White Paper

Accelerating the Deployment of the Evolved Cyber Range

Ixia BreakingPoint Uses Patented Innovation to Deliver a Pragmatic Solution for Arming and Training Cyber Warriors

26601 Agoura Road, Calabasas, CA 91302 | Tel: 818.871.1800 | Fax: 818.871.1805 | www.ixiacom.com | 915-6751-01 Rev. B, June 2013

Table of Contents

Executive Summary

Organizations worldwide face a dangerous shortage of cyber warriors with the skills required to defend against cyber terrorism. This urgent situation is made worse by the weaknesses and vulnerabilities that continue to pervade critical IT infrastructures—despite billions of dollars invested in cybersecurity measures.

Answering these problems requires Internet-scale simulation environments, along with a comprehensive training curriculum and proven methodologies, to develop elite cyber warriors and simulate attacks on IT infrastructures. Military commanders, defense contractors, and even commercial analysts such as Gartner refer to these environments as "cyber ranges."

Although cyber ranges are a necessity for training cyber warriors, in recent years the old approach to building them has been exposed as a costly and futile exercise. Flagship cyber range projects relying on that outmoded approach have wasted years and hundreds of millions of taxpayer dollars merely to study the problem.

> Although cyber ranges are a necessity for training cyber warriors, in recent years the old approach to building them has been exposed as a costly and futile exercise.

Yet Ixia BreakingPoint has harnessed patented network processor technology to deliver a better approach — one that creates an Internet-scale cyber range environment from a single 7-inch-high device. This breakthrough invention removes the obstacles that once prevented the widespread deployment of cyber ranges for arming and training cyber warriors. This paper illustrates how government, intelligence, and military organizations throughout the world can leverage that innovation to rapidly deploy a battle-proven, operationally relevant closed environment that reflects the entire Internet for a small fraction of the cost of traditional models.

Leveraging its cyber range experience, BreakingPoint has formulated a four-point strategy for preparing organizations to defend national interests by assessing, educating, and certifying elite cyber warriors and equipping those forces to harden the resiliency of critical network and data center infrastructures. The capabilities and strategy described are not a research project or an exorbitant consulting arrangement; they are available and ready for cost-effective deployment today.

The Global Cyber Range Imperative

Those who do not remember the lessons of the past are doomed to repeat them. Yet today the same complacency that has led to catastrophic losses so many times is placing the world's leading nations at risk, this time in the fifth battlespace—the cyber domain. Without urgent action and investment to harden the resiliency of national cyber defenses, the impacts of cyber attacks will continue to multiply.

Just as every military and police force needs a firing range to hone weapons skills and battle tactics, every cyber warrior needs access to a cyber range. Only with an Internet-scale, operationally relevant, and ever-current cyber range can commanders produce the empirically valid war-gaming exercises necessary to develop their troops' skills and instincts for offensive and defensive action. Similarly, the only way to understand the resiliency of IT infrastructures is to assault every element within them using the high-stress real-world conditions created in the controlled environment of a cyber range.

Why Traditional Approaches Have Failed

Unfortunately, the enormity of today's cybersecurity crisis has outstripped the unmanageable, inefficient approach of traditional cyber range models. At one military base, commanders were struggling to scale to the performance necessary to replicate a realistic environment. The organization had followed the old cyber range model to build out a lab filled with hundreds of servers cabled together to simulate the load of 15,000 users — with limited application coverage. Its mission, however, required 250,000 users to exercise target devices across the full complement of today's applications.

Unfortunately, the enormity of today's cybersecurity crisis has outstripped the unmanageable, inefficient approach of traditional cyber range models.

The traditional cyber range model involves massive investments in hardware, software licenses, electricity, and real estate. It also requires dozens of skilled professionals from the military or defense contractors to set up, configure, integrate, and maintain. It then requires dozens more network and security professionals with the knowledge to continually research and create an evolving mix of sophisticated attacks.

Rather than use cost-effective, adaptive, and scalable technology that is now readily available, too many military organizations and government agencies have answered the cyber range challenge by throwing taxpayer money, outmoded hardware, and expensive consultants at it—because that is what suits the business interests of defense contractors. That approach is destined to fail, however, because it will never keep pace with the rapid evolution of cyber threats.

In the face of escalating cyber risks, increased public pressure, and cuts to defense budgets, a far more pragmatic, cost-effective, and scalable approach is required to bolster cyber forces and defenses against today's threats.

