

— HANDBOOK —



Professional Master  
» in **CYBERCRIME**  
Investigation

2021 - 2022





# Overview



The Faculty of Law at the British University in Egypt “BUE” is launching Cybercrime Investigation Professional Master’s programme.

This programme is considered the first of its kind in the MENA region.

It is intended for professionals interested in studying cyber criminology, particularly those with an interest in cybercrime, cyber security investigation, counterterrorism and cyber laws.

Despite the growing public interest in cybercrime and its consequences for businesses and individuals, only scant attention has been given in the criminological discipline to investigation and understanding of this new type of crimes.

The challenging nature of the digital environment which constantly affecting everything from government policies to secure citizen’s privacy and rights require specialised education.



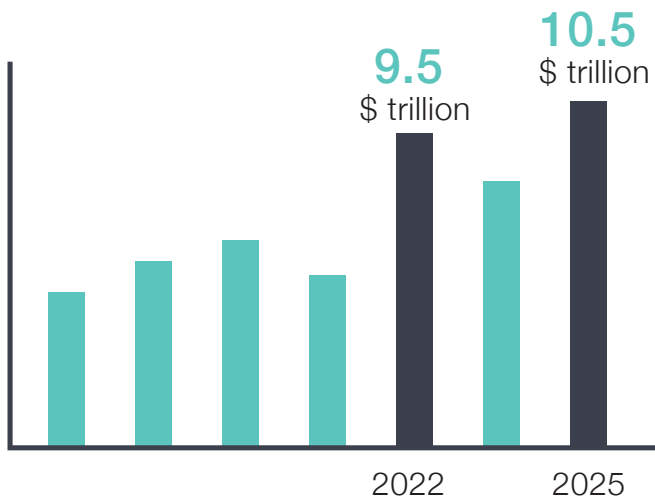
This programme is considered the first of its kind in the MENA region.



## Programme Focus

To achieve academic excellence and graduate independent learners, with the best UK professional and academic standards, who are equipped as effective lifelong learners able to make a significant contribution to the field of cyber law, cyber investigations and security.

### Expected cost of cybercrime to global economy



# Programme aims

The Professional Master's in Cybercrime Investigations programme aims to:



Provide students with an in depth theoretical and practical overview of contemporary issues in cybercrime and cyber security.



Equip students with an understanding of the relationship between developments in ICT and its effect on society and law.



Provide students with an understanding of the legal, criminological context of cybercrime and the necessary computing skills and capabilities to research and prepare to address cybercrime and cyber-related offences.



Provide students with a critical understanding of how the study of cybercrime challenges existing criminological theories, research methodologies and criminal law.



Equip students with relevant theoretical and practical understanding of tools, techniques, procedures and skills necessary to effectively carry out effective digital forensic investigations especially relating to computer incidents and computer misuse.



Equip students with knowledge of legal and professional issues relevant to computer-related crimes, digital evidence and digital forensic investigations.



## Programme Management Team



Professor

**Hassan Abdelhamid**

- Professor of philosophy of Civil Law.
- Dean of Faculty of Law.
- Director of Centre for Law and Emerging Technologies.
- Professor at the Department of Law and Justice, at Laurentienne University (Canada).



Dr.

**Mohamed Elguindy**

- Cybercrime and Cyber Security International Consultant to the UNODC.
- Programme Director.
- Advisor to the Director of Centre for Law and Emerging Technologies.
- Digital Transformation Expert, Public Prosecution Office.



Dr.

**Marwa Zein**

- Assistant Professor of International Private Law.
- Programme Director.
- Head of Research Programmes - Centre for Law and Emerging Technologies.
- Expert in Internet Governance and Data Privacy.

# Teaching staff



Dr.  
**Tamer Eldomyaty**

- Associate Professor of Law.
- Deputy Director, Centre for Law and Emerging Technologies.



Dr.  
**Alex Atanosouf**

- Assistant Professor of Law.
- BA, LL.B., Mîtrise en droit, LL.M., PhD.
- Expert in AI Laws.



