The Indo–Dutch
Cyber Security School 2025

Study Guide for participants

Contents

Welcome

Welcome to the 8th edition of the Indo-Dutch Cyber Security School (IDCSS)! In this school, we will uncover a plethora of cyber-related topics together. Furthermore, you are challenged to engage with hands-on cyber issues in a practical way, together with your fellow students.

IDCSS25 is a joint initiative of The Hague Centre for Strategic Studies (HCSS), the Cybersecurity Centre of Excellence (CCoE), the Data Security Council of India (DSCI), The Hague Municipality, the Netherlands Embassy in India, and the Government of Telangana, along with several partner organisations. This school is made possible by the Dutch Ministry of Foreign Affairs.

About IDCSS25

Just like in previous editions, the school will take place via Microsoft Teams. For the functioning of the school, **it is of paramount importance that you login to MS Teams with the same email as the email you used to sign up for the school in Mera Events.** The school will be structured as follows: The Inaugural session of the school will take place on **October 6th**. In the first part of the school (October 7th until October 24th), you will be given 20+ lectures, provided by various experts in the field and from academia. You will find the full programme for these lectures below, including the links to the MS Teams meetings.

After the lecture period, the practical part of the school will start. From October 25th until November 5th, you will be tasked with working on practical challenges, together with your fellow students. There are 5 challenges, provided by different organizations and partners:

- **Challenge 1** - Responsible State Behaviour in Cyberspace (UNIDIR)
- **Challenge 2** – Combating online disinformation: Cybersecurity approach (Municipality The Hague)
- **Challenge 3** – Digital Threat Landscape for a NATO Summit (Hunt & Hackett)
- **Challenge 4** – Securing Smart Cities – Protecting Critical Urban Infrastructure (NXP)
- **Challenge 5** – The Impact of Artificial Intelligence in the Cybersecurity Industry (Microsoft)

More information on the challenge will be sent soon via email. A survey will also be sent for you to choose your top two preferences for the challenges. We cannot guarantee that you will be assigned to your chosen Challenge.

We will wrap up IDCSS25 during the Closing Ceremony on **November 7th**.

Certification

Students who successfully take part in the school will receive official certificates from IDCSS. The school issues two types of certificates:

1. **Certificate of Attendance**
   Students who take part in the lectures of IDCSS will receive a Certificate of Attendance. In order to receive the certificate, students **are required to attend at least 75% of all lectures.** Additionally, students are required to **actively participate** in the online Strategic Cyber Resilience Game by attending at least **two out of three** game sessions and submit the **final deliverable** for the Game. In order for the IDCSS team to track your attendance, **it is of paramount importance that you login to MS Teams with the same email as the email you used to sign up for the school and use this consistently.** This is also the email address you will use to access the Game.

2. **Certificate of Participation**
   The Certificate of Participation will be granted to students who successfully complete a challenge, the second part of the school which is optional. More information on the requirements for this will be provided at a later stage on our website and via email.

Questions

If you have any additional questions, please first consult the FAQ on the IDCSS25 website. For any additional questions please email cyberschool@hcss.nl.

IDCSS25 Official lecture programme

Date	Time (CEST)	Time (IST)	Lecture title	Lecturer	MS Teams link
6 October	12:30-14:00	16:00-17:30	**Inaugural IDCSSS25**	High-level dignitaries opening & Panel discussion:	IDCSS25 - Inaugural | Meeting-Join | Microsoft Teams
7 October	16:00-17:00	19:30-20:30	**Data Privacy in Focus: An Overview of GDPR & DPDPA**	Mahi Gupta	IDCSS - Data Privacy in Focus: An Overview of GDPR and DPDPA | Meeting-Join | Microsoft Teams
8 October	14:30-15:30	18:00-19:00	**Security for AI and AI for Security**	Kerissa Varma	IDCSS - Security for AI and AI for Security | Meeting-Join | Microsoft Teams
8 October	16:00-17:00	19:30-20:30	**Web Application Security**	Srinivas Naik	IDCSS - Web Application Security | Meeting-Join | Microsoft Teams
9 October	14:30-15:30	18:00-19:00	**Automotive Security**	Vinod Babu	IDCSS - Automotive Security | Meeting-Join | Microsoft Teams
9 October	16:00-17:00	19:30-20:30	**Cyber Game Session 1**	Michel Rademaker	IDCSS - Cyber Game Session 1 | Meeting-Join | Microsoft Teams
10 October	14:30-15:30	18:00-19:00	**Internet Way of Networking**	Olaf Kolkman	IDCSS - Internet Way of Networking | Meeting-Join | Microsoft Teams
10 October	16:00-17:00	19:30-20:30	**Ransomware**	Chris Painter	IDCSS - Ransomware | Meeting-Join | Microsoft Teams
13 October	16:00-17:00	19:30-20:30	**Digital Forensics**	Hans Henseler	IDCSS - Digital Forensics | Meeting-Join | Microsoft Teams
14 October	14:30-15:30	18:00-19:00	**Threat Analysis NATO Summit The Hague**	Tom Moester	IDCSS - Threat Analysis NATO Summit | Meeting-Join | Microsoft Teams
14 October	16:00-17:00	19:30-20:30	**IoT Security: Current Landscape and Future Outlook**	Amit Rao	IDCSS - IoT Security: Current Landscape and Future Outlook | Meeting-Join | Microsoft Teams
15 October	14:30-15:30	18:00-19:00	**Cybersecurity Career Pathways**	Gaurav Gupta/ Khushboo Sehgal	IDCSS - Cybersecurity Career Pathways | Meeting-Join | Microsoft Teams

