গণপ্রজাতন্ত্রী বাংলাদেশ সরকার
বাংলাদেশ পুলিশ
পুলিশ হেডকোয়ার্টার্স
৬, ফিনিক্স রোড, ফুলবাড়ীয়া
ঢাকা-১০০০
www.police.gov.bd

স্মারক নং-৪৪.০১.০০০০.০১১.৩৯.০০৪.২৩- ১৭৫৮ তারিখ : ০১ /৬/২০২৩ খ্রি.

বিষয় : পুলিশ স্টাফ কলেজ বাংলাদেশ-এ পোস্ট গ্র্যাজুয়েট ডিপ্লোমা ইন সাইবার সিকিউরিটি কোর্সের প্রথম ব্যাচে ভর্তির লক্ষ্যে মনোনয়ন প্রসঙ্গে।

উপর্যুক্ত বিষয়ে পুলিশ স্টাফ কলেজ বাংলাদেশ, ঢাকা এর স্মারক নং-৪৪.০১.০৪০০.০৫১.২৮.০০৩.২৩.১৬৮৩, তারিখ-৩০/৫/২০২৩ খ্রি. এতদসঙ্গে প্রেরণ করত জানানো যাচ্ছে যে, জাতীয় বিশ্ববিদ্যালয়ের অধীনে Post Graduate Diploma in Cyber Security কোর্সে ভর্তির জন্য সহকারী পুলিশ সুপার হতে তদূর্ধ্ব আগ্রহী কর্মকর্তাগণের আবেদন ও বিস্তারিত জীবন বৃত্তান্ত সার্টিফিকেটের সত্যায়িত কপিসহ নামের তালিকা আগামী ০৭/৬/২০২৩ তারিখের মধ্যে নিম্নস্বাক্ষরকারীর নিকট প্রেরণের প্রয়োজনীয় ব্যবস্থা গ্রহণের জন্য নির্দেশক্রমে অনুরোধ করা হলো।

সংযুক্ত : বর্ণনামতে

০১/৬/২০২৩
(মোহাম্মদ আনোয়ার হোসেন, বিপিএম-সেবা, পিপিএম-বার)
বিপি-৭৩০৩০২০৯০২
অ্যাডিশনাল ডিআইজি (পার্সোনেল ম্যানেজমেন্ট-১)
বাংলাদেশ পুলিশ
পুলিশ হেডকোয়ার্টার্স, ঢাকা।
ফোন : ০২-২২৩৩৫৫৩০১, ফ্যাক্স : ০২-৫৫১০১৬১৬
E-mail : addldigestt@police.gov.bd

কার্যার্থে :