A Pragmatic Strategy for Arming and Training Elite Cyber Warriors

Drawing on its years of experience in delivering breakthrough cyber range innovations to military organizations and global enterprises, BreakingPoint has developed the following pragmatic and sustainable four-point strategy for arming organizations to assess, educate, and certify a national force of cyber warriors to carry out Information Assurance (IA), Information Operations (IO), and Mission Assurance (MA) duties. As this document details, the same innovative technology and scalable approach used for training cyber warriors can be leveraged to assess and harden IT infrastructure resiliency.

1. Modern Cyber Range Deployment

Leap-ahead technological advantages and proven methodologies have made it possible to rapidly deploy a massively scalable cyber range like those already in service within dozens of military organizations worldwide. The nucleus of those modern cyber ranges is the patented BreakingPoint Firestorm™ and Storm™, which deliver an operationally realistic closed environment that replicates conditions across the Internet from a single compact device.

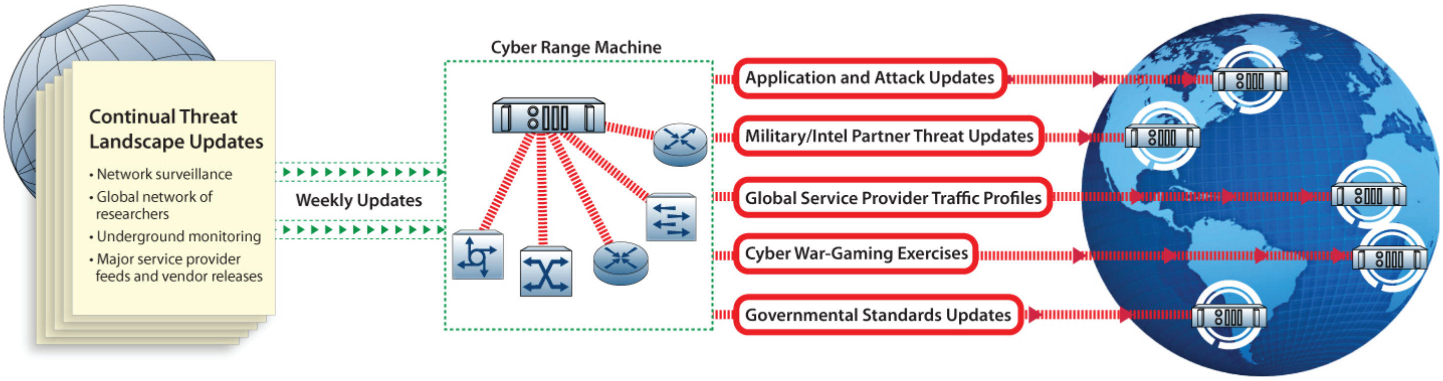

Continual Threat Landscape Updates
• Network surveillance
• Global network of researchers
• Underground monitoring
• Major service provider feeds and vendor releases
Weekly Updates
Cyber Range Machine
Application and Attack Updates
Military/Intel Partner Threat Updates
Global Service Provider Traffic Profiles
Cyber War-Gaming Exercises
Governmental Standards Updates

Figure 1. A single BreakingPoint product provides centralized Command and Control to monitor and manage a distributed network of remote cyber ranges.

With the evolved cyber range enabled by BreakingPoint, organizations can create Internet-scale cyber war in a controlled environment, interpret the results, and provide the insight to enable rapid response to cyber threats—all from an easily-configured machine with a simple, intuitive interface. These powerful capabilities enable users to conduct sophisticated war-gaming exercises for cyber warrior assessment, training, and certification, and enable personnel to attack their own defenses to harden the resiliency of critical infrastructure and to conduct research. The real-world scenarios produced within these single-box cyber ranges give defenders the conditions needed to prepare Incident Response teams, hone digital battlefield techniques, and develop strong defenses for networks and data centers.

With the evolved cyber range enabled by BreakingPoint, organizations can create Internet-scale cyber war in a controlled environment, interpret the results, and provide the insight to enable rapid response to cyber threats—all from an easily-configured machine with a simple, intuitive interface.

