Course Code – Understanding Cyber Security Strategies and Cyber Threats

Programme – Autumn 2026

Course Information

Course Duration: 45 hours of lectures (1 lecture for 3 hours per week)
Credit Hours: 45 hours of lectures
Meetings:
Location**:**
Prerequisites: The student should have a keen interest in knowing about Cyber Security and how it helps contribute to the different countries' National Security.
Equivalent Courses:
Exclusive Courses:

Instructor Information

Instructor: Dr. Gitanjali Sinha Roy
Biography: Assistant Professor
Email: gitanjalis.roy@jgu.edu.in
Phone: +91-9811109256
Office:
Office Hours: Tuesday 11am-12pm
Homepage: https://jgu.edu.in/jsia/faculty/prof-gitanjali-sinha-roy

1. Course Description

The course aims at assessing various countries' cyber security strategies globally. The course will focus on understanding why a particular country adopted their strategies and these strategies are in sync with their foreign policy and security scenario. The objectives are to understand the different cyber security strategies and analyse each of them in the broader bandwidth of the global increase of cyber threats. Understand the various cyber threats faced by the countries.

Course Intended Learning Objectives (Aim)

Course Intended Learning Outcomes	Teaching and Learning Activities	Assessments/Activities
• Understanding what is cyber security? • Analysing the different cyber threats. • Comprehend and trace the history of Cyber security strategies by different countries and cover its effects in the changing world events around them. • While tracing Cyber threats and cyber security, students will be equipped to also understand the different global events and how those global events had an impact on the different countries. • Understand the Cyber Security policy of Estonia and other countries.	• Increase classroom participation. • Student teacher interaction. • Quiz • Map Reading • Learning to read Official Government Documents • Simulation exercises. • Learning to write a well-developed research paper with feedback from the teacher. • Career counselling. • Mentorship. • Lectures by Experts	**Mid-term examination** • It will take place on the 9th week. It consists of a research paper or policy paper of 2000-3000 words which students need to write on their chosen topic from the course. If time remains, students will be granted to make class presentations. **Mid-term Research paper/ policy paper 40 marks** • **Group Simulation Exercise-15 marks** • **Quiz-15 marks** Total Mid-term is 70% (Including research paper/policy paper, group simulation activity and quiz) • **End-term examination (Externals)** It will take place on the 15th week. It consists of an end term question paper. End Term Examination is 30%

2. Scheme of Evaluation and Grading

Evaluation breakup

- **Internals Breakup**
  - It will take place on the 9th week. It consists of a research paper or policy paper of 2000-3000 words which students need to write on their chosen

topic from the course. If time remains, students will be granted to make class presentations. **Mid-term Research paper/ policy paper 40 marks**

- **Group Simulation Exercise-15 marks**
- **Quiz-15 marks**

• Total Mid-term 70% (Including research paper/policy paper, group simulation activity and quiz)

• Externals breakup

It will take place on the 15th week It consists of an end term question paper. End Term Examination 30%

Grade Definition

Grading and Comments			
Letter Grade	**Percentage of Marks**	**Grade Points**	**Comments**
O	80 and above	8	**Outstanding:** Exceptional knowledge of the subject matter, thorough understanding of issues; ability to synthesize ideas, rules and principles and extraordinary critical and analytical ability.
A+	75 - 79	7.5	**Excellent:** Sound knowledge of the subject matter, thorough understanding of issues; ability to synthesize ideas, rules and principles and critical and analytical ability.
A	70 - 74	7	**Very Good:** Sound knowledge of the subject matter, excellent organizational capacity, ability to synthesize ideas, rules and principles, critically analyse existing material and originality in thinking and presentation.
A-	65 -69	6	**Good:** Good understanding of the subject matter, ability to identify issues and provide balanced solutions to problems and good critical and analytical skills.
B+	60 - 64	5	**Fair:** Average understanding of the subject matter, limited ability to identify issues and provide solutions to problems and reasonable critical and analytical skills.
B	55 - 59	4	**Acceptable:** Adequate knowledge of the subject matter to go to the next level of the study and reasonable critical and analytical skills.
B-	50 - 54	3	**Marginal:** Limited knowledge of the subject matter and irrelevant use of materials, and poor critical and analytical skills.
P1	45 - 49	2	**Pass 1:** Pass with Basic understanding of the subject matter.
P2	40 - 44	1	**Pass 2:** Pass with Rudimentary understanding of the subject matter.
F	Below 40	0	**Fail:** Poor comprehension of the subject matter; poor critical and analytical skills and marginal use of the relevant materials. Will require repeating the course.

