Submission to: 19th ICCRTS

Title: Need for Agility in Security Constraints for Distributed Simulation (024)

Topics: Primary Topic: 5. Modelling and Simulation,
Alternates: 4. Experimentation, Metrics and Analysis, and
1. Concepts, Theory, and Policy

S. K. Numrich, Ph.D., CMSP
Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311
Email: snumrich@ida.org
Phone: 703-845-6807

Amy E. Henninger, Ph.D.
Technical Advisor
Center for Army Analysis
6001 Goethals Road
Ft. Belvoir, VA 22060
Email: Amy.e.henninger.civ@mail.mil

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **JUN 2014**	2. REPORT TYPE	3. DATES COVERED **00-00-2014 to 00-00-2014**
4. TITLE AND SUBTITLE **Need for Agility in Security Constraints for Distributed Simulation**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Institute for Defense Analyses,4850 Mark Center Drive,Alexandria,VA,22311**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the 18th International Command & Control Research & Technology Symposium (ICCRTS) held 16-19 June, 2014 in Alexandria, VA. U.S. Government or Federal Rights License

14. ABSTRACT
The network is a critical enabler for distributed simulation, a mainstay for test and evaluation, acquisition, and training. Realistic Joint training frequently involves multiple, private networks and entails the stimulation of command and control systems. One of the most significant capabilities trained in Joint, distributed simulation is the conduct of Joint command and control for missions and major operations. A delicate balance exists between policies and processes that mitigate security risks and the need to expose the force to new capabilities and a variety of mission-oriented scenarios. Certification of software and other security agreements adds weeks and months to the preparation time for exercises. When scenarios require communication across security domains and include collaboration with international partners, security issues become more complex and delays increase. The rapid evolution of communication and computational media (web-based operations, mobile communication, cloud computing) and the strategic orientation toward expeditionary operations create an even greater need for agile processes. This paper will examine some barriers to the vision of a persistent, distributed training environment and point to several proposed solutions.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**23**	

Need for Agility in Security Constraints for Distributed Simulation

ABSTRACT

The network is a critical enabler for distributed simulation, a mainstay for test and evaluation, acquisition, and training. Realistic Joint training frequently involves multiple, private networks and entails the stimulation of command and control systems. One of the most significant capabilities trained in Joint, distributed simulation is the conduct of Joint command and control for missions and major operations. A delicate balance exists between policies and processes that mitigate security risks and the need to expose the force to new capabilities and a variety of mission-oriented scenarios. Certification of software and other security agreements adds weeks and months to the preparation time for exercises. When scenarios require communication across security domains and include collaboration with international partners, security issues become more complex and delays increase. The rapid evolution of communication and computational media (web-based operations, mobile communication, cloud computing) and the strategic orientation toward expeditionary operations create an even greater need for agile processes. This paper will examine some barriers to the vision of a persistent, distributed training environment and point to several proposed solutions.

1. Introduction

Distributed simulation has become a mainstay for a number of communities within the Department of Defense (DoD). For test and evaluation (T&E) distributed simulation provides a common execution environment capable of linking one or more test ranges and with actual equipment (live assets) being tested. In like manner, the training community depends upon distributed simulation to provide the common synthetic environment to link instrumented training ranges with simulators of various types all participating in the same, mission-oriented scenario. This common operational environment is displayed on military command and control (C2) systems to permit the higher-echelon staffs to exercise command and control and to “train as they fight.”

A. The Training Environment

The training community divides simulated exercises into three categories: live, virtual and constructive. The live component refers to the simulation of warfare in which humans employ actual equipment and whose actions are reported and displayed as the common operational picture on command and control displays such the Command Post of the Future (CPOF) – real humans in a real environment. Virtual simulation is most readily thought of as simulators in which the human interacts with a synthetic or computer-generated environment through actual systems or in simulators – real humans interacting in a computer-generated environment. In constructive simulation, simulated humans interact with a computer-generated environment. While these distinctions are important to understand, most distributed simulation exercises involve virtual and constructive or live, virtual and constructive simulations running concurrently and interacting with each other. The mix of live, virtual and constructive (LVC) simulation is becoming the accepted means of accomplishing multi-echelon training in a realistic environment. It augments and enhances live training by affording individuals and units the opportunity to explore new concepts and train in environments, or with equipment, that would otherwise be inaccessible. A major LVC event is often characterized by participation of more than one service; inclusion of coalition partners; and a need to communicate across more than one security domain. The purpose of this section is to examine the complexity of the network infrastructure required to support Joint distributed training exercises.

The distributed simulation environment that enables LVC exercises makes a number of relatively unique demands upon the network infrastructure. The network has to be stable with known, acceptable latencies; it must handle high volumes of traffic that surge at irregular intervals; it must be capable of handling potentially thousands of multicast groups; and it must be capable of working across a wide variety of security devices (edge protection devices – typically firewalls, cross-domain security devices like Radiant Mercury switches and rule-based security guards for working with coalition partners). For these reasons, among others, distributed simulations are normally run on dedicated networks.

1. Evolution of the Network Environments

The first massive, distributed simulation exercise was coordinated and run by US Joint Forces Command (JFCOM) in 2002. Named Millennium Challenge 2002 (MC02), the exercise involved over 13,000 personnel at locations across the United States using more than forty individual simulations working together to create the operational

environment fed back into Joint and Service situational awareness displays.[1] The use of a private, high-speed, experimental, ATM-SONET network researched and developed by DARPA simplified many of the certification and accreditation issues present for operational networks. In the aftermath of MC02 and with indications from the training community that they would seek additional opportunities for distributed joint training and experimentation, JFCOM embarked upon the creation of an environment that would reduce the overhead resources needed to plan and execute such events. The Distributed Continuous Experimentation Environment (DCEE) proposed to "reduce overhead by creating a standing simulation infrastructure, including the Joint Experimental Federation (JEF) [the set of simulations or federates used in MC02] embedding new models in the existing federates, and linking with other federations." [2] In addition to developing a large set of warfighting models together with supporting and compatible terrain databases, JFCOM initiated the development of a network infrastructure to support the distributed execution of simulation events, the Joint Training Enterprise Network (JTEN).[3]

