have the potential to expose internal system code to connected participants. ITAR/EAR approvals for integrated events must consider both cyber and physical safeguards to prevent exports.

Integration Testing

Development of, implementation of, and adherence to a formal test plan to ensure proper LVC integration/interoperability is of vital importance to the success of an LVC event. For OBW 2015, testing included 5 basic steps from 20 Oct – 30 Nov (9 days architecture, 21 days integration, 3.5 days integration/validation). The steps included: Distributed Training Center (DTC) network architecture testing, system-to-system "ping" tests, enumeration tests, load tests, and finally, on-site integration validation tests.

DTC network architecture testing was the initial step. Prior to connecting participant systems to the DTC network, each component within the network architecture was tested independently. Further DTC network testing included all components within a workstation, then as a complete DTC, and finally with increased loads on the components. Architecture testing took 9 days to complete. A principle challenge encountered involved stability of various Semi Automated Force (SAF) applications on the network.

Participant integration / interoperability testing with the DTC network (system-to-system "ping" tests, enumeration tests, and vignette load tests) was conducted in person at a facility in Orlando. To better manage space and testing times over the available three weeks, participants were divided into three groups based on the vignettes within which they were participating. Those groups were: aviation centric vignettes, cyber and human centric vignettes, and C2/maritime centric vignettes. Each group consisted of seven to ten participants and tests were performed over the span of four days during their assigned week.

The principle challenges uncovered in "ping"/connectivity testing centered on using the incorrect network mode (7 participants as discussed above), communications settings (8 participants; 1 comms modulation, 7 network mode), video settings (all participants; fidelity balancing for presentation purposes), and gateway/architecture configurations (2 participants with 1 needing to re-architect their integration plan).

Multiple challenges were uncovered during enumeration testing. The most common being disparities between the entities in JSAF and NGTS (missing in one, different enumerations, or duplicate entities). Three challenges are worth noting. First, "dead" NGTS aviation entities would spin to a negative elevation (below earth surface) in JSAF. A form of ground clamping was employed to rectify. Second, there were elevation mismatches between NGTS and

JSAF. It was discovered that the NGTS database was set for meters, but the data was entered in feet. And lastly, one participant's entities were displayed in a frozen entity state; the systems PDU settings were not in sync with the rest of the network and needed re-setting. While functions normally addressed in a Federation Agreement Document (FAD) were discussed in planning meetings, a specific OBW 2015 FAD was not developed.

The DTC network was very stable throughout testing and on the exhibit floor. Individual vignette load testing, once identified challenges were addressed, was accomplished during the off-site integration period without further incident. A challenge did arise, however, during I/ITSEC on-site integration validation tests. The first time all 31 participants were on the network simultaneously, the network experienced a rapidly expanding entity swarm that caused many of the networked systems to "crash." It was uncovered that two of the participants were using different versions of the same gateway; a gateway that communicates with its' peers and performs load-balancing between them. The incompatibility between the two versions caused them to create more and more entities in an attempt to load-balance. The issue was remedied by upgrading the older of the two gateway versions to match the newer version.

For OBW 2016, different testing processes (distributed and on-site) are being investigated in an effort to preclude reoccurrences of these challenges. Additionally, a more formalized FAD development process is planned.

<u>Finding</u>: Inclusion of distributed pre-event LVC integration testing and formalized documentation into plans and processes should reduce on-site integration challenges.

Terrain and Visual Model Databases

Perhaps the most significant challenge to LVC events (rivaled only by HLA's RTI/FOM issue discussed above) is the lack of uniformly accepted databases (terrain, EW, Cyber, etc) for use within virtual environments. Multiple factors go into the selection and creation of virtual terrain: Digital Elevation Model, density of data (PPI - postings per inch), geo-specific or geo-typical, cartographic references, methods of measurement (meters, feet, AGL, MSL, etc) and resolution of data. Each program or platform creates/employs a terrain database that is optimized for their particular use, training mission areas and warfare domains. While understandable when examined in isolation, integration challenges occur when conducting combined or joint operations. While the selection of terrain that supports airborne, ashore, and afloat simulations of varying resolution was potentially an artificial aspect of OBW (other LVC environment providers would dictate the terrain and offset integration costs), the integration of multiple formats to create a common environment remains a universal challenge.

