NATIONAL UNIVERSITY

Syllabus

For

PGD in Cyber Security

Effective from the Session: 2022-2023

NATIONAL UNIVERSITY
BANGLADESH

NATIONAL UNIVERSITY
Syllabus for PGD in Cyber Security
Session 2022-2023

Paper Code	Paper Title	Credits
Semester – 1		
816501	Introduction to Cyber Criminology	4
816503	Cryptography and Data Security	4
816505	Network and Communication Security	4
816507	Cyber Security Laws, Policies and Strategies	4
816509	Cyber Crime Investigation and Digital Forensics	4
Semester – 2		
826511	Social Media and Digital Privacy	4
826513	Cyber Risk Management and Crime Prevention	4
826515	Cyber Terrorism and Threat Management	4
826517	Cyber Economic Crime and Management	4
826518	Capstone Project/Internship	4
Total		40

NATIONAL UNIVERSITY
DETAILED SYLLABUS

Course Code	Course Title	Credit
816501	Introduction to Cyber Criminology	4

Course Objectives:
This course is designed to provide students with knowledge of cybercrime and theoretical approaches to studying cybercrime. It examines the causes of crime in cyberspace and the major challenges of fighting cybercrime. The course also covers patterns of cyber violence and strategies to combat cyber victimization.

Learning Outcomes:
After completing this course students will be able to:

- Understand forms of cybercrime and their impact on society
- Develop their knowledge about the causation of cybercrime
- Better understand the strategies and policies in relation to fighting cybercrime

Understanding Cybercrime: Definition, History of cybercrime, Classification/Typology of cybercrime, Extent and impact of cybercrime offenses; Cybercrime vs. Traditional Street crime
Crime and social media and offensive online behavior;
Theoretical Approaches to Cybercrime: Criminological and Social learning theory, psychological theories, Self -control theory;
Causation of Crimes in the Cyberspace: Space transition theory of cybercrimes, Deviance and criminal sub-culture in cyberspace
Cyber aggression and cyber-bullying, Impact of cybercrime on society
Understanding the Cyber Victimization: Lifestyle routine activities theory for cybercrime victimization
Cyber Violence: Technology – facilitated sexual violence; Online sexual exploitation and sexual abuse of children; Harassment, Violation of privacy, Offenses against social groups or communities; Cyber violence against women and girls in Bangladesh
Victims of Cyber Crime Combating cyber victimization
Cyber-stalking: Typology, etiology, and victims
Cybercrime Prevention: Predicting the cyber attackers; Strategies for prevention of cybercrime; Role of education, training, and awareness; Role of regulators in fighting cybercrime; Cybercrime legislation, Cybercrime policy;
The Challenges of Fighting Cybercrime: General and legal challenges
Criminal Justice Response to Cybercrime: The future for the policing of cybercrime in Bangladesh
Investigating cybercrime: Legal issues, and challenges in the context of Bangladesh
Human rights infringement in the digital age: Steps to reinforce human rights in the digital age

Recommended Readings

Jahankhani, Hamid (2018). *Cyber criminology*. New York: Springer

Jaishankar, K. (2011). *Cyber criminology: Exploring internet crime and criminal behavior.* Boca Raton, FL: CRC Press.

Course Code	Course Title	Credits
816503	Cryptography and Data Security	4

Course Objectives:

This course aims to introduce the students to the basic ideas on cryptography, cryptanalysis, and data protection techniques and develop a working knowledge. The course emphasizes giving a basic understanding of previous attacks on cryptosystems with the aim of preventing future attacks. The basic cryptoanalysis techniques will help the students understand the challenges of data security. Data security is the means of ensuring that data is kept safe from corruption and that access to it is suitably controlled. Data security also ensures the privacy and protection of personal data. The hands-on experiences on technology-based productivity tools, foundational knowledge, and understanding of data security give secured ways from designing a system to ensuring security with increase productivity and efficiency. Discussion about risk management, its principles, methods, and types will be included in the course. The course will explain the different ways of securing and protecting data on both hardware and software platforms. After completion of the course, the students shall be able to ensure data security and privacy in any system and can investigate the flaws included in an existing system.