16 October	14:30-15:30	18:00-19:00	**State Responsibility in Cybersecurity**	Moliehi Makumane	IDCSS - State Responsibility in Cybersecurity | Meeting-Join | Microsoft Teams
16 October	16:00-17:00	19:30-20:30	**Cybersecurity of Operational Technology**	Johan De Wit	IDCSS - Cybersecurity of Operational Technology | Meeting-Join | Microsoft Teams
17 October	14:30-15:30	18:00-19:00	**Cyber Game Session 2**	Michel Rademaker	IDCSS - Cyber Game Session 2 | Meeting-Join | Microsoft Teams
21 October	14:30-15:30	18:00-19:00	**The Quantum Threat to Cryptography**	Thomas Attema	IDCSS - The Quantum Threat of Cyrptography | Meeting-Join | Microsoft Teams
22 October	14:30-15:30	18:00-19:00	**Accountability in the Digital Age**	Frits Bussemaker	IDCSS - Accountability in the Digital Age | Meeting-Join | Microsoft Teams
23 October	14:30-15:30	18:00-19:00	**Cyber Mercenaries**	Charlotte Lindsey	IDCSS - Cyber Mercenaries | Meeting-Join | Microsoft Teams
24 October	16:00-17:00	19:30-20:30	**Cyber Game Session 3**	Michel Rademaker	IDCSS - Cyber Game Session 3 | Meeting-Join | Microsoft Teams
24 October	14:30-15:30	18:00-19:00	**Challenge 1 (UNIDIR) Q&A Session**	Moliehi Makumane	IDCSS - Challenge 1 Q&A Session - UNIDIR | Meeting-Join | Microsoft Teams
24 October	14:30-15:30	18:00-19:00	**Challenge 2 (Municipality The Hague) Q&A Session**	Daan Rijnders	IDCSS - Challenge 2 Q&A - Municipality The Hague | Meeting-Join | Microsoft Teams
27 October	13:30-14:30 (CET)	18:00-19:00	**Challenge 3 (Hunt & Hackett) Q&A Session**	Tom Moester	IDCSS - Challenge 3 - Q&A Session - Hunt & Hackett | Meeting-Join | Microsoft Teams
27 October	13:30-14:30 (CET)	18:00-19:00	**Challenge 4 (NXP) Q&A Session**	Preet Yadav	*TBC*
TBC	*TBC*	*TBC*	**Challenge 5 (Microsoft) Q&A Session**	*TBC*	*TBC*
29 October	13:30-14:30 (CET)	18:00-19:00	**Cybersecurity Career Pathways Q&A Session**	Gaurav Gupta/ Khushboo Sehgal	IDCSS - Cybersecurity Career Pathways Q&A Session | Meeting-Join | Microsoft Teams
7 November	*TBC*	*TBC*	**Closing Ceremony**	High-level dignitaries & Panel discussion, Winning Challenge groups	*TBC*

Note: Several speakers are still TBC. Please keep an eye on your inbox and the IDCSS25 website as we will add more lectures to the schedule over the first week of the school. All updates to the school will be sent via email!