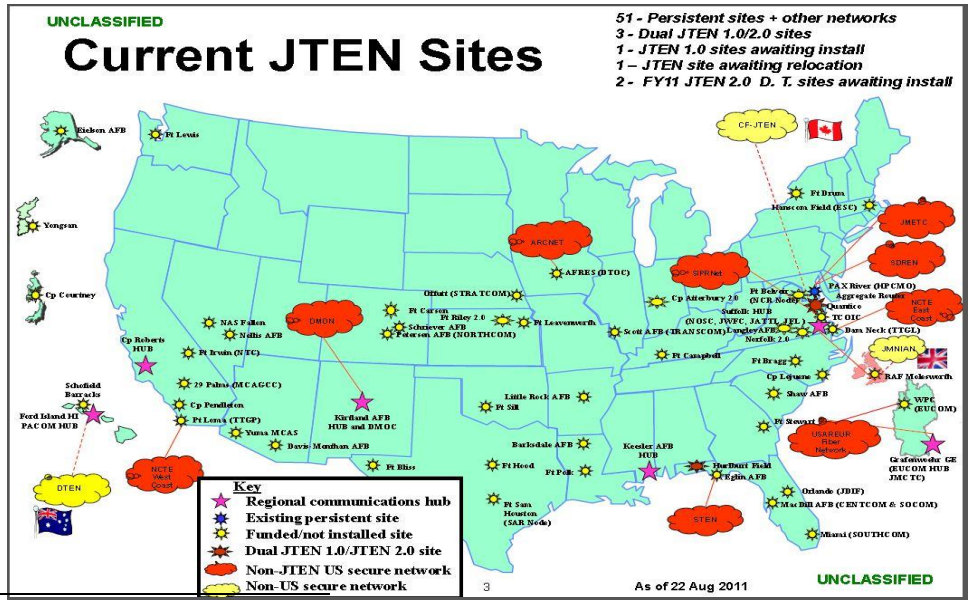

Figure 1 JTEN site map as of August 2011 [Vinett 2011, slide 3]

[1] Experimental Federation." Proceedings of the 2002 Interservice/Industry Training, Simulation and Education Conference, Orlando, 2002

[2] Ceranowicz, A., Dehncke, R., Cerri, T., "Moving toward a Distributed Continuous Experimentation Environment," Proceedings of the 2003 Interservice/Industry Training, Simulation and Education Conference, Orlando, December 2003

[3] Vinett, J., "Joint Training Enterprise Technical Updates, " Worldwide Joint Training and Scheduling Conference, September 2011 http://www.dtic.mil/doctrine/training/conferences/wjtsc11_2/working_groups/4.%20%20WJTSC%2011-2%20JTE%20WG%20-%20JCW%20JOSE%20Technical%20Update%20WJTSC%2011-2.pdf

The JTEN is one of many networks that form the DoD's Information Network (DODIN). The clouds in Figure 1 indicate the JTEN Points of Presence (PoPs) where JTEN can connect to other private networks in the DODIN. An examination of the JTEN nodes reveals that most of the network nodes (yellow stars) are at US Army sites. Both the US Air Force and the US Navy chose to create their own simulation network infrastructure to link their Service sites. This decision simplified the management of events using their networks and reduced the number of authorities involved in certifying and accrediting the applications using their networks including simulations, test and training ranges, and simulators. The impact of consolidating networked assets under a single management will be discussed in detail later in this paper.

The execution of a large, distributed training event, whether initiated through the Joint National Training Capability (JNTC) or one of the Service distributed training centers, normally involves numerous networks each of which brings to the event unique simulations, ranges or simulators. As an example, the US Air Force routinely conducts distributed training events out of its Distributed Mission Operations Center (DMOC) at Kirtland Air Force Base. The site map below shows the locations of assets used for the Virtual Flag Exercise in 2006.[4]

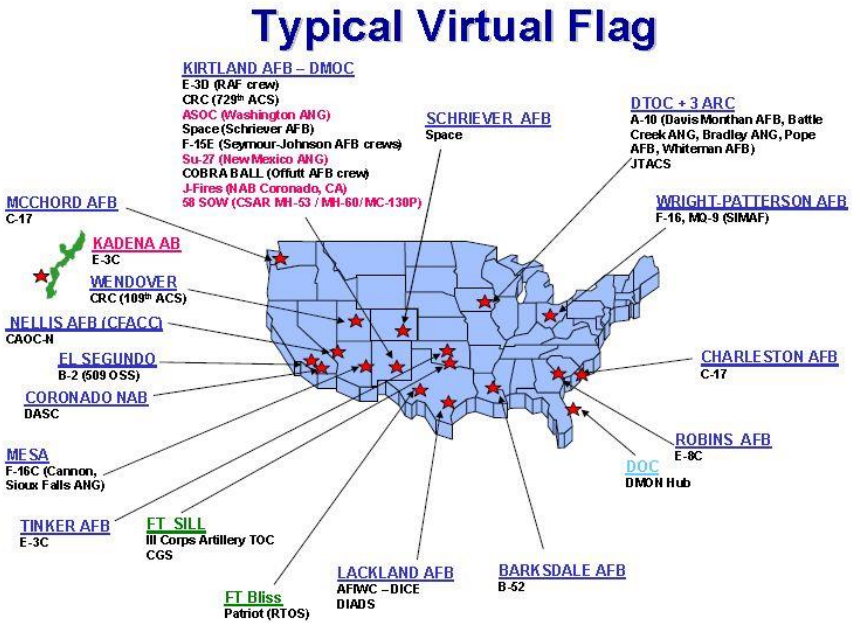

Figure 2 Geographically disparate simulation assets in Virtual Flag [Drechsler 2006, slide 9]

[4] Drechsler, D., "Distributed Mission Operations," briefing for 505th Command & Control Wing, 2006 http://www.dtic.mil/ndia/2006psa_psts/drex.pdf

The simulators, command and control, and other simulation assets required by the scenario are listed under the name of the networked location in Figure 2. The two Army locations, Fort Sill and Fort Bliss, are accessed through the JTEN network shown in Figure 1. By using a distributed architecture geographically-separate, high-value resources can be included in the exercise. However, to enable a single, large exercise, the network connections operated at DMOC can be complicated. Figure 3 is a snapshot from 2006 of the networks accessible through DMOC

In addition to the networks specifically called out and defined in Figure 3, DMOC connects to the Navy Continuous Training Environment (NCTE) via its NCTE Enterprise Tactical Training Network (NETTN) at the Navy Warfare Development Command in Virginia. The Defense Research and Engineering Network (DREN) is the network infrastructure for test ranges and affords links to industry and academic sites not present on the DISA-managed networks.