Learning Outcomes:

The learning outcome of this course includes but not limited to:

1. To gain basic knowledge on cryptography, crypto-analysis, and data security required to work with any IT system;
2. To gain hands-on experiences for securing a system from different types of cyber-attacks;
3. To attain risk analysis and ability to manage risks in an IT system;
4. To obtain knowledge about the importance of privacy and its practices in real life;
5. To obtain knowledge about intrusion detection and prevention systems; and
6. To understand ISO/IEC 27001 guidelines.

Detailed Course Contents:

Introduction to Cryptography: Classical cryptosystem, block cipher, Caesar Cipher,

Data Encryption Standard (DES): Triple DES, Advanced encryption standard (AES),

Cryptosystem: Public-key cryptosystem, RSA cryptosystem, key exchange and management, cryptographic hash function, secure hash algorithm (HSA), digital signature, message authentication, data vs. information

Introduction to Information Security: The CIA triad, Security framework, Threats and attach modes, Spoofing, Social engineering, Application and web attacks, Malware,

DoS and DDoS attack, Access control, Firewall and security tools, Identification and authentication,

Operation System Security: Security for electronic commerce, Passwords security, Email security, Intrusion detection, and prevention systems,

Vulnerabilities and Risk management: Incident response process, Privacy laws, Penalties, and privacy issues, ISO/IEC 27001 guidelines.

Required Text(s) and Recommended Readings:

Required Textbooks:

John R. Vacca, Computer and Information Security Handbook, Elsevier, 2nd Edition 2013, ISBN: 978-0123943972.

Nataraj Venkataramanan and Ashwin Shriram, Data privacy principles and practice, Chapman and Hall, CRC, 2017, ISBN: 978-1498721042.

Recommended Books for Readings:

Ahmed Elngar, Ambika Pawar, Prathamesh Churi, Data Protection and Privacy in Healthcare: Research and Innovations, CRC Press, 2021, ISBN: 978-0367501082.

Filip Johnssen and Sofia Edvardsen, Data Protection Officer, BCS, 2019, ISBN: 978-1780174365

Course Code	Course Title	Credits
816505	Network and Communication Security	4

Course Objectives:

Communication and Network security consists of the policies, processes, and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. By the end of this course, the students will be fully aware of the wired and wireless computer networks basics, devices, network-based vulnerabilities, and protocols at a step-by-step pace. They will also reach the professional level in networks security in terms of concepts, technologies, and tools. The course requires no background or pre-requisite, yet the students will be able to understand all the up-to-date terminologies in the network and communication security and shall be able to make their network secured.

Learning Outcomes:

After studying this course, the students shall be able to:

- identify some of the factors driving the need for network security;
- identify and classify particular examples of attacks;
- define the terms vulnerability, threat, and attack;
- identify physical points of vulnerability in simple networks; and
- compare and contrast symmetric and asymmetric encryption systems and their vulnerability to attack, and explain the characteristics of hybrid systems.

Detailed Course Contents:

Understanding the Functionalities of the OSI Model: Data encapsulation and de-encapsulation, TCP/IP model,

The Functionalities of Internet Protocol: IP address, IPv4 and IPv6, transmission control protocol, three-way handshake, user datagram protocol (UDP), TCP and UDP ports, address resolution protocol, host-to-host packet delivery using TCP, threats to communication networks, Wireshark,

TCP/IP Vulnerabilities: ICMP vulnerabilities, Session hijacking, UDP vulnerabilities,
Secure Access: Implementing VPN, VLAN, ACL, secure routing and switching,
Firewall Technologies: Implementing firewall technologies, Implementing intrusion prevention,

Securing Network Devices: AAA, Securing local area network, managing a secure network

Required Text(s) and Recommended Readings:

Required Textbooks:

Chris McNab, Chris (2016). *Network security assessment (3rd edition).* O'Reilly Media Inc,

Troy McMillan, Troy (2018). *CCNA security study guide.* John Willey and Sons

Recommended Books for Readings:

Bejtlich, Richard (2013). *The practice of network security monitoring: Understanding incident detection and response*. San Francisco: No Starch Press.