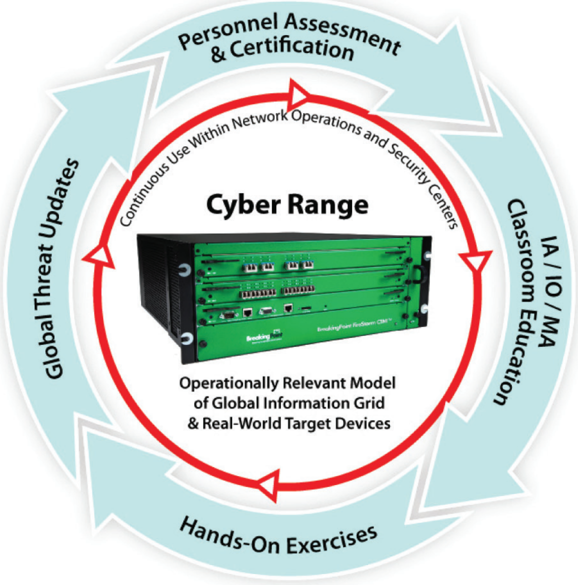
2. Cyber Range Command and Control, Maintenance, and Global Threat Updates

In distributed cyber range environments, commanders require a centralized unit for command and control. With it, they have the ability to consolidate and standardize cybersecurity awareness, information sharing, and cyber war-gaming exercises across entire militaries. A central authority will disseminate uniform, perpetually up-to-date global threat intelligence and cybersecurity expertise to satellite cyber ranges deployed around the world, keeping all cyber warriors prepared to face—or launch—the latest attacks.

In traditional cyber ranges, information about viruses, malware, and other threats is compartmentalized across multiple systems. The BreakingPoint model, by contrast, enables organizations to monitor and manage a distributed network of remote cyber ranges uniformly for more complete situational awareness and standardized, compliant IA and IO initiatives.

Unlike the traditional approach of replicating security researchers at every base, this model allows a centralized command to collect the most current global attack data and distribute it to remote operations worldwide. It also enables the creation of realistic and repeatable exercises to measure expertise and resiliency. This provides full control over exercises delivered to cyber warriors, ensuring that personnel are trained to confront the most current threats, and trained consistently regardless of geographic distribution.

The Making of An Elite Cyber Warrior


Personnel Assessment & Certification
IA / IO / MA Classroom Education
Hands-On Exercises
Global Threat Updates
Continuous Use Within Network Operations and Security Centers
Cyber Range
Operationally Relevant Model of Global Information Grid & Real-World Target Devices

The new approach works best with a global network of researchers dedicated to gathering and sharing network traffic and attack intelligence from vendors, telecom carriers, and other sources. By using the cyber range as a repository and distribution vehicle for that information, organizations can measure and harden the resiliency of network and application infrastructures with the most current mix of traffic—and do so consistently across the globe.

> The new approach works best with a global network of researchers dedicated to gathering and sharing network traffic and attack intelligence from vendors, telecom carriers, and other sources.

3. Standardized Cyber Warrior Education Curriculum and Certification

Just as soldiers on the battlefield are assessed and certified for marksmanship, cyber warriors must be educated and put to the test to evaluate and refine their skills. With a comprehensive cyber warrior curriculum and certification as outlined in Appendix B of this paper, commanders can educate their forces through a wide range of exercises at increasing levels of difficulty to evaluate expertise and certify capabilities, using both prebuilt and customized war-game scenarios.

With this curriculum, commanders can deploy uniform IA, IO, and MA training modules to the troops under their command. Appendix B presents the outline of a suggested cyber warrior curriculum to ensure comprehensive, consistent, and always-current skills assessment and certification that complies with all military regulations.

Any curriculum adopted should include both self-paced and classroom-based training, combined with standardized, escalating levels of war-game scenarios executed within the cyber range, to allow commanders to certify and develop skills from basic to advanced within IO, IA, and MA disciplines. The curriculum required to assess, educate, and certify should include:

- **Information Assurance (IA) personnel:** Develop accomplished defenders with the expertise to harden and certify IT infrastructure resiliency and ensure authorized access to data. Students should develop scientific methodologies and advanced techniques for measuring the resiliency of every element of every IT infrastructure, remediating vulnerabilities, validating Lawful Intercept (LI) and Data Loss Prevention (DLP) measures, and ensuring compliance with standards and processes. That includes developing a mastery of the tools required to monitor and manage networks and data centers.

- **Information Operations (IO) personnel:** Prepare expert Incident Response teams at network operations and security centers with the ingrained skills to respond to the most current cyber attacks. Ensure that emergency response teams can identify and reverse-engineer attacks and provide the insight to rapidly respond with effective dynamic defenses. Provide instruction in the use of tradecraft techniques and develop a mastery of IO tools and exploits. Develop the skills and mastery of tools needed for cyber warfare, including electronic surveillance and the ability to render an enemy's military and commercial enterprise infrastructures inoperable.