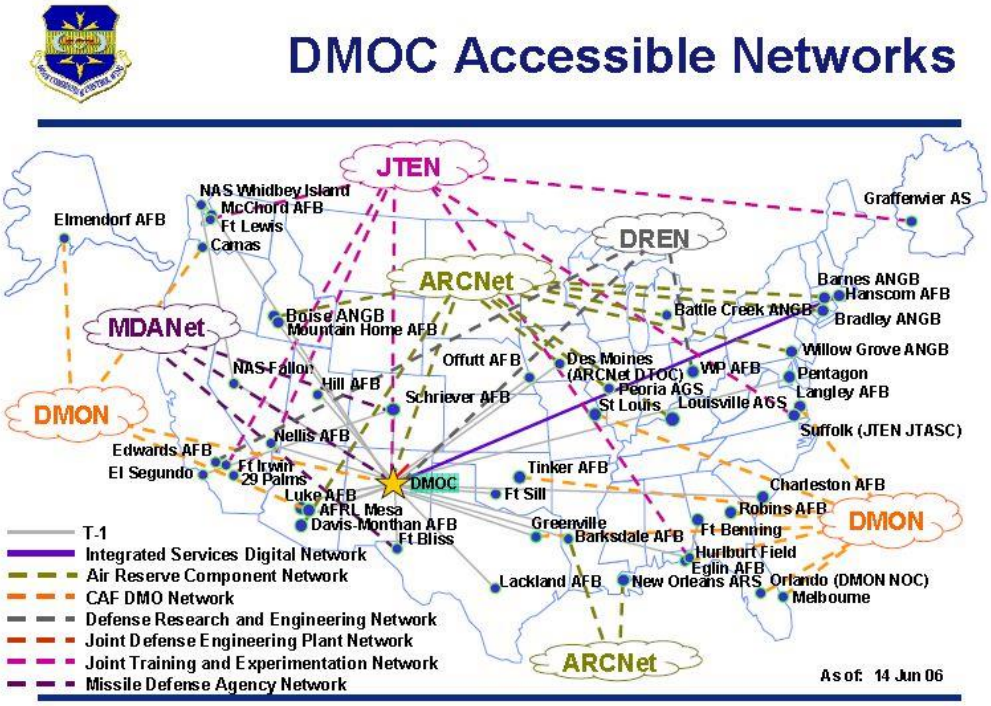

Figure 3 Networks with simulation assets available at DMOC [Drechsler 2006, slide 7]

Each of these networks has its own certification and accreditation authority as does each of the multiple, separate US Army sites. This is significant in terms of acquiring all the authorizations needed to execute events across multiple networks. The more accreditation authorities, the more agreements required and the longer the process of setting up an exercise.

2. The Services Used in Distributed Training Exercises

The network is useful to the extent that it brings the user into meaningful contact with simulations and other services required for training. The Distributed Continuous Experimentation Environment, begun by JFCOM with the Joint Experimental Federation has grown into the Joint LVC Enterprise, including the major Service combat

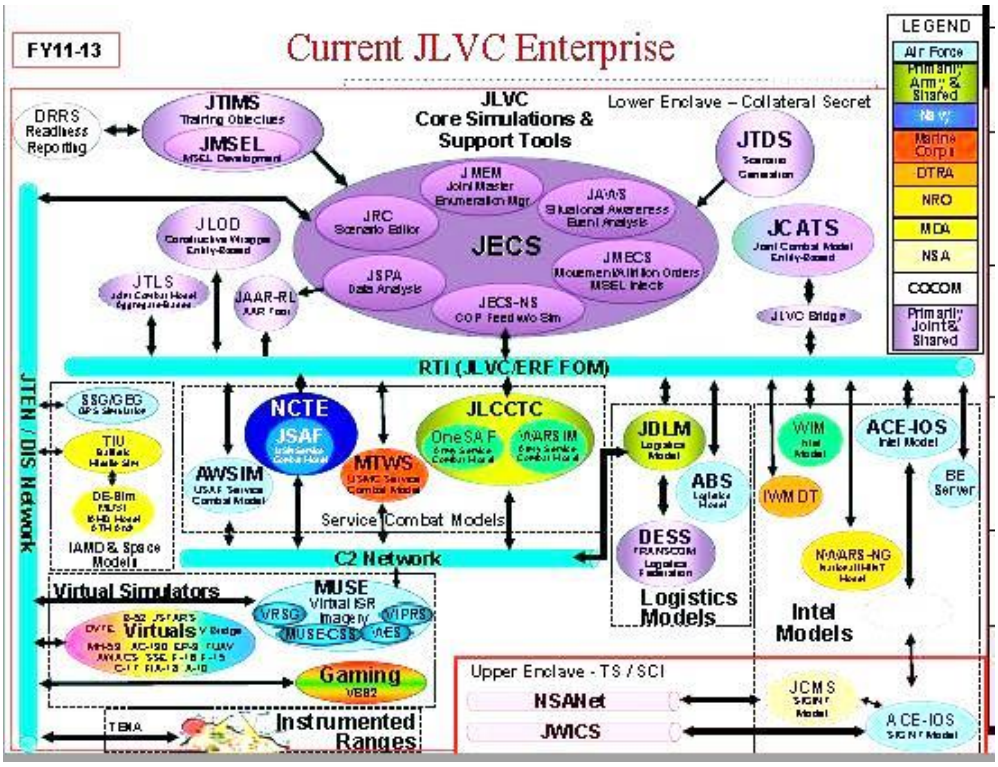

Figure 4 Tools and services in the JLVC Enterprise [Vinett 2011, slide 8]

simulations, a suite of core Joint simulation and support tools, access via the JTEN to simulators, and key models from other communities including logistics and intelligence

simulations. Figure 4 is a simplified display of the tools and services provided to users of the JLVC Enterprise.[5]

The Enterprise includes two security enclaves. The majority of tools run in a Collateral Secret environment as part of the lower enclave, but are bridged to the Upper, Top Secret (TS)/ Sensitive Compartmented Information (SCI) Enclave using the appropriate security apparatus. This type of operation places additional demands on network security and requires additional certifications and accreditations.

