CYBERBIT
PROTECTING A NEW DIMENSION

Cyber Range:
Hands-on Academic Cybersecurity Degree Programs

White Paper

www.cyberbit.com | sales@cyberbit.com

Table Of Contents

The Future of Cyber Security Education

The world's first computer science degree program was established in 1953, just 17 years after Alan Turing published the concept of the "Turing machine". Since then, computer science had become an important field of academic research and one of the most important professions of our time. The age of the internet took Turing's ideas and catapulted them forward. Today data is accessible everywhere and for anyone. Computers are used for all professional and domestic tasks. The world is truly connected.

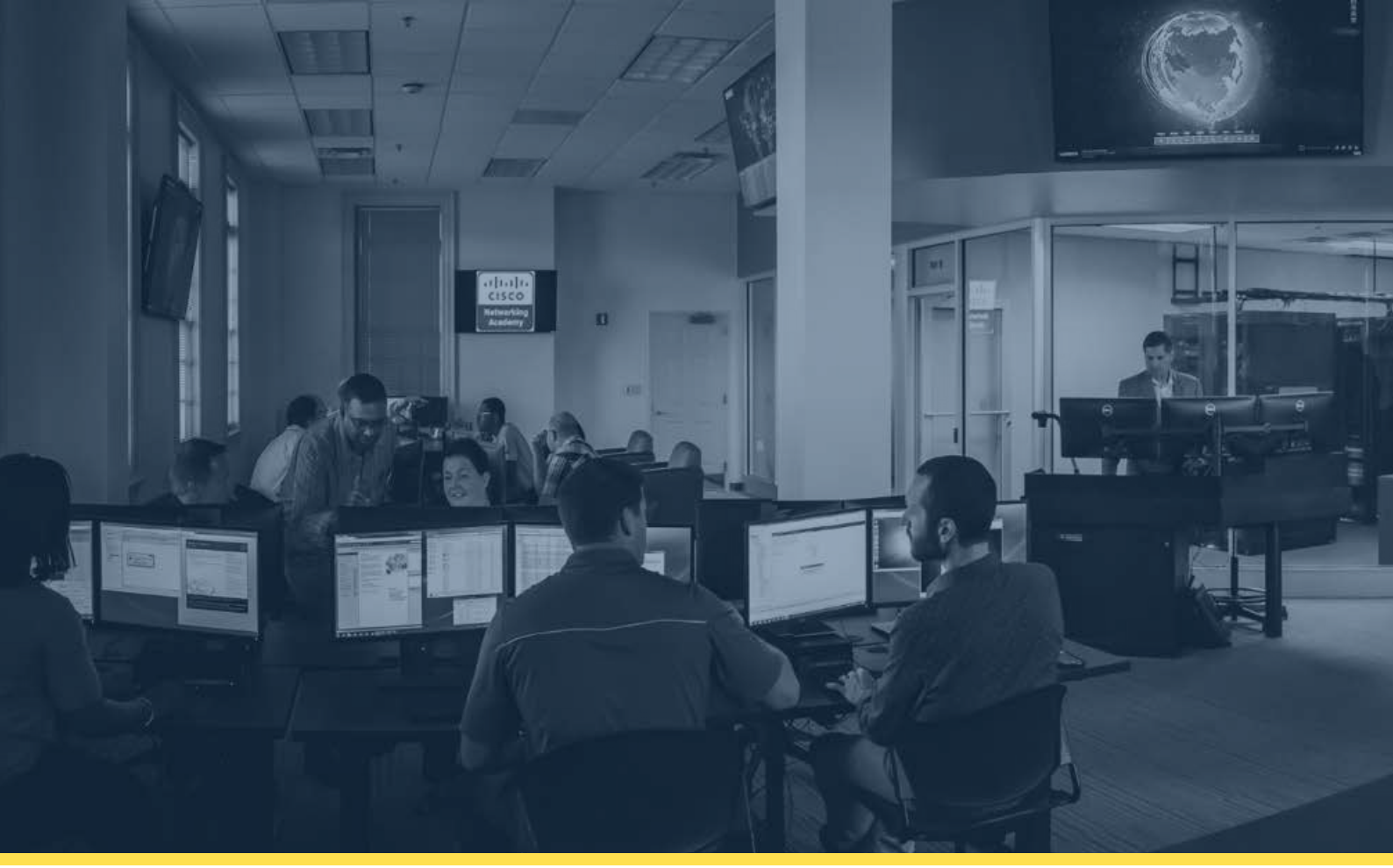
Yet, the internet brought trouble with it as well. The growing sophistication and profusion of cybercrime and warfare will require droves of professionals to keep everything from ecommerce and online banking to critical infrastructure safe and functioning. The demand for highly skilled cybersecurity professionals is skyrocketing, but still very few new professionals enter the market each year.

