The Hague Centre for Strategic Studies

Stellenbosch
UNIVERSITY
IYUNIVESITHI
UNIVERSITEIT

Ministerie van Buitenlandse Zaken

The Southern Africa – Netherlands Cyber Security School 2025

Study Guide for participants

Contents

Welcome

Welcome to the 2nd edition of the Southern Africa - Netherlands Cyber Security School (SANCS)! 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.

SANCS25 is a joint initiative of Hague Centre for Strategic Studies (HCSS), Stellenbosch University, the Municipality of The Hague, the Embassy of South Africa in The Hague, and the Embassy of the Kingdom of the Netherlands in Pretoria, along with several partner organizations. This school is made possible by the Dutch Ministry of Foreign Affairs.

About SANCS25

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 Eventbrite.** The school will be structured as follows: The Inaugural session of the school will take place on **March 3rd**. In the first part of the school (March 4th until March 21st), 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 March 24th until April 10th, you will be tasked with working on practical challenges, together with your fellow students. The SANCS25 team is currently in the last phases of creating these challenges. As soon as we have more information on them, we will reach out to you with an informative email.

We will wrap up SANCS25 during the Closing Ceremony on **April 10th**.

Certification

Students who successfully take part in the school will receive official certifications from the IDCSS. The school identifies two types of certifications.

1. **Certificate of Attendance**
   Students who take part in the lectures of the SANCS will receive a Certificate of Attendance. In order to receive the certificate, students **are required to attend 75% of all lectures.** Additionally, students are required to **actively participate** in the online Strategic Cyber Resilience Game, attend at least **two out of three** game sessions, and submit the **final deliverable** for the Game. In order for the SANCS 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 engage with the challenges, the second part of the school. 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 SANCS25 website. You will find a contact sheet there as well. We are looking forward to working together during these 6 weeks!

The Hague Centre for Strategic Studies

Stellenbosch University Iyunivesithi Universiteit

Ministerie van Buitenlandse Zaken

SANCS25 Official lecture programme

Date	Time (CET)	Time (SAST)	Lecture title	Lecturer	MS Teams link
3 March	13:30-16:00	14:30-17:00	Inaugural SANCS25	High-level dignitaries opening & Panel discussion: Sanjeev Relia, Kerissa Varma, Jabu Mtsweni, Lars Gumede	Click here to go to the meeting
4 March	16:00-17:00	17:00-18:00	Cyber Mercenaries	Charlotte Lindsey	Click here to go to the meeting
5 March	16:00-17:00	17:00-18:00	Game Session 1	Michel Rademaker	Click here to go to the meeting
5 March	17:15-18:15	18:15-19:15	Internet Way of Networking	Olaf Kolkman	Click here to go to the meeting
6 March	14:45-15:45	15:45-16:45	State Behaviour in Cyberspace	Moliehi Makumane	Click here to go to the meeting
6 March	16:00-17:00	17:00-18:00	Cyber Controls	Jesper de Boer & Jeleen Kombrink	Click here to go to the meeting
10 March	14:45-15:45	15:45-16:45	Digital Forensics	Hans Henseler	Click here to go to the meeting
10 March	16:00-17:00	17:00-18:00	Accountability in the Digital Age	Frits Bussemaker	Click here to go to the meeting
11 March	14:45-15:45	15:45-16:45	Cyber Risk Management	Justin Westcott	Click here to go to the meeting
11 March	16:00-17:00	17:00-18:00	Game Session 2	Michel Rademaker	Click here to go to the meeting
12 March	14:45-15:45	15:45-16:45	The Impact of Artificial Intelligence on Cybersecurity	Esther Schagen - van Luit	Click here to go to the meeting
12 March	16:00-17:00	17:00-18:00	Aviation Cyber Security	Dikeledi Mzimba	Click here to go to the meeting
12 March	17:15-18:15	18:15-19:15	Incident Response	Jaco Swanepoel	Click here to go to the meeting
13 March	14:45-15:45	15:45-16:45	The Quantum Threat to Cryptography	Thomas Attema	Click here to go to the meeting
13 March	16:00-17:00	17:00-18:00	Ethics of AI	Jeroen van den Hoven	Click here to go to the meeting
17 March	14:45-15:45	15:45-16:45	Cybersecurity of Operational Technology	Johan de Wit	Click here to go to the meeting
18 March	14:45-15:45	15:45-16:45	Cybersecurity in the Maritime Sector	Barend Pretorius	Click here to go to the meeting
18 March	16:00-17:00	17:00-18:00	The OT Cyber Threat Landscape in Energy: Managing Risk Through Governance	Michelle Govender	Click here to go to the meeting
19 March	14:45-15:45	15:45-16:45	Fortifying the Future: Cloud Security Strategies for Safeguarding Smart Devices	Unathi Mothiba	Click here to go to the meeting
19 March	16:00-17:00	17:00-18:00	Risk Assessment NATO Summit The Hague	Tom Moester	Click here to go to the meeting
20 March	16:00-17:00	17:00-18:00	Security Operations Centre	Tima Soni & Amedeo Cioffi	Click here to go to the meeting
25 March	16:00-17:00	17:00-18:00	Game Session 3	Michel Rademaker	Click here to go to the meeting

