White Paper

Operational Impact of Cyber Range Elements, Simulations and Realism

TABLE OF CONTENTS

1. Introduction 1
1.1. Operational Domains 1
1.2. Cyberspace Domain 1
1.3. Cyber Range Operations 2
2. Cyber Range Simulations 3
2.1. Internet and the World Wide Web 3
2.2. Critical Infrastructure Targets 4
2.3. Multimedia Realism 4
3. Cyber Range User Interface 4
3.1. Background Internet Traffic Map 4
3.2. Critical Infrastructure UI 5
4. Cyber Range Infrastructure 5
4.1. Traffic Generator 5
4.2. Security Systems 8
4.3. Event Management Systems 9
4.4. Network Systems 9
4.5. Virtual Infrastructure 9
4.6. Industrial Control Systems 9
4.7. Learning Management System 9
5. Spirent Cyber Range Solutions 10

1. Introduction

It's all about OPS! The value of a cyber range can be found in its ability to support operations and the multiple roles that OPS personnel perform at security centers, network centers, and data centers. The best cyber ranges are designed and developed by engineering teams with OPS experience in theater operations, security operations, and network operations.

In essence, a cyber range is a training environment used to train cyber warriors to operate in the cyberspace domain. This white paper will discuss how the realism of cyber range simulations and elements have a major impact on the quality of operations training.

1.1. Operational Domains

Until recently, the U.S. military classified operational domains into air, land, sea, and space domains. The establishment of the U.S Cyber Command added cyberspace as a domain. The U.S. military defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology, infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

Ranges are locations where people train to accomplish a mission. Golf ranges are used to train golfers how to improve their golf game. Shooting ranges are used by civilians and military personnel to train how to use and aim a firearm against a target. The U.S military has multiple ranges to train Air Force, Navy, Army, and Marine Corps personnel. Likewise cyber ranges reside in a facility and provide a training environment for cyber warriors operating in the cyberspace domain. The main function of a cyber range is to train personnel on how to defend critical infrastructure assets and launch attacks against simulated critical infrastructure targets.

1.2. Cyberspace Domain

When discussing cyber warfare and cyberspace, the first thing that comes to mind is the Internet. Everyone is familiar with it. It is the most popular computer network ever devised by man and is used by billions of people. Security vulnerabilities and attacks that can be exploited via the Internet are reported in the news on an almost daily basis. Applications and critical infrastructure components connected to the Internet represent the vast majority of exploits, but, there is more to cyber warfare than just the Internet. Cyberspace includes networks and associated elements that do not use the TCP/IP protocol suite that is traditionally associated with the Internet.

Industrial Control System (ICS) and Guidance Navigation Satellite Systems (GNSS) that may not be connected to the Internet need to be protected against security attacks and intrusions. ICS systems control refineries, utilities and the electric grid. The U.S. Guidance Positioning System (GPS) provide essential services for both military and commercial applications. Bad actors capable of exploiting ICS and GPS vulnerabilities could cause incredible damage to the military and civilian population. The recent discovery of GPS vulnerabilities has created a new sense of urgency to train cyber warriors to detect, isolate and block signal attacks against satellite systems. This is why modern cyber ranges are incorporating ICS test & measurement equipment along with GPS signal generators that simulate GNSS security vulnerabilities.

1.3. Cyber Range Operations

Operations are performed in multiple facilities that may include Data Centers, Network Operations Centers (NOC) and Security Operations Centers (SOC). In recent years there has been a trend to consolidate network operations and security operations into a Network Operations and Security Center (NOSC). An Incident Response Team (IRT) responsible for mitigating and neutralizing security attacks reports to a SOC. A Director of Operations manages the NOSC and is responsible for both network and security OPS.

The similarities between a football game and a cyber range exercise are many. Both require good defense and offense strategies. Government and military often use the terms red team and blue team to reference offensive and defensive operations. Red teams play the role of attack teams and blue teams play the role of network defenders. A cyber range that does not provide realism in its simulations does not prepare cyber warriors to succeed in the cyber space domain.

1.3.1. Operational Views

Operational managers can leverage multiple frameworks in support of their operations. The Department of Defense Architecture Framework (DoDAF) can be useful in the development, capturing and streamlining for all types of operations including security and network OPS. DoDAF defines multiple views including operational view, systems view and technical view. Operational views are developed by enterprise architects to capture and define operational nodes, operational activities, and operational information exchanges performed at operations and mission centers.

