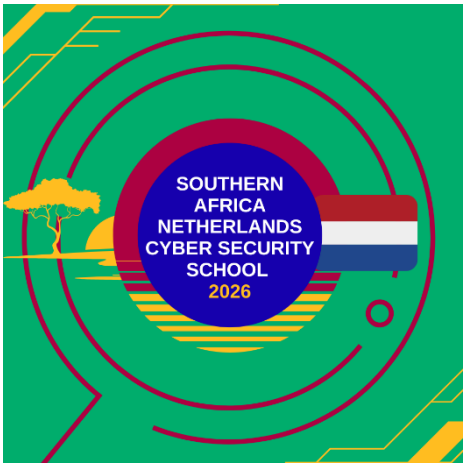
The Southern Africa - Netherlands Cyber Security School 2026

Study Guide for participants



The Hague Centre for Strategic Studies

Stellenbosch UNIVERSITY IYUNIVESITHI UNIVERSITEIT

Kingdom of the Netherlands

Contents

Welcome

Welcome to the 3rd edition of the Southern Africa - Netherlands Cybersecurity 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.

SANCS is co-organised and supported by a wide range of partners from industry, research and government. Our partners for 2026 include The Hague Centre for Strategic Studies (HCSS), Stellenbosch University, the Cyber Security Institute (CSI) and the Embassy of the Kingdom of the Netherlands in South Africa.

About SANCS26

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 log in 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 2nd**. In the first part of the school (March 2nd – 26th March), you will be given 22 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 27th until April 7th, you will be tasked with working on practical challenges, together with your fellow students. There are 7 challenges, provided by different organizations and partners:

- **Challenge 1** – by DataSync
- **Challenge 2** – by UKZN
- **Challenge 3** – by Deloitte
- **Challenge 4** – by CSIR
- **Challenge 5** – by DataGr8
- **Challenge 6** – by SS Consulting
- **Challenge 7** – by Reflex

More information on the challenges will be sent soon via email. After which 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 SANCS26 during the Closing Ceremony on **April 10th**.

Certification

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

1. **Certificate of Attendance**
   Students who take part in the lectures of SANCS26 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 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 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 SANCS26 website . For any additional questions please email cyberschool@hcss.nl.

Class Participation and Online Etiquette

To ensure an orderly and focused learning environment, all online sessions follow a structured format. At the beginning of each class, microphones and cameras are automatically switched off. This is done to minimise background noise and distractions. The chat function is also disabled during the lecture in order to maintain concentration and allow the speaker to present without interruption.
Students are encouraged to engage actively with the content. Questions are welcome, but they are handled in a structured manner to ensure fairness and efficiency.

Here follows a guideline for asking questions:

- Use the **Q&A function in Microsoft Teams** to submit your question during the lecture. Make sure that **Microsoft Teams is downloaded and updated on your laptop**, as the Q&A functionality might not be available in older versions or phone.
- If you do not have access to the Q&A function, we cannot take your questions.
- All questions, whether submitted via Q&A or raised verbally, will be addressed **only at the end of the lecture**. The number of questions taken will depend on the **time remaining** after the presentation.

These procedures are designed to ensure clarity, equal opportunity to participate, and a respectful academic atmosphere for all participants.

SANCS26 Official lecture programme

Date	Time (CEST)	Time (SAST)	Lecture title	Lecturer	MS Teams link
03/03/26	**16:00-17:00**	**17:00-18:00**	**An Overview of South African Cyberlaw and Policy**	**Dr. Ramluckan**	https://events.teams.microsoft.com/event/815b0fe9-c6af-48cc-8cdd-5073c33ac41f@3edc02d8-23dd-4d85-9532-a56b22584b53 Meeting ID: 331 180 418 233 55 Password: mm6rs6Fa
04/03/26	**14:30-15:30**	**15:30-16:30**	**The Quantum Threat to Cryptography**	**Thomas Attema**	https://events.teams.microsoft.com/event/e0c95dfe-64c9-48b6-b635-

