You Do need a Cyber Lab or Range

Let's explore some of these reasons and discuss some of the bigger challenges inherent in building and operating a Range capability.

Thoughts from a leader in the Field

J D Lovett

Creator of the DoD Cyber Security Range (CSR)

Technical Director (2009 – 2017) of the DoD CSR and MCCR

Consulting SME, Labs & Ranges, STAHL Consulting LLC

So, you need a Cyber Range – a pretty common thought these days as Cyber Labs/Ranges are proliferating across the government, education and commercial sectors. With the explosion of all things network it's not surprising; organizations are trying to build their own capabilities to assist in the defense and expansion of their portfolios as popular Range offerings are packed, making you wait for weeks or months to conduct a critical test. And they are expensive.

Let's explore some of the reasons people are building Ranges to help deal with their challenges in the ever-expanding world of Cyberspace.

Range Need – Most organizations building their own capability have a specific and recurring need that falls into one of the two major categories; test or training. When this need has to be timely it is important to have available Range cycles to immediately inject an event, not six months from now

Testing **-** Test Ranges focus on supporting the acquisition community's investment in new systems by creating a virtual world where the system can be tested to validate how they will perform once installed. As the Technical Director of the CSR, I supported many test events for DoD acquisition components including DISA, the Air Force, Marine Corps, Navy and also special agencies like DIA and NSA.

System-under-test - Systems under test is a common practice across the cyber community as the impact of the new system on existing networks needs to be identified, particularly the systems effect on the security posture. Systems that lack strong security elements will be identified and these shortcomings can be rectified before they are fielded so as not to contribute to a loss of the security posture. It's critical to these events that the "event" or virtual world closely mimics the actual planned fielding location. Why? Because every network enclave has a certain amount of security installed (and some have quite a lot) and the system will benefit from being inside that protective umbrella. Additionally, the system may draw many resources (services) from the enclave like everything already installed there and seeing how it does this is important as we look at system vulnerabilities. The goal is to have it as closely as possible to actually be able to gauge the upcoming fielding. A poor virtual world will mean a poor gauge of the actual fielding and then the test will be a waste of time.

New product testing - It's important to remember that placing a new product in a planned or potential location allows the product to benefit from the network's security posture, just like for system-under-test. The new product won't have to depend on itself, it inherits security from the receiving enclave. It's also good to note the "test" team that does the screening has a set of tools/toolsets that need to be injected into the virtual world to conduct the assessment. Lastly, the components of the event architecture that capture the results of the testing is paramount – without the raw data from the scans the analyst will just be writing in generalities. Expect these raw data points to go away at the end of the event for off-site analysis, so be prepared to offload the data.

The bottom line; you don't have to trust the vendor sales pitch when you can test the product within the Range. You'll know what it can and cannot do! Don't worry, the sales rep can still take you to lunch.

Training **-** Training Ranges are similar to test ranges as they also build virtual worlds to support the event, but these worlds focus on Warfighters and the tools they need to conduct their work. And since cyber-Warfighters come in many different types a one-size-fits-all approach will typically only benefit a vendor, not the personnel attending the event. Some of these events focus heavily on traffic generation to allow an instructor to inject a "hack" into the event and see how well the participants defend it. Other events focus on creating a chess board to allow a free-form red-on-blue event where defenders must maintain network services while attackers try to disrupt them. Of course, there are simpler training events where users are just simply trying to learn to operate new cyber tools; firewalls, sensors, routers, switches and/or scanners.

Warfighter Training - As the Technical Director of the CSR, I supported a hundred or so training events for DoD COCOMs and components; including STRATCOM, CYBERCOM, SOCOM, DISA, the Army, Air Force, Marine Corps, and Navy and also special agencies like the FBI, DIA and the NSA. One of the quickest lessons learned was that even though we all have similar needs; the details are always specific and different. Don't plan a one-size-fits-all approach to your training Range, it will not work!

Note: It is critical that training events be cooperative efforts. The instructors must be clear in their needs early in the process to ensure the event architecture supports the training objectives and the master scenario list (MSEL). Additionally, special tools may need to be injected to assist the instructor in the grading as well as data captures for offsite analysis (very common).

Other Types of Needs

Of course, there are many more types of needs beyond just training and testing; IT and Cyber departments the world-over have challenges. Two of those frequent challenges are modernization and modeling of threats.

Modelling persistent threats and IoT - The need to monitor the state of the enemy in terms of new attacks as they appear is not going away, it is accelerating. The ability to model persistent threats and identify potential points of impact are critical in protecting our network enclaves. That is especially important in terms of the Internet of Things (IoT). IoT is exploding across the networks as new tools are installed that contain some small ability to use the Internet.