For OBW 2015, the NAVAIR Portable Source Initiative (NPSI) data was selected as the source for terrain for the majority of the OBW region (southwest USA). The resolution of NPSI data, however, was soon determined to not support vignettes requiring higher fidelity graphics. To compensate, several participants created and shared higher resolution subsets of the OBW region using organic capabilities. The time and effort participants used to create the higher resolution terrain and associated features, and to modify the NPSI data to their needs, eclipsed even their time spent during integration testing (based on anecdotal reports from 24 participants).

A similar challenge occurred with the model databases. A master enumeration list to include unique entities was tailored from an existing Navy baseline. Despite a sound approach and effort, challenges typical of any LVC event were uncovered: missing entities or need to substitute entities, mismatched entities (color or entity version function), and lack of operable entity sub-systems (guns, chaff, etc). The task of rectifying each conflict to the maximum degree possible comprised a large percentage of enumeration testing. Though not specifically noted as a challenge in OBW 2015, skeletal animation, shaders, articulation and other similar conventions are not standardized and, as a result, could pose issues during integration. This is the model composability issue that Davis & Anderson (2003) address to great effect.

<u>Finding</u>: Single terrain and model databases to support disparate warfare domains (i.e., air, surface, and electronic warfare) and emerging warfare domains (i.e., cyber) do not exist. Event by event development is a schedule driver.

Trainee Performance Measurement

The data generated within a networked environment like OBW 2015 is, by definition, of a quality and quantity beyond the scope of any single simulator. Performance measurement collection efforts show great promise in LVC events.

Significant behavioral information extracted from the context of the scenario (being open and distributed), and the content of the scenario (the prescribed events), can support increases in mission readiness while decreasing the cost of military training.

For context, many simulators produce excellent content for operator consumption, but publish, or make machine readable, very little. Specifically, most lack sufficient operator input data to support automated performance measurement. Trainers are built around the user experience; providing rich stimuli and content to the operator, but the operator's actions often do not carry a data signature. As a consequence, performance measurement is typically limited to entity state changes and a human observer's notes. To better leverage the LVC events performance measurement potential, a purposefully configured outside agent was networked in. A vast amount of operator behavioral data was collected during OBW without impacting the network performance or architectural design.

Though performance measurement data were collected across all fifteen vignettes, two of the vignettes were deemed best to illustrate the value of LVC event performance measurement collection: the Air-to-Air engagement and the Air Lift vignettes. Between these two vignettes, nine (9) simulated assets were tracked: four (4) Blue and (5) Red assets, respectively. An additional asset, a ground-based SA-6 Surface-to-Air Missile (SAM) platform was targeted by Blue and thus tracked.

For these vignettes, performance measures focused on the Air-to-Air engagements between Blue and Red assets. Blue assets were expected to target, engage and destroy Red assets while adhering to Hard Deck restrictions (do not drop below 5000 meters). Table 5 features a list of captured performance measures.

The challenge of performance measurement capture in most networked events lies not in the collection of individual entity states, but in combining the data in such a way to elicit a better understanding of an individual's performance, and ultimately their readiness. In many cases, individual state measures served as triggers so that a different computational measure can assess a particular skill, or competence.

Table 5. OBW Air Asset and Air-to-Air engagement measures.

