Creating a Network Digital Twin using Full-Fidelity Virtual Hardware

Dr. Deepinder Sidhu,
Cyberspace Analytics, Corp.
Columbia, Maryland
dsidhu@CyberSpaceAnalytics.com

Charles D. “Chuck” Burdick, CAP
Innovative Decisions, Inc.
Vienna, Virginia
cburdick@innovativedecisions.com

Abstract

Cyberspace Analytics (CSA) has developed an unprecedented cyber capability using virtual hardware and internet software to map, reverse engineer, clone network “digital twins”, and create full-fidelity emulations of specific networks to execute network defense, cyber missions, network response predictions, and cyber exercises effectively and affordably. This capability has recently begun supporting multiple clients and delivering deep visibility into total network assets in near real-time, while providing mechanisms to control networks, minimize their vulnerabilities, promote agile defense, respond to adversaries, and examine future changes and additions in both hardware and software. And its affordability, compared to hardware-based network emulation, makes possible “Complete Life Cycle Network Awareness” rather than occasional testing

The CyberSpace Emulation (CSE) environment discovers all network assets, IP addresses, configurations and vulnerabilities. The emulation illuminates and maps whole networks, segmentation, boundary nodes, VLANs, virtual overlays, unmanaged nodes, and rogue nodes and reliably exposes spoofed nodes, honey-pots and honey nets.

In support of forward operations, CSA has developed a CSE powered portable Cyber Range Appliance (CRA) for network emulation to develop on site “what-if” scenarios, support opportunistic cyber mission planning, execute mission rehearsals, conduct cyber skills training and certification and support cyber exercises. The CRA has a small (9”x5”x5”), lightweight (9 lbs.) form factor and can seamlessly connect to and interface with actual networks.

This presentation is unclassified using data from participating university clients, but the vulnerabilities, mostly unintentional, are found on all networks.

ABOUT THE AUTHORS

Deepinder P. Sidhu received the B. S. degree in EE from the University of Kansas, and the M. S. and Ph. D. degrees in Computer Science and Theoretical Physics respectively from the SUNY, Stony Brook. He is a Professor of Computer Science & Electrical Engineering with the University of Maryland-Baltimore County (UMBC). He served Editor-in-Chief of Journal of High Speed Networks; Advisory Board Member of Cisco's Internet Protocol Journal; Program Chair ACM SIGCOMM '92 and Program Chair for ACM SIGCOMM '93; invited speaker for major conferences; ACM National Lecturer for 10 years; Principal Investigator for major R&D projects for NSA, DARPA, NSF, NASA, NIST, IBM, SUN, Sprint, MCI, Unisys, Nortel Networks and Fore Systems. He contributed to significant advances in theoretical physics (contribution cited by S. Weinberg in 1979 Nobel Prize Acceptance Speech, published in Rev. Mod. Phys. Vol. 52, No. 3, July 1980). Dr. Sidhu published 300+ papers in refereed technical journals and conference proceedings. He supervised 24+ Ph.D. dissertations and 100+ M.S. dissertations in Computer Science. He is currently President and CEO of Cyberspace Analytics, Inc. in Columbia, MD.

Chuck Burdick has more than 35 years of experience developing and applying tactical and operational simulations to analytic, training, and testing applications for both the military Services and DoD agencies. His efforts have ranged from manned simulators to campaign and above campaign modeling. He was involved in early DIS development and multi-resolution modeling in both technical and leadership roles. He has led four multi-million-dollar simulation and wargaming developments with emphasis on C4ISR and Land operations. He is a retired Army Intelligence Colonel with 7 years active (two in combat with one as an advisor) and 23 in the Reserves ultimately serving in senior G2 positions in the Pentagon. He is currently a Senior Principal Analyst at Innovative Decisions, Inc.

Creating a Network Digital Twin using Full-Fidelity Virtual Hardware

Dr. Deepinder Sidhu,
Cyberspace Analytics, Corp.
Columbia, Maryland
dsidhu@CyberSpaceAnalytics.com

Charles D. “Chuck” Burdick, CAP
Innovative Decisions, Inc.
Vienna, Virginia
cburdick@innovativedecisions.com

BACKGROUND

Last year, the Department of Defense initiated a Digital Engineering Approach to Acquisition that will cut across the entire life cycle of any system under development.

Digital Engineering (DE) is an integrated digital approach that uses authoritative sources of systems' data and models as a continuum across disciplines to support life cycle activities from concept through disposal. In June 2018, the Office of the Under Secretary of Defense for Research and Engineering (USD(R&E)) released a Digital Engineering Strategy (DASD/SE 2018) built on five foundational elements necessary for a Digital Engineering Ecosystem to thrive:

1. Formalize the development, integration, and use of models to inform enterprise and program decision making
2. Provide an enduring, authoritative source of truth
3. Incorporate technological innovation to improve the engineering practice
4. Establish a supporting infrastructure and environment to perform activities, collaborate, and communicate across stakeholders
5. Transform the culture and workforce to adopt and support digital engineering across the life cycle

Of most interest to this audience, the first of the five foundational elements stresses the development, integration, and use of models to inform enterprise and program decision making. Essentially, models are to serve as a continuum across disciplines to support a system’s lifecycle activities from concept through disposal.

Three Conceptual Ideas are critical to the success of the effort.