Three pipes (aqua cylinders in Figure 4) represent different types of data transport. The C2 network uses the messaging structure required to communicate with C2 systems and each of the major simulation tools connected to that network convert simulation data into C2 messages and can receive and interpret such messages sent out over the C2 network. This is not the native mode of data exchange among the simulations. Three different architectures, each with its own data transmission format, participate in this federation. The DoD's High Level Architecture (HLA) uses a Run Time Infrastructure (RTI) that allows the various simulations to communicate using a publish and subscribe data management schema. The network that manages this data transfer is labeled RTI (JLVC/ERF FOM) in Figure 4. The Entity Resolution Federation (ERF) is a set of US Army simulations, simulation command, control communications, computers and intelligence (C4I) interfaces, data collection and other tools capable of representing forces at the resolution of the individual soldier, sensor, or platform and is consistent in resolution with other Semi-Automated Force (SAF) including Joint SAF used to represent maritime and air assets. The Federation Object Model (FOM) comprises a set of all the data exchange capabilities of the sum total of simulations in the federation.

The large ellipse at the top of the illustration contains simulation utilities and analytic tools linked to the training requirements tools in the upper left and several Joint simulations to the left and right. Below the RTI are the four major Service simulation tools: Air Warfare Simulation (AWSIM), the US Navy Continuous Training Environment that includes all the simulations and simulators accessible at US Navy sites and that use the RTI to communicate with JSAF as the core simulation, MTWS (the Marine Air-Ground Task Force Tactical Warfare Simulation) representing the Marine Corps' assets, and the Joint Land Component Constructive Training Capability

[5] Vinett, J., "Joint Training Enterprise Technical Updates, " Worldwide Joint Training and Scheduling Conference, September 2011 http://www.dtic.mil/doctrine/training/conferences/wjtsc11_2/working_groups/4.%20%20WJTSC%2011-2%20JTE%20WG%20-%20JCW%20JOSE%20Technical%20Update%20WJTSC%2011-2.pdf

(JLCCTC) used by the US Army. Each Service looks at simulated, entity-level combat through the lens of these tools or federations. To the left of the Service models are missile defense and space models; however, note that these models and the virtual simulations below them do not communicate through the RTI, but use a different simulation architecture, Distributed Interactive Simulation (DIS) represented in Figure 4 as JTEN/DIS Network. DIS uses a different data specification and communications via broadcast to all participating simulations. The data running on the DIS Network is connected to the RTI via a gateway that interprets and repackages the data as required. The use of multiple data communication formats complicates the task of the edge devices that preserve the security at each site. While key simulations can all be run from a central site, nearly all the virtual assets and many of the simulation assets must be run off-site in networked configurations similar to those shown in Figures 2 and 3.

The vision of the training community is to have a continuous, persistent environment in which individuals and groups can train whenever they need to and from wherever they are using whatever access mode is most readily available, including mobile devices – the epitome of agility. This glimpse of what goes on behind the curtain in a distributed simulation event forms the backdrop for examining the information assurance and network security issues that constitute the primary barrier to achieving that vision.

2. Security Issues in Distributed Simulation

The reason for examining the tools and services is to expose the complexity of the software and data required for a distributed simulation. Each software, hardware and firmware element must be certified and accredited by the certifying authority (CA) and designated accrediting authority (DAA) for the network on which it operates before being granted the authority to operate (ATO). In addition to the information assurance requirements that must be satisfied before an ATO is issued, there are network security requirements including intrusion protection at the boundary of each site, certification of appropriate security appliances to provide cross-domain operation for enclaves operating at different levels of security, and development and certification of security guards when operating with coalition partners. When each distributed simulation event, whether for training or for T&E, operates across security enclaves, involves multiple private networks and includes a significant array of tools and simulations, the number of certifications,

ATOs and memoranda of agreements (MOSs) among DAAs is significant and takes orders of magnitude more time than the event itself.

A. The Quest for an ATO

The DoD Information Assurance Certification and Accreditation Process (DIACAP) is the means for ensuring that the people, processes and technology used in any cyber activity provide adequate protection for our information assets. The DIACAP was developed to streamline DoD's information assurance practices and bring them in line with the provisions of the Federal Information Security Management Act (FISMA). DIACAP applies to the acquisition, operation, and sustainment of any application, network, circuit, enclave, site, infrastructure or environment that receives, processes, stores, displays, or transmits unclassified or classified information.[6]

1. Certification

Certification applies to both threats to and vulnerabilities inherent in hardware, software and firmware that are part of an information system. Threats can be posed by natural disasters or man-made interventions and may be imposed internally or externally, intentionally or unintentionally. Vulnerabilities are circumstances or conditions under which a threat may actually cause damage to the information system. Taken together the likelihood of a threat and its potential vulnerabilities define the risk faced by the information system. Information assurance controls are measures designed and implemented to reduce risk by reducing vulnerabilities.

Certification involves a comprehensive evaluation of technical and non-technical security safeguards of an information system and is required before any piece of hardware, software or firmware can be connected to a DoD network.

2. Accreditation

Accreditation is the formal declaration by an approving authority that the hardware, software or firmware is compliant with established security regulations and may operate on a specific network given a declared set of safeguards. The DAA takes into account the certification provided by the CA and in addition considers the criticality of the system

---

[6] Department of the Navy, "DoD Information Assurance Certification and Accreditation Process (DIACAP) Handbook, Version 1.0, 15 July 2008 http://www.navair.navy.mil/nawctsd/Resources/Library/IA/Files/DON_DIACAP_Handbook_v10_Final-15_July08_v131_508.pdf

to specific missions, current threat levels and the overarching security posture of the DoD Information Network (DODIN). The accreditation decision takes the form of an Authorization to Operate (ATO), but could also be an interim authorization to operate (IATO) or an interim authorization to test (IATT).

