Northern Technical University
الجامعة التقنية الشمالية

First Cycle – Four Levels – 240 ECTS

Bachelor's degree (B.Sc.) – Cybersecurity Engineering Technology

الدورة الأولى - بكالوريوس هندسة تقنيات الامن السيبراني– أربع سنوات – ٢٤٠ وحدة اوربية



Table of Contents

1. Overview
2. Undergraduate Modules 2025-2026
3. Contact

1. Overview

This catalogue is about the courses (modules) given by the program of Cybersecurity Engineering Technology to gain the Bachelor of Science degree. The 4-year program delivers (53) Modules with (6000) total student workload hours and 240 total ECTS. The module delivery is based on the Bologna Process.

نظره عامه

يتناول هذا الدليل المواد الدراسية التي يقدمها برنامج هندسة تقنيات الامن السيبراني للحصول على درجة بكالوريوس العلوم. يقدم برنامج الأربع سنوات (53) مادة دراسية، مع (٦٠٠٠) إجمالي ساعات حمل الطالب و ٢٤٠ إجمالي وحدات أوروبية. يعتمد تقديم المواد الدراسية على عملية بولونيا.

2. Undergraduate Modules 2025-2026

Module 1

Code	Module Title	ECTS	Semester
NTU100	Democracy and Human Rights	2	1
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2		33	17
Description			
This university module examines the principles of democracy, constitutional governance, human rights, and civic responsibility within national and international contexts. Students explore the evolution of democratic systems, the separation of powers, the rule of law, equality, freedom of expression, and the protection of fundamental rights. The course also discusses international human rights conventions, the role of governmental and non-governmental institutions, and contemporary challenges such as discrimination, corruption, and social justice. Through case studies and discussion, students develop critical thinking about citizenship, ethical participation, and respect for diversity. The module encourages learners to understand their legal rights and responsibilities while promoting values that support peaceful coexistence, accountability, and sustainable democratic development.			

Module 2

Code	Module Title	ECTS	Semester
NTU101	English language	2	1
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2		33	17
Description			
This module develops students' ability to communicate effectively in English within academic and engineering environments. Emphasis is placed on grammar, vocabulary, reading comprehension, paragraph writing, listening, and oral communication. Technical terminology related to engineering and information technology is gradually introduced to prepare students for later specialized courses. Learners practice presenting ideas, interpreting technical texts, writing reports and emails, and participating in discussions. Activities strengthen accuracy, fluency, and confidence while improving pronunciation and comprehension. By the end of the course, students possess a stronger linguistic foundation for studying engineering references, collaborating with international colleagues, and engaging with scientific literature published in English.			

Module 3

Code	Module Title	ECTS	Semester
CYBT108	Mathematics	6	1
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
3	1	63	87
Description			
Mathematics establishes the analytical foundation required for engineering and cybersecurity studies. The module covers algebraic manipulation, functions, equations, matrices, trigonometry, complex numbers, limits, differentiation, and introductory integration. Problem-solving techniques are emphasized alongside mathematical reasoning and logical thinking. Students learn to formulate engineering problems mathematically, analyze relationships between variables, and interpret quantitative results. Practical examples demonstrate applications in electrical engineering, programming, communication systems, and data analysis. Regular exercises strengthen computational accuracy while encouraging systematic approaches to solving unfamiliar problems. The mathematical concepts acquired in this course support advanced subjects including signals, cryptography, probability, machine learning, and engineering analysis.			

Module 4

Code	Module Title	ECTS	Semester
CYBT101	Fundamentals of Electrical Engineering	5	1
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	62
Description			
This course introduces the fundamental concepts governing electrical circuits and electronic components used in modern engineering systems. Topics include electric charge, voltage, current, resistance, power, energy, Ohm's law, Kirchhoff's laws, series and parallel circuits, capacitors, inductors, and basic measuring instruments. Students gain experience interpreting circuit diagrams and performing elementary circuit calculations. Laboratory activities reinforce theoretical concepts through practical measurements and safe handling of equipment. The module highlights the relationship between electrical principles and computing hardware, embedded systems, communication devices, and cybersecurity infrastructure. A solid understanding of these concepts prepares students for subsequent courses involving electronics, digital systems, and computer architecture.			

Module 5

Code	Module Title	ECTS	Semester
CYBT103	Fundamentals of Programming	5	1
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	62
Description			
Fundamentals of Programming introduces algorithmic thinking and software development using a structured programming language, with emphasis on Python. Students learn variables, data types, operators, input/output, conditional statements, loops, functions, lists, dictionaries, file handling, and basic debugging techniques. Considerable attention is given to designing clear algorithms before implementation and writing readable, maintainable code. Practical programming exercises develop logical reasoning and computational problem-solving skills while introducing simple automation tasks relevant to cybersecurity. The course also familiarizes students with development environments, program testing, and documentation. By completing the module, students can construct small applications, analyze program behavior, and build a strong programming foundation for advanced software and security courses.			