White, Gregory B., Fisch, Eric A. & Pooch, Udo W. (1996). *Computer system and network security.* New York: CRC Press,

Course Code	Course Title	Credits
816507	Cyber Security Laws, Policies and Strategies	4

Course Objectives:

- To introduce the students to cyber-related laws
- To educate the students about cyber policies and strategies
- To understand the application, investigation, and punishments under the acts
- To comprehend the investigation process of digital crimes
- To provide knowledge on the philosophy of cyber strategies

Learning Outcomes:

- To have comprehensive knowledge of cyber-related laws
- To internalize the cyber policies and strategies
- To have a better understanding of the application, investigation, and punishments under the acts
- To be able to apply strategy according to the philosophy

Detailed Contents:

Digital Security Act, 2018

Objectives of the act, Definitions, Preventive Measures, Digital forensic lab, National Digital Security Council, Critical Information Infrastructure, Offence and Punishment: Punishment for illegal access to any critical information infrastructure, etc., Offence, Investigation, Trial and Punishments under the Act.

The Information & Communication Technology Act, 2006

Objectives Of The Act, Definitions, Digital Signature & Electronic Records, Controller & Certifying Authorities, Duties Of Subscribers, Breaching Rules, Prevention, Penalties Etc., Offences, Investigation, Adjudication, Penalties Etc., Establishment Of Cyber Tribunal, Investigation Of Offences, Adjudication, Appeal Etc., Establishment Of Cyber Appellate Tribunal

The Pornography Control Act, 2012

Objectives of the act, Definitions, conservation and marketing of pornography prohibited, search and seizure, Value of evidence of expert opinions, punishments, some areas where this act will not be applicable, cognizance of offences, Trial Procedure, Appeal, Punishment for false/fake cases or complaints,

The Bangladesh Telecommunication Act, 2001

Objectives of the act, Receipt and disposal Consumer-complains, Inspection and Compulsory Enforcement, Offence, Penalty, Investigation and Trial

The Public Examinations (Offences) Act, 1980

Objectives of the act, Publication or distribution of question papers before public examination, Altering or tampering with any marks, etc., Making, etc., of false mark sheet, certificate, diploma or degree, Conducting public examinations or examining answer scripts by unauthorized persons, Obstructions in public examinations, Offences by officers or employees of University or Board, Abetment of and attempt to commit offences under this Act.

Code of Criminal Procedure, 1898

General Provisions Relating to Searches and Seizure: Direction of search-warrants

Arrest generally: Arrest how to make, Resisting endeavor to arrest, Search of place entered by person sought to be arrested, and Procedure where ingress not obtainable.

Arrest without Warrant: When police may arrest without warrant, Arrest of vagabonds, habitual robbers, etc., Procedure when a police officer deputes subordinate to arrest without warrant

Warrant of Arrest: Form of warrant of arrest Continuance of warrant of arrest,

Cyber Security Laws and Strategies: Regional and International perspectives

Cyber Related Laws:

United Kingdom: Data Protection Act, 2018, Computer Misuse Act, 1990, Digital Economy Act, 2010

USA: Cyber security Information Sharing Act, 2015, Cyber security Enhancement Act, 2014, National Cyber security Protection Advancement Act, 2015, Federal Information Security Modernization Act, 2014

India: National Cyber Security Policy, 2013, Information Technology Act, 2000

Cyber Security Strategies:

Cyber Security Strategy of the United Kingdom: Context; Guiding Principles; Security and Liberty; Partnerships and stakeholders; Threats, Vulnerabilities, Impacts and Opportunities; Links to the National Security Strategy; A Coherent Response; Approach and Strategic Objectives; New Cyber Structures.