					bb908d038a2d@3edc02d8-23dd-4d85-9532-a56b22584b53 Meeting ID: 318 310 608 692 61 Passcode: cA3a7XF2
04/03/26	**16:00-17:00**	**17:00-18:00**	**Cyber Resilience Game Session 1**	**Michel Rademaker**	https://events.teams.microsoft.com/event/e8cdd202-3792-417c-9d86-513aae12d801@3edc02d8-23dd-4d85-9532-a56b22584b53 Meeting ID: 325 974 778 182 03 Passcode: gy7Nx9jx
05/03/26	**14:30-15:30**	**15:30-16:30**	**Cybersecurity in large educational institutions**	**Godert Jan van Manen**	https://events.teams.microsoft.com/event/f0e9b0a9-47c5-4fb5-ae45-9f50aeb7d4b0@3edc02d8-23dd-4d85-9532-a56b22584b53 Meeting ID: 325 522 937 903 52 Passcode: Wc7cV29t
05/03/26	**16:00-17:00**	**17:00-18:00**	**EU Regulation**	**Louk Faesen**	https://events.teams.microsoft.com/event/06096447-cc28-4e76-9ee5-ce1bcc818869@3edc02d8-23dd-4d85-9532-a56b22584b53 Meeting ID: 374 968 423 268 31 Passcode: qj7bN6Y8
10/03/26	**14:30-15:30**	**15:30-16:30**	**Social Engineering and the impact of AI**	**Dr. Heloise Meyer**	https://events.teams.microsoft.com/event/0b089890-ba04-4cdb-bf3f-d0edac27093f@3edc02d8-23dd-4d85-9532-a56b22584b53 Metting ID : 355 467 654 981 78 Password : TJ22rr78
10/03/26	**16:00-17:00**	**17:00-18:00**	**From Risk to Resilience, OT and Supply Chain in Practice**	**Justin Westcott**	https://events.teams.microsoft.com/event/b2736885-5833-443a-b873-c762a55fb898@3edc02d8-23dd-4d85-9532-a56b22584b53 Meeting ID: 366 627 248 490 15 Password : Rz97sT7p
11/03/26	**14:30-15:30**	**15:30-16:30**	**State Responsibility in Cybersecurity**	**Moliehi Makumane**	https://events.teams.microsoft.com/event/935e3689-4401-432e-950e-72148b9dc19b@3edc02d8-23dd-4d85-9532-a56b22584b53 Meeting ID: 382 649 452 935 89 Passcode: eo9rH7EQ
11/03/26	**16:00-17:00**	**17:00-18:00**	**Addressing AI misuse risks through international governance**	**Pablo Rice**	https://events.teams.microsoft.com/event/0a89587c-f703-4d8c-a560-56927feaea4a@3edc02d8-23dd-4d85-9532-a56b22584b53 Meeting ID: 338 877 724 863 32 Passcode: YM6bb3q6

12/03/26	**14:30-15:30**	**15:30-16:30**	**Cybersecurity of operational technology**	**Johan De Wit**	https://events.teams.microsoft.com/event/3c478747-5227-498a-b856-383eb208f687@3edc02d8-23dd-4d85-9532-a56b22584b53 Meeting ID: 343 419 938 546 81 Passcode: n92W3J9Z
12/03/26	**16:00-17:00**	**17:00-18:00**	**Cyber Resilience Game Session 2**	**Michel Rademaker**	https://events.teams.microsoft.com/event/08519ccb-4ddd-442f-a1a9-d97a970b0a5f@3edc02d8-23dd-4d85-9532-a56b22584b53 Meeting ID: 333 524 464 283 74 Passcode: uj25Dm7B
17/03/26	**14:30-15:30**	**15:30-16:30**	**TBA**	**Kerissa Varma**	https://events.teams.microsoft.com/event/ac3d8bd7-c4ca-4a78-80ac-3c4534dcc3e1@3edc02d8-23dd-4d85-9532-a56b22584b53 Meeting ID: 313 923 240 769 77 Passcode: dY9uz7qy
17/03/26	**16:00-17:00**	**17:00-18:00**	**Ransomware**	**Chris Painter**	https://events.teams.microsoft.com/event/309ecf1c-4ba1-4c5d-a184-21947fce5446@3edc02d8-23dd-4d85-9532-a56b22584b53 Meeting ID: 344 871 644 113 88 Passcode: 5Pc2Hv9i
18/03/26	**14:30-15:30**	**15:30-16:30**	**AI Agents in the Wild: What Companies Are Getting Wrong About Security**	**Samantha Hanreck**	https://events.teams.microsoft.com/event/3b20cb24-ace8-4761-91a0-5edc23ffdccf@3edc02d8-23dd-4d85-9532-a56b22584b53 Meeting ID: 379 331 625 395 04 Passcode: Vb2vM2rd
18/03/26	**16:00-17:00**	**17:00-18:00**	**TBA**	**Unathi Mothiba**	https://events.teams.microsoft.com/event/46e10976-aa1a-42cd-b60b-422360c2fdc7@3edc02d8-23dd-4d85-9532-a56b22584b53 Meeting ID: 363 531 842 003 38 Passcode: Y5wW7bg3
19/03/26	**14:30-15:30**	**15:30-16:30**	**TBA**	**Dr. Simphiwe Hector Mayisela**	https://events.teams.microsoft.com/event/cd78b997-982a-4304-b48d-bfb82d3d9eb9@3edc02d8-23dd-4d85-9532-a56b22584b53 Meeting ID: 314 147 772 590 Password: p7uX2Am6
19/03/26	**16:00-17:00**	**17:00-18:00**	**Cyber Resilience Game Session 3**	**Michel Rademaker**	https://events.teams.microsoft.com/event/a0e24ff1-7ac7-4742-a845-619f99608237@3edc02d8-23dd-4d85-9532-a56b22584b53 Meeting ID: 342 364 248 899 29 Password: CA3vM7Z3