1. The first is the **Digital Artifact** produced within, or generated from, the digital engineering ecosystem. These artifacts provide data for alternative views to visualize, communicate, and deliver data, information, and knowledge to stakeholders. And in a network Digital Twin, emulated virtual networking hardware serves much of this role.
2. The second is the **Digital System Model** a digital representation of a defense system, generated by all stakeholders, that integrates the authoritative technical data and associated artifacts, which defines all aspects of the system for the specific activities throughout the system life cycle. (DAU Glossary, 2018)
3. And the third is the **Digital Twin, a**n integrated multiphysics, multiscale, [probabilistic] simulation of an [as-built system], enabled by Digital Thread, that uses the best available models, sensor information, and input data to mirror and predict activities/performance over the life of its corresponding physical twin.

The bottom line is that Modeling and Simulation and where possible Emulation will attempt to provide more standardization and potentially cooperative sharing of the digital artifacts that will comprise the components of the Digital Twins, a concept of providing a digital replica of the proposed system over its complete life cycle.

There have already been a few successful Digital Engineering experiments reported, one of which was the recent redesigned of the A-10’s wings using digital engineering (Cronk, 2018). But while most people are fixated on the digital models of weapon systems, the digital artifacts which DDR&E most envisions as providing, there is another category of systems where the concept of Digital Twins or virtual clones has been maturing for a considerable period of time. This is in the application of digital engineering to networking and the networks that link almost all systems in our digital world.

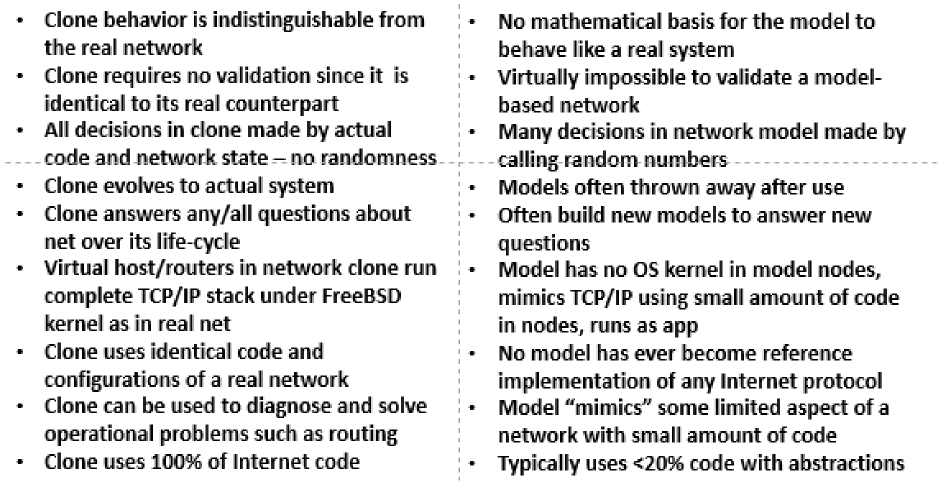
Cyber threats to our networks and digital devices are one of the areas of greatest concern and greatest need in both our national defense and everyday life. And while there is a great deal of network simulation and cyber wargaming being developed and used. Neither of these is predictive of the outcome of attacks on a network. Almost ten years ago, to address this problem, DARPA created a networking testbed that could emulate networks, now named the National Cyber Range. It decided that the fastest way to provide one was to create a hardware-based network emulation and spent $100 million dollars to create it. This approach, while effective in replicating the responses of a network, is expensive involving purchasing the hardware and software licenses for the hardware, building the facility to house the center, and maintaining and operating the Center. Thus, while it is an effective tool, a hardware-based Cyber Center is not a model of a network but rather a replica of a network and it comes with limitations in that the hardware may or may not reflect the responses of specific brands and models of servers and other network devices of an actual network. DoD Test organizations have been preaching for several years the mantra of Shift Left, i.e. test earlier but a Cyber Center is essentially an “as built” system and cannot easily be manipulated and run over thousands of variations the way a software model that emulates a network can. Likewise, the Digital Twin is supposed to live with its Physical Twin counterpart over its complete Life Cycle. This “Shift Right” concept recognizes the need for a network model that can be used on a daily basis to support life cycle network situational awareness.

Networks are software defined systems; the hardware must obey the laws of physics and always follow the internet rules (protocols). The question is, can we develop a Digital System Model networks to evolve into a Digital Twin and mirror and predict activities/performance over the life of its corresponding physical twin? This paper offers an emphatic yes answer and describes just such a system.

EMULATION VERSUS SIMULATION.

The Digital Twin talks about stochastic simulation, but the Internet is deterministic in almost all aspects. One exception is the signal path through the atmosphere. But in general, the physics of signals passing through various media (copper wire, fiber optics, etc) are well known and predictable. Likewise, the rules under which the internet operates have no randomness and if modeled at the bit level with precise timing, the Digital Twin will respond in exactly the same manner as its physical counterpart. The key aspect of the Network Digital Twin is that the physical hardware is replaced by virtual hardware. Table 1 below shows many of the differences between a network emulation and a network simulation.