Single aircraft measures	
Alive – flag if entity alive	Force ID – Entity's force ID
Destroyed – flag if entity destroyed	Hard Deck – flag if entity violated the hard deck
Speed – entity speed	Health – Percentage of health
Air-to- Air measures	
Range – distance (m) between entities	Angle Off – Angle off in degrees
Engaged – flag if entities < 20,000m apart	Shot – Flag if Entity #1 shot at Entity #2
Disengaged – flag if entities >20,000m apart	
Force measures	
Force Preservation – ∑ current force Health/∑ total force health	Efficiency of Fires – % shots hit/shots taken
General	
Engaged – Flag if any REDFOR is within 5,000m of BLUFOR	Collateral Damage – Force preservation for neutral/other forces
Intensity – Count of missiles currently in air	

Figure 1 represents our primary air-to-air engagement assessment. At a distance of <20,000m, assets are "Engaged". As they engage, dominance is assessed (Angle Off), representing which air asset gains the upper hand, goes on the offensive, launches ordnance and ultimately destroys the other aircraft (Shot Flag). Engagements such as the one illustrated in Figure 1 were tracked across seven separate air-to-air engagements spanning two vignettes.

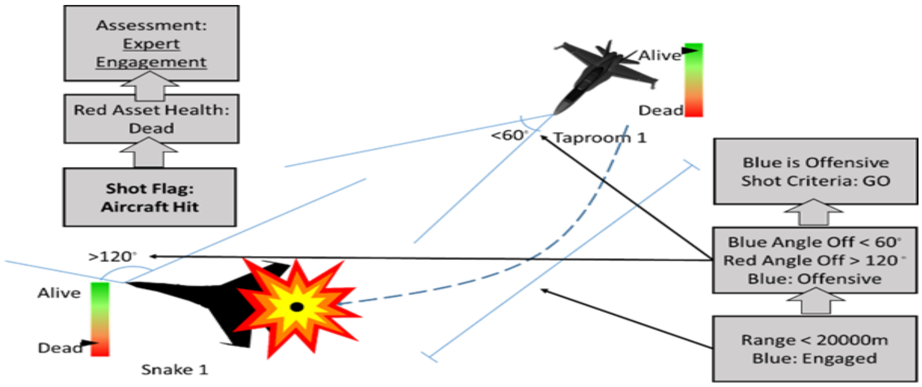

Figure 1: Illustration of Measures and Assessments for Blue Assets

Unobtrusive collection of critical performance measurements in an environment as complex as OBW 2015 is great. Although challenging, only minor administrative issues were uncovered in the collection of this data demonstrating the viability of the approach. Its value to the instructors and performing units is undeniable: the ability to systematically walk through mission replay, targeting evidenced behaviors/actions that need emphasis or correction with minor network adaptation is valuable on multiple levels. Performers gain a deeper understanding of their performance; instructors obtain both quantitative and qualitative data on their personnel; and measured improvements to readiness are available to participating units.

As the complexity of the mission sets and LVC networked environments grow, it is imperative that performance measurement capabilities keep pace. Future work in this space will include expanding the depth and breadth of performance measures collected – not only for aviation vignettes, but across different mission sets and platforms. Planning is underway in these regards for OBW 2016.

Finding: Quality performance measurement of aviation events possible with minimal/no impact to architecture.

Cyber Operations

Following the mantra “train as you would fight”, it is imperative that operations in a cyber contested environment are fully integrated within LVC events. There are technical, cultural and policy challenges to accomplishing this effort. Most LVC events deal with the integration of systems that are principally kinetic in nature. As the evolution of M&S capabilities have grown, so too have systems that can address non-kinetic missions (like EW, Cyber, etc). The technical challenge of integrating the two systems together in a LVC environment comes from differing standards in how to represent the non-kinetic effects and non-kinetic terrain. Specifically, the language being sent that identifies the activity, the ability for the receivers to interpret the language, and the effect database fields required on both sides to hold these integration conversations are known issues. As for cyber, cultural and policy issues exist and are intertwined. Examples include: an over confidence that our IA practices will negate the cyber threat to our systems; a belief that the cyber mission will interfere with the “primary” training objectives; and, a belief that we cannot integrate cyber effects into the network without injecting risk to the network.