Dr.  
**Mohamed Chawki**

- Ph.D in cybercrime, University of Lyon 3, France.
- Chairman, International Association of Cybercrime Prevention (AILCC), France.



Prof.  
**Hazem Shatela**

- Professor of AI.
- Virginia Tech University.
- Lecturer- The Arab Academy for Maritime and Transport.



Dr.  
**Inas Taha**

- Assistant Professor of Public Law.
- Expert in Pubic Finance, Taxes and Digital Economy.



## International Experts



Judge  
**Ali Younis**

- Terrorism Prevention Regional advisor/ Crime Prevention and Criminal Justice officer- UNODC - OGCCR.



Mr.  
**Dan Shefet**

- Lawyer at the Paris Court of Appeal.
- International LegalTech expert at UNESCO.



Mr.  
**Bashir Fancy**

- President of Business and Technology Association of Canada.
- Chairman of the Canada's Association for Information Technology Professionals.
- Executive Vice President - Risk Management & Security - Visa.

"In addition to International experts from reputable technology and engineering organizations around the world to provide our students cutting-edge education and hands-on experience"

# Teaching Support Team



Mr.  
**Ibrahim Sabra**

- Assistant Lecturer.
- Researcher at BUE Centre for Law and Emerging Technologies.



Mr.  
**Ahmed Nasser**

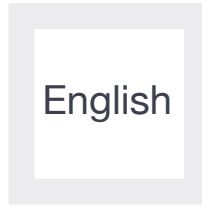
- Assistant Lecturer.
- Researcher at BUE Centre for Law and Emerging Technologies.



Ms.  
**Nesrine Mohamed**

- Senior Executive Administrator.

Language of instruction: English



## Learning Experience

This programme will deliver the cutting edge of global trends in cyber law and policy, digital forensic computing and the complex legalities of cyberspace.

Cybercrime is a multi-disciplinary subject; therefore, this programme has been developed by practitioners in the field to enhance knowledge and practical skills in areas of behavioural psychology, criminal investigation and digital evidence.

International renowned experts and subject matter experts in the legal and technical fields will deliver the programme in addition to delivering specialised workshops and seminars.

The teaching methods vary from lectures to tutorials, workshops and lab tutoring as well. In addition, students will attend obligatory internships in one of the partner institutions.



Every minute, **\$2,900,000**  
is lost to cybercrime  
and top companies  
pay \$25 per minute due to  
cyber security breaches.