Table 1 Comparison of Network Emulation and Simulation (Sidhu 2018)



NETWORK EMULATION	NETWORK SIMULATION
• Clone behavior is indistinguishable from the real network	• No mathematical basis for the model to behave like a real system
• Clone requires no validation since it is identical to its real counterpart	• Virtually impossible to validate a model-based network
• All decisions in clone made by actual code and network state – no randomness	• Many decisions in network model made by calling random numbers
• Clone evolves to actual system	• Models often thrown away after use
• Clone answers any/all questions about net over its life-cycle	• Often build new models to answer new questions
• Virtual host/routers in network clone run complete TCP/IP stack under FreeBSD kernel as in real net	• Model has no OS kernel in model nodes, mimics TCP/IP using small amount of code in nodes, runs as app
• Clone uses identical code and configurations of a real network	• No model has ever become reference implementation of any Internet protocol
• Clone can be used to diagnose and solve operational problems such as routing	• Model “mimics” some limited aspect of a network with small amount of code
• Clone uses 100% of Internet code	• Typically uses <20% code with abstractions

Background on Building a Digital Twin

While working for DARPA on several early protocol problems, Dr. Deepinder Sidhu found himself with far less time on the project hardware than he needed. His solution was to build a software equivalent of the physical system. This early prototype continued to mature over the next 20 years and found a home in the Intelligence Community during the past fifteen years, problem solving and predicting the responses of existing networks, developing and testing proposed network configurations, and testing and evaluating new protocols. The result is the CyberSpace Emulation (CSE) environment which, in software creates virtual networks of sufficient fidelity to predict emergent behaviors in complex system of systems.

CYBERSPACE EMULATION (CSE) ENVIRONMENT

Cyberspace Analytics (CSA) has developed an unprecedented cyber capability using virtual hardware and internet software to map, reverse engineer, clone network "Digital Twins", and create full-fidelity emulations of specific networks to execute network defense, cyber missions, network response predictions, and cyber exercises effectively and affordably. This capability has recently begun supporting multiple clients and delivering deep visibility into total network assets in near real-time, while providing mechanisms to control networks, minimize their vulnerabilities, promote agile defense, respond to adversaries, and examine future changes and additions in both hardware and software. And its affordability, compared to hardware-based network emulation, makes possible "Complete Life Cycle Network Awareness" rather than occasional testing.

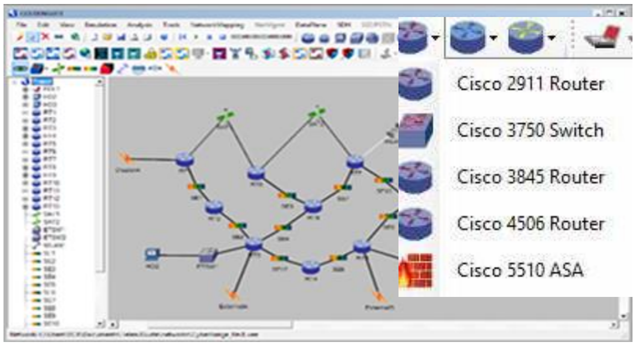


Figure 1 Virtual Network/Components (Sidhu 2018)

Starting at the Beginning of the Network Life Cycle

The initial application of the CyberSpace Emulation environment involved creating networks like the example shown in Figure 1, the CSE can construct a network from the wide range of virtual networking hardware (Digital Artifacts) already resident in the CSE library and easily selected from the dropdown menu at the top. Once the emulation is started, packets flow on the network and Red Teams have not been able to distinguish the packets of the virtual network from those of real networks. The packets can be captured in commercial products such as Wireshark as the virtual network looks just like a real network to any commercial tool currently used on the Internet. Such an "as designed" architecture provides both an interrogatable digital artifact and a dynamic emulation that has been used to evaluate the robustness of several proposed network architectures under given loads and configurations.

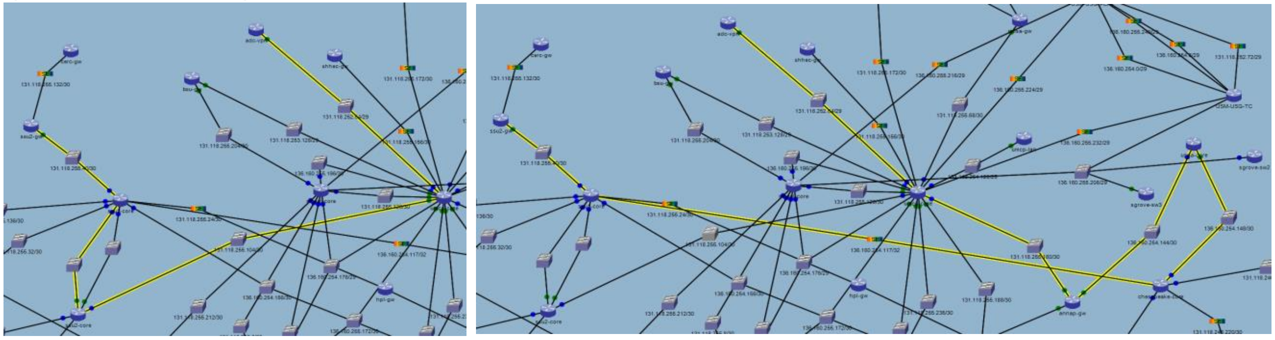


Figure 2a&b Yellow Line is Ping Path Before(a) and After(b) a Switch is Removed

Operating as a virtual network, the CSE can predict emergent behaviors that a typical simulation model cannot envision. It can also determine the impacts of interruptions and non-kinetic attacks and evaluate alternative responses to limit damage or remediate the system. For example, as shown in Figure 2a above, pings can be sent between any two points and the path will display on the screen. If a server, router, switch, etc. is removed, the CSE immediately replots the path precisely as the Internet would and provides the details on the increased time involved.

In Figure 3, a nested VPN tunnel emulation is shown while in a separate window seen in Figure 4 the transiting packets are displayed and can be analyzed by commercial products such as Wireshark^{TM} successfully decoding pcap data captured running in a CRA. All commercial tools that operate on the internet will operate on CSE produced network. And the emulation can be slowed to literally bit by bit movements to allowing complex interactions causing problems to be tracked step by step and the problem solved.