Module 6

Code	Module Title	ECTS	Semester
CYBT100	Linux Administration	5	1
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	62
Description			
Linux Administration familiarizes students with the Linux operating system as a secure and reliable platform widely used in servers, cloud infrastructure, embedded devices, and cybersecurity environments. The module covers Linux architecture, installation, command-line navigation, file system hierarchy, file manipulation, user and group management, permissions, process control, package management, shell scripting, and basic networking utilities. Students perform practical exercises that emphasize system configuration, automation, troubleshooting, and secure administration. The course also introduces common server services and reinforces good security practices such as privilege management and log analysis. Practical laboratory work enables learners to become comfortable operating Linux systems that will be used extensively throughout advanced cybersecurity courses.			

Module 7

Code	Module Title	ECTS	Semester
CYBT109	Engineering Drawing	3	1
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
	3	48	27
Description			
Engineering Drawing introduces the graphical language used to communicate engineering ideas accurately and unambiguously. Students learn standards for technical drawings, line conventions, scales, dimensioning, geometric construction, orthographic projection, isometric views, sectional drawings, and basic tolerancing. The course develops spatial visualization skills required to interpret and create engineering designs. Manual drawing techniques are complemented by introductory computer-aided design concepts to familiarize students with modern engineering practice. Assignments emphasize precision, clarity, and adherence to recognized engineering standards. Mastery of engineering drawings enables students to understand mechanical layouts, equipment documentation, and hardware designs encountered in multidisciplinary engineering projects.			

Module 8

Code	Module Title	ECTS	Semester
CYBT102	Ethics of Information Age	2	1
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2		33	17
Description			
Ethics of Information Age examines the ethical, legal, and social issues arising from the widespread use of information and communication technologies. Students discuss privacy, intellectual property, digital rights, cybercrime, artificial intelligence, surveillance, professional responsibility, and ethical decision-making. Real-world case studies illustrate the consequences of unethical behavior in software development, cybersecurity, social media, and data management. The module encourages critical evaluation of emerging technologies while considering fairness, accountability, transparency, and societal impact. Learners become familiar with professional codes of ethics and develop the ability to recognize ethical dilemmas and propose responsible solutions consistent with legal and professional standards.			

Module 9

Code	Module Title	ECTS	Semester
NTU102	Computer 1	2	2
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	1	48	2
Description			
Computer 1 provides practical experience with essential computer applications and digital productivity tools required throughout university study. Students learn operating system fundamentals, file management, word processing, spreadsheets, presentations, internet services, cloud storage, email communication, and basic cybersecurity practices for everyday computing. Hands-on exercises develop confidence in organizing digital information, preparing academic documents, performing calculations, presenting technical information, and collaborating using online platforms. Attention is also given to safe computing habits, software installation, data backup, and responsible use of information technology. The knowledge acquired supports academic success and establishes the digital literacy expected from engineering students.			

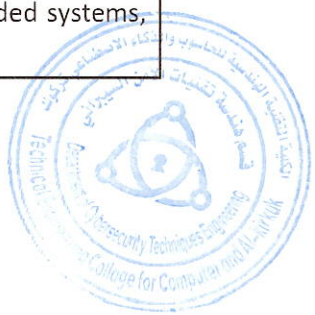


Module 10

Code	Module Title	ECTS	Semester
NTU103	Arabic Language	2	2
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2		33	17
Description			
Arabic Language strengthens students' ability to communicate effectively using Modern Standard Arabic in academic and professional contexts. The module emphasizes correct grammar, spelling, punctuation, vocabulary development, reading comprehension, and coherent writing. Students practice preparing formal reports, summaries, official correspondence, and technical texts while improving linguistic accuracy and clarity of expression. Selected readings encourage critical thinking and appreciation of Arabic linguistic heritage alongside its contemporary applications. Classroom activities also enhance speaking and presentation skills through structured discussions and oral communication. The course enables students to produce clear, well-organized written work and communicate professionally within governmental, industrial, and academic environments.			

Module 11

Code	Module Title	ECTS	Semester
CYBT106	Digital Electronics	5	2
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	62
Description			
Digital Electronics introduces the principles that govern modern digital systems and computing hardware. Students investigate number systems, binary arithmetic, Boolean algebra, logic gates, Karnaugh maps, combinational circuits, and sequential logic. The course explains the operation of multiplexers, decoders, encoders, flip-flops, registers, and counters before examining their integration into larger digital systems. Practical laboratory sessions reinforce theoretical concepts by allowing students to design, simulate, and test digital circuits using logic trainers or software tools. Emphasis is placed on systematic circuit analysis, optimization, and troubleshooting techniques. The knowledge gained forms an essential foundation for later studies in computer architecture, embedded systems, microprocessors, digital communications, and cybersecurity hardware.			



Module 12

Code	Module Title	ECTS	Semester
CYBT105	Introduction to Python Programming	6	2
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	87
Description			
Python has become one of the most widely used programming languages in engineering, data science, automation, and cybersecurity. This module introduces students to Python syntax while emphasizing problem-solving rather than memorizing language features. Topics include variables, data types, operators, decision structures, loops, functions, modules, collections, file processing, and exception handling. Students gradually develop programs that automate repetitive tasks, manipulate data, and solve engineering problems through structured programming techniques. Practical assignments encourage clean coding practices, debugging, documentation, and code reuse. By the end of the course, learners can confidently develop small Python applications and possess the programming skills required for advanced subjects such as scripting, penetration testing, digital forensics, artificial intelligence, and software development.			