OBW 2015 provided two cyber vignettes to address these challenges. A sub-set cyber-vs-cyber event ran parallel to the main event; the results of the cyber event were ported over to an ATO approved Network Effects Emulation System (NE2S) that was installed on selected participant systems within the main event. NE2S allows the introduction of modelled cyber effects into the event without risking any other training objectives or introducing harmful materials on the network. The first vignette demonstrated effects to communications systems (disrupting tactical communications between two of the various live entities within the vignette); the second to visual systems (disrupting one of the multiple UAV video feeds within the vignette).

While minor, the principle cyber related challenge uncovered in OBW 2015 was within the cyber-vs-cyber portion of the event; specifically, the integration of the cyber participants using the Cyber Data Exchange Model (DEM) when one of the key intended systems became unavailable for participation at the last moment. This was not a technical issue, but rather one of familiarity with the still unaccredited DEM. There were no noted challenges with the NE2S system.

Finding: Cyber warfare integration into LVC events supporting the "train as you fight" maxim are doable, and should become more prevalent as interoperability and database standards address emerging warfare domains.

I/ITSEC Feedback

The information presented so far is predominantly representative of activities and challenges normally found in LVC events. But like any event, there were venue-specific challenges; while not all venue challenges are directly relevant to LVC events, many of the challenges remain indirectly relevant. In addition to internally collected lessons learned, all participants were asked for feedback to better improve OBW for future years.

Feedback received on challenges to the OBW event can be characterized as: planning, scheduling, integration/network, development, presentation and location. The earlier identification of technical information (terrain, models, standards, ports and protocols) was cited in the planning category. Better scheduling of practice sessions and vignette dry runs was a consistent complaint. While the plan included 12 hours for practice sessions, 3.5 hours of troubleshooting / fixing the "crash" mentioned in the integration section took precedence and reduced available practice time by 30%. Increased levels of "live" integration was strongly recommended; as was earlier and enforced integration testing to help preclude system "crashes". Consistency in the manner of vignette development was a recurring theme; a valid critique given that 8 different vignette leads developed the 15 OBW vignettes. While the presentation of the vignettes met OBW objectives and attendee expectations, there is much room for improvement in the use of visuals and narration (presentation). Lastly, there was a desire to consider more centrally locating the event on the I/ITSEC exhibit floor, and to alter the vignette presentation format.

On the positive side, there was unanimous response that OBW 2015 met or exceeded participant expectations. Key points cited for these responses included: valuable internal/external market research ("operationally relevant test bed" that could "not be replicated in their lab"); increased networking opportunities ("created future teaming arrangements"); increased booth traffic and product exposure (including "increased Flag/General Officer visits); ability for developers to see firsthand how their products were used, and performed in an LVC environment; and, the high degree of collegiality and collaboration amongst all participants ("environment and temp license sharing" and "valuable LVC experience learned from 'graybeards'".

Finding: OBW (as a LVC integration sandbox and leveraging I/ITSEC intellectual capital) shows great promise in government/industry/academia collaboration to improve time and resources needed to create / execute LVC events.

CONCLUSIONS AND NEXT STEPS

OBW 2015, as a representative LVC event, proved that a significant level of effort (time and personnel) was required to develop the virtual environments and integrate the disparate systems within. The challenges uncovered were not atypical -- and mostly expected. The knowledge learned from development and execution of OBW 2015 has not only provided a baseline from which to measure changes made to future OBW's, but also provided key insights into the areas worthy of additional scrutiny.

New for OBW 2016 is the creation of a multi-tiered IPT structure to address the future direction of Operation Blended Warrior in the most efficient manner possible. Key positions within the Operational IPT (responsible for development and execution of OBW) which were created to optimize the development and execution of the event were: Terrain Database Selection; Integration Testing; Production Director; and Focus Area Subject Matter Experts (SME's). Improvements to level of effort required for terrain and model selection, distributed and on-site integration testing, and aural/visual presentation of the vignettes are expected from the Operational IPT.

Key outcomes from the Strategic IPT include: better defined LVC objectives and metrics from which to measure OBW success; a refinement of OBW focus areas; and, development of government-industry-academia collaborative approach(es) to resolving (or mitigating) the foundational LVC challenges uncovered during OBW events.