In the past, the military was the primary training ground for cyber defenders. Others began in related fields of computer science or information systems management and developed expertise via on the job experience, a patchwork of independent courses and self-taught independent learning. Some very talented cyber professionals have developed this way, but if we are to keep up with growing demands in this highly technical field, dedicated academic degree programs must be made available at the undergraduate and graduate level.

Today, just like in 1953, innovative academic institutions recognize the enormous opportunity of this emerging field. Academic cybersecurity programs will play an important role in preparing students for challenging and rewarding careers and leading research in cybersecurity technology and strategy. Innovative colleges and universities have already launched their own cybersecurity degree programs.

Much like computer science, cybersecurity requires more than just excellent academic coursework. Hands-on experience is highly prized in the workforce. Undergraduate and graduate degree programs that offer in-depth coursework alongside rigorous hands-on training will produce graduates with a competitive edge sought after by leading private and public sector organizations.

This whitepaper will outline hands on exercises that should accompany core courses offered in most academic degree programs in cybersecurity. Faculty and academic programing directors can use this guide to build cyber simulation exercises into every relevant course in their cybersecurity curricula.



What is a Cyber Range?

A cyber range is a simulation platform that provides the ability to emulate any type of network architecture and simulate any cyber security scenario to train and test people, procedures and technologies. Cyber range simulators are used by elite cyber intelligence credits and highly security sensitive enterprises such as financial institutions and public utilities to prepare cybersecurity defenders for real-life attacks. One simulator can be used to practice responding to dozens of immersive cyber security scenarios. Each scenario teaches a set of incident response and cyber security skills, providing students with relevant tools and methodologies to operate a cyber-attack across a variety of attack scenarios, platforms and technologies. The cyber simulation scenarios give students the chance to develop their cybersecurity skills alongside theoretical classroom learning and prepare them to become capable, confident cyber security leaders of the future.

Academic Cyber Range Operations

Facility & Staff

A cyber range training and simulation facility can accommodate any size student body. Smaller institutions can establish a fully functioning Cyberbit Range in a single standard classroom. Larger programs can build multi-room training centers to adequately serve all relevant students in undergraduate, graduate and continuing education courses. Training centers with extra capacity can also generate revenues by offering training sessions to external, private enterprises or government organizations for their in-house cybersecurity staff.

The cyber range can be established and operated by existing computer science and information systems faculty and staff. Minimum classroom size is approximately 100 square meters, though can be larger to accommodate more students, or include several adjacent classrooms.

On Campus or Off Site?

Many colleges and universities will choose to establish their own cyber range training center on campus to make it conveniently available to the entire student body and faculty and allow students to take full advantage of simulation training. However, if setting up your own on campus cyber range simulation facility is not feasible due to program size, budget or other constraints, it is possible to contract with a cyber range facility in your region to offer the desired simulation activities.

Cyber range simulation exercises can be assigned as part of course requirements, just like laboratory assignments in science classes. Below we have listed some of the most common core classes included in cyber security degree programs and simulation activities that complement classroom study.

***Note:** The simulation scenarios in this whitepaper are based on Cyberbit Range training and simulation platform.

Bachelors of Science in Cybersecurity

Cybersecurity professionals are responsible for protecting computers, networks, software, data or private information from unauthorized access, theft, or destruction. The B.Sc. Cybersecurity degree curriculum starts with a fundamental computer science and information systems courses to give students a solid foundation. Specialized cybersecurity courses cover management, techniques and technologies used to secure computer networks, defend against intrusion and investigate and remedy breaches. Graduates will be well versed in cybersecurity theory and have hands-on experience configuring security tools, performing vulnerability assessments, operating during all types of security breaches and carrying out forensic investigations of cybercrimes.