Module 13

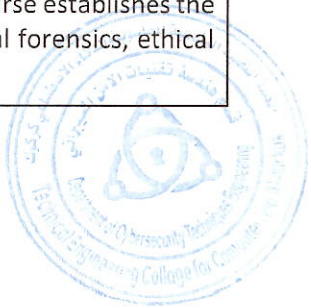
Code	Module Title	ECTS	Semester
CYBT104	Engineering Mathematics	6	2
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
3	1	63	87
Description			
Engineering Mathematics extends the mathematical foundation required for engineering analysis by introducing concepts used to model and solve practical engineering problems. The module typically covers differential and integral calculus, differential equations, vectors, matrices, and introductory numerical methods, with emphasis on their engineering applications. Students learn to formulate mathematical models, analyze system behaviour, and interpret analytical results using logical reasoning and quantitative techniques. Engineering examples demonstrate how mathematical methods support circuit analysis, communication systems, control engineering, signal processing, and cybersecurity algorithms. Continuous problem-solving exercises strengthen analytical thinking and computational accuracy while preparing students for mathematically intensive modules encountered throughout the engineering programme.			

Module 14

Code	Module Title	ECTS	Semester
CAIK100	Physics	3	2
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2		33	42
Description			
Physics provides the scientific principles needed to understand natural phenomena underlying engineering systems. The course examines mechanics, motion, forces, energy, momentum, waves, sound, heat, electricity, magnetism, and basic modern physics through both theoretical instruction and laboratory experiments. Students develop the ability to relate physical laws to practical engineering applications while improving experimental skills such as measurement, observation, error analysis, and data interpretation. Laboratory activities reinforce classroom concepts by encouraging careful experimentation and scientific reporting. The module promotes critical thinking and quantitative reasoning, enabling students to appreciate how physical principles influence the design, operation, and performance of electrical, electronic, communication, and computing technologies.			

Module 15

Code	Module Title	ECTS	Semester
CYBT107	Introduction to Cybersecurity	6	2
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	87
Description			
This module offers students their first comprehensive view of cybersecurity as a multidisciplinary engineering field concerned with protecting digital systems, networks, and information assets. It examines common cyber threats, vulnerabilities, attack techniques, and defensive strategies while introducing the principles of confidentiality, integrity, availability, authentication, and risk management. Students become familiar with malware, phishing, password security, social engineering, network attacks, and basic cryptographic concepts through practical demonstrations and case studies. Ethical responsibilities, legal considerations, and professional conduct are discussed alongside current cybersecurity challenges affecting governments, businesses, and individuals. The course establishes the conceptual framework required for subsequent modules in network security, digital forensics, ethical hacking, cryptography, and secure software development.			



Module 16

Code	Module Title	ECTS	Semester
CYBT200	Fundamentals of Electronic Engineering	4	3
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	37
Description			
Electronic Engineering introduces the operation of semiconductor devices and the electronic circuits that form the basis of modern computing and communication systems. Students study the characteristics of diodes, bipolar junction transistors, field-effect transistors, operational amplifiers, and basic analog circuits while learning how electronic components are combined to perform amplification, switching, and signal conditioning. Laboratory sessions reinforce theoretical concepts through circuit construction, measurement, testing, and fault diagnosis using standard electronic instruments. The module also introduces fundamental design considerations such as power consumption, component selection, and reliability. By understanding electronic circuit behaviour, students establish a strong foundation for embedded systems, communication equipment, hardware security, and advanced digital electronics.			

Module 17

Code	Module Title	ECTS	Semester
CYBT205	Discrete Math	4	3
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
3		48	52
Description			
Discrete Mathematics develops the mathematical reasoning required for computer engineering and cybersecurity by focusing on structures that involve finite or countable elements rather than continuous quantities. Students examine propositional and predicate logic, sets, relations, functions, mathematical induction, recursion, combinatorics, graph theory, and elementary number theory. The course emphasizes rigorous problem solving, logical proof techniques, and algorithmic thinking while demonstrating how discrete mathematics underpins computer programming, cryptography, network design, database systems, and artificial intelligence. Through analytical exercises and practical examples, learners strengthen their ability to model computational problems, evaluate logical arguments, and construct efficient solutions using formal mathematical methods.			

Module 18

Code	Module Title	ECTS	Semester
CYBT201	Database systems	4	3
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	37
Description			
Database Systems examines the principles of organizing, storing, retrieving, and managing structured information in modern information systems. Students learn the relational database model, entity-relationship modelling, normalization, Structured Query Language (SQL), indexing, transactions, and concurrency control while developing practical database applications. The module highlights efficient database design techniques that minimize redundancy and maintain consistency across large datasets. Laboratory exercises provide experience creating databases, writing complex SQL queries, implementing constraints, and optimizing performance. Applications drawn from enterprise systems, web services, and cybersecurity demonstrate the importance of reliable data management in supporting secure, scalable, and high-performance computing environments.			

