# Cyber Virtual Assured Network (CyberVAN)

A cyber environment for experimentation, operational planning, validation and training

**The challenge**

To counter evolving cyber threats, new and improved cybersecurity capabilities are emerging at a rapid pace. In order to ensure that resources are focused on the most promising approaches, there is a need for efficient and accurate evaluation and validation of cybersecurity tools in a realistic, high-fidelity cyber environment. Isolated and contained environments are needed for operational planning and what-if scenario experimentation. In addition, cyber IT specialists need high-fidelity reproducible cyber environments for training.

Such environments must be easy to define and specify, manage and maintain, and deploy and modify. They must also scale to handle tens of thousands of cyber elements, which include hosts, routers, switches, firewalls, infrastructure and ad hoc WiFi, LTE cellular and satellite communications. Finally, capabilities are required to easily define highly diverse computing environments, which could include multiple versions of different operating systems and services, each with their own known and unknown vulnerabilities, organized in different topologies, with different levels of access.

**The CyberVAN solution**

How does one create a cyber environment to represent an enterprise network? The easiest and highest fidelity solution is to deploy an exact replica of a known network by procuring the same equipment and deploying it in the same configuration, including the network elements' setup and connectivity along with the host software and user configurations. Clearly, such an approach is prohibitively expensive, in terms of hardware cost, physical space required and human labor. While it may seem like the natural alternative to deploy a virtual cyber enviornment supplied by a cloud service provider, there are network limitations to this approach as well.

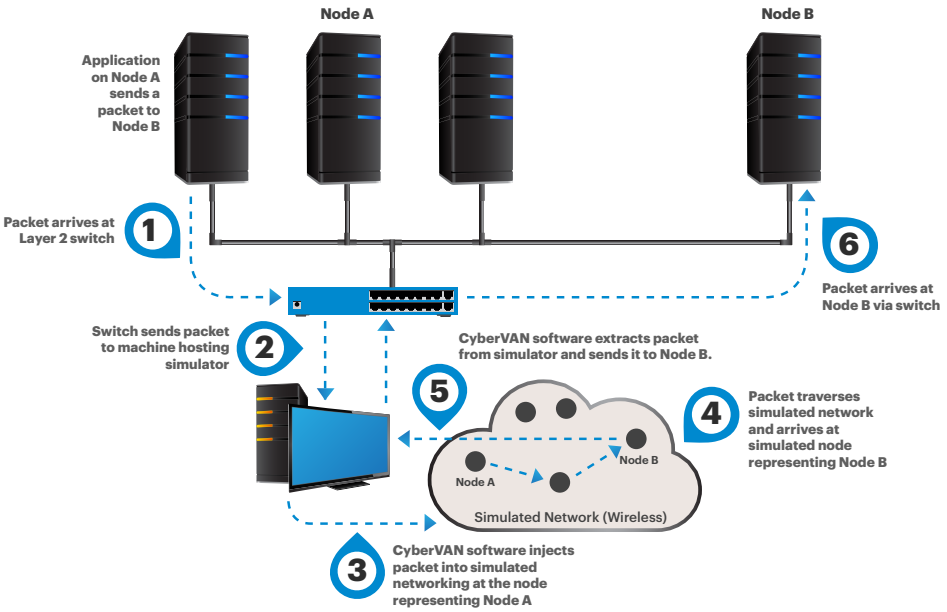
CyberVAN provides the highest possible fidelity representation of a network next to actually deploying the real network, by representing the network in a discrete event network simulator, and enabling hosts represented by virtual machines (VMs) to communicate over this simulated network.

**CyberVAN differentiators**

**High-fidelity network effects**

While existing cloud service offerings can provide high-fidelity representations of different host environments, they are limited in the networking capabilities they provide. For example, it would not be possible to connect two cloud hosted virtual machines via a WiFi Link. Network simulators like ns-3, which is used with cyberVAN, provide high-fidelity simulation of all network effects, including latencies, link capacities and routing protocols. In particular, wireless networks can be modeled with high fidelity, due to the ability to model mobility, interference, and propagation effects, as well as the details of different waveforms. This becomes critically important when cyberattacks that target different aspects of the wireless protocols need to be included in a cyber scenario. Accurate modeling of internet-scale networks is also not achievable using existing cloud service environments because of the inability to model internet protocols and services accurately.

perspecta LABS




**Technical specifications**

- Virtualization Technology: Qemu-KVM
- VM types: HVM (with PV drivers)
- TimeSync support: HVMs
- Management Framework: libvirt
- Containers technology support: LXC on multi-CPU Fedora 20
- Snapshots: Qcow2 external snapshot
- Preferred image format: Qcow2
- OS base: CentOS 7.5
- Bridging: Open vSwitch with static flow rules
- Supported simulators: ns-3.27

CyberVAN's innovative transparent forwarding technology enables IP traffic generated by services running on VMs to be sent via a simulated network to its destination VM. In order to accommodate large network simulations that may run slower than real time, CyberVAN incorporates our patented TimeSync technology that synchronizes the notion of time across VMs and the simulator, thereby enabling experiments to run slower than real time.

## Cyber management framework

CyberVAN provides sophisticated capabilities for managing the design, deployment and archiving of cyber scenarios. Users access CyberVAN via a web portal and use a scenario design graphical user interface (GUI) to design their network. CyberVAN automatically allocates the required hardware resources for the scenario. A scenario management GUI provides an environment for accessing and managing the elements of a scenario, including logging in to the VMs in the scenario, running various analytics tools on these VMs, saving the results of experiments and pausing and restarting experiments.

## Cyber effects library

CyberVAN provides a substantial, growing library of cyber effects, including tools for assessing vulnerabilities, scanning tools, ability to deploy VMs running operating systems with specific vulnerabilities and malware libraries for cyber testing.

## Realistic user traffic

A realistic cyber environment must include realistic traffic, which is generated by users on the network. A simplistic way of generating traffic on a network is to make use of tools like Multi-Generator (MGEN) that generate traffic conforming to specified rates and types between specified endpoints. However, such synthetic traffic can easily be spotted by traffic analysis tools. CyberVAN, on the other hand, provides capabilities for simulating real users driving applications on end hosts which in turn generate realistic network traffic.



**perspectalabs.com | info@perspectalabs.com**
150 Mount Airy Road
Basking Ridge, NJ 07920