Cybersecurity Strategy, USA: Scope; The Cyber Threat; Managing National Cybersecurity Risk; Guiding Principles; Development and Implementation; Risk Identification; Protect the American People, the Homeland, and the American Way of Life

National Cyber Security Strategy, India: Background; Scope; Secure Large scale digitization of public services, Supply chain security, Critical Information Infrastructure Protection, Digital Payment, Sectoral preparedness, State-Level Cyber Security,

National Cybersecurity Strategy- Bangladesh: Strategic Context; Goal; Purpose of Strategy; Ways-Priorities; Cyber Security Priorities Technical and Procedural Measures, Organizational Structures

Recommended Readings:

Chander, H., 2012. *Cyber Laws and IT Protection*. PHI Learning Pvt. Ltd.

Richet, J.L. ed., 2015. *Cybersecurity policies and strategies for cyberwarfare prevention*. IGI Global.

Romaniuk, S.N. and Manjikian, M. eds., 2021. *Routledge companion to global cyber-security strategy*. Routledge.

Sarmah, A., Sarmah, R. and Jyoti Baruah, A., 2017. A brief study on cybercrime and cyber laws of India. *International Research Journal of Engineering and Technology (IRJET)*, *4*(6), pp.1633-1640.

আশরাফুল আলম, *ডিজিটাল নিরাপত্তা আইন ও প্রাসঙ্গিক আইন,* কামরুল বুক হাউস

মোঃ মোবারক হোসেন ভূঁইয়া, *ডিজিটাল নিরাপত্তা আইন, ২০১৮* (হার্ডকভার) সর্বশেষ সংশোধনী

বিচারপতি মোঃ আজিজুল হক, *সাইবার ল এন্ড ক্রাইম* উচ্চতর আদালতের সিদ্ধান্তসহ

দেলওয়ার হোসেন, *বাংলাদেশে সাইবার ক্রাইম তদন্ত ও বিচার ব্যবস্থা,* কামরুল বুক হাউস

Course Code	Course Title	Credit
816509	Cyber Crime Investigation and Digital Forensics	4

Course Objectives

The course will cover various aspects of cybercrime investigation as well as forensic digital evidence and evidence management. Both theoretical orientation and technical know-how in relation to cybercrime investigation will be explored.

Learning Outcomes

The students will gain a better understanding of cybercrime investigation and digital forensic after the completion of this course. It will enable them to better utilize their knowledge in conducting a digital investigation in their area of work. This course aims at helping to improve the cybercrime investigation of the private entity, law enforcement agencies, the regulators, and others concerned.

Detailed Contents

Cybercrime and Cybercriminals: Sociological and criminological study of cybercrime in contemporary society; Cybercrimes in Bangladesh; Cybercrime Case Study in the country context

Sources, Motives, and Methods of Cybercrimes: Threat sources; Attacker's Motives/goals; Attack Methods; Tools and Techniques used to Commit Cyber Crimes; Crimes targeting computer systems; Crimes in which computer systems are used as tools/instruments.

Trends in Cybercrime incidents, Identification and Mitigation Strategy: Crimes in Social Media - Fake News, Hate speech, the spread of extremism, scams and frauds, etc.; Common Crimes and Risks Online - Business email compromise (BEC), Identity theft, Ransomware, Spoofing and phishing, Online predators, etc.; Cyber awareness; Where and how to Report Crime & Fraud.

Cybersecurity Incident Response and Management: Responding to a cyber security incident – (i) Identify cyber security incident, (ii) Define objectives and investigate the situation; (iii) Take appropriate action, (iv) Recover systems, data, and connectivity; Following up a cyber security incident - (i) Investigate the incident more thoroughly, (ii) Report the incident to relevant stakeholders, (iii) Carry out a post-incident investigation review, (iv) Communicate and build on lessons learned, (v) Update key information, controls and processes, (vi) Perform trend analysis.

Digital Crime Investigation: Phases of cybercrime investigation; Crime Scene Investigation: Search and Seizure; Chain of custody; Preparation for deposition of evidence in court; Prosecution of the offender; Challenges in Cyber Security Incident Investigations.

Digital Crime Evidence: Digital Devices – Sources for Digital Evidences; Log File Identification, Preservation, Collection and Acquisition; Identifying, Seizing and Preserving Evidence from - (i) Cloud-Computing Platforms, (ii) Internet of Things Devices; Open Source Evidence; Crime and the Dark Web

Digital Crime Evidence Management: Collection and protection of Digital Evidence; Preservation of the Chain of Custody; Legal Implications of Digital Evidence Collection

Practical Demonstration of Digital Crime Investigation: The Investigation Team; Resources Required; Availability and Management of Evidence; Technical Items; Scene Investigation; Deposition of evidence in court; Prosecution of the offender.