- **Mission Assurance (MA) personnel:** Enable Mission Assurance leaders and practitioners to develop the skills required to integrate distinct assurance activities for addressing critical national and global security issues. Provide the cross-discipline expertise and mastery of system engineering, risk management, quality, and operational management principles required to successfully execute mission-critical initiatives in a uniform and systematic manner.

The modern cyber range must be used as an essential tool for that process.

4. Measuring and Hardening Network and Application Infrastructure Resiliency

Attacking defenses is the only way to know with certainty how resilient those defenses are. Hardening IT infrastructure requires the use of a standardized, scientific methodology to measure and certify the performance, security, and stability (i.e., resiliency) of every network and data center component, individually and across whole systems. The modern cyber range must be used as an essential tool for that process. Besides uniform validation of network and data center equipment, the power of this cyber range device enables military and government organizations to hold vendors accountable throughout their IT supply chain.

The process employed must be as systematic as the materials chemistry or nuclear physics used in kinetic defenses. Every element of IT infrastructures—every chip, device, stack, and application running across them—must be subjected to empirical, repeatable measures of resiliency, and those measures must be mandated for vendors throughout the IT supply chain as well. Only consistent, disciplined use of a standard measure of resiliency can ensure that organizations and the vendors that supply them maintain the performance, stability, and security required to defend vital interests.

With a cyber range in every network enclave, cyber forces have the capabilities and proven methodologies required to maintain the highest levels of resiliency for every element of critical networked infrastructures—not only when they are deployed but also as an ongoing process to reflect changes in traffic, configuration, applications, and attacks that affect networks, data centers, and virtualized environments. This rigorous, uniform process should mirror the accreditation of cyber experts in its use of realistic scenarios and standardized certification.

Summary

A pragmatic and sustainable new approach is urgently needed to prepare cyber warriors to defend critical infrastructures. Only BreakingPoint enables that approach by packaging a cost-effective modern cyber range into a single device. This cyber range machine recreates Internet-scale cyber war in a controlled environment, interprets the results, and provides the insight required to rapidly respond to threats.

The BreakingPoint approach is already in action today. In one example among many, the military base mentioned earlier replaced hundreds of servers with a single BreakingPoint product, enabling cyber warriors at the base to perform the massive simulations required to exercise target devices, train defenders, harden infrastructures, and carry out the unit's strategic mission.

BreakingPoint products are the embodiment of the use of sophisticated innovations to solve a complex problem in a straightforward way. These powerful products address the dual challenges of training cyber warriors and hardening IT resiliency in the only way they can be solved: with a sustainable scientific approach that leverages leap-ahead technology and automation to deliver a cyber range that can be deployed quickly.

Using the patented BreakingPoint line of products and the modern cyber range strategy described in this document, organizations now have the ability to defend critical infrastructure by arming cyber warriors with standardized, up-to-the minute IA, IO, and MA training, and to harden critical infrastructures against the latest threats.

> A pragmatic and sustainable new approach is urgently needed to prepare cyber warriors to defend critical infrastructures.

Appendix A — BreakingPoint FireStorm Features

Military, intelligence, and law enforcement organizations rely on the BreakingPoint FireStorm to produce always-current Internet-scale cyber war conditions in a comprehensive, easy-to-use, and low-maintenance product. The patented network processor architecture of the device enables organizations to maintain perpetually current conditions based on situational analysis and threat updates from their own partners and from BreakingPoint's Application and Threat Intelligence (ATI) security research team. This compact 3-slot device provides the equivalent performance and capabilities of hundreds of racks of high-performance servers, including:

Unprecedented Performance from a Single Product

- 120 Gbps of stateful application traffic
- 120,000+ SSL sessions per second from a single chassis
- 90 million concurrent TCP sessions
- 3 million TCP sessions per second
- 3 million steady-state complete TCP sessions per second

- 38 Gbps SSL bulk encryption with any cipher
- 12 universal 1GE/10GE interfaces

Real-World Application and Network Profiles

- Preconfigured stateful application traffic profiles for a range of networks: mobile, service provider, enterprise, government, higher education, and others
- Blend of more than 180 global applications, including AOL® IM, Google® Gmail, Facebook, FIX, Gnutella, IBM DB2, VMware® VMotion™, HTTP, Microsoft® CIFS/SMB, MAPI, Oracle, Encrypted BitTorrent™, eDonkey, MSN® Nexus, RADIUS, SIP, Skype™, Windows Live™ Messenger, World of Warcraft®, Yahoo!® Mail, Yahoo!® Messenger, and many others, including major SCADA protocols
- No performance degradation with blended protocols
- Thorough protocol fuzzing to determine the effects of malformed packets
- Most current and complete IPv4/IPv6 dual-stack validation
- Stateful recreation of captured traffic, including an industry-leading 2 Gigabytes of capture buffer per port
- Optional Custom Application Toolkit for emulating proprietary applications