Preparation

As you embark on this exciting journey, we have prepared a comprehensive reading list to help you gain a solid foundation in the critical areas of cybersecurity that we will explore during the program.

This collection includes key materials on a broad range of cybersecurity topics. By engaging with these readings, you will not only enhance your technical knowledge but also gain insights into the legal, ethical, and policy dimensions of cybersecurity – a truly interdisciplinary approach that is essential in today's digital world.

Reading these is **optional** and not obligatory for successfully completing the IDCSSS25.

Yet, we encourage you to dive into these resources with curiosity and an open mind. Some texts may challenge your current understanding or introduce complex concepts, but they will serve as valuable building blocks for the workshops, discussions, and hands-on activities you'll experience in the program.

We're excited to have you with us for what promises to be a dynamic and enriching learning experience!

Reading list

1. Data protection in the EU, by the European Commission
2. Risk management - The fundamentals and basics of cyber risk, by the National Cyber Security Centre (UK)
3. Cybercheck: Beware of supply chain risks!, by the Dutch Intelligence Agency
4. What is digital forensics and incident response (DFIR)?, by IBM
5. What is internet governance?, by the Geneva Internet Platform
6. What is network security?, by IBM
7. Privacy vs. Security: Exploring the Differences & Relationship, by OKTA
8. Risk management - Cyber security governance, National Cyber Security Centre (UK)
9. The NIS2 Directive Explained, NIS2 Directive
10. Fundamentals of Cybersecurity [2024 Beginner's Guide], KnowledgeHut

Rewatch lectures from IDCSS24

Through this link, you can rewatch the lectures that were hosted during our previous edition of the Indo-Dutch Cyber Security School (IDCSS24). This is also **optional**.

The IDCSS25 Strategic Cyber Resilience Game

During the Indo-Dutch Cyber Security School, participants play the Strategic Cyber Resilience Game. This game, developed by The Hague Centre for Strategic Studies (HCSS), commences in the first week of IDCSS25 and ends in the third week. The game is played in three different phases, some asynchronous and some synchronously with the other players. We move through the different phases in three game sessions.

Please note that in order to obtain your **Certificate of Attendance**, you will need to:

a) Attend at least **75%** of the IDCSS25 lectures (the three game sessions are not considered to be lectures as such).
b) Attend **at least two** out of the three game sessions, **play actively*** throughout the IDCSS25, and complete the **final deliverable** for the game.

**Game activity is monitored by the IDCSS25 Team, to be able to check your active participation.*

How to access the game

There is no limit to the number of players, meaning every IDCSS25 participant can play the game. The game is played in an online environment, where you can **log in via the following link**:

https://idcss25game.strategicgame.nl/info

Please make sure to log in with the email address you used to sign up for IDCSS25. Only that email address is registered with us and will have access to the game. You will get a login link in your email inbox the first time you register in the game. This can take a few minutes to arrive.

Game sessions

All game sessions are hosted by Michel Rademaker, Deputy Director and co-founder of HCSS. There are three such sessions, which all launch one of the three phases of the game. You are strongly advised to attend all three sessions:

1st game session – Thursday 9th October (16:00-17:00CEST / 19:30-20:30IST):

During this first session, we will be doing two things.

1. Michel Rademaker will explain the IDCSS25 Strategic Cyber Resilience Game and **kick off the game** together with you!
2. The **first phase** of the game will start, where you will write the Situation Card together, based on the scenario we will be playing in the game. In the Situation Card, you make an appreciation of this scenario by identifying main threat actors.

Between session 1 and 2, you will have to fill in the Strategy Card on your own, in the online game portal. **This step of the game is done asynchronously, and you should finish this before the next session.**

2nd game session – Friday 17th October (14:30-15:30CEST / 18:00-19:00 IST):

During the second session, we will be doing two things.

1. You have filled in your Strategy Card by now, in the online game portal. In this session, we will reflect on the Situation Card from session 1 and on the Strategy Cards you submitted, to formulate one definitive Strategy Card.
2. This will be used to kick off phase two of the game, in which you will have to play the capability cards. Additionally, **you will have to be online on the game portal on Thursday 23rd October, 16:00-17:00 CEST / 19:30-20:30 IST, to partake in the Voting.** This step of the game is done asynchronously and requires you to vote for a subset of capability cards (out of all the cards that were played by everyone) that you think should have the highest priority.

Between session 2 and 3, you will have to do two things.