Module 19

Code	Module Title	ECTS	Semester
CYBT202	Python Programming for Cybersecurity	5	3
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	62
Description			
Python Programming for Cybersecurity demonstrates how scripting can automate security tasks and improve the efficiency of cyber defence operations. Students build Python programs for processing files, analyzing logs, scanning networks, communicating through sockets, interacting with web services, and handling structured data formats such as JSON and XML. The module introduces widely used security libraries while emphasizing secure coding practices, modular software development, and effective debugging techniques. Practical assignments involve automating repetitive administrative tasks, parsing network traffic, and developing small security utilities. These skills prepare students for later work in penetration testing, digital forensics, malware analysis, security monitoring, and incident response.			

Module 20

Code	Module Title	ECTS	Semester
CYBT203	Operating Systems	4	3
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
1	2	48	52
Description			
Operating Systems explores the software responsible for managing computer hardware and providing essential services to applications. Students investigate process management, thread scheduling, memory allocation, virtual memory, file systems, device management, synchronization, deadlock handling, and system calls while examining the internal architecture of modern operating systems. Practical activities demonstrate command-line administration, resource monitoring, process control, and system configuration using contemporary operating systems. The module also introduces performance optimization, reliability, and security considerations that influence operating system design. A thorough understanding of these concepts enables students to appreciate how operating systems support modern computing platforms and provides essential preparation for cybersecurity, cloud computing, and system administration.			

Module 21

Code	Module Title	ECTS	Semester
NTU200	Bath Party Crimes	2	3
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2		33	17
Description			
This university requirement examines the history, ideology, organizational structure, and political practices of the Ba'ath regime in Iraq. Students analyze the social, political, economic, and humanitarian consequences of authoritarian rule using historical documents and documented events. The course promotes critical thinking by encouraging objective discussion of governance, human rights, transitional justice, and the importance of preserving democratic institutions. Through lectures and guided analysis, learners gain a deeper understanding of recent Iraqi history while appreciating the value of pluralism, national unity, and constitutional principles. The module contributes to civic awareness and reinforces the importance of rejecting extremism, dictatorship, and violations of fundamental human rights.			

Module 22

Code	Module Title	ECTS	Semester
NTU201	English language	2	3
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2		33	17
Description			
Building upon the first English module, this course strengthens students' ability to communicate in academic and technical settings. Greater emphasis is placed on reading engineering texts, expanding technical vocabulary, writing structured reports, summarizing information, and delivering short presentations. Grammar is reinforced through practical usage rather than isolated exercises, allowing students to communicate with greater accuracy and confidence. Listening activities expose learners to authentic technical discussions, while collaborative tasks improve spoken interaction. By integrating engineering-related content into language practice, the module prepares students to use English effectively throughout their degree and to engage with international scientific literature and professional communication.			

Module 23

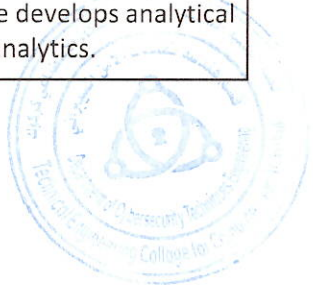
Code	Module Title	ECTS	Semester
CYBT204	Computer Networks	5	3
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	62
Description			
Computer Networks introduces the technologies that enable computers and smart devices to exchange information efficiently and securely. Students study network architectures, transmission media, switching, routing, addressing, and the TCP/IP protocol suite before examining Ethernet, wireless LANs, and Internet services. Laboratory activities provide experience in network configuration, troubleshooting, packet analysis, and basic device management using simulation software and networking equipment. The course also introduces fundamental network security concepts and common performance considerations. Understanding how modern networks operate provides the technical foundation required for advanced modules in network security, wireless communications, cloud computing, and cybersecurity engineering.			

Module 24

Code	Module Title	ECTS	Semester
CYBT206	Data structures	4	4
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	37
Description			
Data Structures focuses on efficient methods for organizing, storing, and processing data in software applications. Students implement arrays, linked lists, stacks, queues, trees, hash tables, and graphs while comparing their performance and appropriate use cases. The module introduces algorithm analysis using time and space complexity, encouraging students to select suitable data structures for different computational problems. Programming assignments emphasize modular design, debugging, and efficient memory usage. Practical examples demonstrate the importance of data structures in search engines, databases, operating systems, artificial intelligence, and cybersecurity tools. Mastery of these concepts significantly improves programming ability and problem-solving efficiency.			

Module 25

Code	Module Title	ECTS	Semester
CYBT207	Probability & Statistics for Cybersecurity	6	4
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
3	1	63	87
Description			
Probability and Statistics for Cybersecurity equips students with quantitative methods for analyzing uncertainty, risk, and data generated by modern information systems. Topics include descriptive statistics, probability distributions, random variables, sampling, hypothesis testing, confidence intervals, correlation, and regression. Engineering and cybersecurity examples illustrate how statistical techniques support intrusion detection, anomaly analysis, reliability assessment, and performance evaluation. Students learn to interpret datasets, draw evidence-based conclusions, and present statistical findings using appropriate numerical and graphical methods. The module develops analytical skills that underpin data science, machine learning, digital forensics, and security analytics.			