Based on data gleaned from OBW 2015, four key areas merit further scrutiny to determine what actions, if any, can and/or should be taken to improve time and resources required to develop / execute a LVC event:

- Policy: are current policies and approval process for IA properly aligned to LVC event risks?
- Standards: are interoperability standards acceptable in their current state, or are there too many, or are they too open to different interpretations?
- Terrain and Model Databases: are the current terrain and model databases adequate, or is a new approach needed to more quickly integrate disparate warfare domains (i.e., air, surface and electronic warfare) and newly emerging warfare domains (i.e., cyber)?
- Integration Testing: are there proven integration testing processes (incorporating both distributed and on-site testing) that would significantly reduce or preclude time consuming integration challenges?

For the Strategic IPT to be successful (i.e., potential for widespread adoption of recommended solutions), analysis of these areas for improvements require subject matter experts from a combination of government, industry and academic backgrounds. It is with this goal in mind that the aforementioned Strategic IPT was created, carefully staffed, and addressing challenges like those mentioned above. With more efficient use of LVC development/execution time and resources as the goal, OBW 2016 and beyond will become the "sandbox" to implement and analyze not only Strategic IPT recommended approaches, but those from various DoD components.

ACKNOWLEDGEMENTS

The participants for the inaugural Operation Blended Warrior at I/ITSEC 2015 were (in alphabetical order):

132 Wing, Det 1, Distributed Training Operations Center (US Air Force National Guard); The Aegis Technologies Group Inc.; Alion Science and Technology Corporation; Aptima, Inc.; BGI, LLC; The Boeing Company; Bohemia Interactive Simulations; Booz Allen Hamilton; C4I Consultants; CAE; Camber Corporation; Cubic Global Defense; Engineering & Computer Simulations, Inc.; FlightSafety International; Immersaview; L-3 Communications, Link Simulation & Training; Lockheed Martin Mission Systems and Training; Marine Corps Systems Command, PM Training Systems; Naval Air Systems Command; Naval Air Warfare Center Training Systems Division; Office of Naval Research; PLEXSYS Interface Products, Inc.; QinetiQ Training and Simulation; Rockwell Collins, Simulation & Training Solutions; SAIC; Soar Technology, Inc.; TRU Simulation + Training, Inc.; US Pacific Command Cyber War Innovation Center; US Navy Surface Warfare Officer School; VT MAK; and ZedaSoft, Inc.

For their tireless and exceptional contribution to Operation Blended Warrior, special acknowledgement to:

Navy Lead for Systems Engineering, OBW 2015, Mr. Troy Bennett, and
Lead for Scenario Development, OBW 2015, Dr. Angus L.M. Thom McLean, III.

REFERENCES

US Department of Commerce, Bureau of Industry and Security 2016 website
http://www.bis.doc.gov/index.php/policy-guidance/deemed-exports

Davis, P.K., & Anderson, R.H. (2003). *Improving the Composability of Department of Defense Models and Simulations*. Rand Monograph MG101, 2003.

Department of Defense Instruction 8510.01, *Risk Management Framework (RMF) for DOD Information Technology (IT)*, 12 Mar 2014 (ch1 24 May 2016)

Henninger, A.E., et al. (2008). *Live Virtual Constructive Architecture Roadmap (LVCAR) Final Report*. M&S CO Project No. 06OC-TR-001, September, 2008.

Loper, M., Goldiez, B., and Smith, S. (1993). *The 1992 I/ITSEC Distributed Information Simulation Interoperability Demonstration.* Proceedings of the 1993 Interservice/Industry Training, Simulation and Education Conference.

Ross, P. (2012). *Comparison of High Level Architecture Run-Time Infrastructure Wire Protocols – Part One.* SimTecT 2012 Conference Proceedings.

Under Secretary of Defense for Acquisition and Technology Memorandum, "*DoD High Level Architecture (HLA) for Simulations*," 10 September 1996.