B. Accreditation and Agility

Accreditations can be done for a variety of sites including enclaves (site specific or distributed), complex or simple networks and sites defined as local area network or unique geographic locations, but regardless of the type of facility or system being accredited, the accreditation process is lengthy because it involves an in-depth, engineering-level examination and an estimation of risk that involves technical as well as non-technical considerations. Establishment of risk may routinely take months to accomplish.

One of the major problems for distributed simulation systems is that accreditation includes certification and applies to a single instance of a specifically configured system for a particular physical or operational environment. If changes are made to the configuration of the system or to the physical or operational environment, the accreditation process must be done for the new configuration.

Consider the configuration of the Virtual Flag event in Figure 2. Suppose that an excursion on the original scenario required the use of a new ground-to-air missile prototype under test at Redstone Arsenal. Inclusion of that prototype would change the physical environment by requiring an additional network connection and a reconfigured software environment that involved communicating with the prototype. The prototype was certified to operate on the network at Redstone, but that is a separate network under a different DAA. The DAA for the Virtual Flag event would have to engage with the DAA from Redstone to agree to accept the certification of the prototype as done for operations at Redstone. This is not as simple as it sounds, because the information assurance controls for operation at Redstone may be different from those at DMOC. While the agreements may be signed in the end, the process to achieve the needed MOA could take months and be completed long after the Virtual Flag event ended.

An obvious excursion to a scenario designed to test the viability of an alternative approach to accomplishing a mission cannot be done under normal circumstances if it involves some hardware, software or firmware or changes the physical configuration of the original system. While this is a major limitation for the training environment, particularly when attempting to train agility into command decisions, it is a disabling condition for T&E.

The very nature of the T&E process, particularly at the developmental T&E stage is to run the test to find the problem, attempt to fix the problem and rerun in the test-and-fix mode until the problem is well-defined and an appropriate fix is found. Without special exemptions such as an interim authority to test, T&E could not be done using DoD information systems. The very act of fixing changes the certification conditions signaling a rework of the certification and ATO.

Clearly some approaches have to be made to allow training and T&E to function effectively. Some of the approaches being used and tested will be explored in the following sections.

1. Certification and Acquisition

Introducing a new simulation or simulator to an existing networked simulation environment requires certification and an ATO for that network. To jumpstart the process of certification, the Services work with the program offices responsible for building the new capability to begin the certification while the new system is being developed. When the coordination works, the certification arrives with the system, the ATO follows shortly thereafter and the new capability can be implemented almost as soon as it arrives. The key is a working collaboration between the owner/manager of the network environment and the acquisition manager. When acquisitions are perennially under-funded and pressed for time to meet delivery schedules, adding the requirement to certify in stride can be met with some resistance as it consumes resources.

The US Army addressed this problem by bringing all training simulations and simulators under a single program office, the Program Executive Office for Simulation, Training and Instrumentation (PEO STRI). The certification process is supported and overseen by the Cybersecurity Services office under the Corporate Information Office. PEO STRI makes sure that the certification is done in stride with development and is ready when the system is ready. However, the ATO is not sufficient for the system to be placed into operation. Rather than developing a single, dedicated simulation network, the US Army made use of the JTEN to link its simulation facilities and bases where simulators are located. Behind each of the JTEN nodes (Figure 1) at Army facilities, is the network that supports the whole facility, including the simulation center. These are different networks with diverse demands driven by the particular functions and needs of the base. The ATO accredits the new system as having all the appropriate information assurance characteristics to operate on an Army network, but requires a certification of networthiness (CON) from Ft. Huachuca that certifies that system to operate on the network at a specific Army installation.

2. Type Accreditation

One of the situations PEO STRI has faced is the installation of a common suite of software tools in all of the US Army's simulation centers. The normal process would involve testing and validating the information assurance controls for the software suite at each of the numerous simulation centers. Type accreditation allows one typical location to be used for test and validation if the argument can be made that all the simulation centers, in terms of operating the software systems, can be considered as identical. The JLCCTC-Multi-Resolution Federation (JLCCTC-MRF) based on WARSIM (JLCCTC-MRF-W) is being distributed under type accreditation.

The Navy distributes simulation software to its US land-based sites and to shipboard sites. In this case, since there are two different networks involved, the Navy Marine Corps Internet (NMCI) and the shipboard network known as the outside continental US (OCONUS) Navy Enterprise Network (ONE-Net), the information assurance controls must be tested and validated in one representative site for each of the identified environments.

In both cases, the installation environments must be described in detail and connections to all other enclaves specified.

3. Cross-Domain Solutions

One of the most difficult and time-consuming certifications is for the use of security appliances that cross two different security domains. All cross-domain solutions are treated as site-specific and thus must be tested and accredited for each site and application. Certification involves testing by an outside group and approval by several external organizations including the National Security Agency (NSA) and the DoD Information Assurance/Security Accreditation Working Group (DSAWG).

The US Army is currently seeking a pilot test case employing type accreditation for cross-domain solutions. The proposal involves using a single test and validation process for several identical installation locations. In establishing the need to develop such an approach the Army was able to cite a single case involving a Radiant Mercury implementation for a single laboratory environment and two fielded sites. The time required for the full certification of the three separate sites was in excess of two years and the cost, not including equipment, was well into six figures.

The US Navy and the US Air Force have simplified the cross-domain solution problem by working internally with a single, private, simulation network; however, as

soon as additional networks are included, the problem recurs because the initial environment has changed.

4. Exercising with Coalition Partners – Wicked Problems

The ability to work effectively with coalition partners is aided if all the military leaders involved can work together initially in a simulation environment; however, simulation environments are information systems and the very fact of working together reveals information, not all of which is contained in the software or systems. Consider the problems one at a time. The first problem is establishing a simulation environment in which all partners can engage and the second is dealing with the possibility of unintentionally revealing something not encapsulated in the software or scenario.