Digital Evidence in Court: Prosecutor's questions, Validity of evidence, Digital evidence storehouse, MLAT Process, Court Preparation.

Digital Forensics and Analyzing Data: Cyber Forensics - Its Importance, Cyber Forensics Techniques, and Tools; Cyber Forensics Evolution and Its Goals; Current Challenges of Digital Forensics in Cyber Security, Tools Accreditation, Standard Operating Procedure.

Digital Forensic Tools: Demonstration of the forensic tools used by law enforcement agencies.

Visit the Digital Forensic Lab of CID/CTTC/PBI: Daylong visit to the Forensic Lab of CID/CTTC/PBI to impart visual insight on Digital Crime Forensic.

Recommended Readings

Creasey, Jason (2013). *Cyber security incident response guide.* Kettering, UK: Crest Publications

John Bandler, John & Merzon, Merzon, Antonia, (2020). *Cybercrime investigations: A comprehensive resource for everyone.* New York: CRC Press.

O'Shea, Kevin, Steele, Jim, Hansen, Jon R., Jean, Benjamin R., Ralph, Thomas (2007). *Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors.* Rockland, MA: Syngress Publishing.

Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone (2012). *Computer Security Incident Handling Guide.* NIST: U.S. Department of Commerce. Washington, DC.

Course Code	Course Title	Credit
826511	Social Media and Digital Privacy	4

Course Objectives

Social media is undoubtedly the newest and fastest way of sharing information, but the byproduct of all that sharing can turn out to be dangerous. This course will explore Social Media and Networks in a new light so as to make the participants understand what social media and social networks are, how they work, how to protect right to digital privacy, how to recognize and prevent an intrusion or invasion of privacy, what's considered a reasonable expectation of privacy, how to determine who lawfully owns a social media account, what types of information others can prevent you from sharing online, what the potential dangers are involved, relevant laws safeguarding privacy online, etc.

Learning Outcomes

Upon successful completion of the course, the participants will learn about-

(i) what social media and social networks are, how they work, how to make the best use of social media and social networks;

(ii) how to protect the right to digital privacy, how to recognize and prevent an intrusion or invasion of privacy, what's considered a reasonable expectation of privacy, how to determine who lawfully owns a social media account and what types of information others can prevent you from sharing online;

(iii) what is considered reckless misconduct on social media, use social media without violating laws, use social media without infringing on intellectual property rights;

(iv) social media policy for business, corporate social media policy examples.

Detailed Contents

Introduction to Social Media

What is social media, the new means of production and distribution, how social media work, how social networks work, Classification of Social Media, how blogs work, how wikis work, how podcasts work, how forums work, how content communities work, how micro-blogging works, how second life works, A brief list of Social Media websites.

A brief history of Social Media

History of Social Media, Analysis of the evolution of Social Media over time, Future of Social Media

Social Media Management

Social Media Management (Identification of Relevant Social Media Profile Creation, Expanding the Network, Monitoring and analysis, Social Media strategy), Social Media tools (Social Media engagement tools, Social Media monitoring and analysis tools, Professional listening tools, Other tools), Benefits of Social Media for individuals and business.

Privacy on Social Media

Social Media as the New Hacking Target, Doxing on the Rise, Threats to Privacy on Social Media (Data Mining, Phishing Attempts, Malware Sharing, Botnet Attacks).

Causes of Privacy Concern
Various levels of privacy offered (People concern and user awareness in social networking sites), Data access methods (Sharing users' information with advertising and tracking companies, API, Search engines, Location data, Email and phone number leaks), Benefit from data.