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 SANCS25.

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. Understanding the Basics of Cybersecurity, by The Yale Ledger
5. What is digital forensics and incident response (DFIR)?, by IBM
6. What is internet governance?, by the Geneva Internet Platform
7. What is network security?, by IBM
8. Privacy vs. Security: Exploring the Differences & Relationship, by OKTA
9. Risk management - Cyber security governance, National Cyber Security Centre (UK)
10. The NIS2 Directive Explained, NIS2 Directive
11. Fundamentals of Cybersecurity [2024 Beginner's Guide], KnowledgeHut

Rewatch lectures from SANCS24

Through this link, you can rewatch the lectures that were hosted during our previous edition of the Southern Africa – Netherlands Cyber Security School (SANCS24). This is also **optional**.

The SANCS25 Strategic Cyber Resilience Game

During the Southern Africa – Netherlands 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 SANCS25 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 SANCS25 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 SANCS25, and complete the **final deliverable** for the game.

**Game activity is be monitored by the SANCS25 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 SANCS25 participant can play the game. The game is played in an online environment, where you can **log in via the following link**:

https://sancs25.strategicgame.nl/login

Please make sure to log in with the email address you used to sign up for SANCS25. Only that email address is registered with us and will have access to the game.

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 – Wednesday 05-03-2025 (17:00-17:45 SAST / 16:00-16:45 CET):

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

1. Michel Rademaker will explain the SANCS25 Strategic Cyber Resilience Game, and **kick off the game** together with you!
2. The **first phase** of the game will be started, 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 – Tuesday 11-03-2025 (17:00-17:30 SAST / 16:00-16:30 CET):

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 in the game portal on Monday March 24th, from 17:00-18:00 SAST / 16:00-17:00 CET, 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: Monday 24-03-2025, from 17:00-18:00 SAST / 16:00-17:00 CET.

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

3rd game session – Tuesday 25-03-2025 (17:00-18:00 SAST / 16:00-17:00 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 identify 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 in the game portal during this session).**
2. After we have played this round, Michel Rademaker will close the SANCS25 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 SANCS Strategic Cyber Resilience Game is finished. The SANCS25 will continue with the Challenge period.

Please visit our website or rewatch the SANCS25 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 SANCS25 challenge period is set to commence on the March 24th 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 Monday April 7th at 12:00PM (noon) CET / SAST**, after which HCSS will upload it to YouTube.
- You then have 24 hours to accumulate as many YouTube likes as possible before April 8th at 12:00PM (noon) CET / SAST. The amount 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 on time.
- 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 **April 8th 17:00PM CET / SAST** via email, SANCS LinkedIn/Twitter and our website.
- All 4 winning challenge teams will partake in the wheel of fortune during the **Closing Ceremony on April 10th**, in which we will show the 4 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 SANCS25, 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 SANCS25 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 Eventbrite 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 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 register for the Challenges if you are motivated and willing to actively participate in the process. 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 Southern Africa – Netherlands Cyber Security School 2025! We look forward to welcoming you and hope you have a wonderful time.

Good luck!

The SANCS25 Team