1.3.1.1. Operational Nodes Connectivity Diagram

Multiple teams are responsible for NOSC operations. The teams often reside in the same facility and under the same management but they can also be geographically dispersed. Successful operations require that all teams understand the roles and responsibilities of their teammates. An Operational Nodes Connectivity Diagram is used to facilitate understanding of the different roles and responsibilities that the teams play. An operational node represents a team. It could be the management team, network team, security team or IRT team. The diagram connects the nodes that communicate with each other using what is commonly reference as “need-lines.” The need-lines are assigned identification numbers and have labels for the type of information that they represent.

1.3.1.2. Operational Information Exchange Matrix

Information exchanges between operational nodes are captured in an Operational Information Exchange Matrix. The matrix includes the producer and consumer of information. Every record in the matrix includes an information identification number, information description, information producer, information consumer, and associated need-lines from the Operations Nodes Connectivity Diagram.

1.3.1.3. Operational Activity Model

Operational activity models are used to capture all the activities performed at the NOSC. A typical activity model will include over a hundred activities and will be captured using Integration Definition for Function Modeling (IDEF) charts with flow arrows.

1.3.1.4. Organizational Relationship Chart

An Organizational Relationship Chart is a chart that illustrates the multiple roles performed within the organization. It could include roles for network engineers, security engineers, satellite engineers, security analysts, and operations managers.

1.3.2. Offensive Operations

Offensive operations require a cyber range with the ability to generate security attacks using broadband networks, wireless networks and satellite networks. A cyber range should be able to generate security attacks that target Common Vulnerabilities and Exposures (CVE) for application layer protocols, security layer protocols, transport layer protocols, network layer protocols, data layer protocols, and the physical layer spectrum. The cyber range should also be able to launch or simulate Denial of Services (DoS), Distributed DoS (DDoS) and Botnet attacks. Botnet attacks are the most difficult to simulate and detect since they require master to slave transactions at different time intervals.

1.3.3. Defensive Operations

Defensive operations require a cyber range with the ability to detect, isolate and block traffic anomalies and security attacks. This requires a cyber range infrastructure that includes security devices including firewalls, IDS, IPS and SIEM event managers. Defensive operations are probably more important than offensive operations since thousands of enterprises and government agencies cannot launch cyber attacks and are only interested in protecting their networks and mitigating cyber attacks.

2. Cyber Range Simulations

2.1. Internet and the World Wide Web

A true cyber range should be able to simulate the entire Internet and support operations. As mentioned previously the first thing that comes to mind when discussing cyber attacks is the Internet. The Internet is a global network that connects billions of people using billions of computers. It is a public network being used by individuals, businesses, countries, governments, civilians and military organizations. It has been widely adopted by people to conduct retail purchases and banking transactions. Businesses rely on the Internet to provide customer and employees services. Service providers use the Internet to manage their infrastructure and supply chains. It is the World Wide Web that makes it easier for criminals, terrorists and spies to commit fraud, steal financial data, intellectual property, state secrets and target critical infrastructure. A cyber range without a comprehensive simulation of the Internet is at a severe disadvantage in the operations and training domain.

2.1.1. Regional and Country Traffic

A cyber range should simulate traffic for all the countries in the world. In order to simulate multiple countries and regions, a cyber range should emulate real IP addresses using host and network addresses assigned by the Internet Assigned Number Authority (IANA). Using more than one IANA network address per country will inject additional realism and problem solving challenges for personnel being trained. A cyber range that does not provide realism in its simulations does not prepare cyber warriors to operate in the cyber space domain.

2.2. Critical Infrastructure Targets

A cyber range should be able to load critical infrastructure targets and generate security attacks against them. Traffic generators should be able to import data to rapidly configure the target traffic profiles.

2.3. Multimedia Realism

Video and Audio continue to represent a large portion of Internet traffic. Streaming traffic from YouTube and Netflix consume a very large amount of service providers traffic. Skype, Voice over IP (VoIP) and Voice over LTE (VoLTE) also represent a big segment of the Internet traffic mix. Emulation of multimedia voice and audio services should be part of next generation cyber ranges. A cyber range should include traffic generators capable of generating real video and audio that can be seen and heard using Internet client applications such as browsers.

