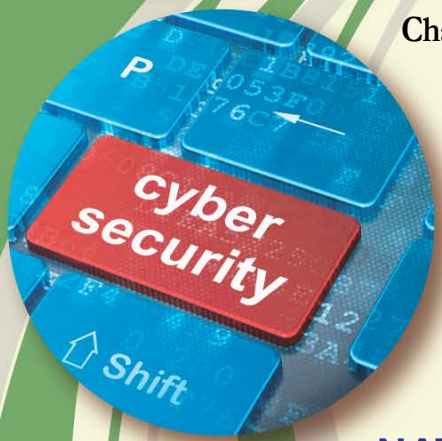



# Seminar Paper

## Challenges and Opportunities of Cyber Security Bangladesh Perspective

**09 May 2016**

**NATIONAL DEFENCE COLLEGE**

**BANGLADESH**


NATIONAL DEFENCE COLLEGE

Seminar on
Challenges and Opportunities of

# Cyber Security

Bangladesh Perspective

Organized by

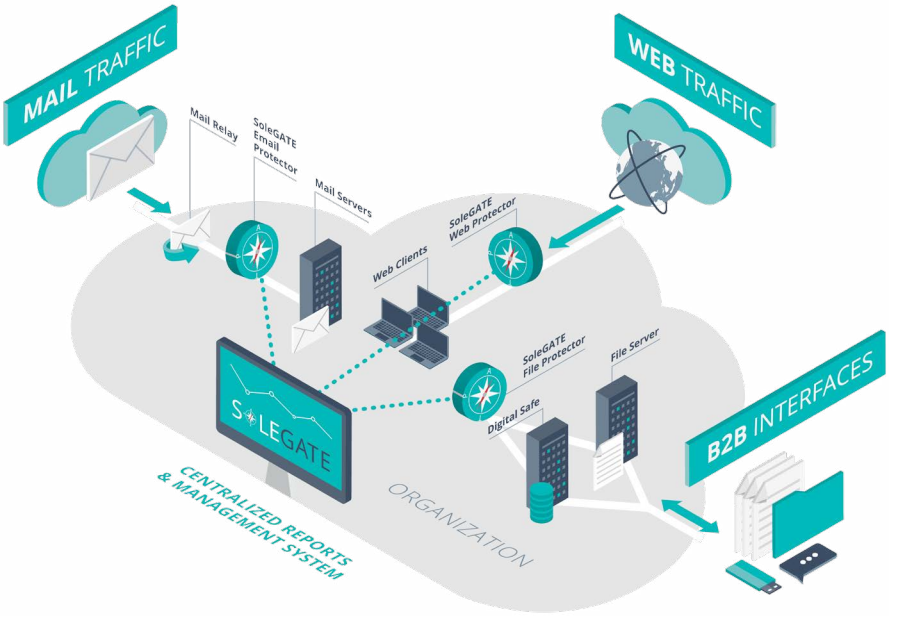
**National Defence College**

and

**Embassy of France, Bangladesh**

# CONTENTS





# Editorial Board

## Chief Patron
**Lieutenant General Chowdhury Hasan Sarwardy**
BB, SBP, ndc, psc

## Editor in Chief
**Air Vice Marshal Mahmud Hussain**
BBP, OSP, ndc, psc, GD(P)

## Editor
**Colonel S M Rakibullah**
afwc, psc, lsc

## Associate Editor
**Lieutenant Colonel A N M Foyezur Rahman**
psc, Engrs

## Assistant Editor
**Lecturer Farhana Binte Aziz**
Research Fellow

## Assistant Editor
**Md Nazrul Islam**
Civilian Staff Officer

# Foreword

Over the course of the past decade, the domain of computer security has grown in complexity and seriousness as information technologies have saturated society, and simultaneously the threats have multiplied in number and sophistication. National Defence College as the apex academic institution is entrusted with enhancing intellectual breadth of senior military officers and civil servants. Threats to cyber world constitute an important element of the course.

Total six IT Experts delivered their lectures in this seminar. Their lectures followed by intense interactive presentations have enhanced the awareness of cyber security. Additionally, the seminar has revitalized the bondages between NDC and the Embassy of France in Bangladesh.

It is a matter of great delight that the seminar paper on "Challenges and Opportunities of Cyber Security: Bangladesh Perspective" is going to see the light. I hope that this paper will be an asset for broadening the interest of general public in cyber security. Moreover, I expect that this noble effort will be a contribution for the greater benefit of our country.

I would like to thank the faculty members and college staff for their tireless effort in organizing the seminar and making it a success. Finally I appreciate the sincere efforts of the Research and Academic Wing and acknowledge the solemn endeavour of the editorial board to bring out the seminar paper.

**Lt Gen Chowdhury Hasan Sarwardy, BB, SBP, ndc, psc**
Commandant
Nationat Defence College

# Editorial

The commonly accepted definition of Cyber Security is the protection of any computer system, software programme and data against unauthorized use, disclosure, transfer, modification or destruction, whether accidental or international. Cyber attacks can come from internal networks, the internet, or other private or public systems. Businesses cannot afford to be dismissive of this problem because those who do not respect, address and counter this threat will surely become victims.

Keeping this in mind, to discuss the stakes and roles of the persons involved in this domain, a day-long seminar was arranged under the title of "Challenges and Opportunities of Cyber Security: Bangladesh Perspective". The seminar was organized jointly by National Defence College and Embassy of France.

The seminar would be devoid of success had it not been for the lively presenters and the enthusiastic attendance. In addition, the relentless efforts and accomplishments of the Faculty and Staff of NDC must also be brought to light.

By the Grace of Almighty Allah, we have the successful publication of the seminar paper. This seminar paper contains the papers of the speakers. These are their individual work. These deserve special appreciation by way of contributing to an understanding of important threat to national security in a particular field.

**AVM Mahmud Hussain, BBP, OSP, ndc, psc, GD(P)**
Senior Directing Staff (Air)
National Defence College

## Programme of Events of the Seminar

| Time | | Event | Respossivility |
|---|---|---|---|
| 0930 | 0945 | Opening Address | Air Vice Marshal Mahmud Hussain |
| 0945 | 1010 | Challenges of Cyber Security and Global Trends | Lt Col Michel Simond |
| 1010 | 1030 | National Cyber Strategy: Bangladesh Perspective | Dr Ahmed Khurshid |
| 1030 | 1050 | The Threat of Cyber Radicalization- Understanding the Challenges and a Way Forward | Mr Shafqat Munir |
| 1050 | 1115 | Tea Break | - |
| 1115 | 1135 | Cyber Security of Financial Sector and Protective Measures | Mr Mohammad Ali |
| 1135 | 1155 | Why Cyber Security Education is Important | Abdus Shamim Khan |
| 1155 | 1215 | Comprehensive Approach to Cyber Security | Brig Gen Emdad-Ul-Bari |
| 1215 | 1225 | Break | - |
| 1225 | 1340 | Open Discussion/Q&A Session | - |
| 1340 | 1350 | Closing Speech | Mr. Zunaid Ahmed Palak, Member of Parliament |
| 1350 | 1400 | Speech by the Special Guest | HE Sophie Aubert |
| 1400 | 1415 | Commandant's Speech/ Exchange of Gifts | Lt Gen Chowdhury Hasan Sarwardy |
| 1415 | 1430 | Photo | |
| 1430 | 1500 | Lunch | |


Seminar
on
Challenges and Opportunities of Cyber Security :
Bangladesh Perspective
Organised by: National Defence College
&
Embassy of France

## Opening Address of Moderator

**Air Vice Marshal Mahmud Hussain**

OSP, ndc, psc, GD(P)

Respected Special Guest, Her Excellency Sophie Aubert, French Ambassador to Bangladesh,

Commandant, National Defence College,

Panelists, Lt Col Michael Simond, Dr Ahmed Khurshid, Mr Shafqat Munir, Mr Muhammad Ali, Abdus Shamim Khan and Brigadier General Emdad-Ul-Bari, Ambassadors and Diplomats,

Senior Officials from the Civil and Military Services,

Resource Persons and Academic Advisors of National Defence College,

Members of the Media,

Guests from the Public and Private Universities and Research Institutes,

Faculty, Course Members and Staff Officers of National Defence College,

Ladies and Gentlemen,

Assalamu-alaikum and a very Good Morning.

National Defence College feels extremely honoured and privileged to host a joint seminar with the French Embassy on "Challenges and Opportunities of Cyber Security: Bangladesh Perspective".

The term "Security" in general, is easily understood, such as explanations about military security or non-military security have defined categorical boundaries. But the term "Cyber-security" poses numerous problems and thus, under-writes serious challenge to the rational of security paradigm. However, the reasons for such problem are not without justification.

First, in global perspective, no issue has advanced so rapidly in threat perception as cyber-attacks on nation-states, yet no issue is so poorly understood by their leaders. Leaders have a good reputation of comprehending military security that always keep them engaged; when briefed about threat to well-being of

their citizens, leaders are worried beyond imagination to change circumstances to improve economic health of states; but if told about attacks emanating from cyber-world, leaders usually whisk that kind of report off by the brush of their hand as the prodigious but politically insignificant work of some hacker. The notion of cyber-attacks as being nothing more than 'nuisance' has not yet completely erased from the minds of those who are pivotal in decision-making process of national security.