Potential Dangers
Identity theft, Preteens and early teenagers, Sexual predators, Stalking, Unintentional fame, Employment, Online victimization, Surveillance, Mob rule, Location updates, Invasive privacy agreements

Protecting social network privacy
Understanding of the threats, Change of attitude (to be thorough all the time, to be careful about taking drastic actions, etc.), Knowledge of the sites, Knowledge of device protection

Digital Privacy
Storing your personal information online, Usernames and Passwords for Websites, Two-factor authentication, Kinds of information that shouldn't be posted online, How to protect information that is posted online.

Securing Home Computer and Network
Data encryption for the home user, Internet games and downloads, Securing home network, Other devices on the network.

Social Media Monitoring
Social Media Monitoring and Privacy Law, Personal privacy rights, Lawful Social Media monitoring practice, Risk of unlawful Social Media monitoring practices.

Privacy Strategy
Policy development (Building a stakeholder coalition, Risk and opportunities, Circulating draft for preview).

Recommended Readings:

Ralph Gross, Ralph (2005). Information Revelation and Privacy in Online Social Networks (The Facebook case)

Saravankumar, K. (2016). On privacy and security in social media – A comprehensive study

Taprial, Varinder & Kanwar, Priya (2012). Understanding social media. BookBoon.

Turculet, Mircea (2014). Ethical Issues Concerning Online Social Networks.

Internet Safety 101 (https://internetsafety101.org/social-media-apps)

https://www.udemy.com/course/lawful-social-media-monitoring/

https://www.udemy.com/course/social-media-policy-development/

Course Code	Course Title	Credits
826513	Cyber Risk Management and Crime Prevention	4

Course Objectives:

This course aims to introduce the students to gain a solid understanding of risk management principles, processes, frameworks and techniques that can be applied specifically to cyber security as well as risk in general. Also emphasize on how to identify, assess and articulate risk as well as options available for treating risk and which may be most appropriate for respective situation. This course also provides examples of tools and techniques as well as useful tips that can help you to successfully implement and maintain a risk management framework within your organization. Managing risk is therefore an element of sustaining a secure environment. Risk Management is a detailed process of identifying factors that could damage or disclose data, evaluating those factors in light of data value and countermeasure cost, and implementing cost-effective solutions for mitigating or reducing risk. The overall process of risk management is used to develop and implement information security strategies. The goal of these strategies is to reduce risk and to support the mission of the organization. This course further explores the measures used to prevent cybercrime as well.

Learning Outcomes:

The learning outcome of this course includes but not limited to-

1. Develop an understanding of what cyber risk is and how it can be managed.
2. How to create a cyber-risk management framework within your organization.
3. How to identify, assess and articulate risk as well as identifying options for treatment and determining which is the most appropriate.
4. How to perform detailed analysis of risk and develop risk treatment plans.
5. How to apply risk management concepts in practice including developing a risk register, governance models, risk bowties and reporting.

Detailed Course Contents:

Risk Terminology and Information Security Concepts

Confidentiality, Integrity, and Availability, Identity and Authentication, Authorization, and Accountability,

Nonrepudiation, Least Privilege, Defense in Depth,

Legal and Regulatory Issues

Compliance with Laws and Regulations, Major Legal Systems, Criminal, Civil, and Administrative Law and Liability,

Due Care and Due Diligence, Legal Aspects of Investigations,

Computer Crime, Intellectual Property, Privacy

International Cooperation

Import/Export Restrictions, Security and Third Parties, Service Provider Contractual Security, Procurement, Vendor Governance, Acquisitions, Divestitures,

Security Policy and Related Documents, Personnel Security.

Recommended Textbooks:

Antonucci, D. (2017). *The cyber risk handbook: creating and measuring effective cybersecurity capabilities*. John Wiley & Sons.

Conrad, E., Misenar, S., & Feldman, J. (2016). *Eleventh Hour CISSP®: Study Guide*. Syngress.

McCarthy, C., & Harnett, K. (2014). *National institute of standards and technology (nist) cybersecurity risk management framework applied to modern vehicles* (No. DOT HS 812 073). United States. National Highway Traffic Safety Administration.