The problem is not the same as the cross-domain solution. The overall network may be operating at the secret level, but not all secret information is releasable to everyone. The U.S. not only makes bilateral exchange agreements with international partners, but under those agreements, the Services tend to make Service-specific agreements with their sister services in the foreign nations. Consider the situation in which the U.S. seeks to exercise with two different European nations. It might be possible to use a different security guard (the device that allows connection with a foreign nation) for each nation; however, if each guard has a different rule base for information exchange and the countries are both exercising in the event at the same time and communicating with the other participants, the differences in revealed information could create a problem. A different solution that rationalized the releasability requirements into a single, lowest denominator set, might be a better idea for conducting the event.

Assume that the US Air Force connected directly to the US Navy and through the US Navy to the foreign nations, the solutions developed by the US Navy would not necessarily work for the US Air Force because of Service to Service agreements. Currently, when DMOC makes a direct connection to NCTE, NCTE must take all its security guards off-line because, in fact, the agreements for release of data are not identical for the two Services. This is a place where a different solution would be preferable, but has not been found.

The current approach to rationalizing guard-enabled communications with foreign nations is to take a tiered approach and establish separate guards with their own rule bases for each tier of international partners. For example, the English speaking countries share most freely with the U.S. and would belong in the one tier.

Figure 5 is an attempt to show the dilution of information with each tier. The lighter the shading the less data is shared.

NATO is looking at the tiered approach for exchanging information with allies. The approach makes sense, but the problem remains for simulation exercises in which all participants are communicating throughout the event.

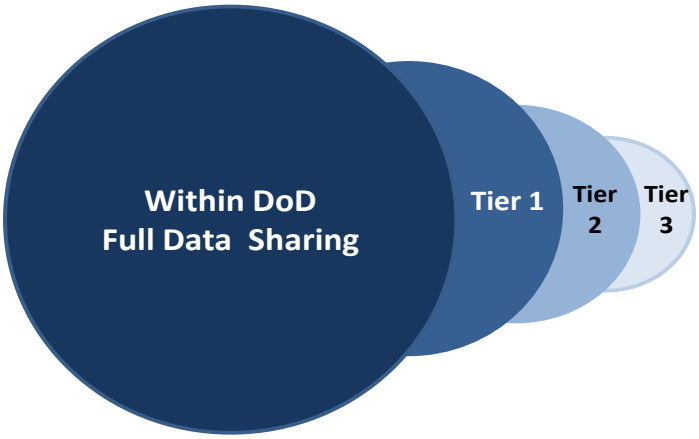

Figure 5 Tiered approach showing information dilution

The second problem is much harder to address and has been the reason for cancelling international, simulation-based experiments after years of careful preparation including a number of certifications, authorizations and MOUs. The nature of the simulation environment is to engage the participant in such a way that he forgets that it is a simulation and reacts as if it were a real event. If all the security guards are in place and the only data exchanged is that which is approved by international exchange agreements, there is still a problem when a warfighter behaves according to the tactics, techniques and procedures (TTPs) ingrained into his performance. The DoD or one of the Services may not wish to divulge actual TTPs, even to close allies. Yet, when a pilot flies his simulator during an exercise, he may react with tactics he had not intended to use in the simulation event.

There are no security guards to prevent this type of information flow. It is both the benefit and liability of a good training environment. And it can be a security risk. Again, there is no current solution to this problem.

C. The Test and Evaluation Environment

The problems faced by the T&E community are similar to those explored for the training community; however, the T&E approach has been different. They run on a dedicated network, but while it is part of the DODIN and abides by the DIACAP restrictions, its management and processes are distinctly different.

The Joint Mission Environment Test Capability[7] (JMETC) maintains a private enclave on the Secret Defense Research and Engineering Network (SDREN), managed under the DoD High Performance Computing Modernization Program. The intention of the SDREN and the unclassified DREN is to support the research, development, test and engineering (RDT&E) part of the DoD. Because of the nature of the RDT&E community, the DREN and SDREN can connect to appropriately managed and secured industry and academic sites (academic largely on the DREN). The management processes are streamlined and based on the knowledge that each node is located at a site where there is considerable computing and networking expertise.

The SDREN affords JMETC dedicated, trusted connectivity with encryption for Secret – System High. DISA maintains the registered IP address space. The SDREN provides active monitoring of network performance and the bandwidth is sufficient to support multiple, simultaneous test events. The SDREN provides connection with major industry sites where DoD prototypes are being developed including Boeing, Northrop Grumman, and Lockheed Martin. Georgia Institute of Technology has established a connection to the SDREN through its Research Institute (GTRI). JMETC includes all the major Service test ranges. Figure 6 shows the geographically dispersed sites connected through the JMETC enclave on the SDREN.

[7] Ferguson, Chip, "Joint Mission Environment Test Capability (JMETC) Improving Test & Training Capability", NDIA Test and Training Crosstalk Forum, 21 February 2012 (sent by the author, chip.ferguson@osd.mil)