1. Play the capability cards.
2. **Vote** for the cards you think should have the highest priority. This can only be done in the game portal, during this timeslot: **Thursday 23rd October, 16:00-17:00 CEST / 19:30-20:30 IST**.

These steps of the game are done asynchronously, and you should finish this before the next session.

3rd game session – Friday 24th October (16:00-17:00 CEST / 19:30-20:30 CET):

During the third and final session, we will be doing two things.

1. We will conduct the Causality-phase of the game. This means that from all cards played, and voted for, players will have to determine causality in the operationalization of those cards. This is the final phase in building a strategy from the capability cards that are now left: here you have to start identifying which capabilities are causally connected, e.g., dependent on another capability to be in place. **This round is played for ca. 30 minutes, synchronously (meaning you will have to actively play on the game portal during this session).**
2. After we have played this round, Michel Rademaker will close the IDCSS25 Strategic Cyber Resilience Game and discuss the results with you. You will receive an evaluation form via email, which includes the **final deliverable** for the game: you will have to write a reflection on the game and what you learned.

After this, the IDCSS Strategic Cyber Resilience Game is finished. The IDCSS25 will continue with the Challenge period.

Please visit our website or rewatch the IDCSS25 Q&A session's recording on our YouTube channel for FAQs. Keep an eye out on your email inbox for other information and updates.

Challenge process

The IDCSS25 challenge period is set to commence on 25th October 2025. You will receive more information at that time, but make sure to be aware of the general challenge process and deadlines:

- Hand in your Challenge submission/solution video of **max. 3 minutes** to cyberschool@hcss.nl **no later than Wednesday November 5th at 11:59 CET / 16:29 IST**, after which HCSS will upload it to YouTube.
- The video must be sent to **cyberschool@hcss.nl** – it must be clear which group the email is from, and the video must be in an accessible format (mp4/accessible through Drive, WeTransfer, etc).
- You then have 24 hours to accumulate as many YouTube likes as possible before November 6th at 11:59 CET / 16:29 IST. The number of likes is factored into the judging of the challenges.
    - Please note that if the video does not meet the requirement of **max. 3 minutes** in length, or is submitted after the deadline, it will not be uploaded and it will not be considered for certification or the prizes.
    - Getting a Certificate of Participation is not based on if you are one of the winning teams or how many likes you get, you simply have to complete the challenge to the best of your ability and in accordance with the formal requirements.
- One winning team per challenge will be determined based on a scoring rubric by the judging committee. We will announce the winner for each challenge on November **6th** via email, IDCSS25 LinkedIn/Twitter and our website.
- All 5 winning challenge teams will participate in the Wheel of Fortune during the **Closing Ceremony on November 7th**, in which we will show the 5 winning videos and allow every group a moment to expand on their work.
- If there are any people in your group that are not contributing, please make sure that your team's Point of Contact, sends an email to cyberschool@hcss.nl explaining the situation.

The challenge period of the school is optional, but we do hope you all take it seriously, plan to actively participate with your group and most importantly: enjoy it!

Need to know

You have received a lot of information about IDCSS25 and more will come your way in the coming weeks. To make sure that the experience is as smooth as possible and you don't miss anything, please remember to flip through this document once in a while. Most of the questions you may have will be answered in here, or in the emails you will receive. A couple of things to keep in mind as a IDCSS25 participant:

- The certification process is automated. This means there is no possibility of manual changes by the organisation in terms of keeping attendance records, etc. (we received questions about this in the past). Therefore, **it is of paramount importance that you login to MS Teams with the same email address and name that you used to sign up for the school in Eventbrite and use this consistently.** This is also the email address you will use to access the Game.
- All communication between the organisation and participants will be done via email, through the Mera Events portal. This means that we can only reach you via the **exact email address and name** that you used to sign up with.
- We aim to record each lecture and share it on the YT channel afterwards, but some lecturers might wish not to be recorded. In such cases, there will be no recording available.
- The Lecture and Challenges parts of the School are separate and are rewarded with separate certificates. This means you can get up to two certificates if you join for both these periods of the school. We urge you to only sign up for the Challenges if you are motivated and willing to actively participate in the process as it is optional. Free-riders harm the fairness of the competition between teams. Free-riders will be reported and will not receive a certificate.

With this Study Guide, you should be up to date and prepared to start the Indo - Dutch Cyber Security School 2025! We look forward to welcoming you and hope you have a wonderful time.

Good luck!

The IDCSS25 Team