3. Cyber Range User Interface

Next generation cyber range systems should leverage graphical User Interfaces (UI) to present information to users. The best UIs should be intuitive and easy to use.

3.1. Background Internet Traffic Map

Cyber ranges used to train military personnel should be able to group IANA IP addresses by regions. A cyber range UI should leverage a map of the world to represent and select source and destination background traffic. The UI background traffic could be selected and grouped by countries, continents, regions or military commands. The map should allow users to select countries or regions to include in the traffic profiles that will generate the IANA IP traffic. User interfaces that group countries by the seven continents should display a user selectable map of the same. Government or military personnel prefer to group countries by military commands or geographical regions. Figure 3-1 illustrates a typical world map that could be use to select background Internet traffic for countries or regions.

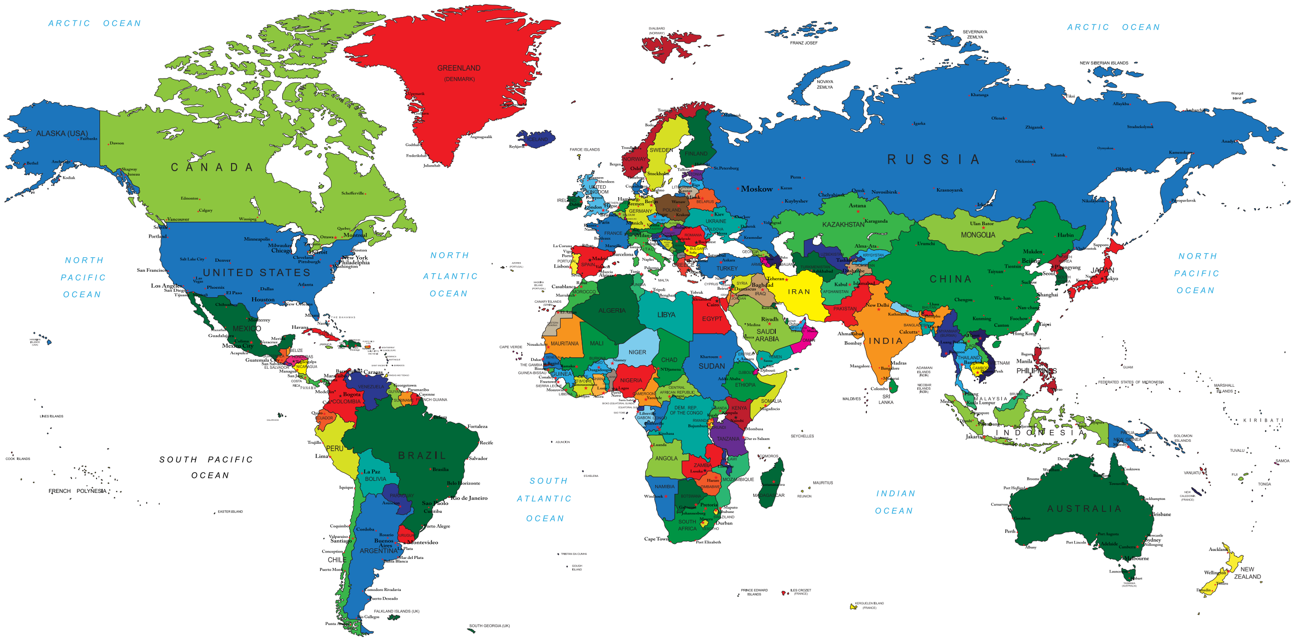

Figure 3-1 Background Internet Traffic Map UI

The advantage of using geographical regions that include North America, Central America, South America, Europe, Middle East, Africa and Asia Pacific is that most military commands are grouped by geography. The United States military is perceived as the predominant military power in the world and many countries use its military command structure as a baseline for operations. The U.S. combatant commands are organized on a functional or geographical basis. The present commands organized by geography include, Northern Command, Southern Command, European Command, Central Command, Pacific Command and Africa Command. Some of the U.S. commands organized by functions include the Cyber Command and Space Command. A flexible cyber range should include default options for grouping countries into geographical regions or the U.S. combatant commands. It should provide users with the flexibility to group countries into their own command structure.