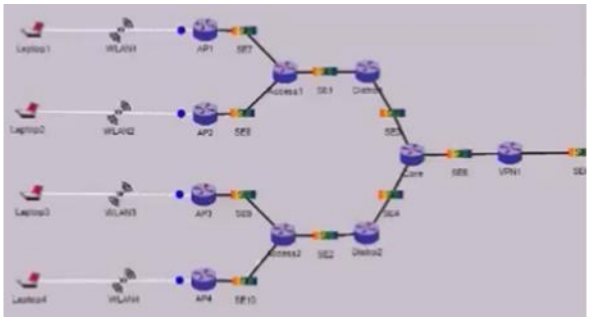
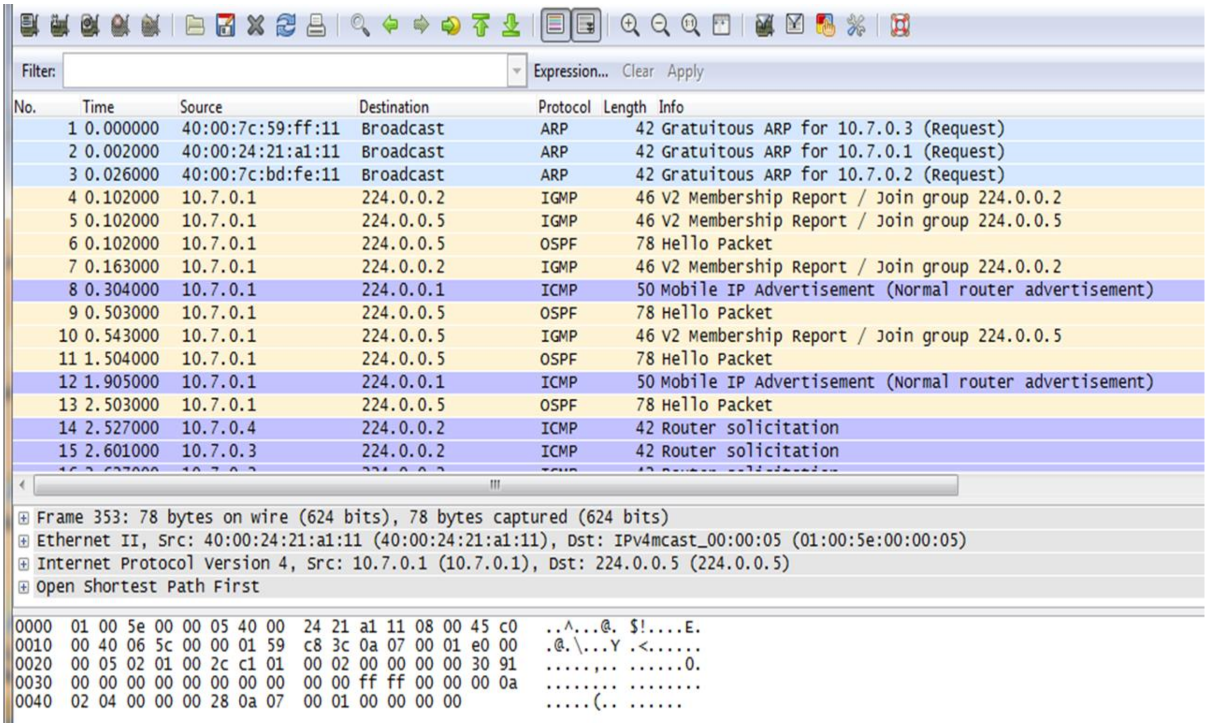


Figure 3 Nested VPN Tunnel Emulation (Sidhu, 2016)



```
No.  Time      Source             Destination  Protocol Length Info
   1 0.000000  40:00:7c:59:ff:11  Broadcast    ARP       42 Gratuitous ARP for 10.7.0.3 (Request)
   2 0.002000  40:00:24:21:a1:11  Broadcast    ARP       42 Gratuitous ARP for 10.7.0.1 (Request)
   3 0.026000  40:00:7c:bd:fe:11  Broadcast    ARP       42 Gratuitous ARP for 10.7.0.2 (Request)
   4 0.102000  10.7.0.1           224.0.0.2    IGMP      46 V2 Membership Report / Join group 224.0.0.2
   5 0.102000  10.7.0.1           224.0.0.5    IGMP      46 V2 Membership Report / Join group 224.0.0.5
   6 0.102000  10.7.0.1           224.0.0.5    OSPF      78 Hello Packet
   7 0.163000  10.7.0.1           224.0.0.2    IGMP      46 V2 Membership Report / Join group 224.0.0.2
   8 0.304000  10.7.0.1           224.0.0.1    ICMP      50 Mobile IP Advertisement (Normal router advertisement)
   9 0.503000  10.7.0.1           224.0.0.5    OSPF      78 Hello Packet
  10 0.543000  10.7.0.1           224.0.0.5    IGMP      46 V2 Membership Report / Join group 224.0.0.5
  11 1.504000  10.7.0.1           224.0.0.5    OSPF      78 Hello Packet
  12 1.905000  10.7.0.1           224.0.0.1    ICMP      50 Mobile IP Advertisement (Normal router advertisement)
  13 2.503000  10.7.0.1           224.0.0.5    OSPF      78 Hello Packet
  14 2.527000  10.7.0.4           224.0.0.2    ICMP      42 Router solicitation
  15 2.601000  10.7.0.3           224.0.0.2    ICMP      42 Router solicitation

⊞ Frame 353: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
⊞ Ethernet II, Src: 40:00:24:21:a1:11 (40:00:24:21:a1:11), Dst: IPv4mcast_00:00:05 (01:00:5e:00:00:05)
⊞ Internet Protocol Version 4, Src: 10.7.0.1 (10.7.0.1), Dst: 224.0.0.5 (224.0.0.5)
⊞ Open Shortest Path First

0000  01 00 5e 00 00 05 40 00  24 21 a1 11 08 00 45 c0   ..^...@. $!....E.
0010  00 40 06 5c 00 00 01 59  c8 3c 0a 07 00 01 e0 00   .@.\...Y .<......
0020  00 05 02 01 00 2c c1 01  00 02 00 00 00 00 30 91   .....,.. ......0.
0030  00 00 00 00 00 00 00 00  00 00 ff ff 00 00 00 0a   ........ ........
0040  02 04 00 00 00 28 0a 07  00 01 00 00 00 00         .....(.. ......
```