Course Code	Course Title	Credit
826515	**Cyber Terrorism and Threat Management**	4

Course Objectives

This course will explain the most probable forms of cyber-terrorism and information security threats and attacks, the definitions of these threats and attacks, how the attacks take place, and the most effective ways to combat these threats from a Cyber Security Practitioner's point of view. Both theoretical orientation and technical know-how in relation to Cyber Terrorism and Threat Management will be explored.

Learning Outcomes

Upon successful completion, the course takers will be able to better understand the underlying reasons and various forms of Cyber Terrorism as well as ins and outs of Threat Management. As such, the course takers will be better equipped with the knowledge to identify specific types of attacks and take preventive or remedial measures whichever is necessary. Overall, this course will enhance the course taker's knowledge to effectively reduce the IT infrastructure vulnerability and cyber-attack threats to individuals as well as organizations.

Detailed Contents

Information, Computer Security and Cyber-Terrorism

The Link between Terrorism and Information Technology, Possible Terrorist Activities against IT, Definition of Cyber-Terrorism and Information Warfare

The nature and scale of terrorist use of the Internet:

Internet use of terrorist, VPN technology, measuring the capacity of cyber-terrorist; Characteristics of Open-Source Tools including Free, Less-regulated, Modifiable; Concepts and uses of Concealment Software including Encryption, Data Hiding/Steganography, Anonymizers (TOR); Malware concepts including Automated Scripts and Documented Author Tools.

Online propaganda and radicalization:

Understanding propaganda, Counternarratives of religious and political views and process of online radicalization

Motivation and goals behind cyber terrorism:

Analyze motivation of nation-state foreign interest; Classify motivations based on (i) Social, political, belief, (ii) Economic, warfare, and trade.

Security vs Privacy vs Anonymity

Privacy, Anonymity, and Pseudonymity; Security, Vulnerabilities, Threats, and Adversaries; Security vs Privacy vs Anonymity

Cyber tactics, techniques used by cyber terrorists

Security Bugs and Vulnerabilities; Hackers, crackers and cybercriminals; Malware, viruses, rootkits and RATs; Spyware, Adware, Scareware, Potentially unwanted program (PUPs) &

Browser hijacking; Phishing, Vishing, and SMShing; Spamming & Doxing; Social engineering - Scams, tricks, and fraud; Darknets, Dark Markets and Exploit kits; Trust & Backdoors

Cyber weapon related to terrorism

Denial of Service Threat; Web Defacements and Semantic Attacks; DNS Attacks; Routing Vulnerabilities; Identity Stealing Attacks

Physical Security to counter cyber terrorism

Issues in Cyber-Physical Security; Advertising the Location; Securing the Perimeter; Protection of Equipment from External Disturbances; Theft of Equipment; Protection Against Eavesdropping; New Form of Attack; Retrieval of Information from Magnetic Media

Vulnerabilities of cyber-related critical infrastructure

The Importance of Patching; Windows 7 - Auto Update; Windows 8 & 8.1 - Auto Update; Windows 10 - Auto Update; Linux - Debian - Patching; Mac - Patching; Firefox - Browser and extension updates; Chrome - Browser and extension updates; Auto updates - The Impact to privacy and anonymity

Methods of Communication by Cyber Terror entities

Describe how Websites are utilized including but not limited to: Rumours and Misinformation, Recruitment, and Remote attack deployment, Explain cyber-related covert communication including but not limited to: Codes, Encryption, Steganography, One-time Use Channels.

Methods of Financial Gain by Cyber Terror entities

Direct/Indirect Contribution methods including but not limited to: Charity sites, Protection Money/Ransom, Physical Harm, Reputation, Data; Methods of theft and fraud including but not limited to: ID Theft/Credit Fraud, Banking Interception/Impersonation, Money Laundering through barter or virtual currency.