3. Academic Integrity

Plagiarism is the use of someone else's words OR ideas without proper acknowledgement. Any idea, sentence, or paragraph you take from a web source or from printed material must be

credited with the original source. If you paraphrase or directly quote in the exam or essays, the source must be explicitly mentioned. You should not plagiarize content, be it from scholarly sources (i.e., books and journal articles) or from the Internet.

4. **Keyword Syllabus-**National Security, Cybersecurity, strategies, cybercrime.

5. **Course Material**

Module 1: Introduction to course

Module 2: What is cyber security?

1. Cavelty, M. D. (2022). Cyber-security, in Contemporary Security Studies 6e. Contemporary Studies Studies.
2. P.S, Seemma & Sundaresan, Nandhini & M, Sowmiya. (2018). Overview of Cyber Security. IJARCCE. 7. 125-128. 10.17148/IJARCCE.2018.71127.

Module 3: Understanding various cyber threats

1. Kalakuntla, Rohit & Vanamala, Anvesh & Kolipyaka, Ranjith. (2019). Cyber Security. Holistica. 10. 115-128. 10.2478/hjbpa-2019-0020.
2. Zebari, Dilovan & Asaad, Renas. (2022). A Cyber Security Threats, Vulnerability, Challenges and Proposed Solution. Applied computing Journal. 227-244. 10.52098/acj.202260.

Module 4: Estonia's Cyber Security

1. CYBERSECURITY STRATEGY-Republic of Estonia.
2. Estonia's National Cybersecurity and Cyberdefense Posture-Policy and Organizations, CYBERDEFENSE REPORT, Centre for Security Studies. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Estonia.pdf

Module 5: India and the Cyber Security

1. DSCI. National Cyber Security Strategy 2020. https://www.dsci.in/files/content/knowledge-centre/2023/National-Cyber-Security-Strategy-2020-DSCI-submission.pdf
2. Debopama Bhattacharya.(2022). India's Cyber Security Policy: Strategic Convergence and Divergence with Quad,ISDP. https://www.isdp.eu/content/uploads/2022/08/Brief-Aug-19-2022-Debopama-Bhattacharya.pdf

Module 6: Group Simulation Exercise (15 marks)-Mid-Term (Internals)

Module 7: Evolution of the US Cyber Security

1. NATIONAL CYBERSECURITY STRATEGY.
MARCH 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
2. Chris Jaikaran.2023. "The National Cybersecurity Strategy—Going Where No Strategy Has Gone Before", Congressional Research Service (CRS). https://crsreports.congress.gov/product/pdf/IN/IN12123

Module 8: Quiz (15 marks)-Mid-Term (Internals)

Module 9: Research Paper/Policy Paper (40 marks)-Mid-Term (Internals)

Module 10: Cyber Security of France

1. French National Digital Security Strategy
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf
2. Amber Darwish and Scott Romaniuk. (2020). Cyber security in the French Republic. 10.4324/9780429399718-5.

Module 11: Australia and Cyber Security

1. 2023-2030 Australian Cyber Security Strategy.
https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

2. Mike Bareja and Alexandra Caples. "Australia's new cybersecurity strategy tackles the tough issues", Australian Strategic Policy Initiative, 28 November 2023.
https://www.aspistrategist.org.au/australias-new-cybersecurity-strategy-tackles-the-tough-issues/

Module 12: Japan's Cyber Security

1. CYBERSECURITY STRATEGY(2015). The Government of Japan. Cabinet Decision. https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf
2. Ministry of Foreign Affairs (2023). The 1st Japan- U.S.-ROK Trilateral Diplomacy Working Group for Foreign Ministry Cooperation on North Korea's Cyber Threats. https://www.mofa.go.jp/press/release/pressite_000001_00031.html