Figure 4 WiresharkTM successfully decoding pcap data captured from a CSE into packets (Sidhu, 2016)

Shifting from Developmental Networks to Emulate the "as built" Network Digital Twin

As a Digital Twin counterpart network moves from development to test to implementation or a legacy network signs on to be mapped, the orientation of the CSE shifts from the manually-input networks shown above to much larger systems that the CSE maps and reverse-engineers to automatically create a full representation of a network, end-to-end, out to its farthest boundaries and create a clone (an authoritative Digital Twin). To do this, the CSE software utilizes a wide variety of data sources rapidly collected from the network itself including Pcap, OSPF, EIGRP, BGP, Router Configs, Switch Configs, NetFlow, Nmap, Bro, VPNs, MPLS, SNMP, firewall data and inputs from commercial products such as Splunk, Tanium, and Traceroute. In most cases this data is obtained passively from the network itself or from tools that the network administrator is already using. Other data sources are being added as they are shown to reduce the effort in mapping some of the most complex networks in the nation's infrastructure. This mapping is reverse engineered and cross-checked until all anomolies are accounted for and a valid clone of the network exists.

For complex systems such as large networks, visualization integrated with easily accessible data is the best way to impart understandable views of the network configuration, its capabilities, limitations, and vulnerabilities. For this, the CSE provides a searchable display with zoom-in/out and query capabilities. At this point, the mapping is still a static Digital Twin of the actual network, but already has the capability to act as a baseline where data coming off the net can be quickly checked against the baseline and displayed for the user according to prioritized rules rather than requiring a manual inspection of every change for level of seriousness or not in line with the baseline.

Figure 5 below shows a map of the University of Maryland, Baltimore Campus (UMBC) network used with their permission. While this is only a small sample of the available network data, the CSE provides an ability to view the whole network and then drill down into specific segments or nodes and view all their associated data including IP/Name and/or any combination of device and generic properties as well as Compliance/ Vulnerability Results. With the CSE enabled mapping and visualization, automated reports can be generated thru simple commands and users can tailor those reports to meet individual needs or build new ones as needed. The types of report in additions to standard compliance reports is considerable, encompassing external addresses, internal addresses, external clients/servers, internal clients/servers, mapping logs, end-node attributes, router degree, sensor logs, configuration drift, and compliance scores.

Some of the inspections and other actions that can be conducted on the network map include:

- Displaying temporal changes to network such as changes to nodes, IP addresses, attributes, ports, etc. such as the additions and deletions from the network and allowing the user to select which to highlight.
- Validating network configurations against policies and generating automatic compliance reports such as DISA STIGS, USGCB, HIPPA Compliance, PCI Compliance, and Vulnerability Scans,

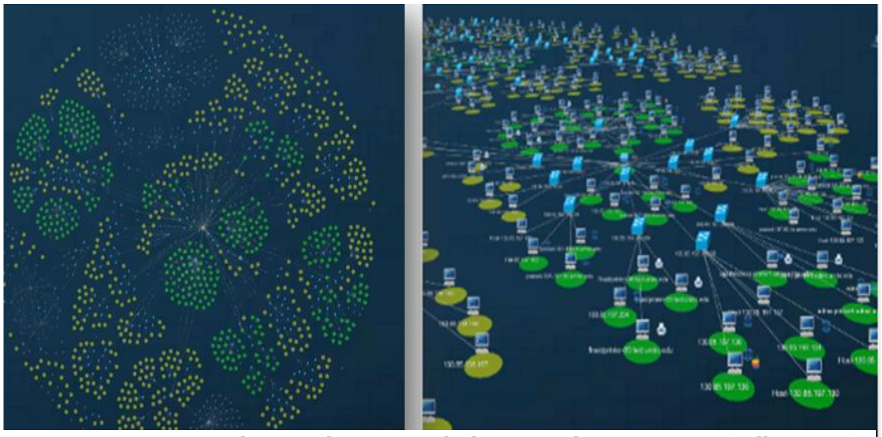


Figure 5 CSE Sample Visualization: Whole Network & Zoom-In (Sidhu 2017)

- Displaying cyber vulnerabilities and threats in graphic detail
- Displaying options for hardening networks against cyber-attacks
- Displaying the network in 2D and 3D at various abstraction levels such as Executive view and Mission Manager View
- Enriching network map with metadata including flow metrics, services, sensor locations, and geolocation
- Storing and sharing network maps for a variety of purposes

Emulating the Network Digital Twin and Matching the Dynamics of the Actual Network (Physical Twin)

The CSE also has the capability to emulate the network Digital Twin, particularly to conduct "what-ifs" and test new hardware and software. Note that this illustrates the ability of the CSE to seamlessly interface with both the internet and network related hardware including SCADA devices.