From my time as the Technical Director, I saw many of these new tools (toys) being installed without a thought to how they affect the security posture of the network. Often, the customer would visit the CSR after some sort of exploitation occurred to try and find out what went wrong – the answer was pretty simple. Successful defense teams have learned that spending time to identify the status of new IoT items (before install) is critical to controlling the security posture of your networks.

Modernization - The DoD Network Modernization effort created a lot of need to model existing networks and identify potential security vulnerabilities based on design, separation of functions and data flow; and these needs are never done. Since the modernization plan changed multiple architectural components across the design model (workgroup, distribution and core were all affected) a special set of tests was needed to inform the architects. Sometimes a new theoretical model needs to be created, like the JIE model to prepare for the move to the cloud. It is also

important to understand the needs of the NetOps team and how new systems impact their work, as well as the task of simply replacing aging equipment.

Creating an As-Is model benefited the network architects greatly as they worked to develop the To-Be. It also better supports a decision-matrix that quickly shows how the new items will impact operations and staff and whether additional things (funds, SOP updates) are needed.

Unique Cyber Range Challenges

C&A challenges – There are numerous challenges for a new cyber system beginning with how it can protect itself from its normal daily function; re-creating typical "hacker" functions in a controlled environment. Understanding the scope of the system and the planned use cases allow an experienced range designer to begin the process. The designer should be in constant communication with the system owner and the official who will authorize the system to operate, as certain aspects of normal IT and cyber systems are complicated in Range systems, due to the hacking function noted above.

Note: I should mention the CSR C&A effort took constant work for 6 months to meet the desires of the authorizing official (USMC DAA). It went smoothly as I had a close working relationship with our executive and we exchanged ideas weekly and stopped to focus on issues as necessary (at least three times) so they wouldn't slow progress.

Distribution challenges – The use of distribution techniques for cyber ranges is an added benefit of being part of DoD – an organization that prides itself on network prowess and the ability to extend networks anywhere in the world, securely and quickly. The CSR made wide-use of the network-heavy talent of the staff to create a number of network distribution capabilities to allow for the remote use of the Range. These tools use encryption to accomplish the establishment of the tunnel through which the system will operate. If the tunnel happens to get shaky, all traffic stops until the tunnel is whole again, so nothing spills out.

Cloud Center vs Data Center – A common discussion across the community today is whether a Range be hosted in the cloud or should it be a stand-alone data center. The CSR was the first of its kind so a special data center was created for the numerous systems of differing classifications, while the PCTE project decided on a new private cloud specifically for the DoD Range portfolio. The ever-present challenge is how best to provide Range services to the customer without impacting production transport mechanism they may want to use for delivery.

Realism – It is important to understand that most customers don't really want a high-level of network fidelity in their Range events; something like 5% of the first three years, actually used high-fidelity. I should note that high-fidelity does increase system build costs – a cost benefit analysis should be conducted to ensure funds are spent wisely.

It's also important to provide real-world looking traffic to keep defenders engaged. All of the early modeling systems gave away "red" traffic as it was the only type of traffic that wasn't a set packet size. This allowed cyber defenders to quickly create a filter to show the red traffic and exclude all the regular stuff. Which meant the actual training value to high-level practitioners was nil.

The role of Concept of Operations (ConOps)

An aspect of the Range operation that is critical to identify early on; who will implement event areas. Many traditional labs only allowed customer access when the event was beginning, meaning lab operators did all the pre-event setup. This can be good but it can also be bad. Many customers won't have a lot of time to create their areas and prepare them for the event, so the ability of lab operators to implement them is good. Some events will use very specialized tools that require the customer professionals to install, and update them before the event. Lastly, there are a number of DoD customers with specialized tools that cannot be touched except for the professionals that operate them – to ensure their intellectual property is kept safe.

It's also important to note that Ranges have similar needs to a normal IT department but with a few small differences; mainly the focus of the staff and the automation and orchestration tools. Like a cloud center, the Range is always building new events where IT departments support a steady-state environment and only occasionally surge. The need for constant event builds means the Range staff will leverage automation tools to quickly roll out new systems to meet the event build plan. These tools will roll-out dozens of Microsoft and Linux devices of different flavors in the time it takes for one regular install. Another automation tool can be used to install and configure a set of network devices to allow for routing and switching, while yet another may be needed to install and configure a vendor-specific firewall or intrusion device.

The orchestration framework allows all the disparate automation tools to be managed efficiently through one "manager" toolset. As you probably noted above the Range will use a number of different automation tools because they typically require precise replication of manual functions, so a VM rollout tool will be different than a firewall tool which will be different from the networking tool. Having an orchestration tool lets you pull all of these together in a cohesive framework that will then support disparate systems across the event build without the need to write a tone of extraneous code (though there are times for this too). It also keeps you from relying too heavily on any single vendor-specific automation, which is helpful as you consider Range modernization.