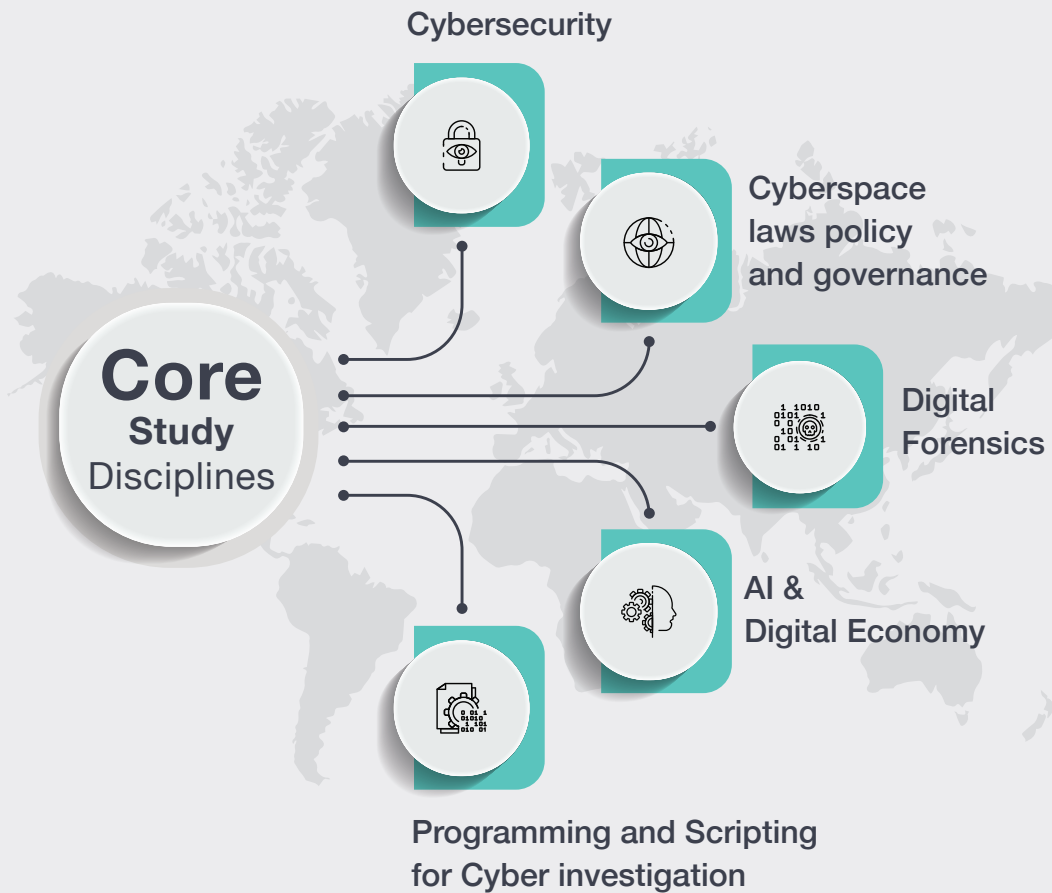


## Accreditation and Validation

Under the Ministerial Decree No. 1892 dated 14/2021/06/, The Programme is approved by Egyptian Ministry of Higher Education, the Supreme Council of Higher Education and the Supreme Council of the Private Universities.

The Programme now is under the accreditation process from UK professional accreditation bodies, in addition to , validation from reputable British University.

# Core Study Disciplines





“

Supply chain attacks are expected to grow **420%** in just **12** months.

# Programme Modules



## 1. Cybercrime

The purpose of this module is to expose students to a range of trends in cybercrime and to develop their ability to find and evaluate their value for cybercriminals.

Students will explore cybercrime definitions and categories, gain knowledge about methods, techniques and emerging technologies that cybercriminals use, how they operate, and how they engage with victims in the cyberspace with the goal of becoming better equipped to prevent, detect and react to cybercrime.



“

The module provides also the necessary skills related to researching cybercrime from criminological perspectives.

## 2. Cyber Law

This module will expose students to the importance of cyber laws from both national and international perspectives.

It will examine the emerging trends that signify the formation of the information society and also its relationship with law, technology, and public policy.

This module will cover UK and European Union laws along with a variety of international regulatory perspectives that seek to harmonise law.

The module will analyse the many legal and regulatory challenges that the information society generates for society, particularly with regard to privacy, the creation of products, and the media.

Particular focus will be upon whether these challenges can be best resolved by law or some other means, for example, technology, education or simple market forces. The aim of the module is to make students aware of the legal and regulatory policy issues which are intimately connected with the information society.





# Programme Modules



## 3. Cyber Investigations

This module will expose students to advanced cyber investigation skills. It is intended to provide students with an understanding of information that is freely available on the internet that is referred to as Open Source Intelligence.

To introduce research skills and techniques to produce efficient and effective searches in databases and social networking sites, developing an understanding of computer security and leaving footprints whilst making online enquiries, the identification of email addresses whilst ensuring such investigations are lawful, necessary and proportionate.

The module will include advanced topics such as social media investigation, website and email identification and criminal intelligence analysis skills. Practical moot court is also addressed in relation to intelligence and evidence presentation.



## 4. Digital Evidence

This module will equip students with an understanding of the technical issues involved in the handling of digital evidence.

While digital evidence is the focus of the module, it discusses the wider issues including mobile devices, network-based evidence, interpretation of evidence, and acquisition of digital evidence.