The Digital Twin emulation capability of the CSE can generate very large quantities of data associated with the operations of the physical network, but without disturbing the network. To process that data CSA has leveraged its analytic capabilities to build a set of Real-Time Network Mapping Analytics to both process data into the network clone and support operations to support the network and report on its health including:

- Big Data Network Data Fusion Analytics

- Big Data Network Mapping Analytics
- Analytics Identifying Anomalies across Network
- Large-scale Correlation Logic
- Generic Enrichment Engine

Typical discoveries made in the mapped networks include Duplicate Addresses, Phantom Devices, Phantom OSPF Interfaces, Unmanaged Devices (Security), and unknown Back Channels (Tunnels). Many of the problems found such as weak passwords are the fault of operators, while others come from miscommunication among the network's administrators, especially when there is a change in personnel. Shift Left, a standing OSD cyber test requirement asks developers to test earlier in the network development cycle in order to detect design laws. But Shift Right is even more crucial and requires complete life cycle network awareness. CSE offers a low-cost solution to catch the human errors which occur almost daily, detect misconfigurations and missing updates, and identify who is on the network. Annual inspections are only guaranteed for the immediate timeframe of their conduct. During operations to date, continuous monitoring has discovered misconfigured tunnels, firewall rules inconsistencies, unauthorized web servers, weak passwords, unprotected wireless access points, text files containing passwords to sensitive systems, and unpatched software & firmware to name just some of the vulnerabilities. The availability of a CSE-enabled monitoring system also offers opportunities for optimizing the network to reduce attack surfaces, improve network hygiene, fingerprint network assets, and baseline network configurations.

Packaging the CSE for Portable All-In-One Capabilities

Cyberspace Analytics has taken the CSE ability to create or map networks and then emulate them and implanted it into a highly portable form and combined it with capabilities to support network testing, cyber exercises and all levels of cyber training. As shown in Figure 6 the Cyberspace Range Appliance (CRA) is 9'' x 6.5'' x 6.5'' and weighs less than 9 pounds. It is composed of off-the-shelf computer boards and solid-state memory and is rapidly configurable for all its capabilities.

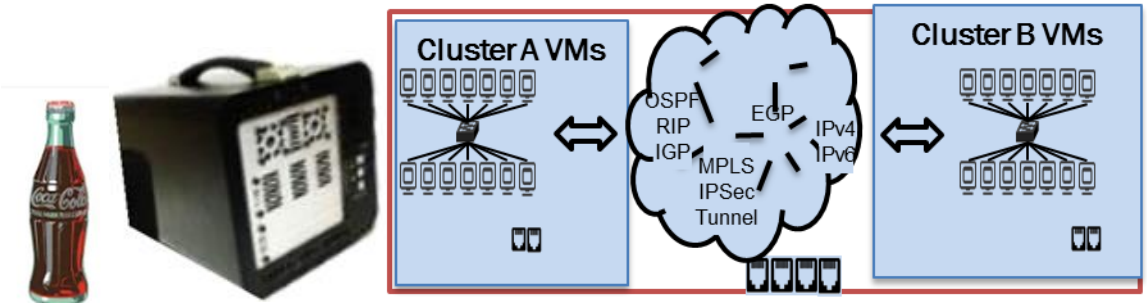


Figure 6 CRA, A Cyber Range Toolbox no Taller than a Coke Bottle (Sidhu 2018)

The CRA is a combination of physical <u>and</u> virtual infrastructures. Cluster A: Virtual Machines (VMs) (servers, cyber tools), Cluster B: VMs (servers, cyber tools) and the Cluster Core contains scalable hypervisor and the CSE network emulation software. The CRA has ports to connect to real routers, switches, servers, and laptops, i.e. to connect to live systems/networks as well as connect to other CRAs. This latter capability allows for daisy-chaining CRAs to create larger network environments. Some of the cyber tools already installed on the CRA are penetration testing tools such as Kali Linux and Metasploit, but users can also install their own hacking tools into one of the clusters. The CRA supports OSPF, BGP, STP, DoS, and Man-in-the-Middle attacks.

Another significant CRA application is the extreme shortfall in realistic cyber training environments. The DoD is attempting to address this with its initiative to develop Persistent Cyber Training Environments (PCTE), which we applaud, but Dr. Sidhu took a portable CRA to the Army Center for Cyber Excellence at Fort Gordon almost two years ago and conducted a demonstration of its capabilities. The reviewers were impressed but bemoaned the fact that they had not envisioned the existence of such a product and had no requirements for it. Thus, it would take at least two years to get the requirement "through the system" before they could act. We believe that every active and reserve cyber unit in the U.S. needs a capability like the CRA loaded with digital twins of every network they are expected to, or could be called in to, defend. These devices would belong to the unit and thus could be used whenever they wanted. The cyber warriors can try out risky defensive techniques on them without fear of bringing down an actual network, but with the confidence that if it works on the CRA Digital Twin it will work on its Physical Twin.

The CRA can be configured for either individual or team cyber training. For example, there are currently seven increasingly difficult cyber "Capture the Flag" exercises on the CRA and more practical exercises are planned. Having the CRA available allows both individuals and teams to learn by doing and to demonstrate their cyber skills by solving problems in increasingly shorter times. Two-sided exercises can also be performed on the CRA with one side defending a network and the other attacking. Each sees only what they would see with the tools they normally use to monitor a network. A separate "total" view is available to allow a White Team to track the exercise and collect data.

Like training, the portability of the CRA is also major advantage for testing. A Cyber Test Team or a Red Team can hand-carry the CRA on-board commercial or military aircraft and take the cyber test equipment to the system rather than the other way around. If a weapon system's network has been fully mapped and cloned, much of the testing can take place on the CRA.