Module 26

Code	Module Title	ECTS	Semester
CYBT208	Computer Organization and Architectures	5	4
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	62
Description			
Computer Organization and Architecture examines how computer hardware executes software instructions through the coordinated operation of processors, memory, storage, and input/output subsystems. Students study data representation, instruction sets, arithmetic logic units, CPU organization, control units, memory hierarchy, buses, interrupts, and performance enhancement techniques. The relationship between hardware architecture and system efficiency is emphasized through practical examples and block-level analysis. Learners also explore the interaction between operating systems and hardware resources, providing a solid understanding of modern computing platforms. This knowledge supports advanced studies in embedded systems, operating systems, digital forensics, malware analysis, and cybersecurity engineering.			

Module 27

Code	Module Title	ECTS	Semester
CYBT209	Network Security	6	4
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	87
Description			
Network Security focuses on protecting computer networks against unauthorized access, cyberattacks, and service disruption. The module introduces security principles before examining firewalls, virtual private networks, intrusion detection and prevention systems, authentication mechanisms, access control, wireless security, and network monitoring. Students analyze common attacks such as spoofing, denial-of-service, packet sniffing, and man-in-the-middle attacks while evaluating appropriate defensive strategies. Practical laboratory exercises provide experience configuring security mechanisms, analyzing network traffic, and identifying vulnerabilities. The course develops the technical skills required to design, implement, and maintain secure communication infrastructures in enterprise and industrial environments.			

Module 28

Code	Module Title	ECTS	Semester
NTU203	Arabic Language	2	4
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2		33	17
Description			
This advanced Arabic language module enhances students' academic writing and professional communication skills through the study of formal linguistic structures and effective written expression. Learners practice preparing technical reports, research summaries, official correspondence, and presentations using precise grammar, appropriate vocabulary, and coherent organization. Selected texts encourage analytical reading and strengthen the ability to extract, evaluate, and communicate information accurately. Discussions and writing activities promote clarity, logical argumentation, and correct stylistic conventions. The module supports engineering students in producing high-quality documentation and communicating confidently in governmental, industrial, and educational settings.			

Module 29

Code	Module Title	ECTS	Semester
CYBT210	Network Administration and Infrastructure	4	4
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
1	2	48	52
Description			
Network Administration and Infrastructure provides practical knowledge for deploying, configuring, and maintaining modern enterprise networks. Students work with switching, routing, VLANs, IP addressing, DHCP, DNS, network services, and infrastructure documentation while learning systematic approaches to troubleshooting and performance optimization. Laboratory exercises emphasize device configuration, network monitoring, backup procedures, and maintenance of reliable communication services. Attention is also given to scalability, availability, and security considerations when designing organizational networks. By combining theoretical principles with hands-on practice, the module prepares students to administer professional network environments and establishes a strong basis for cloud networking and advanced cybersecurity courses.			



Module 30

Code	Module Title	ECTS	Semester
NTU202	Computer 2	3	4
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	1	48	27
Description			
Computer 2 expands students' digital proficiency by introducing more advanced computer applications and productivity tools used in engineering and research. The module develops practical skills in spreadsheet analysis, database fundamentals, technical presentations, collaborative platforms, cloud applications, and responsible information management. Students learn techniques for organizing data, producing professional documents, analyzing numerical information, and presenting technical results effectively. Practical exercises reinforce efficient use of software tools while promoting digital collaboration, cybersecurity awareness, and ethical use of information technology. These competencies support coursework across the engineering curriculum and improve workplace readiness.			

Module 31

Code	Module Title	ECTS	Semester
CYBT300	Introduction to Cryptography	6	5
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	87
Description			
Introduction to Cryptography presents the mathematical and practical techniques used to secure digital information. Students explore classical and modern encryption methods, symmetric and asymmetric cryptography, hash functions, digital signatures, key exchange, certificates, and public key infrastructure. The course explains how cryptographic algorithms protect confidentiality, integrity, authentication, and non-repudiation in real-world systems. Practical examples demonstrate the use of cryptography in secure communications, e-commerce, authentication protocols, and data protection. Security strengths, limitations, and implementation considerations are discussed to help students understand both theoretical foundations and practical deployment. The module establishes the knowledge required for advanced studies in cybersecurity, secure software, network security, and digital forensics.			



Module 32

Code	Module Title	ECTS	Semester
CYBT301	Introduction to Hardware security	7	5
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	112
Description			
Introduction to Hardware Security examines threats targeting physical computing devices and embedded systems. Students study secure hardware design principles, trusted execution, firmware security, secure boot, hardware vulnerabilities, side-channel attacks, fault injection, and tamper resistance. The module explains how attackers exploit weaknesses in processors, memory, peripherals, and embedded platforms, while introducing techniques for protecting hardware assets throughout their lifecycle. Laboratory activities and case studies expose learners to practical security challenges involving microcontrollers, IoT devices, and trusted hardware components. By understanding hardware-level attacks and defenses, students gain an appreciation of security beyond software and networks.			