Being in a constant build state is why the focus of the Range is necessarily placed on event operations with particular emphasis on efficiency and a structured approach. I prefer using a Scrum process as it supports multiple (event) builds very well. Lastly, I use the senior technical professionals as event leads so one person is in charge of each event build, assuming the operations tempo will require this (the CSR did over a hundred events a year after year three). This staffing model allows for a few high-level professionals to mentor a large number of junior professionals who will be responsible for performing a specific function, as needed by the operations manager and the event leads.

Two non-IT staff members need inclusion for Range operations; test engineers and red team professionals. Normal IT staffs don't conduct test events for customers so they are unaware of the strenuous needs of that profession. Having a staff Test Lead is very important and helps all of the pre-test event needs. Additionally, a trained red team is necessary for Range operations as most events (all types) want an opposing force of some kind. A senior red team member is important for Range design to allow the proper establishment of regional players and their particular styles – Range necessary parts of the dark web. I'll leave it there as the red team needs

are so great that a separate white paper focused solely on red teaming would be needed to make the discussion complete.

Scope Discussion

It's critical to review and identify the scope of the project before anything else. If not, certain desired types of events won't be supportable or at least in a timely manner. It will also point the way to the staffing footprint and potentially an operational process (ITIL, ISO, SCRUM).

The largest components of the system will be the 3 major sub-systems; network, storage and compute. Additional components for data capture, traffic injection and the distribution typically take longer to plan, order and receive on-site, so it's best to plan for small simple events early and more complex distributed events a bit later in the schedule. As you probably guessed from the red team perspective above a red-flavored sub-system will be included in the virtual Internet.

I also try and identify the design principles that will guide the build as part of the scope discussion. For the CSR and MCCR we practiced a very important principle – only use Internet Standards. We worked hard to not use any proprietary systems/protocols as eventually they will let you down or keep you from being able to exchange data, kind of a key component today. The guiding thought was simple; the Internet works so well for everyone because it's open, so stay away from tools/toolsets that aren't.

Recommendations

As a guy whose built a few of these systems and operated within a number of them, I always recommend a multi-day session to discuss the design, potential ConOps and the number and type of events be supported. It's the best starting point as it brings the scope of the system into focus. A design document (draft) would be the planned output from this session. It should capture every key aspect of the system and the planned use (events) as well as the design principles.

Once the design document is mostly final, the hardware/software list can be prepared and the request to order begun. As mentioned above, certain components of the system will take longer so planning for that can account for early success while the build is still underway.

Additional benchmarks along the timeline include system test (validate build), and certification. Adding a benchmark for distribution is also good as you can now support remote events in addition to on-site events.

Don't be afraid to outsource this work, it's how we manage key IT and Cyber functions the world-over. Lastly, a seasoned Range professional is needed inside the government PMO to ensure the compass keeps pointing toward the PM's desired end state. There are a number of very difficult but different issues that will need resolution as this project gets underway, you'll want a seasoned veteran helping you through the process.

What is STAHL Channels

He is one of the bench that STAHL has in its employment.

Who is JD Lovett?

JD is a Marine veteran with wide experience across the community (Lead Engineer, Firewall Engineer, Server Administrator, Network Assessor, NOC Manager, Base Network Manager) and the creator of the DoD Cyber Security Range (CSR). JD pitched the Range idea to STRATCOM in 2008, during an update session for the 8570 series, while working on a team of network auditors. The pitch was successful and the CSR pilot began the next year (2009) with a budget of 10 million.

After designing the CSR, JD served as the Technical Director from 2009 through 2017 and during this time developed an unmatched understanding of cyber range operations, having personally led over 100 events. The CSR design was the first DoD cyber lab/range to be certified by the Joint Interoperability Test Command (JITC) to support developmental and operational test (DT/OT) for IT and cyber systems. It also became the De Facto design for Ranges across the country. More importantly, it allowed the Military community to advance cyber training from a very basic capability in 2008 to a much more advanced capability today. A capability that supports the Defense Secretary's vision of building training that supports our warfighters in their true warfare space often referred to in the motto "train-as-you-fight".

JD was the thought leader inside the DECRE technical working group that pushed the Range community to enhance the portfolio and create standards. He was a principal contributor to the DECRE document library; Range Interface Standards Guide (2015), the Cyber Range Framework Vision (2017) and the DECRE Enterprise Reference Architecture (DRAFT)(2017).

His efforts through DECRE won funding for the 330-million-dollar PCTE pilot, which is now the biggest cyber training endeavor ever undertaken by the DoD. JD is also a plank-holder in the PCTE pilot, joining the project in 2017 and departing once success was proclaimed (2019). He is also the co-creator of the Marine Corps Cyber Range (MCCR)(2014) with his good friend and fellow IT and cyber SME Ernest McCaleb.