3.2. Critical Infrastructure UI

Cyber ranges should be able to allow users to select multiple targets representing critical infrastructure. Targets should be grouped by their industry classification. Industry groups should include financial, utilities, electrical grid, ecommerce, transportation, refineries and petrochemicals, food supply, and other critical infrastructure segments.

A critical infrastructure user interface should at the minimum include a drop down menu that allows users to select one or multiple targets within the critical infrastructure segment. A cyber range should be able to import target data and simulation data to make it easier on users to simulate background and target traffic of their choice.

4. Cyber Range Infrastructure

A cyber range environment consists of multiple infrastructure elements that enable operations training. The first element is the traffic generator. Other elements include event management systems, security systems, network systems, virtual systems, Industrial Control Systems (ICS), GNSS and Learning Management Systems (LMS).

4.1. Traffic Generator

Cyber range need traffic generators for multiple functions. They are needed to emulate realistic IP addresses for all the countries in the world using the pre-defined IP blocks managed by the Internet Assigned Number Authority (IANA). A traffic generator needs to be able to generate traffic for hundreds of IANA country codes. Traffic generators also need to simulate thousands of server and client computers with their respective application, security, transport and network protocols. The ability to generate security attacks is essential to any cyber range environment and has to be supported by the traffic generator.

4.1.1. Apps & Services Requirements

In order to simulate the entire Internet, the cyber range traffic generator needs to generate Layers 2-7 protocols. Layer 2 protocols include the Ethernet protocol specification. Layer 3 protocols include the IPv4 and IPv6 protocols. In the United States, IPv4 is the most common network protocol while IPv6 is widely used in Asia Pacific and European countries. A cyber range traffic generator needs to simulate transport protocols including the connectionless UDP and connection-oriented TCP protocols. In addition, a cyber range requires the ability to generate enterprise traffic.

4.1.1.1. Social & Internet Apps

Cyber range traffic generators need to be able to generate realistic Internet traffic. Video and audio account for most of the Internet traffic, with Netflix and YouTube video streaming making the bulk of video streaming traffic. It is very important that a traffic generator can render real video and audio streams from the traffic generator server ports. The ability to simulate Netflix, Hulu, YouTube and similar traffic is a must for a cyber range traffic generator.

The cyber range traffic generator should be able to generate traffic simulating the most popular Internet social Apps. Web site traffic rankings for any country show that social Apps like twitter and facebook are always ranked in the top five. A cyber range traffic generator should also simulate search engine traffic for Google, Yahoo, and Bing in addition to web mail and chat services like Gmail, Yahoo Mail, Hotmail and Yahoo Messenger. The traffic generator should also simulate entertainment Apps and games.

4.1.1.2. Mobile Apps

Mobile Apps continue to grow, accounting for a big chunk of the Internet traffic. A cyber range traffic generator should be able to simulate hundreds of mobile Apps for the most popular mobile devices. The traffic generator should generate Android and iOS client to server transactions for multiple user agents and App IDs.

4.1.1.3. Enterprise Services

A cyber range traffic generator should be able to simulate the enterprise services that an IT organization provides to their user base. These services range from email services based on the IMAP, POP and SMTP protocols to database services for MySQL and Oracle databases. Enterprise services include voice services based on the SIP protocol and should be included as a requirement for cyber range traffic generators.

4.1.2. Satellite Apps

A cyber-range traffic generator should be able to generate satellite signals including Global Navigation Satellite System (GNSS) signals. It has to be able to generate accurately modulated signals for all Open Service frequencies on all usable GNSS constellations (e.g., Global Positioning System (GPS), GLONASS, Galileo, Beidou), regional augmentation systems (QZSS, IRNSS) and Space Based Augmentation Systems (EGNOS, WAAS). The cyber-range traffic generator also needs to have the capability of being used to simulate the classified service signals to authorized users.

In addition to providing accurate simulations of the Radio Frequency (RF) characteristics of these GNSS signals, a cyber-range traffic generator needs to be able to generate or replay realistic interference waveforms and allow the user to position the interference source accurately in static or dynamic scenarios. Ideally the cyber-range would allow users to replay interference waveforms that have been detected in the real world. The cyber-range must also be able to recreate GNSS navigation messages in full and have the capability of permitting the user to alter the contents of the navigation message in order to simulate hacking of the navigation message. The cyber-range traffic generator should be able to provide a facility for generating invalid navigation message data to simulate Zero-Day attacks that exploit the GNSS navigation message.