Module 33

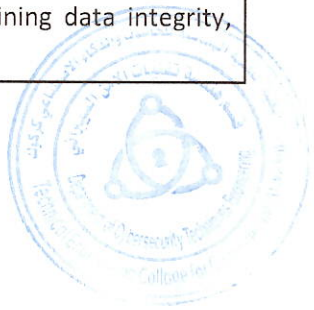
Code	Module Title	ECTS	Semester
CYBT302	Communication Systems	5	5
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2		33	92
Description			
Communication Systems introduces the principles governing the transmission of information over electrical, wireless, and optical media. The course covers analog and digital signals, amplitude, frequency and phase modulation, multiplexing, bandwidth, noise, sampling, and basic digital communication techniques. Students learn how information is encoded, transmitted, received, and reconstructed while evaluating factors that influence communication quality and system performance. Engineering examples illustrate the operation of radio, satellite, mobile, and fiber-optic communication systems. The module provides the theoretical background required for wireless networking, software-defined radio, telecommunications, and secure communication technologies.			

Module 34

Code	Module Title	ECTS	Semester
CYBT303	Microprocessors	5	5
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	62
Description			
Microprocessors explores the architecture and operation of programmable processing units used in computers and embedded systems. Students examine processor organization, instruction execution, addressing modes, memory interfacing, interrupts, timers, input/output techniques, and assembly language programming. Practical laboratory exercises involve programming microprocessor development boards, interfacing external devices, and troubleshooting hardware-software interactions. Particular emphasis is placed on understanding how low-level software controls hardware resources, making the module especially valuable for embedded security, reverse engineering, firmware analysis, and industrial automation. The knowledge gained bridges digital electronics with advanced computer engineering applications.			

Module 35

Code	Module Title	ECTS	Semester
CYBT304	Database security	5	5
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	62
Description			
Database Security focuses on protecting databases against unauthorized access, data leakage, manipulation, and service disruption. Students investigate authentication, authorization, access control models, encryption, auditing, backup strategies, transaction security, and secure database configuration. The course also addresses SQL injection, privilege escalation, insider threats, and methods for identifying and mitigating database vulnerabilities. Practical exercises reinforce secure administration, policy implementation, and monitoring techniques using relational database management systems. By combining database technologies with cybersecurity principles, the module prepares students to safeguard organizational information assets while maintaining data integrity, confidentiality, and availability.			



Module 36

Code	Module Title	ECTS	Semester
CAIK301	Entrepreneurial Capacity Building	2	5
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2		33	17
Description			
Entrepreneurial Capacity Building equips students with the mindset and practical skills needed to transform technical ideas into viable business opportunities. The module introduces innovation, opportunity recognition, market analysis, business models, intellectual property, financial planning, project management, and entrepreneurial leadership. Students examine successful technology startups, develop business proposals, and evaluate the commercial feasibility of engineering solutions. Team-based activities encourage creativity, communication, decision-making, and problem solving while highlighting ethical and sustainable business practices. The course inspires students to become innovators capable of creating value through technology, whether by launching new ventures or contributing to organizational growth.			

Module 37

Code	Module Title	ECTS	Semester
CYBT305	Intrusion Detection and Prevention Systems	5	6
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	62
Description			
Intrusion Detection and Prevention Systems examines the technologies used to identify, analyze, and block malicious activities within modern computer networks. Students study signature-based and anomaly-based detection techniques, network and host intrusion detection systems, event correlation, alert management, and automated response mechanisms. Practical laboratory sessions involve configuring IDS/IPS platforms, interpreting security logs, analyzing attack traffic, and developing detection rules. The module also discusses false positives, performance considerations, and integration with broader security monitoring solutions. Through realistic scenarios, students learn how intrusion detection contributes to proactive cyber defense and incident response.			

Module 38

Code	Module Title	ECTS	Semester
CYBT306	Cryptosystems	5	6
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	62
Description			
Cryptosystems expands upon introductory cryptography by examining the design, implementation, and evaluation of complete cryptographic solutions. Students investigate block and stream ciphers, public key algorithms, key management, authentication protocols, digital certificates, secure communication protocols, and cryptographic standards. Attention is given to selecting appropriate algorithms based on security requirements, computational efficiency, and implementation constraints. Practical exercises demonstrate how cryptographic mechanisms are integrated into secure applications, operating systems, and communication networks. The course also introduces current challenges such as quantum-resistant cryptography and implementation vulnerabilities, preparing students for advanced security engineering.			

Module 39

Code	Module Title	ECTS	Semester
CYBT307	Operating system security	5	6
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	62
Description			
Operating System Security explores techniques for protecting modern operating systems against internal and external threats. Students examine user authentication, privilege management, access control models, kernel protection, process isolation, memory security, secure boot mechanisms, logging, auditing, and system hardening. Common vulnerabilities, malware behavior, privilege escalation attacks, and defensive countermeasures are analyzed through practical examples. Laboratory activities strengthen students' ability to configure secure operating system environments, monitor system integrity, and investigate suspicious activity. The module demonstrates how operating system security forms a critical layer in protecting enterprise infrastructures and cybersecurity operations.			