Second, as a branch of knowledge, cyber-security is still struggling to find a proper place for its discourse. The field is becoming crucial to our privacy and some advanced countries, as intimate as the future of world politics. Yet it is a domain only well known by the "Computer Wizards": it seems that only the young and the computer savvy are well engaged with it. As a result, non technical normative aspects that under-gird the essence of global security and mutual trust are left undebated and often ignored at the cost of national security. So, knowledge matters and it is vital that we explore the mysticism of cyber world if we want to secure it from harming us.

Third, the threat analogy of cyberspace can be compared to risks involved with free-market economy transgressed by oligopolistic cyber experts who do care neither for nationality nor ethno-centricity but profiteering through their trade. The rise of cyber-security perception is also associated with the recruitment of best talents in computer science without their identity being compromised by firms or organizations involved with anti-state, anti-global and anti-social acts. Trans-border financial institutions are also not without being influenced by the evil designs of market externalities. So, market can be a strong force that can work against the national interest to secure the state's cyber realm. The booming cyber-space may be more willing to buy and sell the vulnerabilities in a direction that is harmful to wider cyber-security. Here again, just like in any other marketplace that starts to move from white-to black-market activity, be it drugs or arms, the government has to stay aware and be prepared to defeat it when any actions become socially destructive.

Fourth, the constitution of cyber-security is multi-dimensional. Therefore, a comprehensive approach is a must. Let us take a hypothetical example in which multi-directional high profile cyber-attacks are initiated simultaneously against

a particular state. One against its State Bank, the other against its export infra-structures and the third against its military command center. These three cases reflect wildly different threats. The attack against the Bank is about financial fraud, the attack against export infra-structures is industrial theft and the attack against the military command center is a form of warfare. So, we see that it is not merely a realm where governments have all answers and all liabilities. So, cyber-security depends on all of us. It is with this purpose in mind to grow awareness about cyber-security in all of us that today's seminar is planned and organized.

Today's seminar, we hope will be extremely useful for all of us by way of strengthening our knowledge about the impact of cyber-security on state sovereignty in terms of both as blessing and dereliction. We have arranged for the seminar discourse to proceed in the style of "Deductive Method". We start from a general idea of the subject that encompasses global perspective, and then gradually build up hypothesis on reaching particular case study of Bangladesh. The focus is on two variables, namely challenges and opportunities.

To hold discussions on the subject, we have six speakers that include Lt Col Michael Simond, Dr Ahmed Khurshid, Mr Shafqat Munir, Mr Mohammad Ali, Mr Abdus Shamim Khan and Brigadier General Emdad-Ul Bari.

Now let me explain briefly how we would like to conduct the session.

After the Welcome Address, Lt Col Micheal Simond will open the session with his talk on "Challenges of Cyer-Security and Global Trends."

Then we will listen to the next two speakers. Each one of them will have twenty minutes to speak.

At 1055 hours, we will have a tea break for about 0:25 minutes.

From 1115 to 1215 hours, we will listen to three more speakers with twenty minutes each to speak.

From 1215 to 1225 hours, we will take again a short break.

At 1225 hours, we will assemble here once again for the interactive session. In this session, the learned audience will have the opportunity for asking questions, giving comments, opinions and observations. Time allotted for this part is 1:15 minutes.

There will be final remarks on today's session by our Special Guest Her Excellency Sophie Aubert, the Commandant and the Chief Guest, the State Minister for Information and Communication Technology.

The Seminar will end with a Vote of Thanks and exchange of Crests.

After the Seminar, we will have lunch, and the programme ends at 1515 hours.

As the Sponsor Senior Directing Staff of this event, I am sure you will enjoy the moment, and reward us with your gracious and valuable presence.

Thank you, ladies and gentlemen.

## Profiles of Keynote Speakers

**Lt Col Michael Simond**

Lieutenant Colonel Michael Simond is a Signal Officer of French Air Force. He was graduated from the French Air Force Academy and National School of Telecommunications of Paris. He began his career in 1998 in Mont de Marsan base and was integrated into the air control unit. He had participated in different missions in former Yugoslavia and was in charge of confidential networks deployed for French forces. He was appointed in the French Air Force Academy as a telecommunications instructor and was in charge of educational programs of officer cadets in CIS domains. He had also worked in the Strategic Affairs Directorate of the Ministry of Defense where he was in charge of the cyber defense. Presently he is in charge of cyber issues in the French Joint HQ in Abu Dhabi.

**Dr. Ahmed Khurshid**

Dr. Ahmed Khurshid is a Co-Founder and Principal Engineer of Veriflow Systems, Champaign, Illinois, USA. He did his PhD in Computer Science from University of Illinois at Urbana-Champaign (UIUC), and Bachelor and Master of Science in CSE from BUET. He worked as Co-Op. student worker, Cisco Systems, Inc. San Jose, CA, and USA. He also served as faculty of Department of CSE, BUET. He obtained 1st runner-up award in Illinois Innovation Prize 2015, administered by the Technology Entrepreneur Center in the College of Engineering at UIUC. He also obtained the International Fulbright Science and Technology PhD Award for the year 2008-2009 sponsored by the Bureau of Educational and Cultural Affairs, US Department of State.

**Mr. Shafqat Munir**

Mr. Shafqat Munir is currently an Associate Research Fellow at the Bangladesh Institute of Peace and Security Studies (BIPSS). His research at the institute is focused on issues of Countering Violent Extremism, Cyber Security, Maritime Security in the Indian Ocean and other regional security issues. He also coordinates the track 1.5 and track-2 dialogues undertaken by BIPSS. As part of his research he focuses extensively on analyzing the threat of cyber radicalization. He was graduated from the Australian National University with a Bachelor of Arts in International Relations and Security Studies. He subsequently obtained a Master of Science in Strategic Studies and a post graduate diploma in Counter Terrorism Studies from Nanyang Technological University in Singapore.

**Mr. Mohammad Ali**

Mr. Mohammad Ali is working in the ICT industry for 20 years and presently he is serving as Deputy Managing Director and CTO of Pubali Bank Limited. Under his leadership, Pubali Bank Ltd, has developed core banking solution, different value added services. He has started his career as lecturer of Ahsanulla University. Later he joined Dhaka Ahsania Mission as one of the Directors to look after ICT based development projects. He had worked as IT management specialist for the e-Government Projects. He was graduated from BUET in the department of CSE and also obtained Master Degree in the same subject. He also has Masters in Development Studies from Dhaka University, Executive MBA in marketing from IBA and MBA in finance from AUST.

**Mr. Abdus Shamim Khan**

Abdus Shamim Khan, presently, is serving as independent IT consultant. He was principal consultant in Technuf Inc., Maryland, USA and Senior Vice president of Tista Science and Technology Corp., Maryland, USA. He has more than 40 years teaching experience in different institutions both in home and abroad e.g. Florida International University, USA and Notre Dame College, Dhaka, Bangladesh. He did his graduation in Physics from St. Xavier's College, Calcutta, India and completed MS from University of Calcutta, India. He also completed MS in Operations Research (Applied Mathematics) from Case Western Reserve University, Ohio, USA.

**Brig Gen Emdad-Ul Bari,** ndc, psc, te

Brigadier General Md Emdad-Ul Bari is a Telecommunication Engineer, trained in Radio Relay Communication and Electronic Warfare. He is the Director General of Systems and Services Division of Bangladesh Telecommunication Regulatory Commission, and coordinates the Bangladesh Computer Security Incidence Response Team (BD-CSIRT). Earlier, he commanded 86 Independent Signal Brigade, and served as the Chief of Land Warfare Branch in the Doctrine Division of Army Training and Doctrine Command, as well as a Directing Staff in Defence Services Command and Staff College. He is also an NDC alumni.


# Keynote Speech-1: Challenges of Cyber Security and Global Trends

**Lt Col Michael Simond**

The speaker begins by highlighting the cyber space as new combat field since 2006 with its own characteristics. Recent history shows that many crisis and conflict had their own cyber aspects. Since then, he enumerates cyber defense has been top priority for French Government and Ministry of Defense.

The speaker describes cyberspace as part of state sovereignty and emphasized on the national coordination to protect it. Cyber attack is equally detrimental for state sovereignty like land or air attack as it cripples the national economy, power, communication network, he added. He also explained how the cyber space became a operational domain for the military.

The speaker also very lucidly defined some common terminologies and concepts generally used in cyberspace related studies. He also explained that the level of cyber security relies on following three kinds of measures:

- **Cyber Resilience.** The technical measures which insure service continuity, data restoration, etc.
- **Cyber Protection.** It includes technical security measures e.g. antivirus, software update for weaknesses, firewall, encryption, etc.
- **Cyber Defense.** It relies on operational measure to face an attack : IDS (Intrusion Detection Systems), SIEM (Security Information and Events Management), malware analysis, response. Cyber defense also includes an intelligence part to anticipate the threat.

**The speaker identified three levels of threats to cyber security:**

- The first level is linked to cyber activism, most of the times it results to website defacement or unavailability.

- The second level is linked to cyber crime, actually at that stage, the complexity and the gravity of consequences is not highest, even if the financial impact for the companies can be great.
- In the third level is faced by states or great organization with resources and finances, they have the capacity to create their own tools and have strategic motivations.

The speaker also underlined that there was no clear border between threats because a market for hackers exists and people work for people who offer much money. He argued that the coordination at governmental level is mandatory for information exchange and the continuity between defense and security is the paradigm.