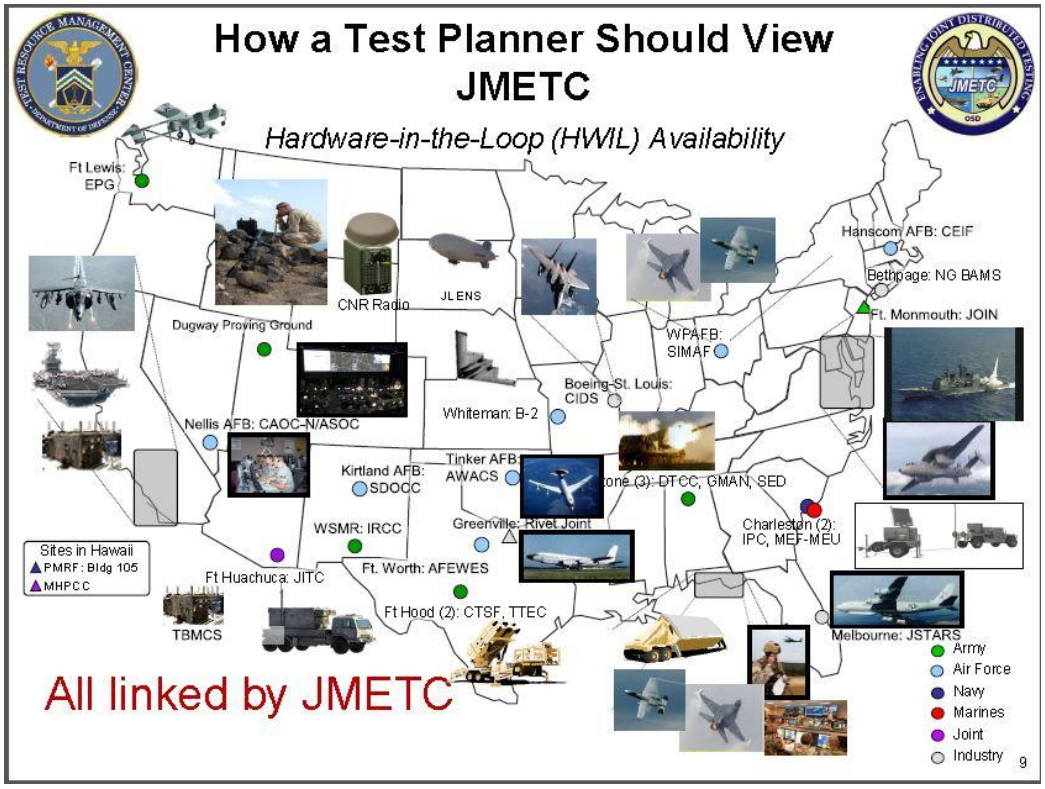

Figure 6 Assets available through JMETC sites on the SDREN [Ferguson 2012, slide 9]

One of the major advantages in accreditation accorded to the T&E community is the ability to run under interim authority to test (IATT), an authorization that is limited by time rather than by event. Certification by event where an event is described as having no alterations in environment or systems, would not permit the test-modify-test process so critical to developmental testing. JMETC can switch out modules (hardware, software, or firmware) separately certified or add additional test locations without having to obtain a new authorization to operate. Currently the authorizations extend for several years. This management approach allows the T&E community to maintain a persistent environment for T&E.

This type of flexibility has enabled the Test Resource Management Center to develop a National Cyber Range (NCR) for testing and training. The NCR is a self-contained facility, but is remotely accessible through the Joint IO Range network (JIOR) and JMETC. The certifications and authorizations allow the facility to support at least two independent, concurrent events. The test suites can be used at different security levels and all assets are sanitized after each event and returned to the available pool.

The T&E community has achieved persistent, flexible capabilities by working under a different network management while at the same time satisfying all the DIACAP and other security requirements. The ability to certify and accredit for an extended time rather than by event is an approach that could be of tremendous benefit to the training community, but would have to be accompanied by some type of consolidation of networks.

3. Thoughts for the Future

Providing agility in a simulation-based, distributed training environment presents a number of problems, some of which might well be managed by new technology or changes in management processes and others that will remain hard problems.

A. Opportunities Afforded by Technology

The rise of the mobile world has made the concept of a cloud a reality in the hands of most individuals. Mobile devices pull live data from cloud-based applications on a routine basis and we think nothing of it. As tablets begin to replace laptops, users depend upon storage in "the cloud". DoD has begun moving toward some version of cloud computing and storage, but it presents a new suite of security problems to be solved including issues with protecting mobile communications.

One vision for the future of simulation-based Joint training includes some type of cloud environment for the data, applications and computing assets used in Joint simulations together with some form of operational cloud to link to the deployed assets with security guards for coalition operations. A cloud environment would simplify the certification and authorization issues by containing them in a single operational environment – no need for MOAs among multiple DAAs. Managing the edge that connects to the operational environment would have many of the same problems it has today, but without the proliferation of networks on the simulation side. Information transfer among coalition partners would remain a wicked problem as would the unintentional transfer of TTPs accounted for by all the certifications.

Without moving to a cloud environment, there are opportunities to establish special enclaves with the current fiber technology that are not being used routinely.

B. More Flexible Management

Consolidation of networks would make the accreditation process much simpler. Some degree of commonality in information assurance controls across all training networks would make the adoption of certification from one simulation network to another a much simpler process. Site-specific and Service-specific controls would have to be adjusted for the dedicated simulation networks to achieve this type of simplification. It would be most difficult for the US Army because none of its networks are dedicated simulation networks. However, modern technology and increased bandwidth might well afford the opportunity to isolate the simulation centers to the extent that some of these simplifications could be achieved.

If simulation events could be regarded more like tests than like operations, perhaps the ATO could be changed to an IATT extending over a reasonable period of time. This would provide a far greater degree of agility than currently exists. If all the assets available to any simulation network (DMON or NETTN) were certified for a year and could be swapped in and out as needed to support different events, the exercise overhead would be decreased and time and money saved. Incremental additions, software improvements, inclusion of new databases and other small changes would also require some degree of management flexibility, but if supported by approved certification processes, these incremental changes could be accommodated without restarting the accreditation process.

C. Hard and Wicked Problems

Hard problems are those for which solutions take considerable time and effort to implement. Managing cross-domain issues and information exchange with internations problems fall into this category. Managing cross-domain solutions will still require time and resources, but streamlining the number of independent networks would require fewer separate accreditations resulting in increased agility and decreased cost.

Managing information exchange with international partners participating in the simulation events would continue to be difficult. The problem of establishing viable rule bases in the face of bilateral agreements when exercising in a multi-national environment would not change.

Wicked problems resist solution because of their complex interdependencies replete with incomplete, contradictory and changing requirements. Unintentional release of information through an interactive simulation environment is a wicked problem. Understanding how to manage the unintentional release of information though the

behavior of participants in the LVC environment is a particularly difficult problem to solve, but solving it is essential if the exercises are to engage in realistic C2 with multinational players.

4. Conclusions and Recommendations

The current approaches to improving the agility of training, particularly joint, distributed training, will not achieve the vision of a persistent training environment in the near future. Adopting a spirit of innovation with limited, and controlled risk-taking and implementing a series of planned, graduated experiments with new technologies and methods could bring the future closer to the present. Many of the current roadblocks are self-imposed and can be addressed either through changes in management coupled with a willingness to exploit technologies in new ways. Using experiments to work through some of these options would help achieve the vision of a persistent training environment in a well-reasoned and cost-effective manner.