The world's most effective military cybersecurity training programs incorporate hands-on simulation training at every stage of education. We believe this principle should be adhered to as closely as possible in the academic setting as well. Pairing classroom coursework with targeted exercises in a cyber range training facility deepens learning and gives students valuable experience that employers seek. Below is a guide to cybersecurity range lab sessions that should accompany common courses throughout the degree program.

Program length: 4 years

Skills Acquired:

- Fundamentals of computer science, information technology and communications
- Write and implement network security policies
- Align network security practices with organizational strategy
- Build and configure secure computer networks:
  - Corporate IT
  - Financial institution with online services
  - Government and public sector
  - Critical infrastructure and heavy industry (ICS/SCADA)
- Operate and configure leading network security tools
- Test network security to discover vulnerabilities and harden infrastructure
- Ethical hacking
- Perform forensic investigations of cyber crimes
- Write and implement network security policies
- Align network security practices with organizational strategy
- Malware research
- Security incident response theory and playbooks

B.Sc. Cybersecurity Required Courses (30 credits)

Year 1

Course	Weekly Hours
(CS) Computer Networking A	3
(CS) Computer Networking B	3
(CS) Programming	3
(CYBER) Intro to Network Security	3
(RANGE) Networks, Tools & Threats Hands-on experience with several large network environments and an array of leading cybersecurity tools. Face common threats and perform basic operational methodologies	12
Total	**24**

Year 2

Course	Weekly Hours
(CS) Routing and Switching	2
(CS) Operating Systems: Unix and Linux	2
(CS) Operating Systems: Mobile	2
(CYBER) Network Security Tools	6
(CYBER) Security Audits	2
(CYBER) Access Control	2
(CYBER) Communication Security & Encryption	2
(RANGE) Cybersecurity Toolkit Learn to operate cybersecurity tools and platforms, including; Firewalls, IDS/IPS, end-point security, SIEM	3
(RANGE) Cyber Attack Scenarios Experience operating in several advance attack scenarios: SQL injection, Apache shut-down, web defacement	3
Total	**24**

B.Sc. Cybersecurity Required Courses (30 credits)

Year 3

Course	Weekly Hours
(CS) Information Systems	3
(CYBER) Intrusion Detection	3
(CYBER) Ethical Hacking	2
(CYBER) Digital Forensics	2
(CYBER) Web Application Security	2
(CYBER) Internet/Intranet Security	2
(RANGE) Advanced Threats Hands-on experience facing the most malicious advanced threat scenarios: Trojan Data leakage, JS Trojan upload, Java Sendmail, DDoS SYN Flood, DB dump, Trojan privilege escalation	4
Total	**18**

B.Sc. Cybersecurity Required Courses (30 credits)

Year 4

Course	Weekly Hours
(CS) Information Systems Analysis & Design	3
(CYBER) Information Security Management	3
(CYBER) Network Defense	3
(CYBER) Digital Law & Privacy	3
(CYBER) Contingency Planning & Disaster Recovery	3
(CYBER) Malware Research	3
(RANGE) Cyber Attack Scenarios Experience operating in several advance attack scenarios: SQL injection, Apache shut-down, web defacement **Simulation scenarios:** Killer Trojan Windows management instrumentation worm Ransomware SCADA DDoS DNS amplification WPAD man-in-the-middle SCADA – Factory overload SCADA – Factory shutdown SCADA – Factory silent attack	3
(RANGE) Incident Response Simulate operating breaches according to incident response playbooks	3
(RANGE) Capstone Project Student teams build ad secure computer system and classmates probe it to discover vulnerabilities	Open
Total	**24+**

Masters Degree in Cybersecurity

Masters Degree in Cybersecurity offers advanced studies in cybersecurity techniques, tools and management to propel graduates to leadership positions public and private sector organizations. Graduates will learn how to develop comprehensive cybersecurity solutions for any type of network and manage the day to day operations of the security operations team.