Going the Next Step – Cyber Systems of Networked Systems

Combining CRAs with actual networks creates full fidelity Virtual-Live integrations for cyber testing. The Department of Defense is under Congressional mandate to test all its legacy weapon systems for cyber vulnerabilities by December 2019. This is almost an impossibility if each must be tested by the available Red Teams who must be given access to the actual networks to detect these vulnerabilities and cannot use some of their tools for fear of disturbing the network. As shown in Figure 7, above, the Cyber Range Appliances (CRA) can rapidly build multiple digital twins (software-based virtual clones) that can both replicate the networked operations of the systems under test and link them to actual systems to discover potential vulnerabilities. Furthermore, once the vulnerabilities of the

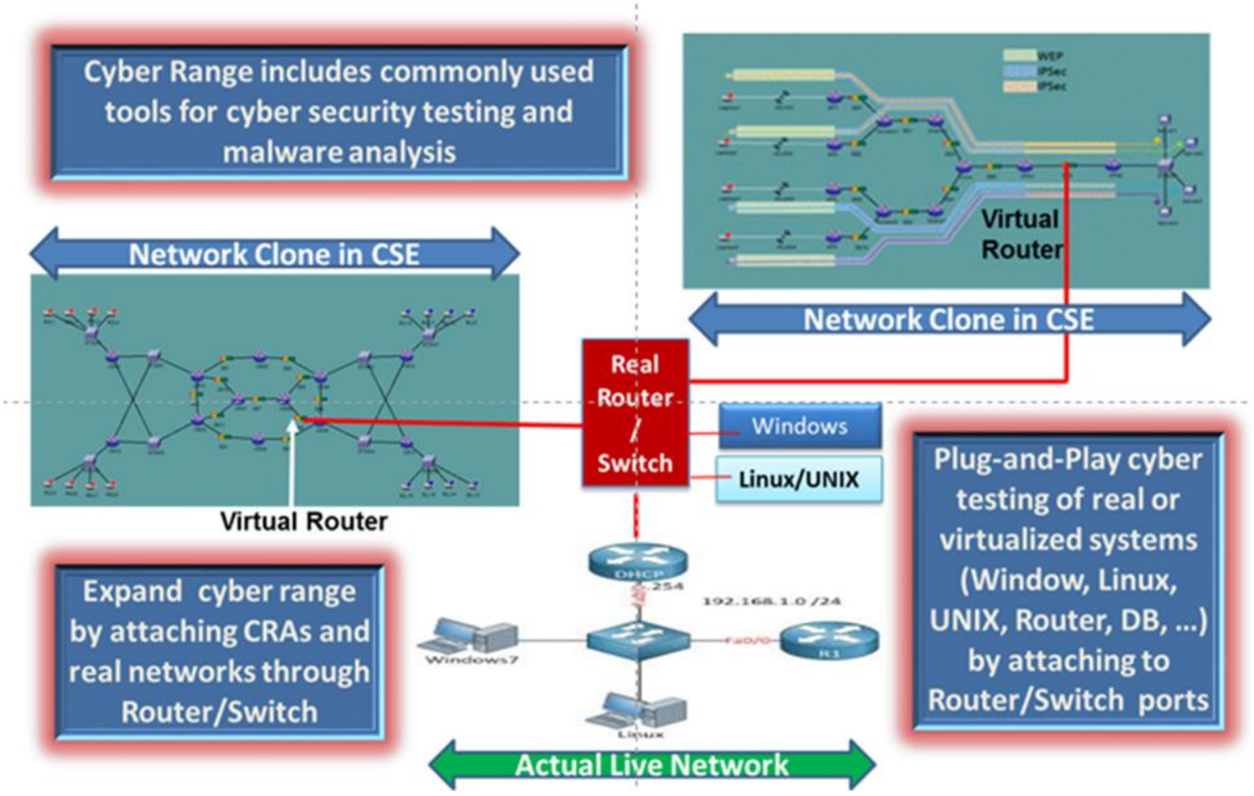

Cyber Range includes commonly used tools for cyber security testing and malware analysis
WEP
IPSec
IPSec
Virtual Router
Network Clone in CSE
Network Clone in CSE
Real Router / Switch
Windows
Linux/UNIX
Virtual Router
Plug-and-Play cyber testing of real or virtualized systems (Window, Linux, UNIX, Router, DB, ...) by attaching to Router/Switch ports
Expand cyber range by attaching CRAs and real networks through Router/Switch
DHCP
.254
192.168.1.0 /24
Fa0/0
R1
Windows7
Linux
Actual Live Network

Figure 7 Creating a Live-Virtual Integration of Networks (Sidhu, 2016)

individual networks are resolved, Digital Twins can be linked to form a System of Systems. Figure 8 shows some of the many combinations of virtual networks that could be linked in an integrated environment using multiple CRAs. This tests not only the network of the individual weapon systems, but the security and vulnerability of all the linkages to external networks that the network or weapon system might have to establish. Likewise, rather than collecting large amounts of hardware and corralling administrators from all the participating networks for a cyber test, the CRA could "stand in" for much of that hardware while still replicating the peripheral networks involved. There are a wide range of opportunities to test combinations of networks including ones that are still in development or in the middle of being deployed. Furthermore, once the test is completed, the Digital Twin should be left behind as a baseline against which changes or anomalies in the network can be automatically detected and compared and, based on user-input rules, either displayed as immediate alerts or saved for later review. Some can be accepted and added to the Digital Twin as valid changes, while others are investigated to determine their provenance.