Module 40

Code	Module Title	ECTS	Semester
CYBT308	Mobile and Wireless Networks	5	6
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	62
Description			
Mobile and Wireless Networks introduces the technologies that enable wireless communication between mobile devices, sensors, and distributed systems. Students study cellular network evolution, Wi-Fi, Bluetooth, Zigbee, satellite communications, wireless routing, mobility management, and quality of service. The module explains radio propagation, channel access methods, spectrum utilization, and network architecture while addressing performance, reliability, and security challenges. Laboratory exercises provide experience with wireless configuration, traffic analysis, and troubleshooting. Understanding mobile and wireless technologies prepares students for advanced work in wireless security, Internet of Things, software-defined radio, and next-generation communication systems.			

Module 41

Code	Module Title	ECTS	Semester
CYBT309	Engineering Analysis	4	6
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	37
Description			
Engineering Analysis integrates mathematical, computational, and engineering principles to solve complex technical problems systematically. Students learn to formulate engineering models, evaluate assumptions, apply analytical and numerical methods, and interpret results critically. The module introduces optimization techniques, error analysis, modelling strategies, and computer-assisted problem solving using representative engineering case studies. Emphasis is placed on selecting appropriate analytical approaches, validating solutions, and communicating technical findings effectively. By combining theoretical reasoning with practical applications, the course strengthens the analytical skills required for communication systems, cybersecurity engineering, embedded systems, and multidisciplinary engineering design.			



Module 42

Code	Module Title	ECTS	Semester
CYBT310	Cloud Computing Security	6	6
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	87
Description			
Cloud Computing Security examines the challenges of protecting virtualized infrastructure, cloud services, and distributed computing environments. Students explore cloud deployment models, shared responsibility, identity and access management, virtualization security, container protection, encryption, secure storage, and compliance requirements. The course also addresses cloud-specific threats including insecure APIs, misconfiguration, data leakage, and multi-tenant vulnerabilities. Practical activities demonstrate security controls implemented across Infrastructure-, Platform-, and Software-as-a-Service environments. Upon completion, students are able to evaluate cloud security architectures and recommend appropriate controls for securing modern enterprise cloud deployments.			

Module 43

Code	Module Title	ECTS	Semester
CYBT400	Mobile and Wireless Networks Security	6	7
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	87
Description			
Mobile and Wireless Networks Security focuses on defending wireless communication systems against evolving cyber threats. Students investigate authentication protocols, wireless encryption standards, secure roaming, cellular security, Wi-Fi protection mechanisms, Bluetooth security, and vulnerabilities affecting mobile devices and Internet of Things platforms. Laboratory exercises include wireless traffic analysis, security assessment, attack simulation, and implementation of defensive configurations. The module highlights current threats such as rogue access points, spoofing, eavesdropping, denial-of-service, and protocol weaknesses while introducing effective mitigation strategies. Students gain practical skills needed to secure modern wireless infrastructures and mobile computing environments.			



Module 44

Code	Module Title	ECTS	Semester
CYBT401	Research Methodology	3	7
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2		33	42
Description			
Research Methodology prepares students to conduct scientific investigations using structured and ethical research practices. The module introduces problem identification, literature review, hypothesis formulation, research design, data collection, experimental methods, statistical analysis, citation techniques, and academic writing. Students learn to evaluate published research critically, distinguish credible sources, and present findings clearly through technical reports and presentations. Ethical considerations including plagiarism, research integrity, and responsible use of information are emphasized throughout the course. These competencies provide the foundation for successful graduation projects, postgraduate studies, and evidence-based engineering practice.			

Module 45

Code	Module Title	ECTS	Semester
CYBT402	AI for Cybersecurity Engineering	6	7
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	87
Description			
Artificial Intelligence for Cybersecurity Engineering explores how intelligent algorithms enhance the detection, analysis, and mitigation of cyber threats. Students study machine learning fundamentals, supervised and unsupervised learning, anomaly detection, malware classification, intrusion detection, natural language processing, and predictive security analytics. Practical exercises involve preparing datasets, training models, evaluating performance, and interpreting results using modern AI tools. The module also discusses adversarial machine learning, ethical considerations, explainable AI, and limitations of automated decision-making. By integrating artificial intelligence with cybersecurity concepts, students develop advanced analytical skills for protecting modern digital infrastructures.			



Module 46

Code	Module Title	ECTS	Semester
CYBT403	Ethical Hacking and Penetration Testing	6	7
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	87
Description			
Ethical Hacking and Penetration Testing provides students with the methodology used by security professionals to evaluate the resilience of computer systems against cyberattacks. The module covers reconnaissance, vulnerability assessment, exploitation, post-exploitation, privilege escalation, reporting, and remediation. Students gain practical experience using professional security tools to identify weaknesses in networks, operating systems, web applications, and wireless environments within controlled laboratory settings. Equal emphasis is placed on legal boundaries, professional ethics, authorization requirements, and responsible disclosure. The course develops a structured approach to security assessment while preparing graduates for defensive cybersecurity roles.			