4.1.3. Security Requirements

Cyber ranges need to be able to generate security attacks against critical infrastructure targets. Attacks should exploit client and server computers, network devices, security devices, ICS and SCADA controllers, and satellite systems. Security attacks should target all protocol layers.

4.1.3.1. Common Vulnerabilities and Exposures

A cyber range exploit database should follow the industry Common Vulnerabilities and Exposures (CVE) classification. Every year, thousands of security exploits are detected. It is imperative that a traffic generator is able to support thousands of CVE exploits in its database and that the database is updated periodically.

4.1.3.2. Denial of Services

A cyber range should be able to generate stand-alone and Distributed Denial of Services (DDoS) attacks. DDoS attacks should target the network layer, transport layer and application layer protocols.

4.1.3.3. BOTNETS

A cyber range should be able to simulate the master and slave transactions behavior of BOTNET programs. It should mimic BOTNET master operations for scanning client and server targets, exploiting the targets and communicating periodically with the exploited slave.

4.1.3.4. Fuzzing

The most dangerous security exploits are known as Zero-Day exploits. These types of exploits suddenly appear at a time when the security industry has yet to develop patches or fixes for the Zero-Day exploit. Fuzzing technology can help find Zero-Day exploits by generating invalid data that has not been specified for a protocol specification. It is imperative that cyber range traffic generators are capable of simulating Zero-Day attacks using fuzzing technology.

4.1.3.5. GNSS Vulnerabilities

The signal strength of GNSS signals reaching the surface of the Earth is very low. This makes GNSS receivers vulnerable to various types of interference that includes signal jamming and spoofing cyber attacks. A cyber range needs to be able to simulate these types of GNSS threats to provide value to receiver manufacturers and integrators, allowing them to assess the robustness and ability of their system to detect, warn and reject faked or spoofed GNSS signals.

GNSS interference can occur by natural or man-made mechanisms. One example of natural interference is multi-path interference. GNSS Receivers need to be able to cope with signal reception in a high multipath environment that involves discriminating between direct path and multipath signals in the receiver’s Digital Signal Processor (DSP).

A man-made attack vector can consist of a custom jammer disguised as a cigarette lighter that generates an L1 ½ Watt broadcast Chirp signal. GNSS receivers should be as robust as possible against this kind of jamming and need to have mechanisms in place to avoid processing hazardously misleading information. In the GNSS Receiver itself, the implementation of multi-constellation and multi-frequency architectures can provide a high degree of protection from portable L1 jammers. DSP mitigation techniques, INS augmentation and the use of active excision techniques could also play a part in a defense against more sophisticated or powerful jammers.

Spoofing attacks are more complex and are always the result of a malicious attack against the GNSS Receiver. Spoofing requires that a GNSS receiver accepts a fake signal as the real signal. This requires the synchronization of the fake signal with the authentic signal in order for the correlators of the target receiver to lock onto the false signal. There are then two possible attack vectors. Conventional spoofing involves adjusting the pseudoranges of the fake GPS signals so that the GNSS Receiver reports that it is located at a false position in space and time. The second attack vector is to disable or degrade the GNSS receiver by hacking the GNSS navigation message – this can be carried out with all GNSS Open Service signals; for example, by setting satellite statuses falsely to “unhealthy” or issuing a clock or ephemeris adjustment. The cyber range needs to be able to simulate all of these threat vectors.

GNSS Receivers also have the capability to report position, velocity and time on demand via communications channels that may include Ethernet or 3G wireless links. This means that the GNSS receiver could be subjected to other types of attack vectors including DDOS via the communications link used for reporting. Next generation cyber ranges need to have the capability of simulating this type of GNSS attack.

4.2. Security Systems

A cyber range environment requires security devices in order for trainees to be able to detect, isolate and block security attacks and exploits. Perimeter firewalls are used in the perimeter between the Internet and an enterprise network. The firewall protects internal enterprise traffic from exploits by filtering inbound and outbound traffic. Application level firewalls that can perform deep packet inspection and detect social network protocols such as facebook, twitter, and linkedIn should also be part of the security systems.