A. Think Layered Nationally

The layered approach being considered by NATO for implementing multi-national exercises could be used within the US for simplifying network approval processes and laying a foundation for period-based rather than event-based authentications. The model of period-based approvals for the T&E community is probably too hard for the full suite of DoD training nodes (Joint and Service combined); however, it should be relatively easy to identify candidate groups of nodes and applications (simulations and simulators) for which authentication can be provided for a year or two. The JTEN suite of applications would be a clear candidate for participation. One might consider adding the JTEN collection a suite of stable simulations and simulators on NCTE and DMOC, but for a restricted and pre-approved set of scenarios. These stable assets would then be the suite of tools used for experiments over the period of accreditation, and any change in the software would invalidate the accreditation agreements. The most difficult inclusion would be the Army because of the number of independent authentication authorities involved. Work with a core and then expand based on success.

B. Move to Consolidation

The objective here is the reduction of authentication authorities. The Navy has already placed all of its training sites on a single network with a single authentication authority. The Air Force has only three networks. The Army has the problem with the way simulation centers are subject to the authentication authorities at its various home stations where the simulation centers are located, and the problem becomes more severe if the Army Reserve and National Guard are included. However, the Army is in the process of upgrading the network infrastructure at its bases and updating the protocols. As the updated network services go into a base, the Army might consider creating a training enclave as a separate, gradually growing Army-wide capability managed by a single designated authentication authority. As bases are upgraded, their simulation centers could join the enclave. Under such a system, simulation centers might use the base network solely as a transport layer, much the same way the Navy and the Air Force use JTEN for transport. The technology exists to do this today and implementation could be gradual and in-stride with planned infrastructure improvements.

C. Exploit the Cloud

This could be done at both the Joint and Service levels by moving constructive simulation applications into the cloud. There would be work to determine how best to build the federations needed for a specific training exercise. A brief review of Figures 2, 4 and 6, provides ample evidence that for many simulation events, not every asset can be in the cloud. Thus, as part of the cloud experiments, care needs to be taken to streamline the inclusion of virtual assets (simulators) that will remain firmly planted on their network nodes and not in the cloud. Certification and accreditation of data for sharing can be facilitated by use of proper data tagging and careful definitions of Communities of Interest or some other designation of those sets of entities entitled to share specific data. The problem of edge connections is one that must be addressed in a well-planned and graduated manner if cloud computing is to provide the advantages that we anticipate.

D. Think Layered Internationally

A successful, layered approach will require that the Services work together to build a viable set of agreements for international exchange within the training domain. While it is certainly true that the US Army can and will continue to engage in international, land-based exercises, as will the US Air Force and US Navy with their international partners, having consensus on some set of agreements with our most frequent international partners would help reduce the problems of setting up security guards. The

work might begin for a class of military activities, perhaps humanitarian assistance and disaster relief (HA/DR) and then progress to other types of military operation.

The problem of disclosing TTPs through live play would not be addressed by the above approach; however, the use of HA/DR scenarios would reduce the severity of the problem and permit the hard, but not wicked issues to be addressed.

E. The Regionally Aligned, Expeditionary Force

As it stands today, were the interests of the United States to necessitate the assembly of an expeditionary capability within a matter of months, DoD's distributed simulation architecture and processes would likely be unable to provide the kind of environment that would allow for timely pre-deployment combined training of that force. This may be the most stressing problem for distributed simulation as the forces would be gathered from multiple sites and Services to be formed together in a fraction of the time a single Service requires for pre-deployment training. The commanders will also have to develop the ability to command this rapidly assembled joint force. One of the most effective means for creating such capability is to work with regionally aligned forces prior to their being called for deployment using simulation as the medium for building the trust relationships that create a highly capable force. Without an agile, persistent, distributed, training environment, preparing the expeditionary force will be more difficult and likely lest cost-effective.

5. Acknowledgments

The authors would like to thank the representatives from JTEN, the US Navy's NCTE, the US Air Force's DMOC, the US Army's PEO STRI, and OSD's TRMC for taking time to speak with us and share their experiences and information. Without their assistance this paper would not have been possible.

Acronym List	
ACE-IOS	Air and Space Constructive Environment - Information Operations Suite
ARC	Air Reserve Component
ARCNet	Air Reserve Component Network
ATM-SONET	Asynchronous Transfer Mode-Synchronous Optical Networ
AWSIM	Air Warfare Simulation
CAR DMO	Combat Air Force Distributed Mission Operations
CPOF	Command Post of the Future
DARPA	Defense Advanced Research Projects Agency
DCEE	Distributed Continuous Experimentation Environment
DESS	TRANSCOM logistics federation
DMOC	Distributed Mission Operations Center
DMON	Distributed Mission Operations Network
DREN	Defense Research and Engineering Network
DRRS	Defense Readiness Reporting system
DTOC	Distributed Training Operations Center (Iowa Air National Guard)
DODIN	Department of Defense Information Network
IAMD	Integrated Air and Missile Defense
IWMDT	DTRA Integrated WMD Tool Set
JAAR-RL	Joint After Action Review
JCATS	Joint Conflict and Tactical Simulation
JCMS	Joint Cryptological Mission Simulation
JDLM	Joint Deployment Logistics Model
JECS	Joint Exercises Control System
JEF	Joint Experimental Federation
JLCCTC	Joint Land component Constructuve Training Capability
JLOD	JCATS Low Overhead Driver
JLVC	Joint Live Virtual Constructiive
JMEM	Joint Master Environmental Manager
JNTC	Joint National Training Capability
JSAF	Joint Semi-Automated Forces
JTEN	Joint Training Enterprise Network
JTIDS	Joint Tactical Information Distribution System
JTIMS	Joint Training Information Management System
JTLS	Joint Theater Level Simulatoin
LVC	Live, Virtual, Constructive
MC02	Millennium Challenge '02
MDANet	Missile Defense Agency Network
MTWS	Marine Air-Ground Task Force Tactical Warfare Simulator
MUSE	Multiple Unified Simulation Environment
NCTE	Navy Continuous Training Environment
NWARS-NG	National Warfare Simulator - Next Generation
SDREN	Secret Defense Research and Engineering Network
TENA	Test and Training Enabling Architecture
WIM	WARSIM Intelligence Modues