Module 47

Code	Module Title	ECTS	Semester
CYBT404	Applied Cryptosystems	3	7
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	12
Description			
Applied Cryptosystems bridges cryptographic theory with real-world implementation by examining how encryption technologies are integrated into modern applications and communication systems. Students study secure protocol design, key lifecycle management, authentication frameworks, transport layer security, public key infrastructure, digital certificates, and secure software development practices. Practical activities demonstrate cryptographic libraries, implementation pitfalls, side-channel considerations, and performance trade-offs. The course emphasizes selecting appropriate cryptographic solutions based on operational requirements while maintaining confidentiality, integrity, authenticity, and non-repudiation across enterprise environments.			



Module 48

Code	Module Title	ECTS	Semester
CYBT405	Graduation Project Design	6	7
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
	2	33	117
Description			
Graduation Project Design guides students through the planning and preparation stages of their capstone engineering project. Learners identify a significant technical problem, review relevant literature, define objectives, evaluate existing solutions, and prepare a detailed project proposal. The module emphasizes project planning, methodology selection, feasibility analysis, risk assessment, scheduling, resource allocation, and documentation. Regular supervision supports students in refining their research direction while ensuring academic integrity and engineering rigor. Successful completion results in a comprehensive project design that provides a clear roadmap for implementation.			

Module 49

Code	Module Title	ECTS	Semester
CYBT406	IT Project Management	6	8
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2		33	117
Description			
IT Project Management introduces the principles and practices required to plan, execute, monitor, and successfully deliver information technology projects. Students examine project life cycles, scope definition, scheduling, budgeting, procurement, quality assurance, stakeholder communication, and risk management. Modern project management methodologies, including Agile and traditional approaches, are compared through practical case studies. Teamwork, leadership, decision-making, and resource coordination are emphasized alongside the effective use of project management software. The module prepares future engineers to manage complex technical projects within organizational, financial, and time constraints.			



Module 50

Code	Module Title	ECTS	Semester
CYBT407	Graduation Project Implementation	3	8
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
	2	33	42
Description			
Graduation Project Implementation represents the culmination of the engineering programme, where students transform their approved project designs into fully developed technical solutions. Under academic supervision, learners design, implement, test, validate, and document their systems while applying engineering standards and professional practices. The module requires integration of knowledge acquired throughout the curriculum, including technical analysis, experimentation, troubleshooting, and performance evaluation. Students present their work through formal reports, demonstrations, and oral defenses, demonstrating technical competence, innovation, teamwork, and effective communication.			

Module 51

Code	Module Title	ECTS	Semester
CYBT408	Digital Forensics	7	8
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	112
Description			
Digital Forensics equips students with the knowledge and investigative techniques required to identify, preserve, examine, analyze, and present digital evidence. The module covers forensic acquisition, chain of custody, file system analysis, memory forensics, log analysis, mobile device investigations, timeline reconstruction, and forensic reporting. Students use specialized forensic tools to recover deleted information, examine artifacts, and investigate security incidents while maintaining evidential integrity. Legal procedures, ethical responsibilities, and standards governing digital investigations are integrated throughout the course, preparing graduates for incident response and forensic analysis roles.			

Module 52

Code	Module Title	ECTS	Semester
CYBT409	IoTs and Cybersecurity	7	8
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	112
Description			
Internet of Things and Cybersecurity examines the security challenges associated with interconnected smart devices, embedded platforms, industrial control systems, and cyber-physical environments. Students explore IoT architectures, communication protocols, authentication mechanisms, firmware protection, secure device management, vulnerability assessment, and privacy considerations. Practical case studies demonstrate attacks targeting connected devices and appropriate mitigation techniques. The course highlights secure design principles that improve the resilience of IoT ecosystems deployed in homes, healthcare, transportation, and industrial environments.			

Module 53

Code	Module Title	ECTS	Semester
CYBT410	Reverse Engineering-Malwares Analysis	7	8
Class (hr/w)	**Lect/Lab./Prac./Tutor**	**SSWL (hr/sem)**	**USWL (hr/sem)**
2	2	63	112
Description			
Reverse Engineering and Malware Analysis introduces advanced techniques for understanding malicious software by examining its internal structure and behaviour. Students learn static and dynamic analysis, executable formats, disassembly, debugging, decompilation, sandboxing, memory inspection, and behavioural analysis using professional reverse engineering tools. The module investigates common malware families, persistence mechanisms, obfuscation techniques, command-and-control communication, and anti-analysis methods. Practical laboratories enable students to safely analyze malware samples, extract indicators of compromise, and develop defensive strategies. These skills support malware research, incident response, threat intelligence, and advanced cybersecurity operations.			



3. Contact

Program Manager:

Hayder Touran Mahdi Assafli | Ph.D. in Electrical Engineering | Lecturer

Email: hayder.assafli@ntu.edu.iq

Mobile No.:

Program Coordinator:

Deniz Nisham Anwer Ismail | M.Sc. in Computer Engineering | Assistant Lecturer

Email: deniz.anwer@ntu.edu.iq

Mobile No.:

