CICA

SECRETARIAT OF THE CONFERENCE ON INTERACTION AND CONFIDENCE BUILDING MEASURES IN ASIA

СЕКРЕТАРИАТ СОВЕЩАНИЯ ПО ВЗАИМОДЕЙСТВИЮ И МЕРАМ ДОВЕРИЯ В АЗИИ

№ NCT/ICT/308

The Secretariat of the Conference on Interaction and Confidence Building Measures in Asia (CICA) presents its compliments to the CICA Member States and has the honor to inform that in addition to the CICA Plan of Implementation of CMBs for 2023 the Republic of India proposes to organize CICA Virtual Workshop on Misuse of Internet to be held tentatively on 25-26 May 2023.

The corresponding draft Concept paper, Agenda and Administrative note are conveyed herewith. The Secretariat kindly requests Member States to provide suggestions or comments, if any, they might have regarding the event concept paper by 14 April 2023.

Should there be no objections by this date the proposed Workshop will be included in CICA Plan of Implementation of CMBs for 2023.

The Secretariat avails itself of this opportunity to renew to the CICA Member States the assurances of its highest consideration.

Enclosure:
as stated, on 8 p.

Astana, 24 March 2023

Секретариат СВМДА - Astana - CICA Secretariat - Астана

MEMBER STATES
OF THE CONFERENCE ON INTERACTION AND
CONFIDENCE BUILDING MEASURES IN ASIA

CICA

SECRETARIAT OF THE CONFERENCE ON INTERACTION AND CONFIDENCE BUILDING MEASURES IN ASIA

СЕКРЕТАРИАТ СОВЕЩАНИЯ ПО ВЗАИМОДЕЙСТВИЮ И МЕРАМ ДОВЕРИЯ В АЗИИ

№ NCT/ICT/308

Секретариат Совещания по взаимодействию и мерам доверия в Азии (СВМДА) свидетельствует свое уважение государствам-членам СВМДА и имеет честь сообщить, что в дополнение к Плану СВМДА по реализации мер доверия на 2023 год Республика Индия предлагает провести, предварительно 25-26 мая 2023 года, виртуальный семинар на тему «Неправомерное использование сети Интернет».

Соответствующие проект концепции, повестка дня мероприятия и административная записка прилагаются. Секретариат любезно просит государства-члены направить свои предложения или замечания, при наличии, к концепции указанного мероприятия в срок до 14 апреля 2023 года.

Приложение:
упомянутое,
на 8 л.

При отсутствии возражений к указанному сроку предложенный семинар будет включен в План СВМДА по реализации мер доверия на 2023 год.

Секретариат пользуется случаем, чтобы возобновить государствам-членам СВМДА уверения в своем весьма высоком уважении.

город Астана, 24 марта 2023 г.

Секретариат СВМДА · Astana · CICA Secretariat · Астана

ГОСУДАРСТВАМ-ЧЛЕНАМ
СОВЕЩАНИЯ ПО ВЗАИМОДЕЙСТВИЮ И
МЕРАМ ДОВЕРИЯ В АЗИИ

бейресми аударма

Азиядағы өзара іс-қимыл және сенім шаралары кеңесінің (Азия Кеңесінің) Хатшылығы Азия Кеңесінің мүше мемлекеттеріне өзінің зор ілтипатын білдіре отырып, Азия Кеңесінің 2023 жылға арналған сенім шараларын жүзеге асыру жөніндегі жоспарына қосымша ретінде Үндістан Республикасы шамамен 2023 жылғы 25-26 мамыр аралығында “Интернет желісін заңсыз пайдалану” тақырыбында виртуалды семинар өткізуді ұсынатынын хабарлауды өзіне мәртебе санайды.

Тиісті тұжырымдама жобасы, іс-шараның күн тәртібі мен әкімшілік жазба қоса беріліп отыр. Хатшылық мүше мемлекеттерден аталған іс-шараның тұжырымдамасына ұсыныстарын немесе ескертпелерін 2023 жылғы 14 сәуірге дейін жіберуді сұрайды.

Қосымша:
аталған,
8 п.

Белгіленген мерзімге дейін қарсылықтар түспеген жағдайда ұсынылған семинар Азия Кеңесінің 2023 жылға арналған сенім шараларын жүзеге асыру жөніндегі жоспарына енгізілетін болады.

Хатшылық осы мүмкіндікті пайдалана отырып, Азия Кеңесінің мүше мемлекеттеріне өзінің зор ілтипатын тағы да растайды.

Астана қаласы, 2023 жылғы 24 наурыз

АЗИЯДАҒЫ ӨЗАРА ІС-ҚИМЫЛ ЖӘНЕ
СЕНІМ ШАРАЛАРЫ КЕҢЕСІНІҢ
МҮШЕ МЕМЛЕКЕТТЕРІ

30 YEARS

Conference on Interaction and Confidence Building Measures in Asia (CICA)

Virtual Workshop on “Misuse of Internet”, May 25-26, 2023

CONCEPT NOTE

BACKGROUND

A workshop on Misuse of Internet is being organized by the Bureau of Police Research & Development (BPR&D) jointly with its outlying training unit, the Central Detective Training Institute (CDTI), Ghaziabad in the virtual mode on May 25-26, 2023.

Misuse of Internet continues to present a serious threat to international peace and security. Initiatives in the field of study of ‘Misuse of Internet’ can address potential vulnerabilities to prevent nefarious designs of inimical elements from exploiting sophisticated technology, communication, and resources to incite support for criminal acts, create resilience and enhance international cooperation among States, especially the Law Enforcement Agencies (LEAs) for effective investigation and prosecution of cybercriminals.

The rapid proliferation of technology and its diffusion has had unintended consequences. The spectre of cybercrime haunting modern-day society is intensified by the ease of communications, facilitation by procurement networks, sourcing and channelling of funds as well as targeting a vulnerable population. Internet is being used by organised criminals in drug trafficking, human trafficking, etc. Internet is also being used for radicalisation, recruitment and financing of terrorism. Cybercriminals are increasingly building their software applications and much of these depend on re-using existing codes and software.

Internet is being increasingly exploited for terrorist purposes. The world has seen the effective use of organized propaganda over Internet to unleash terrorists to cause havoc across the globe. Evolving technologies like Artificial Intelligence, thinking machines, robotics technologies, big data analytics, and bot technologies are all susceptible to misuse for criminal purposes including terrorist activities. It is essential that Law Enforcement Agencies' (LEAs) capabilities need to be constantly augmented to face these evolving challenges.

The workshop is also an effort to highlight that cyberspace being misused by criminals for crimes against women, children and other vulnerable groups. The usage of cyberspace for financial crimes and misuse of platforms like Dark Web and Deep Web by criminals and terror outfits will also be discussed.

The workshop would focus on promoting discussion on national approaches and sharing of experiences and expertise. It will broadly be focusing on ways and means to prevent misuse of Internet; including success stories, good practices and illustrative case studies. Sharing of experiences of Member States is expected to help in capacity building of national law enforcement authorities.

OBJECTIVES

1. Raising awareness about how criminals seek to exploit social media platforms for operations ranging from spreading propaganda, recruitment, communication, planning and execution.
2. Enhancing the understanding of professionals on how cooperation among authorities can contribute in countering the misuse of internet for financial crimes, crimes against women and children globally;
3. To understand the process of misuse of Internet by terrorists and criminals;
4. To increase awareness about usage of malware and ransomware as tools for financial crimes;
5. To develop an insight on approach to deal with futuristic cyber crime including IoT hacks.

-----

30 YEARS

Conference on Interaction and Confidence Building Measures in Asia (CICA)

Virtual Workshop on “Misuse of Internet”, May 25-26, 2023

AGENDA

Day 1

Starting Time of Workshop: 10.00 hrs (Indian Standard Time)

Opening Ceremony: 30 Minutes

Session 1: Misuse of Internet in organised crime

i.	Expert session	: 40 Minutes
ii.	Presentations	: 10 Minutes each
iii.	Q&A	: 10 Minutes

The first session will discuss the emerging threats due to Misuse of Internet in organised crime. As a communication tool, information source, marketplace, recruiting ground and financial service, the internet facilitates all types of offline and online organised crimes, including illicit drug extraction, synthesis and trafficking, trafficking in human beings for sexual exploitation, illegal migration, Mass Marketing Fraud (MMF), tax fraud, counterfeiting and the trade in prohibited firearms. In particular, the perceived anonymity afforded by communications technologies such as email, instant messaging and Voice over Internet Protocol (VoIP) has led to them being used increasingly by Organised Crime groups as a countermeasure to law enforcement detection and surveillance.

Session 2: Use of Malware and Ransomware as a tool for financial crime

i.	Expert Session	: 40 Minutes
ii.	Presentations	: 10 Minutes each
iii.	Q&A	: 10 Minutes

Malware can be used by attackers to perform variety of malicious actions like spying on the target using spyware, destroying data and resources, causing errors in the system and slowing down the performance. Viruses, Trojan horses, worms and spyware are various types of malware along with a few others.

Ransomware is a type of specialised malware that is designed to block user access from their system until a ransom fee is paid to ransomware creator. Ransomware is considerably more dangerous than regular malware and is spread through phishing emails having infected attachments. Ransomware has emerged over the last few years as a major threat and can attack individuals or organizations.

The session will primary focus on issues related to improving domain awareness about the uses of malware and ransomware as a tool for financial crime.

Session 3: Prevention of Cybercrime against women and children

i. Expert Session : 40 Minutes
ii. Presentations : 10 Minutes each
iii. Q&A : 10 Minutes

Women and children are the most vulnerable targets of cyber criminals on Internet. Though crime against women and children is on a rise in all fields, being a victim of cybercrime could be the most traumatic experience for them. Cyber technologies are misused in carrying out crimes in the cyber world that include offences, unwarranted surveillance, prostitution, invasion of privacy, unsolicited emails and child pornography among others.

The session will primary focus on issues related to improving domain awareness about misuse of cyberspace as a tool for crime against women and children.

Day 2

Session 4: Use of Dark Web and cryptocurrency in illegal trade and terror

i. Expert Session : 40 Minutes
ii. Presentations : 10 Minutes each
iii. Q&A : 10 Minutes

Bitcoin has become the prominent currency of the ‘Dark Web', where it is often used to purchase illegal goods online, such as weapons and drugs. However, the intersection of Bitcoin and the Dark Web for terrorist activities has not been sufficiently documented. Anecdotal evidence suggests that terrorists are already employing Bitcoin, but more work is needed to ascertain whether groups are using a combination of Bitcoin and the Dark Web to finance, plan, and perpetrate terrorist attacks. This has raised questions about cryptocurrency enabling illegal behaviour. The intersection of the Dark Web and Bitcoin, popularized by organized crime, perhaps poses the most significant threat. Much like organised criminals, terrorist organisations could use Bitcoin to purchase and arrange weaponry, including firearms or bomb-making materials, or even false passports on the Dark Web.

The session will primary focus on issues related to improving domain awareness about misuse of Dark Web and cryptocurrency in illegal trade and terrorism.

Session 5: Futuristic Cybercrime and Internet of Things (IoT) hacks

i. Expert Session : 40 Minutes
ii. Presentations : 10 Minutes each
iii. Q&A : 10 Minutes

Advanced IoT technologies are paving the way for a revolutionized future in which many of our daily devices would be interconnected. Such devices should be able to connect and interact with each other and their surroundings. This allows the automation of many activities. The adoption of IoT technology and a wide variety of sensing and acting capabilities have led to smart, intelligent devices that are more realistic but still highly enticing targets for cyber-attacks and cybercrimes. The main line of protection against cyber-attacks and cybercrime is vigilance and preparedness.

This session will sensitize participants on Futuristic Cybercrime and IoT hacks to create resilience.

Session 6

i. **Panel discussion with experts**: 40 Minutes
ii. Q & A: : 20 Minutes

Valediction: 30 Minutes

Workshop module on “Misuse of Internet” for CICA Member States to be held on May 25-26, 2023

Session Time	**Topics**
	25.05.2023 **Day -1**
1000-1030 hrs. (IST)	**Inauguration**
	Session – I
1030-1130 hrs. (IST)	**Misuse of Internet in Organized Crime.**
1130-1145 hrs. (IST)	**Break**
	Session - II
1145-1245 hrs. (IST)	**Use of Malware and Ransomware as a tool for Financial Crime.**
1245-1300 hrs. (IST)	**Break**
	Session – III
1300-1400 hrs. (IST)	**Prevention of Cybercrime against Women and Children.**
	26.05.2023 **Day - 2**
	Session – I
1000-1100 hrs. (IST)	**Use of Dark Web and Cryptocurrency in Illegal Trade and Terror.**
1100-1115 hrs. (IST)	**Break**
	Session - II
1115-1215 hrs. (IST)	**Futuristic Cybercrime and Internet of Things (IoT) Hacks.**
1215-1230 hrs. (IST)	**Break**
	Session - III
1230-1330 hrs. (IST)	**Panel Discussion with Experts**
1330-1400 hrs. (IST)	**Valediction**

----

30 YEARS
Conference on Interaction and
Confidence Building Measures
in Asia (CICA)

Virtual Workshop on "Misuse of Internet", May 25-26, 2023

Administrative Note

INTRODUCTION

The Republic of India welcomes participants of the Conference on Interaction and Confidence Building Measures in Asia (CICA) Member States for virtual workshop on Misuse of Internet to be held on May 25-26, 2023.

EVENT DATES AND PROGRAMME

The workshop on Misuse of Internet is being organised by the Bureau of Police Research & Development (BPR&D) jointly with its outlying training unit, the Central Detective Training Institute (CDTI), Ghaziabad on May 25-26, 2023 in virtual mode.

NODAL POINT

The following representatives of the Bureau of Police Research & Development (BPR&D), Ministry of Home Affairs, Government of India are appointed as focal points and are ready to assist you with all emerging issues you may have regarding the workshop.

i. Shri Anurag Kumar, IPS
Deputy Director, Training
Bureau of Police Research & Development
Ministry of Home Affairs
Government of India
Email ID: ddtrg@bprd.nic.in

ii. Shri Ambar Kishore Jha, IPS
Director, Central Detective Training Institute, Ghaziabad
Bureau of Police Research & Development
Ministry of Home Affairs
Government of India
Email: principalcdtsgzb2012@gmail.com

PLATFORM FOR THE VIRTUAL WORKSHOP

The seminar will be held on CISCO WebEX.

WORKING LANGUAGE OF THE WORKSHOP

English

MODALITY OF THE WORKSHOP

The workshop has been designed with thematic inputs wherein specific sessions would be moderated/conducted by the countries as specified in the enclosed programme. The member countries would be making a presentation on the topic (duration 10-15 minutes), followed by deliberations/country intervention amongst the participants. In addition to the thematic sessions, panel discussions are also planned. These deliberations would be done to produce the good practices that can be adopted by the Member States for understanding, preventing, and countering misuse of Internet and radicalization. The workshop will broadly cover various topics on these two subjects focusing on the matrix and ways and means; including success stories and illustrative case studies. The workshop also recognizes the importance of cooperative action by Member States aimed at preventing nefarious designs of inimical elements from exploiting sophisticated technology, communication, and resources to incite support for criminal acts. It makes it imperative that there are concerted efforts to identify the platforms that are being used by the terrorist/extremist groups and devise a system-based approach to tackle them.

NO. OF PARTICIPANTS FROM EACH MEMBER STATES

3-4 participants from each Member State. Participants may include representatives from counter-terrorism agencies, intelligence departments, investigation agencies, security task forces, and agencies that specifically deal with cyberspace and terrorism.

FACULTY MEMBERS

Experienced eminent faculty members and domain experts will be drawn from various important organizations. All the sessions will be interactive and knowledge-based. Special care will be taken to ensure the content of the course is of the highest quality keeping in mind the sizeable number of participants from different countries. For the preparation of the programme in a time-bound manner, Member States are requested to expeditiously forward the list of all the officers attending the workshop and resource persons/experts on the subjects, if any.