১। অ্যাডিশনাল আইজি (প্রশাসন), বাংলাদেশ পুলিশ, পুলিশ হেডকোয়ার্টার্স, ঢাকা
২। পুলিশ কমিশনার, ডিএমপি, ঢাকা
৩। মহাপরিচালক, র‌্যাব, র‌্যাব ফোর্সেস হেডকোয়ার্টার্স, কুর্মিটোলা, ঢাকা
৪। অ্যাডিশনাল আইজি, এসবি, বাংলাদেশ পুলিশ, ঢাকা
৫। অ্যাডিশনাল আইজি, এন্টি টেররিজম ইউনিট, বাংলাদেশ পুলিশ, ঢাকা
৬। রেক্টর, পুলিশ স্টাফ কলেজ, মিরপুর, ঢাকা
৭। অ্যাডিশনাল আইজি, রেলওয়ে পুলিশ, বাংলাদেশ পুলিশ, ঢাকা
৮। অ্যাডিশনাল আইজি, নৌ পুলিশ, বাংলাদেশ পুলিশ, ঢাকা
৯। অ্যাডিশনাল আইজি, পিবিআই, বাংলাদেশ পুলিশ, ঢাকা
১০। অ্যাডিশনাল আইজি, আর্মড পুলিশ ব্যাটালিয়ন, বাংলাদেশ পুলিশ, ঢাকা
১১। অ্যাডিশনাল আইজি, হাইওয়ে পুলিশ, বাংলাদেশ পুলিশ, ঢাকা
১২। অ্যাডিশনাল আইজি, পুলিশ টেলিকম সংস্থা, বাংলাদেশ পুলিশ, ঢাকা
১৩। অ্যাডিশনাল আইজি, শিল্পাঞ্চল পুলিশ, বাংলাদেশ পুলিশ, ঢাকা
১৪। প্রিন্সিপ্যাল, বাংলাদেশ পুলিশ একাডেমী, সারদা, রাজশাহী
১৫। অ্যাডিশনাল আইজি, সিআইডি, বাংলাদেশ পুলিশ, ঢাকা
১৬। অ্যাডিশনাল আইজি, ট্যুরিস্ট পুলিশ, বাংলাদেশ পুলিশ, ঢাকা
১৭। ডিআইজি, ঢাকা রেঞ্জ/চট্টগ্রাম রেঞ্জ/রাজশাহী রেঞ্জ/রংপুর রেঞ্জ/খুলনা রেঞ্জ/বরিশাল রেঞ্জ/সিলেট রেঞ্জ/ময়মনসিংহ রেঞ্জ/এপিবিএন/বিশেষায়িত সিকিউরিটি ও প্রটেকশন ব্যাটালিয়ন /পিবিআই /ট্যুরিস্ট পুলিশ/নৌ পুলিশ, বাংলাদেশ পুলিশ
১৮। পুলিশ কমিশনার, সিএমপি/কেএমপি/আরএমপি/বিএমপি, বরিশাল/এসএমপি, সিলেট/গাজীপুর মেট্রোপলিটন পুলিশ/ রংপুর মেট্রোপলিটন পুলিশ
১৯। পরিচালক, কেন্দ্রীয় পুলিশ হাসপাতাল, রাজারবাগ, ঢাকা
২০। কমান্ড্যান্ট, পিটিসি, টাংগাইল/নোয়াখালী/রংপুর/খুলনা/টিডিএস, মিলব্যারাক, ঢাকা
২১। কমান্ড্যান্ট, এপিবিএন ও বিশেষায়িত ট্রেনিং সেন্টার, খাগড়াছড়ি
২২। কমান্ড্যান্ট, আরআরএফ, ঢাকা/চট্টগ্রাম/রাজশাহী/ খুলনা/বরিশাল/সিলেট/ রংপুর/পিএসটিএস, বেতবুনিয়া, রাঙ্গামাটি
২৩। অ্যাডিশনাল ডিআইজি (হেডকোয়ার্টার্স), বাংলাদেশ পুলিশ, পুলিশ হেডকোয়ার্টার্স, ঢাকা
২৪। অধিনায়ক, এপিবিএন/এসপিবিএন, ...(সকল)
২৫। এআইজি .... (সকল), বাংলাদেশ পুলিশ, পুলিশ হেডকোয়ার্টার্স,ঢাকা
২৬। এআইজি (আইসিটি), বাংলাদেশ পুলিশ, পুলিশ হেডকোয়ার্টার্স, ঢাকা। ওয়েব সাইটে প্রকাশের প্রয়োজনীয় ব্যবস্থা গ্রহণের জন্য নির্দেশক্রমে অনুরোধ করা হলো
২৭। পুলিশ সুপার, ... (সকল)
২৮। কমান্ড্যান্ট (পুলিশ সুপার), ইনসার্ভিস ট্রেনিং সেন্টার, ... (সকল)
২৯। বিজ্ঞপ্তি/অফিস নথি

অতিরিক্ত ডিআইজি (পার্সোনেল ম্যানেজঃ ১)
২১২৮ ৩১/০৫/২৩
ডায়েরী নং.... তারিখ....
পুলিশ হেডকোয়ার্টার্স, ঢাকা।

১৬

গণপ্রজাতন্ত্রী বাংলাদেশ সরকার
বাংলাদেশ পুলিশ
পুলিশ স্টাফ কলেজ বাংলাদেশ
মিরপুর-১৪, ঢাকা।

স্মারক নং- ৪৪.০১.০৪০০.০৫১.২৮.০০৩.২৩.১৬৮৩ তারিখ: ৩০/০৫/২০২৩ খ্রিঃ।

প্রতি

অতিরিক্ত ডিআইজি (পারসোনেল ম্যানেজমেন্ট-১)
বাংলাদেশ পুলিশ
পুলিশ হেডকোয়ার্টার্স, ঢাকা।

বিষয়: পুলিশ স্টাফ কলেজ বাংলাদেশ-এ পোস্ট গ্র্যাজুয়েট ডিপ্লোমা ইন সাইবার সিকিউরিটি কোর্সের প্রথম ব্যাচে ভর্তির লক্ষ্যে ৮০ জন পুলিশ কর্মকর্তার নাম মনোনয়ন প্রসঙ্গে।

পুলিশ স্টাফ কলেজ বাংলাদেশ-এ জাতীয় বিশ্ববিদ্যালয়ের অধীনে Post Graduate Diploma in Cyber Security কোর্স চালুর অনুমোদন পাওয়া গেছে। গত ১০/০৫/২০২৩ তারিখ মাননীয় মন্ত্রী, স্বরাষ্ট্র মন্ত্রণালয়, গণপ্রজাতন্ত্রী বাংলাদেশ সরকার, এঁর সভাপতিত্বে অনুষ্ঠিত পুলিশ স্টাফ কলেজ বাংলাদেশ এর ১৯ তম বোর্ড সভায় PGD in Cyber Security কোর্স শুরু করার নির্দেশনা প্রদান করা হয়েছে। বর্তমান বিশ্বে প্রযুক্তিগত উন্নয়নের সাথে সাথে সাইবার অপরাধের সংখ্যা উল্লেখযোগ্য হারে বাড়ছে। সাইবার অপরাধ প্রতিহত এবং তদন্তের জন্য পুলিশ কর্মকর্তার সক্ষমতা বৃদ্ধি একান্ত প্রয়োজন। জাতীয় বিশ্ববিদ্যালয়ের অনুমোদন অনুযায়ী কোর্সটির ১ম ব্যাচে ৫০ জন ছাত্র/ছাত্রী ভর্তি করা যাবে। উক্ত কোর্সটির প্রথম ব্যাচে ইন্সপেক্টর হতে তদূর্ধ ৫০ জন পুলিশ কর্মকর্তা মনোনয়ন করা যেতে পারে। এ লক্ষ্যে ইন্সপেক্টর হতে তদুর্ধ ৮০ জন পুলিশ কর্মকর্তার নাম প্রথম ব্যাচে প্রস্তাব করা প্রয়োজন। নিম্নবর্ণিত যোগ্যতার ভিত্তিতে প্রার্থী মনোনয়ন করা হবে:

শিক্ষাগত যোগ্যতা:	ন্যূনতম ব্যাচেলর ডিগ্রী (৩ বছর মেয়াদী)
কম্পিউটার বিষয়ে দক্ষতা:	এমএস ওয়ার্ড, এক্সএল, পাওয়ার পয়েন্ট ও ইন্টারনেট ব্রাউজিং
চাকরির অভিজ্ঞতা:	ন্যূনতম ০৩ (তিন) বছর

প্রস্তাবিত ৮০ জনের মধ্য হতে ৫০ জনকে পুলিশ স্টাফ কলেজ বাংলাদেশ এর নির্ধারিত প্রক্রিয়ায় Computer Efficiency, Viva এবং সাইবার মামলা তদন্তে আগ্রহ যাচাইয়ের মাধ্যমে ভর্তির জন্য চূড়ান্ত করা হবে। মনোনীত প্রশিক্ষণার্থীদের PGD in Cyber Security এর অনুকূলে নির্ধারিত কোর্স ফি পুলিশ স্টাফ কলেজ বাংলাদেশ এর অনুকূলে প্রদান করতে হবে।

উল্লেখ্য যে, কোর্সটি মেয়াদ হবে ১০ মাস, যা দুটি টার্মে বিভক্ত। উক্ত কোর্সে সপ্তাহান্তে দুইদিন বৈকালিক ক্লাস অনুষ্ঠিত হবে। কোর্সটির ৬০% ক্লাস হবে ব্যবহারিক। আগামী ১৫ জুলাই, ২০২৩ হতে কোর্সটি শুরু হবে। এমতাবস্থায়, আগামী ২৫ জুন, ২০২৩ এর মধ্যে ৮০ জন পুলিশ কর্মকর্তা মনোনয়ন পূর্বক তালিকা পুলিশ স্টাফ কলেজ বাংলাদেশ-এ প্রেরণের জন্য নির্দেশক্রমে অনুরোধ করা হ'ল।

পার্সোনেল ম্যানেজমেন্ট-১ শাখা
ডায়েরী নং- তারিখ- ৩১/০৫/২৩

সংযুক্তি:-

১. সিলেবাস
২. জাতীয় বিশ্ববিদ্যালয় অধিভুক্তি পত্রের কপি।
৩. ১৯তম বোর্ড সভার সিদ্ধান্তের কপি (২ পাতা)।

৩০/৫/২৩
(সুফিয়ান আহমেদ)
বিপি-৭৮০৫১৬৮৭৭৮
পরিচালক (একাডেমিক)
পুলিশ স্টাফ কলেজ বাংলাদেশ
মিরপুর-১৪, ঢাকা।

C:\Users\Assignment Officer\Desktop\Cyber security-23\Cyber Security- Letter 2023.docx

PGD in Cyber Security

National University

Course Code	Course Title	Credit
	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
	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

29

Course Code	Course Title	Credits
	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
	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
	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
	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
	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
	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
	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
	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.

পরিচালনা বোর্ড এর ১৯তম সভা

তারিখ : ১০ মে, ২০২৩ খ্রি:

স্থান : সম্মেলন কক্ষ

পুলিশ স্টাফ কলেজ বাংলাদেশ

পুলিশ স্টাফ কলেজ বাংলাদেশ
মিরপুর-১৪, ঢাকা-১২০৬।

বিগত ১৮তম সভার সিদ্ধান্তসমূহ	সিদ্ধান্তের বাস্তবায়ন অগ্রগতি
সিদ্ধান্ত-১: পুলিশ স্টাফ কলেজ বাংলাদেশ এর সাথে বাংলাদেশ লোক প্রশাসন প্রশিক্ষণ কেন্দ্র (বিপিএটিসি) ও Defence Services Command and Staff College (DSCSC) এর সাথে সমঝোতা স্মারক চূড়ান্ত করার বিষয়ে প্রয়োজনীয় কার্যক্রম গ্রহণ করতে হবে।	বোর্ড সচিব বলেন, সমঝোতা স্মারক স্বাক্ষরের বিষয়ে পুলিশ স্টাফ কলেজ বাংলাদেশ এর সাথে BPATC ও Defence Services Command and Staff College (DSCSC) এর পত্রালাপ হয়েছে। কার্যক্রম প্রক্রিয়াধীন রয়েছে। এ প্রসঙ্গে DSCSC, কমান্ড্যান্ট বলেন, পুলিশ স্টাফ কলেজ এর সাথে শুধু এমওইউ স্বাক্ষরের মধ্যে সীমাবদ্ধ না রেখে অন্যান্য ক্ষেত্রেও সহযোগিতা করতে চাই। বিদেশী প্রতিষ্ঠানের সাথে DSCSC'র কাজ করার অভিজ্ঞতা রয়েছে। তিনি আরও বলেন, বাংলাদেশে ইউনিফর্মধারী হিসেবে পুলিশের সাথে Leadership, Management এবং অন্যান্য সমসাময়িক ইস্যু ভিত্তিক প্রশিক্ষণ বিনিময় করে সহযোগিতা বৃদ্ধি করা যেতে পারে। অপরদিকে রেক্টর, BPATC বলেন, কর্মকর্তা পর্যায়ে এ বিষয়ে একাধিকবার যোগাযোগ হয়েছে। ফোকাল পয়েন্ট কর্মকর্তা মনোনীত করা হয়েছে। উভয় প্রতিষ্ঠানের কর্মকর্তাদের সাথে আলোচনার ভিত্তিতে খসড়া এমওইউ প্রস্তত করা হয়েছে। আশা করছি, স্বল্প সময়ের মধ্যেই চুক্তি স্বাক্ষরের আনুষ্ঠানিকতা সম্পন্ন করা যাবে। সিদ্ধান্ত-১: ১.১ BPATC সাথে MoU স্বাক্ষরের আনুষ্ঠানিকতা সম্পন্ন করার কার্যক্রম গ্রহণ করতে হবে। ১.২ DSCSC এর সাথে MoU স্বাক্ষরের কার্যক্রম এগিয়ে নেয়াসহ Leadership, Management এবং অন্যান্য সমসাময়িক ইস্যু ভিত্তিক প্রশিক্ষণ বিনিময় করার বিষয়ে আলোচনা অব্যাহত রাখতে হবে।
সিদ্ধান্ত-২: ২.১ সংশ্লিষ্ট স্টেকহোল্ডারদের সমন্বয়ে Post Graduate Diploma in Security Management Course অধিকতর পর্যালোচনা ও পরামর্শ গ্রহণের এক বা একাধিক ওয়ার্কশপের আয়োজন করার কার্যক্রম গ্রহণ করতে হবে। ২.২ Post Graduate Diploma in Cyber Security Course শুরুর জন্য প্রয়োজনীয় সফটওয়্যারসহ আধুনিক কম্পিউটার ল্যাব স্থাপন করার বিষয়ে ভারত ও তুরস্কসহ উন্নয়ন সহযোগী দেশসমুহের ঢাকাস্থ দূতাবাসের মাধ্যমে যোগাযোগ করে ল্যাব স্থাপনের বিষয়ে বোর্ড সচিব যথাযথ কর্তৃপক্ষের মাধ্যমে প্রয়োজনীয় ব্যবস্থা গ্রহণ করবেন।	বোর্ড সচিব বলেন, Post Graduate Diploma in Security Management Course এর কারিকুলাম প্রস্তত করাসহ অন্যান্য কার্যক্রম সম্পন্ন করা হয়েছে। অধিভুক্তির কাজ সম্পন্ন করার বিষয়ে ভিসি, জাতীয় বিশ্ববিদ্যালয় মহোদয় সার্বিক সহযোগিতা করার আশ্বাস প্রদান করেছেন। বোর্ড সচিব বলেন, Post Graduate Diploma in Cyber Security Course আরম্ভ করার জন্য ল্যাব স্থাপনের শর্তে জাতীয় বিশ্ববিদ্যালয়ের অধিভুক্তি পাওয়া গেছে। ল্যাব স্থাপনের জন্য ৭ কোটি ৯০ লক্ষ টাকার প্রাক্কলন করা হয়েছে। অর্থ বরাদ্দের বিষয়ে আইজিপি মহোদয়ের সদয় সম্মতি পাওয়া গেছে। আগামী অর্থ বছরে (২০২৩-২০২৪) ল্যাব স্থাপনের কার্যক্রম সম্পন্ন হবে। ভাইস চেয়ারম্যান বলেন, ল্যাবের কারনে কোর্স বন্ধ রাখা সমীচিন হবেনা। সিআইডি ও আইসিটি মন্ত্রণালয়ের ল্যাব এ কাজে ব্যবহার করা যেতে পারে। তিনি প্রস্তাব করেন বর্ণিত কোর্স ছাড়াও ছয় মাস মেয়াদী কিছু প্রয়োজনীয় অনলাইন কোর্স চালু করা যেতে পারে। যথা-i-Bass, Management,

	Logistic Management, Supplychain Management etc. তিনি আরও বলেন বর্ণিত কোর্সগুলো তদন্ত কর্মকর্তাদের জন্য খুবই প্রয়োজন। তাদের এ বিষয়ে তাত্ত্বিক জ্ঞান থাকলেও ব্যবহারিক জ্ঞানের অভাব রয়েছে। সিদ্ধান্ত-২: ২.১ Security Management Course এবং Cyber Security Course এর কার্যক্রম আগামী অর্থ বছরের মধ্যে চালুর কার্যক্রম গ্রহণ করতে হবে। ব্যবহারিক প্রশিক্ষণের জন্য সিআইডি ল্যাব, আইসিটি মন্ত্রণালয়ের ল্যাব এবং অন্যান্য যে প্রতিষ্ঠানে এ ধরণের ল্যাব আছে সেগুলো ব্যবহারের সম্ভাব্যতা যাচাই করতে হবে। ২.২ কলেজের ল্যাব রক্ষণাবেক্ষণের জন্য প্রয়োজনীয় টেকনিক্যাল জনবল নিয়োগের কার্যক্রম গ্রহণ করতে হবে। ২.৩ তদন্ত কর্মকর্তাদের সাইবার ল্যাব ব্যবহার বিধিতে দক্ষ করার জন্য প্রশিক্ষণ আয়োজন করতে হবে।
সিদ্ধান্ত-৩: বাধ্যতামূলক প্রশিক্ষণ কোর্সের জন্য বৈদেশিক প্রশিক্ষণ ১ সপ্তাহের পরিবর্তে ২ সপ্তাহ করার প্রস্তাব জননিরাপত্তা বিভাগ, স্বরাষ্ট্র মন্ত্রণালয়ে পুনরায় প্রেরণ করতে হবে।	বোর্ড সচিব বলেন, বাধ্যতামূলক প্রশিক্ষণ কোর্সের বিষয়টি ইতোপূর্বে বোর্ড সভায় আলোচিত হয়েছে। প্রশিক্ষণার্থী কর্মকর্তাগণ এক সপ্তাহের জন্য বিদেশে গেলে ফলাফল আশানুরুপ পাওয়া যায় না। ১৮তম বোর্ড সভায় পূর্বের সিদ্ধান্ত অনুযায়ী বৈদেশিক প্রশিক্ষণের মেয়াদ ১ সপ্তাহের পরিবর্তে ২ সপ্তাহ করার প্রস্তাব বিবেচনার জন্য জননিরাপত্তা বিভাগ, স্বরাষ্ট্র মন্ত্রণালয়ে পত্রালাপ করা হয়েছে। ১০টি বাধ্যতামূলক কোর্সের প্রশিক্ষণার্থীগণ কোর্সের ২ সপ্তাহের বিদেশে প্রশিক্ষণ অংশ মুলতবী রয়েছে। এ প্রসঙ্গে মাননীয় বোর্ড চেয়ারম্যান বলেন, বাধ্যতামূলক প্রশিক্ষণ অব্যাহত রাখতে হবে। অতিরিক্ত পুলিশ সুপার থেকে পুলিশ সুপার হিসেবে পদোন্নতির ক্ষেত্রে General Administration and Financial Management Certificat Course অতিরিক্ত পুলিশ সুপারদের জন্য বাধ্যতামূলক থাকবে। এক্ষেত্রে পাঠক্রমে ক্রিমিনোলজি, সাইবার ক্রাইম ও ফিন্যান্সিয়াল ক্রাইম বিষয়গুলো অন্তর্ভুক্ত করতে হবে। বোর্ড সচিব বলেন-বিদেশে প্রেরণের প্রস্তুতি পুলিশ স্টাফ কলেজে রয়েছে। জননিরাপত্তা বিভাগ, স্বরাষ্ট্র মন্ত্রণালয় ১ সপ্তাহের পরিবর্তে ২ সপ্তাহের বিদেশী প্রশিক্ষণ সদয় বিবেচনা করলে পরবর্তী কার্যক্রম গ্রহণ করা হবে। এ প্রসঙ্গে ইন্সপেক্টর জেনারেল বলেন, বাধ্যতামূলক কোর্সের দেশের অংশ সম্পন্ন করায় প্রশিক্ষণে বিদেশে অংশগ্রহণের জন্য প্রশিক্ষণার্থীগণ অপেক্ষমান রয়েছে। বাধ্যতামূলক ৩টি কোর্সের (এএসপি, অতি: এসপি, এসপি) বিদেশে যাওয়ার অংশ বিভিন্ন কারণে স্থগিত রয়েছে। এ কোর্সগুলো নিয়মিত করা হলে কর্মকর্তাগণ প্রশিক্ষণকে প্রণোদনা হিসেবে গ্রহণ করবে এবং বৈশ্বিক পুলিশের উত্তম চর্চা আয়ত্ব করে দেশের সেবাগ্রহীতাগণকে ভালভাবে সেবা প্রদান করতে পারবে। সেবা প্রদানের ক্ষেত্রে ইতিবাচক ভূমিকা পালন করবে। বোর্ড সদস্যগণ এ বিষয়ে সহমত পোষণ করেন।