Live Security Attacks

- Searchable library of more than 34K+ security attacks, plus the very latest live malware such as Stuxnet and Zero-day vulnerabilities
- Comprehensive Microsoft® Tuesday coverage
- More than 80 evasions to validate common security defenses
- Comprehensive DDoS simulation, with millions of concurrent botnet clients
- Sophisticated Markov text generator for realistic spam simulation
- Optional Custom Strike Toolkit for generating custom attacks

All-in-One Application and Threat Intelligence (ATI)

- The latest attacks and applications as well as new product features, upgrades, maintenance, service, and support
- Backed by dedicated ATI team of security researchers

Lawful Intercept, Signals Analysis, and Data Loss Prevention Validation

- Sophisticated multilingual needle-in-a-haystack scenarios to verify accuracy of trigger matching

- Evergreen Protocol program to ensure always-current versions of the most popular webmail and instant messaging applications, including Google® Gmail™, Microsoft's Hotmail™, AOL Messaging™, ICQ, and Jabber
- Stateful high-performance traffic to stress and measure the performance of deep packet inspection (DPI) engines

Easy to Use, Easily Scalable

- Intuitive object-oriented user interface for creating realistic simulations
- Wizard-like labs for accelerating configuration
- Ability to scale to unlimited performance levels

Appendix B — BreakingPoint Cyber Warrior Curriculum

Information Assurance Fundamentals

A mastery of fundamental IA capabilities is a requirement for all cyber command personnel, whether their mission is IA, Information Operations (IO), or Mission Assurance (MA). A structured Cyber Warrior Training curriculum should combine self-paced training modules with hands-on cyber range exercises to develop IA personnel with the skills to defend critical Internet infrastructure and military communications networks while remaining firmly grounded in standards. Once student have achieved certification in IA Basic Training, they should follow the appropriate development path for them: either Intermediate and Advanced training in IA, or Basic, Intermediate, and Advanced training in IO, with the option to move into MA training.

IA curriculum provides comprehensive basic, intermediate, and advanced instruction in the architecture, testing, deployment, protection, and maintenance of modern networks, data centers, and applications. Students should develop a thorough understanding of how networks, data centers, applications, and attacks have evolved over the years, along with the implications of that evolution for hardening network resiliency and ensuring compliance with standards. The training will emphasize the transformative effects of the use of deep packet inspection (DPI) technology throughout modern networks, servers, and security devices, highlighting the risks and benefits that DPI has introduced.

Once students have mastered the self-paced component of their instruction, they will be introduced to the essential tools used to analyze and troubleshoot networks in a lab-like setting or cyber range. Within the cyber range, students are able to create real-world networking and attack scenarios and examine their effects on resiliency—performance, security, and stability. The hands-on cyber range experience allows students to experience real Internet-scale network operations and attacks firsthand, cementing the knowledge developed in self-paced training modules.

Information Operations Fundamentals

Upon achieving Basic IA certification or higher, students will have the foundation required to begin developing effective Information Operations and Incident Response skills. Students following an IO path will have the opportunity to achieve certification in basic, intermediate, and advanced IO techniques through exposure to the strategy, fundamental concepts, major components, and methodologies of IO.

Advanced candidates will master both offensive and defensive IO, developing the skills needed to conduct electronic surveillance and offensive measures. Instruction is reinforced through tactical-level IO planning and war-game exercises, through which warriors will build mastery of the tools used to analyze and troubleshoot attacks.

Mission Assurance Fundamentals

Ensuring that military missions continue under all circumstances—including under the spectrum of cyber threats—is essential to deter and defeat aggressors. Threats to mission success can come in many forms: organized crime, nation states, hackers, and terrorists. In addition to developing MA techniques that will defeat those adversaries, curriculum should provide training in skills that ensure IT mission assurance even when IT systems have been compromised.

Integrated net-centric capabilities are part of MA operations and must be approached holistically, because this perspective is directly associated with overall mission performance. This cross-discipline curriculum requires at least a basic level of skills in both IA and IO. Working from that foundation, students will learn the skills necessary for MA, including MA fundamentals, Mission Assessment Methodology (MAM), Situational Awareness and Mission Correlation, and Continuity of Operations Planning (COOP).

For more information see http://www.ixiacom.com/