24/03/26	**14:30-15:30**	**15:30-16:30**	**The Internet way of networking**	**Olaf Kolkman**	https://events.teams.microsoft.com/event/0afdd7bb-f24a-4112-8675-14b9b40f5340@3edc02d8-23dd-4d85-9532-a56b22584b53 Meeting ID: 386 365 636 423 14 Passcode: 2P8tB2w9
24/03/26	**16:00-17:00**	**17:00-18:00**	**From Controls to Continuity: Embedding Cyber Resilience into IT Audit**	**Jeleen Kombrink and Gijs Van Zuilen**	https://events.teams.microsoft.com/event/b52913ef-93e9-43c1-a78d-dc9d0f790944@3edc02d8-23dd-4d85-9532-a56b22584b53 Meeting ID: 334 809 149 548 68 Passcode: TM2GC2J6
25/03/26	**14:30-15:30**	**15:30-16:30**	**Cybercrime Investigations in South Africa**	**Johnny Botha**	https://events.teams.microsoft.com/event/6a599b9c-be32-4d73-b57b-09ee785376e4@3edc02d8-23dd-4d85-9532-a56b22584b53 Meeting ID: 397 475 908 914 30 Passcode: 3B6M9Pm2
25/03/26	**16:00-17:00**	**17:00-18:00**	**Ethics of AI**	**Jeroen van den Hoven**	https://events.teams.microsoft.com/event/015230cd-7c4f-48f2-a6d5-3ae50571e90a@3edc02d8-23dd-4d85-9532-a56b22584b53 Meeting ID: 326 262 909 956 1 Passcode: dK9Sd3XZ
26/03/26	**14:30-15:30**	**15:30-16:30**	**Ethical Hacking, the Why, How and What**	**Barry Van Kampen**	https://events.teams.microsoft.com/event/3bafc973-2785-4c35-a175-047dece001fe@3edc02d8-23dd-4d85-9532-a56b22584b53 Meeting ID: 387 912 563 906 36 Passcode: 6Pr7jR2w
10/04/26	**TBA**	**TBA**	**Closing Ceremony**	**N/A**	TBA on email through Eventbrite

Note: Several lecture topics are still To Be Announced. Please keep an eye on your inbox and the SANCS26 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 SANCS26.

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. What is digital forensics and incident response (DFIR)?, by IBM
4. What is internet governance?, by the Geneva Internet Platform
5. What is network security?, by IBM
6. Privacy vs. Security: Exploring the Differences & Relationship, by OKTA
7. Risk management - Cyber security governance, National Cyber Security Centre (UK)
8. The NIS2 Directive Explained, NIS2 Directive
9. Fundamentals of Cybersecurity [2026 Beginner's Guide], KnowledgeHut

Rewatch lectures from SANCS25

Through this link, you can rewatch the lectures that were hosted during our previous edition of the Southern Africa-Netherlands Cybersecurity School (SANCS25). This is also **optional**.

The SANCS26 Strategic Cyber Resilience Game

During the SANCS, participants play the Strategic Cyber Resilience Game. This game, developed by The Hague Centre for Strategic Studies (HCSS), commences in the first week of SANCS26 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 SANCS26 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 SANCS26, and complete the **final deliverable** for the game.

**Game activity is monitored by the SANCS26 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 SANCS26 participant can play the game. The game is played in an online environment, where you can **log in via the following link**:

https://sancs26.strategicgame.nl/info

Please make sure to log in with the email address you used to sign up for SANCS26. 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 when you register in the game via the above link. 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 – Wednesday 4th March (16:00-17:00 CET / 17:00-18:00 SAST):

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

1. Michel Rademaker will explain the SANCS26 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 – Thursday 12th March (16:00-17:00 CET / 17:00-18:00 SAST):

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 Monday 16th of March, 16:00-17:00 CEST / 17:00–18:00 SAST, 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 & 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 16th of March, 16:00-17:00 CEST / 17:00-18:00 SAST, to partake in the voting.

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

3rd game session – Thursday 19th March (16:00-17:00 CET / 17:00-18:00 SAST):

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 and be present in the Teams session).**

2. After we have played this round, Michel Rademaker will close the SANCS26 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 SANCS26 will continue with the Challenge period.

Challenge process

The SANCS26 challenge period is set to commence on 27th March. 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 Tuesday April 7th at 11:59 CET / SAST**, 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 April 8th at 11:59 CET / SAST. 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, is not submitted in an accessible format, 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 April 9th via email, SANCS26 LinkedIn/Twitter and our website.
- All 5 winning challenge teams will participate in the Wheel of Fortune during the **Closing Ceremony on April 10th**, 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 SANCS26 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 SANCS26 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 exact 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 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 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 Southern Africa-Netherlands Cybersecurity School 2026! We look forward to welcoming you and hope you have a wonderful time.

Good luck!

The SANCS26 Team