The module also focuses on the international standards and procedures related to digital evidence from collection to presentation in the court room.



“

Practical moot court is also addressed in relation to digital evidence presentation.

# Programme Modules



## 5. Cyber Terrorism

Terrorism is a nightmare for investigators; especially when terrorists use complex technologies.

This module will introduce students to the wider issue of terrorist use of the internet, legal issues, cyber terrorism and cyberwarfare, cyber terrorism case studies, cyber weapons, international frameworks that are applicable to cyber conflicts and other related topics.

It examines also the capabilities that a non-state actors can achieve and whether this can constitute a real threat to the national security of states.



## 6. Digital Economy

The purpose of this module is to explore a number of legal issues (and associated cultural and social issues) which are related to the digital economy.

The module considers the coherence of the regulatory system (particularly questions of scope and jurisdiction), and explores the substantive law of electronic commerce in more detail (e.g. tax and consumer issues, electronic contracts and signatures, fraud).

Trending technologies are also discussed such as Cryptocurrencies and Blockchain technology.



“

By 2022, worldwide  
spending on blockchain  
solutions will reach  
**\$11.7** billion.

# Programme Modules



## 7. Graduation Project

After passing the modules students will start their graduation project journey supervised by top notch experts in the legal and technical fields, this will be the concluding part of the programme and the harvesting point of all practical experience the students gained throughout their study.

According to Forbes, there will be 1.8 million unfilled cybersecurity jobs by 2022.





# Duration



”

**The programme**  
is taught over full calendar  
year **(12 months)** for full  
time students and two  
calendar years for part-time  
students **(24 months)**.

full time



12 months

part-time



24 months



# Why to join

There are countless reasons to join the programme:

- Earn Professional Master's (PM) degree in Cybercrime and cyber Security Investigations.
- The first Professional Master's programme in Cybercrime and cyber Security Investigation to be accredited by the Egyptian Supreme Council of Universities.
- Learn from Top-notch international and national legal and technical experts and academics who will deliver the programme.
- The first Master's programmes in MENA Region to provide such practical experience in the interdisciplinary areas of law and emerging technologies.
- Cooperation with reputable international organizations and entities, such as UN, IEEE, BCS and ISSA.
- Internships at governmental and non-governmental institutions.



## Upon graduation, the graduates will have the opportunity to work as:

- E-investigation officer
- Social media safety officer
- Anti-money laundering Investigator
- Cyber Threat Intelligence analyst
- Compliance officer
- Cyber Security Auditor
- Data Security Officer
- Data Privacy Officer
- Information Strategist
- Business continuity and disaster recovery officer
- Incident handling officer
- Licensed Digital Forensics Examiner







## Fees and Scholarships

Special discounts for candidates from:

- Judicial Entities.
- Governmental institutions.
- BUE graduates.



Visit the **BUE** website for more information about the scholarship and fees policy.



# Admission Requirements

”

- Original B.Sc. or B.A certificate.
- Accreditation from the Supreme Council of Universities for Graduates of Academies and Higher Institutes offering BS.c. or B.A degrees (N/A for Universities' Graduates).
- Original IELTS certificate (Score 6).

- Original Birth certificate.
- Curriculum Vitae.
- Motivation Letter (why do you want to join and your field related experience).
- A copy of the National ID (for Egyptians) or Passport (for non-Egyptians).
- 4 Personal photos (4X6).

“



[www.bue.edu.eg](http://www.bue.edu.eg)



The British University in Egypt  
EL Sherouk City, Suez Desert Road, Cairo11837 - P.O. Box 43



19283, +202 26890000, +202 26300013 / 14 / 15/ 16 /17 /18



[Pg.law@bue.edu.eg](mailto:Pg.law@bue.edu.eg)



[www.facebook.com/BUE.Faculty.of.law](https://www.facebook.com/BUE.Faculty.of.law)



[twitter.com/buefacultyoflaw](https://twitter.com/buefacultyoflaw)