Intrusion Prevention Systems (IPS) should be included in the cyber range. They should be used to detect known and unknown security attacks. Known security attacks are attacks that have already been classified as Common Vulnerabilities and Exposures (CVE)s. There are two types of IPS systems; behavior-based and signature-based. Signature-based IPS are only good against previously known CVEs while behavior-based are effective against certain types of Zero-Day attacks.

In order to avoid a single point of failure, Next Generation (NG) Firewalls used in a cyber range environment should not be configured to perform all security functions in one appliance. Multiple layers of protection or defense-in-depth is still the best risk mitigation architecture to protect enclaves and enterprises.

A cyber range needs to be able to detect BOTNET security attacks. BOTNETS are programs or malware that exploit servers and other network devices. BOTNETS could appear to be dormant for a period of time but can be awakened by a Master application. The behavior of BOTNETs is very difficult to detect and is based on master and slave communication transactions. A dedicated behavior based IPS that has a proven record in detecting BOTNETS should be part of any cyber range environment.

4.3. Event Management Systems

A Security Information & Events Manager (SIEM) application is essential in a cyber range environment. SIEMs are used to display the data collected by network and security systems. SIEMs generate events or alarms that are used to visualize and prioritize the workload of network engineers, security engineers and analysts. Without a SIEM, operations personnel are flying blind.

Cyber range operators have multiple choices when selecting SIEMs applications. Next generation SIEM applications have opened their Application Program Interface (API) allowing developers and Network Equipment Manufacturers (NEM) to write their own SIEM apps.

4.4. Network Systems

A cyber range requires network devices to route Internet traffic from client computers to server computers. Network devices are also needed in order for trainees to be able to switch and route network traffic, isolate network links and block devices using Access Control Lists (ACL)s. Ideally a cyber range should include Layer-2 & Layer-3 switches and routers. Network devices should support both IPv4 and IPv6 network protocols in addition to the most popular routing protocols. OSPF, BGP, IGMP and multicast protocols should be supported.

4.5. Virtual Infrastructure

Virtualization of data centers components offers many advantages. Virtual components such as servers, network devices and security devices enable Incident Response Teams (IRT) to accelerate the response time for mitigating security attacks. In a virtual world you can stop a compromised Virtual Machine (VM) and instantiate a good VM in a matter of minutes. The compromised VM can easily be cloned for forensics analysis. Virtualization requirements for cyber ranges include being able to virtualize traffic generators, test and measurement tools as well as network and security devices.

4.6. Industrial Control Systems

A cyber range should be able to simulate ICS and SCADA systems. A specialized ICS firewall should be a required component in a cyber range environment. A few companies specialize and market ICS firewalls.

4.7. Learning Management System

Learning Management Systems (LMS) are often bundled with cyber ranges to help deliver training lectures and operational exercises. Although LMS can be very useful in a cyber range, the reader should be careful. There are multiple integrators in the federal segment that market cyber ranges that do not generate realistic traffic and are nothing more than an LMS providing little value to operations training.

5. Spirent Cyber Range Solutions

Realism is the most important characteristic in a cyber range. It has a major impact on the quality of operations training. Real audio and video streams from a cyber range simulation should be able to play on a web browser such as Firefox or any other web client application. A cyber range that cannot render real video and audio traffic streams is of little value for OPS training. A next generation cyber range should be able to simulate GNSS traffic including GPS signals and vulnerabilities. It should be able to simulate 4G LTE and 3G GPRS cellular, wireless and data networks.

Spirent cyber range solutions leverage the strength of our Apps and Security platforms, GNSS platforms and mobile platforms to create the most realistic OPS training environment in the industry. Spirent provides the most realistic audio, video, web and Internet simulations for operations training.

Spirent Communications
1325 Borregas Avenue
Sunnyvale, CA 94089 USA

AMERICAS 1-800-SPIRENT | +1-818-676-2683 | sales@spirent.com
EUROPE AND THE MIDDLE EAST +44 (0) 1293 767979 | emeainfo@spirent.com
ASIA AND THE PACIFIC +86-10-8518-2539 | salesasia@spirent.com

The information contained in this document is subject to change without notice and does not represent a commitment on the part of Spirent. The information in this document is believed to be accurate and reliable; however, Spirent assumes no responsibility or liability for any errors or inaccuracies that may appear in the document.

TESTED WITH SPIRENT