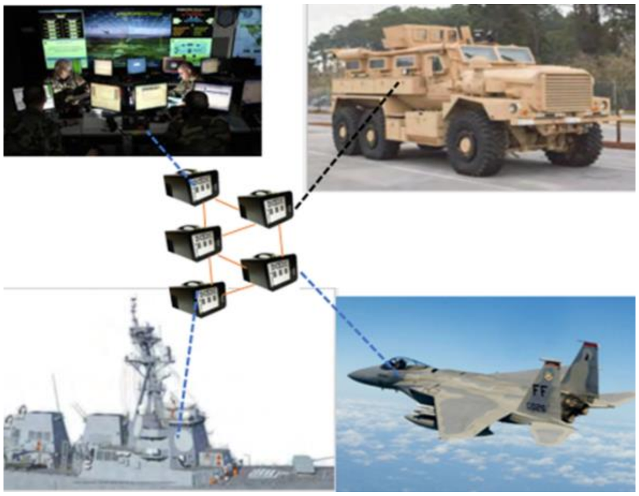


Fig 8 Joint/Combined System of Systems Tests (Sidhu, 2018)

Other Applications

In addition to training and testing with a Digital Twin capability, there are two more areas where they can be applied.

- The first is Analysis. DoD has been working on a Cyber JMEM for several years and expects the task to take several more. The CRA or some combination of them and live networks could serve as a low-cost Cyber Testbed for their JMEM calculations and experiments. Physical weapons such as bombs have test ranges where they are dropped under controlled conditions on a target or collection of targets allowing calculations of lethal ranges. CRA could serve a similar purpose for the JMEM effort.
- The second is offensive Mission Planning. While we cannot go into details about this area, we can mention that the full fidelity of the CSE/CRA promotes confidence in the outcome. They also offer the opportunity to estimate and minimize collateral damage and to first predict expected bomb (cyber) damage assessment and later, post attack, to assess the actual Cyber Damage.

SUMMARY

While DoD (Title 10) has been hesitant to adopt a CSE-based network Digital Twin, parts of the Intelligence Community (Title 50) and, since last year, the Department of Energy (Title 17) have made considerable use of the capability. On the non-government side, a variant of the CRA Digital Twin continuous network monitoring system has been adopted by several universities. As word spreads, more schools are being impressed by the relatively low-cost and observable reduction in cyber vulnerabilities that had not been previously achievable with the Cyber Tools and Checklists they had been using.

The nation is facing major cyber challenges. The demand for Cyber training, exercises, testing continues to outstrip supply, while building, installing, operating, and maintaining hardware-based cyber ranges remains costly and time consuming. The affordable 9lb. network Digital Twin generator can potentially satisfy a good deal of that demand.

Furthermore, technical obsolescence of cyber ranges is a perpetual challenge given the dynamic pace of technology changes and the huge expansion of the Internet of Things (IoT). Digital Artifacts of the hardware components of the Internet can be rapidly developed and easily distributed, possibly by the manufacturers themselves. These standardized artifacts would also address the most troubling of all cyber challenges, the fact that no hardware-based cyber range can truly replicate an operational network since they do not match the specific hardware models used in the actual network nor reflect the combinations of old and new hardware from different vendors and they cannot afford to do so.

The Digital Artifacts of a network are designed to properly represent their vendors specifications, but all are required to meet the strict interface standards of operating on the Internet, just like their hardware counterparts.

The CyberSpace Emulation Digital System Model is available to support network development and continue to predict the behavior of these networks as they are fielded. Even when only a few copies of a new network system are available, the CSE remains capable of predicting what the network can achieve at Full Operational Capability and how it will respond to future disruptions and attacks. CANES is one example, where we are interested in predicting its attack surfaces and potential vulnerabilities at Full Operating Capability.

Every operational network needs a Digital Twin for its full life cycle as the fielded network will start to change almost as soon as it is installed. These networks need the continuous monitoring and protection that systems such as the Cyber Range Appliance and its successors can provide not only against outside attacks but also from the many unintentional insider errors that produce unwitting vulnerabilities discussed earlier in this paper.

The concept of network Digital Engineering and Digital Twins is succeeding, but the applications are all too few in face of the nations' need.

REFERENCES

Office of the Deputy Assistant Secretary of Defense, June 2018 Department of Defense, Digital Engineering Strategy, https://www.acq.osd.mil/se/docs/2018-DES.pdf

Defense Acquisition University, Nov 2018 DAU Glossary, https://www.dau.mil/tools/t/dau-glossary

Cronk, T. M., DoD News, Defense Media Activity, Sep 2018, Digital Engineering Strategy Streamlines How Defense Systems Are Designed, https://dod.defense.gov/News/Article/Article/1631487/digital-engineering-strategy-streamlines-how-defense-systems-are-designed-offic/

Sidhu, D, Burdick, C, Eckenrode, M, 2018 A Virtual Network Environment for Cyber Operations, Testing and Training that is Scalable, Affordable, Supportable, and Effective, presentation to the MORS 2018 Emerging Techniques Forum. Available from authors or MORS.

Sidhu, D, Boteler, A, Engelbach, G. Taylor, R., Creating Near Real-Time and End-to-End Cyber Situational Awareness of University Networks (2017) Internet2 2017 Technology Exchange, San Francisco, CA, October 15-18, 2017. Available from authors.

Sidhu, D, Burdick, C, Low Cost Cyber Security Testing on a Plug & Play Virtual Cyber Range (2016). Presentation to the 84th Military Operations Research Society Symposium (MORSS). Available from the authors or MORS.