Cyber Range Labs:

Cybersecurity is a battlefield where fierce opponents are faced every day. Leasers must bring both stellar academic learning and a wealth of hands on experience grappling with real cyber threats and breaches. The graduate degree in cybersecurity must include hands-on experience so that graduates can make critical decisions and communicate across the organization, with general employees, the security operations team, executive management and outside media and law enforcement. Including simulation training alongside coursework ensures graduates can perform flawlessly under pressure and lead the entire organization through any cyber event.

Program length: 2 years

Skills Acquired:

- Develop and implement network security policies
- Build and manage a security operations team
- Test network security to discover vulnerabilities and harden infrastructure
- Benchmark and improve incident response performance
- Evaluate new cybersecurity technologies
- Manage a cyber breach crises
- Lead forensic investigation of cyber breach
- Align network security practices with organizational strategy

M.A. Cybersecurity Required Courses (30 credits):

Year 1

Course	Weekly Hours
(CYBER) Information Systems Security	3
(CYBER) Internet & Network Security	3
(CS) Database Systems	2
(CYBER) Digital Forensics	2
(CYBER) Information Security Management	4
(RANGE) Disaster Recovery & Business Continuity	3
(RANGE) Risk Management & Compliance	3
Total	**20**

Year 2

Course	Weekly Hours
(CS) Technology Leadership	2
(CYBER) Digital Law & Privacy	2
(CYBER) Applied Cryptography	2
(CYBER) Artificial Intelligence in Cybersecurity	2
(RANGE) Business & Security Cybersecurity requirements often directly clash with business objectives of the organization. Learn how to align security with business goals without compromising either.	2
(RANGE) Cyber Crisis Leadership Joint simulation with undergraduate students. You will act as the SOC manager directing a group of student analysts through a cyber breach.	3
(RANGE) Decision Making in Cybersecurity Face 'impossible' breach scenarios that pose serious conflicts and require tough decision making. Simulate both SOC manager and analyst roles	3
Total	**16**

Conclusion

The cybersecurity skill gap is quickly developing into a national and global security crisis. Colleges and universities have a vital role to play in developing the highly skilled workforce needed to defend computer networks and keep businesses, public services and critical infrastructure against cyber assailants.

Military and medical teams have always required extensive hands on training as an integral part of training requirements. Simulation training gives us the ability to develop top performing cybersecurity professionals and leaders in a short time period and in a cost-effective manner. Establishing a cyber training center powered by Cyberbit Range training and simulation technology will give your students a competitive edge.

Cyberbit Range powers dozens of cyber security training centers, academic education centers and business training centers around the world training, qualifying and certifying thousands of students every year.

ABOUT CYBERBIT™

CYBERBIT'S battle-hardened cybersecurity solutions detect, analyze and respond to the most advanced, complex and targeted threats. A subsidiary of defense systems provider Elbit Systems Ltd. (NASDAQ: ESLT), Cyberbit has more than 500 personnel on three continents helping organizations protect sensitive assets and maximize security operations performance. CYBERBIT solutions empower enterprises to detect advanced threats in seconds, protect critical infrastructure, automate security operations center (SOC) workflows and train staff. With machine learning, big data and continuous technology advancements, Cyberbit maximizes protection against today's signature-less threats and arms organizations for tomorrow's new dimension of attack.

www.cyberbit.com | sales@cyberbit.com

Headquarters
22 Zarhin St. | Ra'anana 4310602 | Israel
Tel: +972.(0)9.779.9800

US Office
3800 N. Lamar Blvd. | Suite 200 | Austin, TX 78756
Tel: +1.737.717.0385

EMEA Office
United Kingdom | 103 Kingsway | London WC2B 6QX
Tel: +44.(0)2032.069400

Germany Office
Mies-van-der-Rohe-Str. 8 | 80807 Munich
Tel: +49-89-215416-22

APAC Office
300 Tampines Avenue 5 | #09-02 | Singapore 529653
Tel: +65.6679.5771

CYBERBIT
PROTECTING A NEW DIMENSION