Module 13: ASEAN's take on Cyber Security

1. ASEAN CYBERSECURITY COOPERATION STRATEGY (2021 – 2025) https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf
2. Jirapon Sunkpho, Sarawut Ramjan, Chaiwat Ottamakorn. "Cybersecurity Policy in ASEAN Countries." https://www.researchgate.net/profile/Jirapon-Sunkpho-2/publication/324106226_Cybersecurity_Policy_in_ASEAN_Countries/links/5abdc2ea45851584fa6fca37/Cybersecurity-Policy-in-ASEAN-Countries.pdf

Module 14: Cyber Security and the Way Forward

1. Babu, C V & Simon, P. & Kumar, s. (2023). The Future of Cyber Security Starts Today, Not Tomorrow. 10.4018/978-1-6684-8666-5.ch016.

6. Session Plan

Session (with Date)	General Topic	Readings	Approach/Pedagogy
Module 1	Introduction to course	-	Introduction to course, students expectations.
Module 2	What is cyber security?	• P.S, Seemma & Sundaresan, Nandhini &	Understanding the definitions of Cyber security and their

		M, Sowmiya. (2018). Overview of Cyber Security. IJARCCE. 7. 125-128. 10.17148/IJARCCE.2018.71127.	resolutions
Module 3	Understanding various cyber threats	• Zebari, Dilovan & Asaad, Renas. (2022). A Cyber Security Threats, Vulnerability, Challenges and Proposed Solution. Applied computing Journal. 227-244. 10.52098/acj.202260.	Understanding the definitions of Cyber threats and their types
Module 4	Estonia's Cyber Security	• Estonia's National Cybersecurity and Cyberdefense Posture-Policy and Organizations, CYBERDEFENSE REPORT, Centre for Security Studies. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Estonia.pdf	Analysing Estonia's Cyber security
Module 5	India and the Cyber Security-Part 1	• Debopama Bhattacharya.(2022). India's Cyber Security Policy: Strategic Convergence and Divergence with Quad,ISDP. https://www.isdp.eu/content/uploads/2022/08/Brief-Aug-19-2022-Debopama-Bhattacharya.pdf	Evaluating India's Strategy and methods in Cyber security
Module 6	Group Simulation Exercise (15 marks)-Mid-Term (Internals)	• Group Activity	Group based interaction, discussion and simulation-based activity helps increase analyses.
Module 7	Evolution of the US Cyber Security-Part 1	• NATIONAL CYBERSECURITY STRATEGY. MARCH 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf	Evaluating US Strategy and methods in Cyber security
Module 8	Quiz (15 marks)-Mid-Term (Internals)	Syllabus will be Module 2 and 3	Through the quiz students will be tested for module 2 and module 3

Module 9:	Research Paper/Policy Paper (40 marks)- Mid-Term (Internals)	Student has to choose a topic of their choose	Developing research paper skills
Module 10	Cyber Security of France	• Amber Darwish and Scott Romaniuk. (2020). Cyber security in the French Republic. 10.4324/9780429399718-5.	Evaluating France's Strategy and methods in Cyber security
Module 11	Australia and Cyber Security	• Mike Bareja and Alexandra Caples. "Australia's new cybersecurity strategy tackles the tough issues", Australian Strategic Policy Initiative, 28 November 2023. https://www.aspistrategist.org.au/australias-new-cybersecurity-strategy-tackles-the-tough-issues/	Evaluating Australia's Strategy and methods in Cyber security
Module 12	Japan's Cyber Security	• Ministry of Foreign Affairs (2023). The 1st Japan- U.S.-ROK Trilateral Diplomacy Working Group for Foreign Ministry Cooperation on North Korea's Cyber Threats. https://www.mofa.go.jp/press/release/pressite_000001_00031.html	Evaluating Japan's Strategy and methods in Cyber security
Module 13	ASEAN's take on Cyber Security	• ASEAN CYBERSECURITY COOPERATION STRATEGY (2021 – 2025) https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf	Evaluating ASEAN's Strategy and methods in Cyber security
Module 14	Cyber Security and the Way Forward	• Babu, C V & Simon, P. & Kumar, s. (2023). The Future of Cyber Security Starts Today, Not Tomorrow. 10.4018/978-1-6684-8666-5.ch016.	Simulation Exercise