Challenges of cyber terrorism with regard to legal framework and policy responses

Legal framework addressing cyber terrorism; Policy of dealing with social media giant; Coordination among stakeholders countering cyber terrorism

Prevention/deterrence/mitigation efforts of cyberterror activities

Efforts related to SCADA/Control Systems, Business /Governmental Computer Systems, Personal and computers/phones; Other technical and non-technical countermeasures

Recommended Readings

Janczewski, Lech & Colarik, Andrew (2005). *Managerial guide for handling cyber-terrorism and information warfare.*

Yunos, Z, & Sulaman, S (2017). *Understanding Cyber Terrorism from Motivational Perspectives.*

Course Code	Course Title	Credits
826517	Cyber Economic Crime and Management	4

Course Objectives: Cyberspace is considered as an important fact of our daily life. It has become a fundamental feature of the world we live in. Crime is no exception in this domain too. With the very existence of humans, crime exists and it has been a concern for society since time immemorial, but antisocial elements are using the advanced technologies to commit various crimes in cyberspace. Crime is committed to various motives. Greed and illicit monetary gain is a major motive in modern societies. The course will emphasize the understanding of economic/financial crime and financial cybercrime. Specific attention has been made in the context of Bangladesh as well as other developed countries.

Learning Outcomes:

After completion of the course, the students will be able to:

1. Understand, analyze and evaluate the financial cybercrime and its management from different perspectives.
2. Identify the different types of financial cybercrime and threats in the context of Bangladesh.
3. Identify the contemporary issues relating to financial cybercrime with management policies and strategies

Detailed Course Contents:

Introduction

Changing Landscape of Crime in Cyberspace

Cyber Economic Crime: Criminological Studies and Frameworks

Understanding Phenomenon

Exploring the Phenomenon of Cyber Economic Crime

Cyber Economic Crime Typology

Emerging Trends and Patterns of Cyber Economic Crimes

Response to Combating the CEC

Legal Framework for Cyber Economic Crimes: A Review

The Response of Criminal Justice System: Bangladesh and World Perspectives

Holistic Approach to combatting CEC

Cyber Security Mechanism, Preventive Mechanism, Awareness Mechanism, and Cyber Deterrence Mechanism

Required Text(s) and Recommended Readings:

Akdemir, N., Sungur, B., & Başaranel, B. U. (2020). Examining the Challenges of Policing Economic Cybercrime in the UK. *Güvenlik Bilimleri Dergisi*, (International Security Congress Special Issue), 113-134.

Quan, W. (2019). Cyber Economic Crimes: Challenges and Countermeasures of the Chinese Police. *China Legal Sci.*, *7*, 67.

Rajput, B. (2020). *Cyber Economic Crime in India: An Integrated Model for Prevention and Investigation*. Springer Nature

Course Code	Course Title	Credits
826518	**Capstone Project/Internship**	4

Course Objectives:

The capstone project/internship is usually the final assignment which plays a vital role in providing students with hands-on experiences on all the aspects cyber security which have been taught throughout the course tenure. Through its practical applications and ability to help hone professional knowledge and skills, this project is usually undertaken by the students to apply what they have learned throughout the PGD course in Cyber Security. Upon completion of this project, the students will have field-experience for an entire semester from various institutions and organizations both from public, private, and non-government organizations.

Marks Distribution and other features:

- 70% marks on written report and its presentation, 30% marks on viva.
- Students will be placed under the supervision of an officer from Police Staff College for the sound completion of their respective projects. ***They will also be linked with a designated officer within the organization where they will take the capstone project.*** Each student shall be put under close Rader of their respective supervisors.
- The duration of the project will be 4 months in total (One semester). For at least 2 months, a student will work (as an intern) in a relevant organization. He will prepare a written report on his experience (combining his academic learning and professional exposure) for 2 months and make a presentation it in front of faculty members.

Learning Outcomes:

- Demonstrate comprehensive understanding of the discipline of Cyber Operations by:
    - Identifying different threat actors and their motivations in cyberspace
    - Analyzing how information system security design, policies, practices, networks, and people defend against threats in cyberspace
    - Evaluating the effects of laws and gaps in legal guidance and precedent with respect to activities in cyberspace
- Exercise critical thinking strategies including reasoning, problem solving, analysis, and evaluation by:
    - Analyzing and synthesizing theoretical and practical constructs within the field of cyber operations
    - Critically reviewing and evaluating the application of selected theories to practical, real-world situations

Potential Places where a student might take the capstone project: IT Companies, Government Organizations, NGOs, any relevant institutions.