The speaker enumerated the measures taken by the Government of France to ensure cooperation amongst different stake holders who are responsible to secure French cyber space:

- National Agency for Information Assurance (ANSSI), a unique governmental agency at the top of the state in charge of cyber defense. But it also has responsibilities in confidence systems development, critical infrastructure security, telecom operator leading. ANSSI is coordinating the action of the main ministries in relation to cyber security.
- Ministry of Defense who is human resource provider in this domain, which is in charge of defense industry security and who has the responsibility of sensitive and confidential systems.
- The Ministry of interior who is in charge of cyber criminality and legal investigation for justice. This ministry has knowledge of hacker groups in French territory.
- The Ministry of Foreign Affairs supports MOD, MOI and ANSSI in the foreign relationship that country is building in this domain.

The speaker in his speech described how French military was ensuring the cyber defence of France. He mentioned that the operations in this domain can be divided into following three main categories i.e. Intelligence, Cyberspace Supremacy and Cyber Operations. Cyber Operations is further classified into

information operations which are linked to counter speech. Cyber Operation is very sensitive and covered by Defense Secrecy.

The speaker has given a very comprehensive picture regarding the operational procedure of the terrorist in cyberspace. The way cyberspace is used by the terrorist as articulated by the speaker is as follows:

- For communication and recruitment so called Islamic State have a communication cell.

- The use of cyberspace by terrorist is for operation planning. Terrorist groups have developed plenty of tactics to obfuscate their information exchanges.

- Terrorist groups are also frightening population by conducting attacks against any kind of website.

Despite the rampant misuse of cyber space by the terrorists the speaker could also identify some opportunities for the use of the defense and the military domain:

- The first opportunity is intelligence gathering.

- Open another way of action which is not limited to military and that is called strategic communication. In relation with other governmental communication agencies and Foreign Affairs ministries, communication analysis is more efficient and can develop counter speech.

- In this domain, the military can conduct information operation to obtain defection of fighters from terrorist groups: the idea is to show the people that their engagement in terrorist group will be fatal for them.

The speech ended highlighting the numerous challenges in commanding Cyber Space. Speaker mentioned there are challenges to mobilize resources, conducting education and training, cooperating with civilian sphere and compliance with legal framework. Monitoring social network is something completely new and there is no education program for that, the speaker expressed his concern. The speaker also identified the dearth of communication analyst to analyze the communication of terrorist group.

## Keynote Speech -2: National Cyber Strategy: Bangladesh Perspective

**Dr. Ahmed Khurshid**

The speaker at the beginning of his speech identified 5 key areas: awareness, education with practical training, implementation, auditing, and research to ensure cyber security of the nation. He also laid down a bottom up approach to move towards a comprehensive national cyber strategy.

The speaker accentuated on the need to be aware of how sensitive their digital resources are at all levels of an organization, concerned parties, and the severity of cyber attacks. Without proper awareness, higher level policy makers of an organization may not allocate sufficient resources to build a strong security system for its IT infrastructure as he enumerated further.

The speaker marked that required level and depth of education on cyber security depends on the role of the person working with the technology infrastructure. For end users, basic computer usage and security education for day-to-day use of computers and other digital resources need to be arranged. The next group is system administrators and network engineers. They should have a strong educational background on computer systems, application security, software engineering, network design, network security, and network maintenance. The cyber criminals are not sitting idle as new technologies are arriving. They are enriching their knowledge base every day by practicing novel attack techniques. In order to be always one step ahead of the criminals, the system administrators and network engineers have to engage themselves in continuous education to safeguard their organizations' digital resources as narrated by the speaker.

The speaker expressed the implementation to begin with good design. The design of the network infrastructure should not only specify operational requirements, but also list a set of policies that need to be satisfied to ensure a secured environment. There should be policies to control access from external

network to the external network, and also among internal network segments. The speaker also mentioned that cutting edge network management and testing tools need to be used to test the network segmentation, network health, firewall settings and other operational requirements.

According to the speaker, an implementation does not always stay healthy if it is not audited regularly. As a network grows and experience changes, things can change that may not fully comply with the initial policy set designed by the network security team. Therefore, once in a while, the entire networking infrastructure, end user machines, maintenance practices, and system usage culture need to be audited by internal or external auditors as stressed by the speaker.

The speaker stressed upon research so the country can develop advanced tools to safeguard against future cyber attacks and to think ahead of the attackers to beat them even before they try to start an attack. He is optimistic that the universities in Bangladesh have a large body of talented students who are capable of doing quality research under supervision of their professors. He strongly believes that researchers of Bangladesh are capable enough to explore and solve hard cyber security challenges that will eventually make Bangladesh a "producer" of cyber security solutions.


## Keynote Speech-3: Threat of Cyber-Radicalization: Understanding the Challenges and Way Forward

**Shafqat Munir**

The stylish and eloquent speaker Mr Shafqat Munir started his speech with the definition of the word radicalization for better understanding of the audience. He defined radicalization as a process that indoctrinates someone to a certain belief or point of view far beyond the accepted mainstream interpretation or understanding of it and will alter their behavioral boundaries considerably"(Julian Charvat). Although not clearly defined, the speaker added that Cyber radicalization could be referred to the use of digital mediums like internet to spread the radical and extremist ideas among the people. He mentioned that fol are the tools and mechanism used for the spread of cyber radicalization:

- Social Media
- Forums and Chat rooms
- Websites and blogs
- Target and mass-mailing
- Cyber Communities

The speaker with sound logic specifically mentioned that youth, being highly tech-savvy and easy to convince, are the most significant target group for cyber-radicalization. Almost all the new recruits of organizations like ISIS, Al Qaeda are from the youth population. Besides the marginalized people, people with grievance, religious and ethnic minorities, upper urban middle class are the most lucrative target group for cyber-radicalization. He vividly mentioned that fol are the outcome of the cyber radicalization:

- **Cyber Radical Cells.** All the major militant organizations like the ISIS, Al Qaeda have formed their own Cyber-Radical cells. They are efficient in dealing with the internet and know where the target audience could be found.

- **Self Radicalized People.** Some of the radicalized people don't join any militant group They pursue their ideology as a 'lone wolf' with their own actions, Norway Attacks in 2011 by Anders Behring Breivik is the bright example.

- **Cyber Financing.** Many of the radicalized people become involved with Cyber-financing to fund the militant activities. Digital currencies like 'Bitcoin' are popular medium for Cyber-financing. These currencies are devoid of the control of any central bank which makes it impossible to monitor such transactions.

- **Technical knowledge.** Some radicalized people become specialized in making bombs and use of several weapons. Many of them have sound knowledge about information technology and potential nuclear technology.

Suicide bomber, radicalized literature, capability of setting strategic communication etc are also the outcome of cyber radicalization. Finally, the speaker has put forward following recommendations to counter the cyber radicalization:

a. There should be a comprehensive understanding of the threat.
b. Effective awareness programs should be initiated.
c. Deficit of governance and development must be addressed.
d. Effective monitoring should be initiated without suppressing the internet accessibility.
e. Proper space must be provided to the people with different ideologies to share their opinions.

The speaker emphasized on more study and research on the issue and concluded his speech with a quotation of Fareed Zakaria "Ultimate counter-terrorism tool is social resilience; if we are not terrorized, they cannot win."

## Keynote Speech -4: Cyber Security of Financial Sector and Protective Measures

**Mohammad Ali**

At the onset of his presentation, the speaker highlighted on the importance of cyber security for financial sector. Citing the example of Pubali Bank limited, he has outlined the protective measures to be undertaken for a financial sector. While formulating comprehensive ICT security policy and procedures, he has categorically mentioned about the different pillars of cyber security. He has logically mentioned various steps to be followed with respect to ICT security management and pointed out some tips. Similarly, he has highlighted on ICT security policy for ICT operation management and practical tips thereof. Thereafter, he has mentioned in details on the ICT security policy regarding physical security of a financial sector .In this regard, he has mentioned different security arrangement/password for physical security of the financial sector along with some tips.

The speaker with his vast knowledge and experience has designed the network security of financial sector which include relevant elements of cyber security and detail guidelines in this regard. He has emphasized on implementing security standards and best practices. Finally, he stressed upon the cyber policy for software development, acquisition and continual service improvement.


# Keynote Speech-5: Why Cyber Security Education is Important

**Abdus Shamim Khan**

The speaker started his speech by highlighting the importance of education on Cyber Security. He emphasized that education must be the first and major activity in developing a proper Cyber Security Architecture. According to him, a good Cyber Security education would not only help prepare a good ongoing Cyber Security architecture but would proactively prepare to thwart an attack before it materializes. Cyber Security would no longer be a mere IT function; it would be a business need of any enterprise environment. Senior executives need security education for the formulation of Cyber Security policies and guidelines that would be pillar for the development for new and future business strategies. Mid-level management, both of IT and non-IT background, would need education for running day-to-day operations and for preparing tactical plans. All employees would need comprehensive training to safeguard assets of the enterprise

The speaker also called attention to symmetry of knowledge between the attacker and the target audience. According to him, symmetry of knowledge between the attacker and the target would help the enterprise to understand the mentality and psychology of the attackers.

The speech was concluded by highlighting the need for in-depth education of the government executives and policy makers to ensure the development of rules and regulations formulation and National Cyber Security policies. The education would also be needed to confirm the international standards for cross-border data flow and for the development of IT forensic facilities, he added further.


## Keynote Speech-6: Cyber Security: A Comprehensive Approach for Bangladesh

**Brigadier General Md Emdad ul Bari, ndc, psc, te**

The speaker began his speech by mentioning that Cyber Security was becoming increasingly relevant to the fast growing Digital Bangladesh. As the large Internet community is constituted by myriads of interconnected small entities, its security is also a collective responsibility. The speaker suggested in his speech some national approach to address cyber security, basing on the present-day ground realities gathered through his working experience. The speaker noted that the Government of Bangladesh has set the cyber security strategic goal as "creating a safe, secure, and resilient critical national information infrastructure for our economy and society". The speaker mentioned that the real challenge of any cyber security strategy was achieving the security goals and objectives while preserving the fundamental properties of Internet, known as 'the Internet Invariants'. He also mentioned that on top of the Internet Invariants are added the challenges of ensuring human rights such as 'freedom of expression' and 'privacy'. While mentioning about the global cyber security agenda he referred to five major items of International Telecommunication Union's (ITU's) Global Cyber Security Agenda (GCA).

The speaker was very elaborate while discussing the existing cyber security framework of Bangladesh. He mentioned about legal instruments like Bangladesh Telecommunication Regulatory Act 2001, The ICT Act 2006, Digital Security Act 2016 (Draft) are at present available in Bangladesh. He also gave the state of present situation on the technical measures, organization standard, capacity building, international cooperation and coordination amongst government machineries in relation to national cyber security.

While suggesting the approach of Bangladesh to ensure cyber security the speaker made a special emphasis on collaborative security which entails following key elements:

- Preserving Opportunities and Building Confidence ('opportunities' to serve people, and 'confidence' so that they use those)
- Collective Responsibility (since Internet means interdependence)
- Integrated Solutions (solutions should be compatible)
- Evolution and Consensus (flexible solutions to cope with new challenges, open consensus-based participation)
- Think Globally, Act Locally (bottom-up execution)

The speaker recommended following measures in order to ensure security of cyberspace of Bangladesh:

- Immediately establish NCC as the apex policy-making body at the highest level comprising policy-makers from ministries, defense and law enforcement agencies, other Government key critical sector agencies.
- To support the NCC, establish advisory group(s) comprising experts from government, industry and academia.
- Carry out risk and vulnerability assessments to identify and understand the CNII.
- Review the Cyber Security Strategy accordingly and plan protection (prevention, response, and recovery) of the CNII.
- Establish a separate National Cyber Security Agency (NCA) directly under the NCC, which would coordinate policy implementation on behalf of the government as well as provide selected Cyber Security services. The major functions of NCC would include National Policy Implementation, National Technical Coordination Center, Cyber Threat Research and Risk Assessment, Cyber Security Quality Management Services, Cyber Security Professional Development, Cyber Emergency Services Strategic Engagement.
- Organize capacity building of government organs, and enhance public awareness programs.

- Enhance global and regional cooperation by developing collaboration with global and regional cyber security agencies such as Asia Pacific CERT (APCERT), OIC-CERT, IMPACT, Forum of Incident Response and Security Teams (FIRST), etc. Enhancing effective engagement with the apex global organizations such as Internet Governance Forum (IGF), Internet Corporation for Assigned Names and Numbers (ICANN), etc. Exploring Legal Assistance Treaties with selected countries, social media, and IT giants.

## Final Remarks by Moderator

**Ladies and Gentlemen.**

In the most recent times, we have witnessed that there is a renewed and vigorous attention to the debates on cyber-security in Bangladesh. We have also observed the same kind of passionate zeal and keenness in today's seminar here at National Defence College. This is hardly surprising given that cyber-security takes on the form of unconventional but powerful threat to national security as the debates on this issue have demonstrated us today. There is no doubt that our discussion has been able to raise concern about this threat in the manner that we very much like to respond to the challenges of military or economic security issues. As a threat, I find a coherent analogy between cyber-war and air power.

In the initial days of air power, it was the British Prime Minister Stanley Baldwin who was greatly impressed by the appearance of bombers as a weapon. Whenhe said, "Bombers will get through", he made an apocalyptic statement. Countries which had long-range bombers reserved the advantage over the enemy who did not have them. Bombers not only could fly very long distances across continents but they also carried a large store of destruction. The possession of bomber aircraft gave tremendous advantage to countries who invested money in their research and manufacture. The United States and Great Britain nursed the euphoria of having the pleasure of using the bomber as a weapon above the level at which military commanders take decision. Bombers were considered the "Strategic Weapons" whose use and deployment was the choice of the political leadership. Bombers were meant to be offensive and in that, their use was pronouncedly different from any other weapon.

Through our discourse today, one point is clear that cyber-weapons are also offensive and in that, they are strategic weapons. Like bombers, their reach is global. Moreover, they have one more advantage over bombers that they are not the only weapons of rich countries. Had it been so, the advanced countries would have enjoyed maximum security from cyber weapons. While a country needs cash money to build its military capabilities, the development of cyber capabilities depend on the proper aptitudes of brain. Developing world is no short in terms of human resource supply but their challenge is production of capable minds to deal with the problem. But the challenge of intelligent digital brain also offers tremendous opportunities to these countries. It is far less taxing

to develop an offensive cybercapability than it is to defend against the various forms of cyber intrusion andattack. Were the case otherwise, cyber-economic warfare, cyber- crime, and cyber-espionage would not be the problems they are.

A major difference between air and cyber-attacks is that unlike air attacks, cyber warfare activities are highly vulnerable to physical effects. Once a majorair attack designed to produce catastrophic destruction is under way, especially in the case of heavy bombs delivered from the air, there is still in the way of defensive measures that can prevent the attack from succeeding. Missile defenses may be able to reduce the bomber's numbers at the point of releasing bombs, andpassive defenses may place limits on the damage wrought by the attack, andbombers may not be able to achieve desired degree of assurance of destruction. This may not be the case with cyber-attacks, at least not in the case of thosethat must be executed via the Internet. If the target severs its access to theInternet, or if power is cut-off even partially, the ability to deliver a cyber counter-strike,let alone conduct a cyber campaign, may be seriously compromised. Yet,in such cases, the cyber attacker will achieve his objectives in that the defender's severed access to the Internet may prohibit his ability to performkey functions (e.g., financial transactions). Moreover, once the attacker's "exploits" are triggered, he may not be willing torisk that his victim will be able to identify the attack's source. This may make it difficult and perhaps impossible to discernpromptly when a rival has transitioned from acts of cyber-espionage, cyber-crime, and cyber-economic warfare to an attack on its adversary's critical infrastructure. Thus, we can say that so far building cyber-war capabilities are concerned, all states, whether developed or developing, first or third world, stand on equal footing of opportunities offered by the potentials of cyber-technology. Hence, the outcome of today's seminar can be stated as " Bangladesh needs to address the issue of cyber-security in a comprehensive manner on a nation-wide scale in military, financial, economic, academic and strategic plane".

I, on behalf of all the Course Members of the National Defence Course 2016, would like to thank the audience, particularly the faculty and the students of public and private universities,for their intellectual support to this seminar in the form of valuable questions, incisive observations, thoughtful comments, reflective opinions, and above all, ardent participation during the interactive session. We would also like to deeply appreciate the responses given by the panelists to our inquiries which are valuable and rewarding.

Our sincerest gratitude goes to Lt Col Michel Simond, Dr Ahmed Khurshid, Mr Shafqat Munir, Mr Mohammad Ali, Mr Abdus Shamim Khan and Brigadier General Emdad-Ul-Bari for being the panelists and enlightening us with the knowledge of the issue and clarifying points that seemed unclear till the beginning of this seminar. There are so many other resource persons present amongst the audience, including former Services Chiefs, Commandants and renowned academicians that the College feels richly rewarded by your gracious presence.

My special thanks to the Faculty of the National Defence College, and the College Secretary, Brigadier General Ibrahim, and Director, Research and Academic, Colonel Rakib and their teams who worked from behind the scene but made sure that like obedient Colleagues, they provided all the logistic and moral support to this event without complaint.

I thank all the Course Members of National Defence Course 2016, who haveenriched our knowledge and taught us that the greatest threat to cyber-security is ignorance. Theirs is the greatest contribution to learning in the current year 2016.

Our Special Guest Her Excellency Sophie Aubert has always been an encouragement. Had she not been there, our task of bringing international importance to cyber-security would have been difficult. We express our appreciation to herfor making our learning of the subject so rewarding.

The Chief Guest, the respected State Minister, has made himself available despite his extremely busy schedule speaks of his sincere commitment to the issue of cyber-security. We thank him profusely.

Finally, I thank deeply from the bottom of my heart, my Commandant, Lt Gen Chowdhury Hasan Sarwardy for always inspiring and encouraging me in going ahead with my programme including this Seminar. He was always by my side to make sure this Seminar was conducted in a befitting tone.

We are very proud of you. May I request now all of you to rise and on behalf of the Commandant, join me in giving this august gathering a standing ovation.

Thank you, ladies and gentlemen.

## Address of Special Guest

**HE Sophie Aubert**

**Ambassador of France**

H.E. the Ambassador of France started her speech by stating cyber security as a big issue in the interconnected world. She mentioned that the new world has no border and nor it would be possible to pose borders. It took some time for the world to understand this evolution, develop awareness and to generate responses to face this new threat, she added. She emphasized on the need to deal with a new generation of transnational criminals. She identified absence of awareness, poor responses and insufficient knowledge on cyber security as the root causes of failure to deal with the issue.

She described how security breaches or vulnerabilities are exploited by cyber criminals. She cited some examples from the contemporary world scenario and from her personal experience.

She narrated the aspect of cyber security for nation states and emphasized on the importance of cyber defence. She cited some examples of cyber attack on Estonia, Iran and Middle Eastern countries where cyber criminals could destabilize the security systems of those nations.

She divulged that the Government of France put high priority to the issue of cyber security and addressed it at international level. But she admitted that level of international cooperation in this regard was still too low. She said France was in favour of cyberspace governance and implementation of some regulatory rules, but disapproved restrictions in the use of cyberspace.

H.E. the Ambassador of France finished her speech with a hope for a better future but was also pragmatic to declare that it would take time for the global community to reach to a common approach to ensure cyber security. She also identified low level of confidence and huge differences of perceptions amongst the actors regarding cyber defence as impediments to build a secured cyber space.


Seminar
on
Challenges and Opportunities of Cyber Security :
Bangladesh Perspective
Organised by: National Defence College
&
Embassy of France
09 May 2016


AUDITORIUM


Seminar
on

## Address of Commandant, NDC

Hon'ble State Minister for ICT Division, Ministry of Post, Telecommunication and Information Technology

Mr Zunaid Ahmed Palak, MP,

Her Excellency Sophie Aubert, Ambassador of France,

Distinguished Academics, Professionals, Senior Military Officers, Government Officials, Representatives of Civil Society, Resource Personnel, Eminent Guests, Faculty,

Excellences, Members of Media, Ladies and Gentlemen

Assalamu Alikum and very Good Morning.

I, on behalf of all members of National Defence College would like to thank Hon'ble State Minister for kindly accepting the invitation and gracing the occasion as Chief Guest in spite of his busy schedule. I would also like to thank our distinguished speakers, for sparing time out of their very busy schedules to join us in this seminar, for their knowledge based lectures and for sharing their experience with us. My sincere thanks to all the delegates and participants for your kind attention, active participation and contributions. I would like to extend my heartiest thanks and gratitude to Her Excellency Sophie Aubert, the ambassador of France for her whole-hearted cooperation and presenting one of their cyber-specialists to be a key speaker in this seminar. I appreciate the support of the media in covering and disseminating discussions and lessons of today's session to the greater section of the society. All presentations and documents contributed to this seminar will be available on our website.

Excellences, Ladies and Gentlemen

World Economic Forum Reports on Global Risks in 2011,

"Cyber security issues now top the list of risks to watch, ahead of weapons of mass destruction and resource security."

Understanding the future challenges and realizing the consequences of recent cybercrimes is of utmost importance. We do echo the same concern and today's seminar theme is ramification of that perspective. Our speakers are handpicked and they represent their respective fields as top level experts.

Cyber Security is a delicate and challenging issue. The threat of cyber-attacks has been a subject of concern for both military and non military organizations who form the different layers of national security. Increasingly it has been considered as a critical challenge and regarded as 'acts of war' by many countries. In today's seminar, we tried to focus on three basic aspects of cyber security: promoting greater understanding, raising awareness and preparing for all probable scenario.

The information and communication technology (ICT) and Cyber world are almost synonymous. It is making us so dependent that one cannot think of remaining out of the net connectivity even for few minutes. People of Bangladesh are no exception to it. Bangladesh has experienced a technological leap forward in the recent years. Our honourable Prime Minister Sheikh Hasina received "ICT Sustainable Development Award" on 29 September 2015 from International Telecommunication Union for outstanding Advancement in ICT sector. Therefore, it can be well imagined, how much and up to what extent Bangladesh has advanced in this sector. As use of ICT is widespread, its security features were also given due importance. The users of these technologies are being vulnerable like virus attack, fraud, stealing and/or falsifying information etc. Principal forms of cybercrime range from Hacking, Money Laundering, Virus/Worm Attacks, Trojan Attacks, E-mail Bombing, , Intellectual Property Rights, Credit Card Fraud and Cyber Defamation. Bangladesh is quite vulnerable because Bangladesh government has already introduced many online services. Almost all the government agencies including private offices and companies have their own web sites. But their systems are not well protected from the cyber criminals. Use of e-commerce and online banking is on the rise. As a consequence of this online presence and transactions, several cyber security breaches and cybercrimes have also been noticed in recent past. The types of cyber threat that may affect Bangladesh can be broadly categorized into three. These are: Cyber threat against individual, Cyber threat against organization and Cyber threat against Government and State. Out of all these three categories

cyber-attack against state will bring catastrophic effect. However, Bangladesh has not yet been experienced with such attack. Cybercrimes may also have a devastating effect on the traditional cultural and religious values. It also can have a great deal of effect on the law and order situation in the country.

Bangladesh Government has undertaken the programmes to digitalize whole society under the motto of "Digital Bangladesh". Inevitably, cybercrime is in direct proportion with the level of digitalization. The regulatory bodies and the law enforcement agencies are trying hard to curb the cybercrime to an extent. Meanwhile, we have identified that ignorance remains the major problem to arrest cyber-attack. We are yet to have modern cyber law, cyber expertise, hi-tech equipment's, required infrastructure and appropriate motivation to deal with such cyber-attack. Moreover, the pace of cyber security expertise growth is not at per with digitization programmes itself.

From the talk of the speakers, it is revealed that an effective cyber law can play a vital role in ensuring that cyber criminals are prosecuted for their crimes. Mitigating and eradicating cyber threats cannot be done by just using technologies and services. It has to be coupled with a robust and up to date legal framework to cater for the dynamic nature of ICT environments and anti-cybercrime tactics.

Along with awareness and education, training is identified as the most crucial element of handling the cybercrimes which is also identified by the speakers. We need to educate and train our executives, managers, engineers, developers, end-users and customers through briefing, seminar, training, documents, campaign and exercise. Experts opined for systematic integration of these issues into our national educational curriculums in order to educate the entire population. For long term goal, cyber security education is planned to be included in the higher educational institutions also.

Being the member of the Armed Force, I like to highlight some aspects of Cyber Security in our Armed Forces. Everyday cyber-crimes are increasing which can also damage our military and civilian organizations alike as they are increasingly becoming plugged in with network systems. Cyber-attacks could even develop into nightmare scenarios if the networks during any operations are interrupted or are incapacitated. In Bangladesh, cyber threat

awareness level among officers and men are encouraging but long way to reach minimum desired level. The organization level preparedness among the three services are also mentionable. Some important steps like establishing a data centre, separate secured network, separating confidential data from the global network, establishing Army Information and Technological Support Organization (AITSO), establishing a cyber-warfare organization, etc have already been implemented and upgraded on regular basis. However, we are yet to strengthen issues like capacity building, organization and infrastructure development, integrated joint approach, creation of awareness to combat cyber threat. However, the future will certainly face increase in scams and fraud. The complexity of the threat will not be directly related to the complexity of the technology. They will try to locate and exploit the vulnerabilities in wireless networks, web applications, and other technologies for massive data theft.

Dealing of cybercrime in isolation is not a good option to solve the problem. Bangladesh Government's ongoing programmes like induction of expertise, required equipment, and well-coordinated efforts of all concerned with proper education and awareness programmes are likely to deter Cyber-crime to a greater extent. Bangladesh is also incorporating modern technology and knowledge to respond to any cyber related incidents. Different stakeholders and the government agencies are working in collaboration to get the maximum result to safe-guard against cyber threat.

At the end, I would like to thank HE Sophie Aubert the ambassador of France for her keen interest, active participation and wholehearted support for this seminar. Appreciations are also extended to the distinguished speakers. Finally I would like to thank AVM Mahmud for moderating this seminar in a professional manner. This seminar has been an outstanding example of knowledge sharing - our minds have been assailed by a torrent of ideas, information, statistics, interpretations and visions. Indeed, there were plenty of issues discussed to reflect upon and, if this in any way enhances our individual and collective contributions to meeting the future challenges, then the seminar can truly be adjudged a success. I request you all to join me to thank all the speakers of this seminar.

Last but not the least, I would like to thank all of you for your kind participation as well as your kind attention. Your presence has been invaluable and, without any doubt, has helped make the event a great success. I sincerely wish you all to take the knowledge and information shared and learned from these seminars to your own organizations in order to ensure and provide a more secure and overall safer information society for all. Our work does not end here. We all need to continue working together as we face these many challenges. We must use the synergy of our efforts to ensure that people feel safe whenever they work within the cyberspace.

Thank you very much.


Seminar
on
Challenges and Opportunities of Cyber Security :
Bangladesh Perspective
Organised by: National Defence College
&
Embassy of France
09 May 2016


Security :


ন্যাশনাল ডিফেন্স কলেজ
ভিত্তি প্রস্তর স্থাপন করেন
গণপ্রজাতন্ত্রী বাংলাদেশ সরকারের
মাননীয় প্রধানমন্ত্রী
শেখ হাসিনা
CAPS

## Closing Address of Chief Guest

Bismillahir Rahmanir Rahim

Commandant, National Defence College,

Distinguished Participants,

Ladies and Gentlemen,

Assalamu- Alaikum and Good Afternoon.

Let me first express my heartfelt thanks and gratitude to the Commandant, National Defence College for inviting me as the Chief Guest for today's seminar on **"Challenges and Opportunities of Cyber Security: Bangladesh Perspective"**. This is the much talked subject in the context of today's world and I am extremely delighted to see that National Defence College, a premiere national institution of Bangladesh has taken an endeavour to organize a seminar of such magnitude. Once again thanks to Commandant, National Defence College for taking this time worthy initiative. I would like to thank HE Sophie Aubert the Ambassador of France in Bangladesh for her keen interest and whole hearted support for the seminar. I would also like to congratulate all the keynote speakers for their comprehensive and lucid presentation that made the subject interesting to the audience and vibrant question and answer session is the testament of that.

Distinguished Participants

Cyber threat, apparently, may seem to be a threat only affecting computer and networks. Nevertheless, modern life has been so much entangled with computer and network that cyber threat might have great impact on individual, organization, society and, government. It is, therefore, important to adequately understand the term 'Challenges of Cyber Security' and its various forms. This would help us ascertain its impact as well as prospect and opportunities for Bangladesh.

Distinguished Participants

Bangladesh has experienced a technological leapfrog in the recent years. Today numerous government, public and private organizations are using information and communication technology (ICT) for running their business. Though use of ICT is widespread in Bangladesh, its security features were not given due importance. For this reason, users of these technologies are being vulnerable to distresses like virus attack, fraud, stealing and falsifying information. Lack of skilled work force, administrative and structural weakness of various agencies and lack awareness of the most of the ICT users are the prime reason behind these mishaps. Cyber challenges may affect individuals, organizations, and government and society. Again, national security may encompass economic security, monetary security, energy security, environmental security, military security, political security and security of natural resources. Lack of a national level co-ordinating authority, awareness between general mass, skilled work force and technology are few of the challenges Bangladesh is now facing in combating cyber challenges

Distinguished Participants

We had already experienced challenges in the financial sector, among these challenges the use of social media to spread hatred and cyber terrorism for which we should be greatly concerned. The Ramu and the Hefajot incident have already shown us the grave consequence cyber threat may bring against government and society.

Lack of a national level coordinating authority is one of prime challenges that Bangladesh is now facing in combating cyber threat. Numbers of organizations are working without a mechanism to co-ordinate their efforts. Due to our huge population, outreach of any awareness among general mass against cyber threat is going to be another prominent challenge for Bangladesh. Perhaps, lack of skilled manpower and technology is the foremost challenge Bangladesh is now facing in combating cyber threat. In addition, taking a trans-border initiative to combat cyber threat is an added important challenge for Bangladesh to confront cyber threat comprehensively.

The gradual dependence and extensive use of computer and information technology by the financial institutions like bank, insurance company, and other non-government organizations increase the fear of commission of cyber crime here. Computer has been used as a tool of crime like making forged certificates and documents for a number of years in Bangladesh though the incident of targeting computer or computer system is very unusual. The use of information and communication technology has been playing a vital role in the 21st century due to globalization and the government is encouraged to adapting with the coming future. The present government concepts of Digital Bangladesh is an Idea that includes the IT use for management, administration and governance to ensure transparency, accountability and answerability at all levels of society and state. But cyber crime is very important issue within the private and public sector in Bangladesh. Therefore, the biggest challenge is that cybercrime in Bangladesh – A growing threat in digital marketplace.

Distinguished Participants

I think it would be appropriate now to express my deepest appreciation to the Commandant, College faculty, the staff and all other support personnel of the College. Without their sincere, active and whole-hearted commitment and support the seminar could not have been such a success. They have indeed, done a splendid job.

Finally I sincerely hope and pray for your well-being, peace and prosperity in life and a very bright professional career.

Long live Bangladesh.

Thank you all.

# NDC Participants (Faculty and Staff)

| Ser | Rank and Name | Appointment |
|---|---|---|
| 1 | Lieutenant General Chowdhury Hasan Sarwardy, BB, SBP, ndc, psc, | Commandant |
| 2 | Air Vice Marshal M Sanaul Huq, GUP, ndc, psc, GD(P) | Senior Directing Staff (Air) |
| 3 | Rear Admiral Muhammad Anwarul Islam, NGP, ndc, afwc, psc, BN | Senior Directing Staff (Navy) |
| 4 | Major General Hamidur Rahman Chowdhury, rcds, psc | Senior Directing Staff (Army) |
| 5 | Additional Secretary Nurjahan Begum, ndc | Senior Directing Staff (Civil) |
| 6 | Brigadier General Abu Taher Muhammad Ibrahim, ndc | College Secretary |
| 7 | Colonel A K M Saiful Islam, psc | Colonel Administration |
| 8 | Colonel S M Rakibullah, afwc, psc, lsc | Director (Research & Academic) |
| 9 | Lieutenant Colonel Khandoker Anisur Rahman, psc, G+, Arty | Senior Research Fellow |
| 10 | Lieutenant Colonel Md Nishatul Islam Khan, afwc, psc, Inf | General Staff Officer-1(Training) |
| 11 | Lieutenant Colonel A N M Foyezur Rahman, psc, Engrs | Senior Research Fellow |
| 12 | Lieutenant Colonel Md Anwar Hossain Bhuiyan, psc, Arty | General Staff Officer-1 (Administration) |
| 13 | Major Sk Golam Mohiuddin, Inf | General Staff Officer - 2 |
| 14 | Major Md Saiful Islam, psc, ASC | Mechanical Transport Officer |
| 15 | Major Md Masud Amin, Inf | General Staff Officer-2 (Administration) |

| | | |
|---|---|---|
| 16 | Major Mohammad Tanvir Hasan Chowdhury, AEC | General Staff Officer-2 (Staff Duty) |
| 17 | Major Md Monowarul Karim, GL, Inf | General Staff Officer-2 (Accounts) |
| 18 | Major A S M Khairul Hasan, psc, Arty | General Staff Officer-2(Planning & Coordination) |
| 19 | Major Ferdous Ahmed, psc, Arty | General Staff Officer-2 (Coordination) |
| 20 | Major A B M Zahidul Karim, AC | Quarter Master |
| 21 | Squadron Leader Nizam Uddin Ahmed, GD (P), BAF | General Staff Officer-2(Protocol) |
| 22 | Lieutenant Commander Maharun Naher, (S), BN | General Staff Officer-2 (Training Support) |
| 23 | Major Mohammad Shamsil Arefin, Sigs | General Staff Officer-2(Network Administration) |
| 24 | Lecturer (English) Farhana Binte Aziz | Research Fellow (BCS Education) |
| 25 | Md Nazrul Islam | Civilian Staff Officer-3(Library) |

# NDC Participants (National Defence Course Members 2016)

| Ser | Rank and Name |
|---|---|
| **Allied** | |
| 1 | Lieutenant Colonel Mohammad Ismaon bin Haji Zainie (Brunei) |
| 2 | Brigadier Mustafa Mohammad Marzouq Shalaby (Egypt) |
| 3 | Brigadier PS Shekhawat (India) |
| 4 | Commodore Vinay Kalia (India) |
| 5 | Staff Colonel Ali Bin Faiz Al-Asmari (KSA) |
| 6 | Staff Colonel Jamaan Bin Mohsen Saad Al-Zahrani (KSA) |
| 7 | Staff Colonel Aqab Bin Awadh Al-Mutairi (KSA) |
| 8 | Brigadier General Ahmad Tajuddin Bin Abdul Ghani (Malaysia) |
| 9 | Colonel Soe Nyunt (Myanmar) |
| 10 | Colonel NM Jega (Nigeria) |
| 11 | Colonel ASO Onilenla (Nigeria) |
| 12 | Colonel AA Eyitayo (Nigeria) |
| 13 | Colonel BY Baffa (Nigeria) |
| 14 | Captain FN Damtong (Nigeria) |
| 15 | Captain RD Oderemi (Nigeria) |
| 16 | Captain C Onyemaobi (Nigeria) |
| 17 | Group Captain E Elon (Nigeria) |
| 18 | Group Captain HA Adebowale (Nigeria) |
| 19 | Group Captain AG Ochai (Nigeria) |
| 20 | Colonel Sanjay Thapa (Nepal) |
| 21 | Group Captain Saud Mohamed Abdulrahman Al Balushi (Oman) |
| 22 | Brigadier Shah Zaman (Pakistan) |
| 23 | Brigadier H R N Fernando, RSP (Sri Lanka) |
| 24 | Brigadier W A N M Weerasinghe, RSP, USP (Sri Lanka) |
| 25 | Commodore SMDK Samaraweera (Sri Lanka) |
| 26 | Colonel Juma Hidaya Mwinula (Tanzania) |

| Ser | Rank and Name |
|---|---|
| **Bangladesh Army** | |
| 27 | Brigadier General Ashfaque Iqbal, afwc, psc |
| 28 | Brigadier General Md Abdul Wohab |
| 29 | Brigadier General Md Abdul Halim |
| 30 | Brigadier General Syed Ahmed Ali |
| 31 | Brigadier General Abu Mohammad Munir Alim, BSP, psc, G |
| 32 | Brigadier General Md Abdul Mukim Sarker, psc |
| 33 | Brigadier General A B M Salahuddin, afwc, psc |
| 34 | Brigadier General Mahbub Ahmed Zakaria, BP, afwc, psc |
| 35 | Brigadier General Saleem Ahmad Khan, SGP, afwc, psc, te |
| 36 | Brigadier General Shah-Noor Jilani, BSP, psc |
| 37 | Brigadier General Ahmed Tabrej Shams Chowdhury, psc |
| 38 | Brigadier General Moinuddin Mahmud Chowdhury, psc |
| 39 | Brigadier General Md Abdul Bari, psc |
| 40 | Brigadier General Monirul Islam Akhand, psc |
| 41 | Brigadier General Md Zakir Hossain, psc, te |
| 42 | Brigadier General S M Salahuddin Islam, BP, psc |
| 43 | Brigadier General Mizanur Rahman Shameem, BP, psc |
| 44 | Brigadier General Md Mahboob Sarwar, afwc, psc, G+ |
| 45 | Brigadier General Md Zahidur Rahim, afwc, psc |
| 46 | Brigadier General A K M Nazmul Hasan, psc |
| 47 | Brigadier General Md Ashikuzzaman, afwc, psc, G |
| 48 | Brigadier General Md Omar Faruque, afwc, psc |
| 49 | Brigadier General Naquib Ahmed Chowdhury, psc |
| 50 | Brigadier General Abul Kalam Mohammad Ziaur Rahman, psc |
| 51 | Brigadier General Abul Hasnat Mohammad Khairul Bashar, afwc, psc |
| 52 | Brigadier General Abul Mansur Md Ashraf Khan, psc |
| 53 | Brigadier General Mohammed Saidul Islam, psc |
| 54 | Brigadier General Md Moin Khan, Isc, psc |
| 55 | Brigadier General A K M Asif Iqbal |

| Ser | Rank and Name |
|---|---|
| **Bangladesh Navy** | |
| 56 | Commodore M Mahbub-Ul Islam, (N), psc, |
| 57 | Commodore M Shahjahan, (N), psc |
| 58 | Commodore Abdullah Al Mamun Chowdhury, (N), psc |
| 59 | Commodore Syed Misbahuddin Ahmed, (C), NUP, afwc, psc |
| 60 | Captain Wahid Hasan Kutubuddin, (N), afwc, psc |
| **Bangladesh Air Force** | |
| 61 | Group Captain M Moyeenuddin, afwc, psc, ADWC |
| 62 | Group Captain Md Monjur Kabir Bhuiyan, BUP, afwc, psc, GD(P) |
| 63 | Group Captain Haider Abdullah, fawc, psc, GD(P) |
| 64 | Group Captain Md Shafiqul Islam, fawc, psc, GD (P) |
| 65 | Group Captain Md Abu Bakr Siddique, psc, Engg |
| **Bangladesh Civil Service** | |
| 66 | Additional Secretary Shah Muhammad Nasim |
| 67 | Joint Secretary Kajal Islam |
| 68 | Joint Secretary Nanda Dulal Banik |
| 69 | Joint Secretary Ziaul Hasan |
| 70 | Joint Secretary Shahan Ara Banu |
| 71 | Joint Secretary Mohammad Abul Kalam |
| 72 | Joint Secretary A B M Azad |
| 73 | Joint Secretary Shahin Islam |
| 74 | Joint Secretary Md. Abdul Hakim Majumder |
| 75 | Joint Secretary Golam Shafiuddin |
| 76 | Deputy Inspector General Md Mohsin Hossain |
| 77 | Deputy Inspector General Helal Uddin Badri |
| 78 | Director General Shah Ahmed Shafi |

## List of Outside Participants

| Ser | Name | Appointment | Organization |
|---|---|---|---|
| 1 | Mr Zunaid Ahmed Palak, MP | Hon'ble State Minister for ICT Division | Ministry of Post, Tele communication & Information Technology |
| 2 | Lieutenant General Md. Mahfuzur Rahman, rcds, ndc, afwc, psc, PhD | Principal Staff Officer (PSO) | Armed Forces Division |
| 3 | Commander Mohammad Mehadi Amin Miah, psc,(G).BN | PS to PSO | Armed Forces Division |
| 4 | Brigadier General Nayeem Ashfaq Chowdhury, OSP, psc | Director, Military Operations | Army Headquarters |
| 5 | Brigadier General S M Farhad, ndc, psc, | Director Signal | Army Headquarters |
| 6 | Captain M N I Sharif, (E), psc, BN | Director, IT | Naval Headquarters |
| 7 | Commodore M Rashed Ali | Director | Naval Headquarters |
| 8 | Air Vice Marshal Masihuzzaman Sernibat | ACAS (A) | Air Headquarters |
| 9 | Group Captain Sharif Sarker | Director, Air Intelligence | Air Headquarters |
| 10 | Group Captain Maksudun Nabi | Director, C&E | Air Headquarters |
| 11 | Group Captain Khan Shahinul Bari, ndc, psc | Director, Cyber Warfare & IT | Air Headquarters |
| 12 | Sheikh Md. Billal Hossain | Deputy Secretary | Ministry of Defence |
| 13 | Md. Akteruzzaman | System Analyst | Ministry of Defence |

| Ser | Name | Appointment | Organization |
|---|---|---|---|
| 14 | Md. Shamsul Haque | Director General (Africa Wing) | Ministry of Foreign Affairs |
| 15 | Muhammad Anwar Hossain | Maintenance Engineer | Ministry of ICT |
| 16 | Md. Nobir Uddin | Senior System Analyst | Ministry of ICT |
| 17 | Md. Kamruzzaman | Senior Assistant Secretary | Ministry of ICT |
| 18 | Bidhan Kumar Pramanik | Assistant Maintenance Engineer | Ministry of Education |
| 19 | Dr. Md. Faroque Hossain | Joint Secretary | Ministry of Education |
| 20 | Md. Mofakkharul Islam | Senior System Analyst | Ministry of Education |
| 21 | Mohammad Hafizur Rahman | System Analyst | Ministry of Public Administration |
| 22 | Md. Abdur Rauf | Additional Secretary | Ministry of Public Administration |
| 23 | Mohammad Shafiqur Rahman | System Manager | National Board of Revenue |
| 24 | Md. Arfe Elahi | IT Manager | Prime Minister's Office |
| 25 | H.E. Ms. Yasoja Gunasekera | High Commissioner | High Commission of Sri Lanka |
| 26 | H.E. Sophie Aubert | Ambassador | Embassy of France |

| Ser | Name | Appointment | Organization |
|---|---|---|---|
| 27 | Idham Zuhri Mohamed Yunus | First Secretary | High Commission of Malaysia |
| 28 | Mr. Aung Myint | Minister Counsellor | Embassy of Myanmar |
| 29 | Brigeradi Jagjeet Singh Nanda, SM | Defence Adviser | High Commission of India |
| 30 | Lieutenant Colonel Dominick Spenser, ndc | Defence Attache | High Commission of UK |
| 31 | Professor Dr. Imtiaz Ahmed | Professor of IR | Dhaka University |
| 32 | M Helal Uddin Ahmed | Associate Profssor (MIS) | Dhaka University |
| 33 | Dr. Md. Abdus Salam Akanda | Associate Professor (Statistics) | Dhaka University |
| 34 | A B M Alim Al Islam | Assistant Professor, CSE Dept. | Bangladesh University of Engineering & Technology (BUET) |
| 35 | Shahidul Islam Khan | Doctoral Fellow, CSE Dept | BUET |
| 36 | Novia Nurain | PhD Student | BUET |
| 37 | Mohammad Al Amin | 3rd year Student | BUET |
| 38 | Riad Ahmed Zakir | 3rd year Student | BUET |
| 39 | Dr. Dip Nandi | Head, Dept of Computer Science | American International University Bangladesh (AIUB) |

| Ser | Name | Appointment | Organization |
|---|---|---|---|
| 40 | Bayzid Ashik Hossain | Assistant Professor | AIUB |
| 41 | Adib Mehdi | 3rd year Student | AIUB |
| 42 | Professor Dr. Nazmul Ahsan Kalimullah, BFTO | Pro Vice Chancellor | Bangladesh University of Professionals (BUP) |
| 43 | Brigadier General Shaikh Muhammad Rizwan Ali | | BUP |
| 44 | Commander M Moyezuddin, BN | Chairman, ICT Dept | BUP |
| 45 | Md. Khaleduzzaman | | BUP |
| 46 | Hasan Al Monsur | Security Consultant | BUP |
| 47 | Rajib Ahmed | Sr. System Analyst | BUP |
| 48 | Uttam Banik | Student | BUP |
| 49 | Md. Abu Yusuf Siddique | MISS Student | BUP |
| 50 | Dr. Md. Mahbubur Rahman | Professor, CSE Dept | Military Institute of Science & Technology (MIST) |
| 51 | Lieutenant Colonel Mohammed Ali, psc, Sigs | General Staff Officer-1, ICT Dte | MIST |
| 52 | Major Md Enamul Karim | CSE Dept | MIST |
| 53 | Rajib Ahmed | | MIST |
| 54 | Major Muhammad Nazrul Islam | Instr CI-B, CSE Dept | MIST |
| 55 | Colonel Md. Hasan-uz-zaman | Colonel Staff | MIST |

| Ser | Name | Appointment | Organization |
|---|---|---|---|
| 56 | Lieutenant Colonel Md Hafizur Rahman, psc, Inf | | Defence Services Command & Staff College (DSCSC) |
| 57 | Md. Sazzat Hossain | System Analyst | DSCSC |
| 58 | Major General Abul Muneem Mansur Ahmed, psc (retd) | Ex Commandant, NDC | |
| 59 | Major General Jiban Kanai Das, ndu, psc (retd) | Ex Commandant, NDC | |
| 60 | Major General Md Abdur Rashid, psc (Retd) | Resource Person | |
| 61 | Brigadier General Anisuzzaman Bhuiyan, ndc, psc (LPR) | Ex College Secretary, NDC | Bangladesh Army |
| 62 | Brigadier General Md. Mahbub-ul-Alam, afwc, psc | Commander, 105 Infantry Brigade, Jessore Cantonment | Bangladesh Army |
| 63 | Md. Abdus Salam | CEO & MD | Janata Bank |
| 64 | Md. Abdullah Al Mamoon | Executive Vice President | AB Bank |
| 65 | Md. Shaheen Reza | First Vice President | Mercantile Bank |
| 66. | Mohammad Khalilur Rahman | Software Architect | Mercantile Bank |
| 66 | Air Commodore Md Humayun Kabir, BSP, ndc, psc | Director, EALB | Directorate General of Forces Intelligence |
| 67 | Brigadier General Zakir Hossain, ndc, psc | Director | National Security Intelligence |

| Ser | Name | Appointment | Organization |
|---|---|---|---|
| 68. | Brigadier General Selim | | Border Guard Bangladesh |
| 69. | Lieutenant Colonel Mohammad Abul Kalam Azad, BPM, PPM | Intelligence Wing | RAB HQ |
| 70. | Mr. Mizanur Rahman | | Ansar & VDP |
| 71. | Colonel Md. Khairul Islam | | HQ, Recruiting Unit, Dhaka Cantonment |
| 72. | Lieutenant Colonel Md. Rakibul Hasan, Sigs | | National Telecommunication Monitoring Cell (NTMC) |
| 73. | Lieutenant Colonel Abul Hasnat Md. Kamruzzaman Khan, psc, Sigs | | NTMC |
| 74. | Samia Zaman | Research Officer | Bangladesh Institute of International & Strategic Studies (BIISS) |
| 75. | M Ashique Rahman | Research Fellow | BIISS |
| 76 | A N M Asif Hossain | Deputy Manager | Teletalk Bangladesh Ltd |
| 77 | Md. Ahsanul Hauque | Deputy Manager | Teletalk Bangladesh Ltd |
| 78 | Md. Mehfuz | | Bangladesh Telecommunications Regulatory Commission (BTRC) |

| Ser | Name | Appointment | Organization |
|---|---|---|---|
| 79 | Tousif Shahriar | | BTRC |
| 80 | Ahmed Imran Mustafa | ICT Coordinator | United Nations Development Programme |
| 81 | Mr Wazir Uddin Ahmed | Asst Information Officer | Inter Service Press Release |
| 82 | Md Mamun Molla | Reporter | RTV |
| 83 | Md. Al-Masud Imran | Senior Teacher (English) | Mirpur Cantonment Public School and College (MCPSC) |
| 84 | Farzana Anzum | Student | MCPSC |
| 85 | Labiba Anzum | Student | MCPSC |
| 86 | Afsara Tasnim Tanha | Student | MCPSC |
| 87 | Samial Bin Zaidi | Student | MCPSC |
| 88 | Taslima Sultana Jhora | Student | MCPSC |
| 89 | Tahsin Maksud Pathik | Student | MCPSC |
| 90 | Sharif Hossain | Student | MCPSC |
| 91 | Parvage Ahmed | Student | MCPSC |
| 92 | Sumaya Ferdous | Student | MCPSC |
| 93 | Tanjeel Ahmed | Student | MCPSC |

## Moderator/Coordinators

| | | | |
|---|---|---|---|
| 1 | Air Vice Marshal Mahmud Hussain, BBP, OSP, ndc, psc, GD (P) | Senior Directing Staff (Air) | Moderator |
| 2 | Colonel S M Rakibullah afwc, psc, lsc | Director, Research & Academic | Chief Coordinator |
| 3 | Lieutenant Colonel A N M Foyezur Rahman psc, Engrs | Senior Research Fellow | Associate Coordinator |
| 4 | Lecturer Farhana Binte Aziz | Research Fellow | Assistant Coordinator |
| 5 | Md Nazrul Islam | Civilian Staff Officer | Assistant Coordinator |

## Keynote Speakers

| | | | |
|---|---|---|---|
| 1 | Lieutenant Colonel Michael Simond | Charge of Cyber Issues | French Joint HQ in Abu Dhabi |
| 2 | Dr. Ahmed Khurshid | Co-Founder & Principal Engineer | Veriflow Systems, USA |
| 3 | Mr. Shafqat Munir | Associate Research Fellow | Bangladesh Institute of Peace and Security Studies (BIPSS) |
| 4 | Mr. Abdus Shamim Khan | Independent IT Consultant | USA |
| 5 | Mr. Mohammad Ali | Deputy Managing Director & CTO | Pubali Bank Limited |
| 6 | Brigadier General Md Emdad -Ul Bari, ndc, psc, te | Director General, Systems and Services Division | Bangladesh Telecommunications Regulatory Commission |

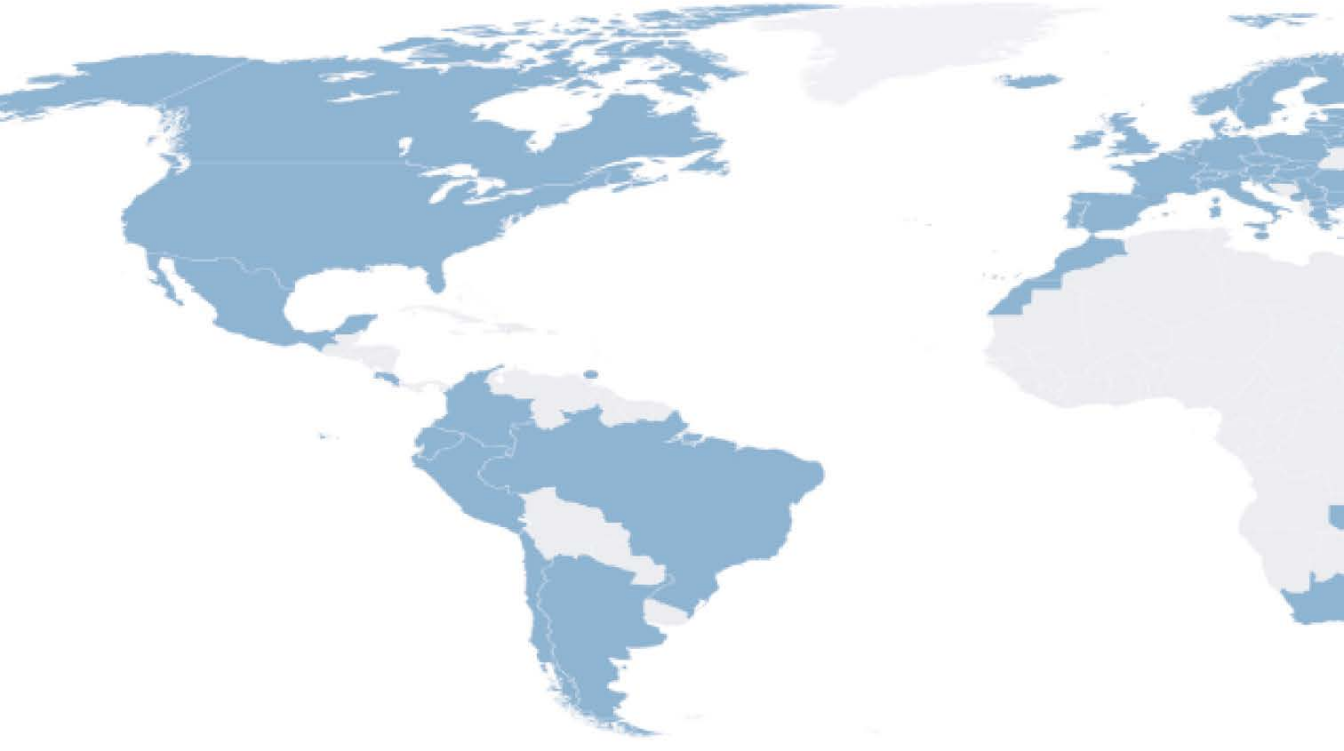
## Rapporteurs

| | | |
|---|---|---|
| 1 | Brigadier General Md Moin Khan, Isc, psc | Chief Rapporteur |
| 2 | Commodore M Shahjahan, (N), psc | Rapporteur |
| 3 | Group Captain Md Abu Bakr Siddique, psc, Engg | Rapporteur |
| 4 | Joint Secretary Md Abdul Hakim Majumder | Rapporteur |


NATIONAL DEFENCE COLLEGE


Cyber Security of Financial Sector & Protective Measures
Seminar on Challenges and Opportunities of Cyber Security : Bangladesh Perspective
Organised by: National Defence College
Embassy of France
Cyber Security of Financial Sector & Protective Measures


NATIONAL DEFENCE COLLEGE



**National Defence College**
Mirpur Cantonment
Mirpur, Dhaka
www.ndc.gov.bd