PROPOSED PROGRAMME (MODULE 1 – LEADERSHIP DEVELOPMENT)

TIME	Session	Session Descriptions	Key Competencies
		DAY 1	
0900 – 1030	**Programme Opening, Course Overview, Participants' Expectations and Introduction** (Facilitated by Lead Faculty Woo Jun Jie)	45 mins – In this opening session, participants will be provided with an overview of the programme as well as the goals and objectives that they can expect to achieve by the end of the programme. Participants will also be invited to introduce themselves and share what they hope to learn and achieve in this programme. This will help set the tone for the rest of the programme and aligning the programme objectives and participants' expectations.	NA
	Welcome and Context Setting by CSA	45 mins - [Reserving for CSA sharing session]	
1030 - 1100	Group Phototaking and Tea Break		
1100 - 1300	**Fireside chat on Future of Digital Governance** (Peter Ong)	Participants will engage with a senior policymaker in this interactive session on the following topics: Leading Through Values, Building Institutions, and Thinking About The Future. Learning Outcomes: • Overview of the key trends and challenges, including cybersecurity, that shape the future of digital governance • Identify the leadership qualities and skills necessary for effectively manage and govern cybersecurity and tech-related agencies. • Participants will engage in discussions about emerging trends and policy innovations that could influence strategy and policy for cybersecurity and tech-related agencies.	• Capability Development • Strategic Insights & Alignment • Strategy, Policy and Planning
1300 - 1400	LUNCH		

PROPOSED PROGRAMME (MODULE 1 – LEADERSHIP DEVELOPMENT)

TIME	Session	Session Descriptions	Key Competencies
		DAY 1	
1400 - 1530	**Agile Leadership and Organisational Transformation in the Cyber Domain** (Goh Puay Guan)	In an increasingly complex policy environment, it will be necessary for leaders and their organisations to adapt and respond effectively to emerging challenges including cybersecurity issues. In this session, we will learn about how public sector leaders and managers can initiate and manage organisational transformation in the cyber domain through agile leadership approaches. Learning Outcomes: • Participants will gain an understanding of the core principles of agile leadership and how agile leadership can drive organisational transformation in the realm of cybersecurity. • Equip participants with the necessary tools and knowledge to lead agile and secure organisations.	• Technology Management • Capability Development • Stakeholder Management • Strategy, Policy and Planning
1530 - 1600	PM BREAK		
1600 - 1730	**Leading Technological and Digital Change: Building a Public Service Ethos** (Lim Siong Guan)	In order to lead change and foster organizational cohesion, leaders need to develop and foster a strong public sector ethos. In this session, we will hear from a senior policymaker about how public sector leaders and managers can build up a strong public sector ethos. The session aims to equip participants with the knowledge and skills needed to lead change in cybersecurity and tech-related agencies while fostering and maintaining a strong public service ethos within their organisations.	• Capability Development • Strategic Insights & Alignment • Strategy, Policy and Planning
1800 - 2000	**Programme Dinner**		

PROPOSED PROGRAMME (MODULE 1 – LEADERSHIP DEVELOPMENT)

TIME	Session	Session Descriptions	Key Competencies
		DAY 2	
0900 – 1030	**Panel Discussion: Challenges and Opportunities of Future Digital Leadership** Proposed Panelists: Ms Jacqueline Poh, MD, EDB Prof Kenneth Mak, Director-General of Health, MOH *Or* Ms Jeanette Kwek, Head, Centre for Strategic Futures	In order to overcome the challenges and exploit opportunities arising from unanticipated digital disruptions and complexities, leaders will need to be future-ready. In this panel discussion, thought leaders will share their views and experience on what it means to be a future-ready leader and lead their organisations through digital change and transformation. Learning outcomes: • Examine case studies and learn from best practices and lessons learned from real-world examples in the context of cybersecurity and tech-related pubic organisations. • Participants will discuss emerging trends and future directions in digital leadership, and how leaders can proactively address upcoming challenges and leverage new opportunities.	• Capability Development • Strategic Insights & Alignment • Strategy, Policy and Planning
1030 - 1100	AM BREAK		
1100 - 1230	**Site Visit: Singapore's Digital Transformation - Open Government Products**	Drawing from their deep experience in digital transformation within the Singapore government context, OGP will share how a team of ops, tech and policy officers worked closely together to build both the policies and technology which have allowed Singapore to roll out population-wide initiatives and solutions quickly and effectively.	• App & Product Management • Technology Management
1230 - 1330	LUNCH		

PROPOSED PROGRAMME (MODULE 1 – LEADERSHIP DEVELOPMENT)

TIME	Session	Session Descriptions	Key Competencies
		DAY 2	
1330 - 1500	**Leading Self – Who am I as a Digital Leader?** (Jeffrey Ong)	This is a visual exploration where participants individually select a picture to represent the kind of leader they'd like to be – a visual anchor, in the context of a cybersecurity or tech-related public organisation. This is in contrast with the leader they see themselves today.	• Capability Development
1500 - 1530	PM BREAK		
1530 - 1700	**Leading Self – Different People, Different Gift in the Digital Age** (Jeffrey Ong)	Participants confirm their MBTI preferences by calibrating their report (questionnaire) and an in-situ self-assessment. They will further understand the concept of preferences (type) through several experiential activities and use this understanding to help them formulate options for leadership behaviour in the digital landscape.	• Capability Development

PROPOSED PROGRAMME (MODULE 1 – LEADERSHIP DEVELOPMENT)

TIME	Session	Session Descriptions	Key Competencies
		DAY 3	
0900 – 1030	**Leading Others – Goleman Leadership Styles for Digital Transformation**	Participants learn more about the six leadership styles identified by Daniel Goleman that will help them get results at work. The six leadership styles are coercive, authoritative, affiliative, democratic, pace setting, and coaching.	• Capability Development
1030 - 1100	AM BREAK		
1100 – 1230	**Leading Others – Strengths Spotting for Cyber Leaders**	Participants reflect on their VIA Strengths report and work in small groups to find ways to utilise their character strengths at work through an activity. Participants will also explore how they can use their character strengths to align with their purpose and find meaning through the work they do.	• Capability Development
1230 – 1330	LUNCH		
1330 - 1500	**Enhancing ICT Team's Performance**	Through an experiential activity, participants will learn about the GROW coaching model and the distinctions between directive and non-directive coaching, as well as when they can be best applied. Participants will also be introduced to the Roffey Park's Flexible coach model participants learn four different coaching styles to match the development or performance level of the person s/he is coaching.	• Capability Development
1500 - 1530	PM BREAK		
1530 - 1700	**Leading Organisation – Breaking Silos and Encourage Collaboration Between ICT Teams**	Organisations often face challenges where their ICT teams are operating in silos which hinder the organisation's capacity and efficiency to achieve its strategic objectives. In this session, participants will explore techniques and approaches as leaders to strengthen collaboration across teams to achieve the organisation's strategic goals.	• Capability Development
Note: Sessions may be subject to change based on availability of Faculty			

PROPOSED PROGRAMME (MODULE 2 – STRATEGIC MANAGEMENT)

TIME	Session	Session Descriptions	Key Competencies
		DAY 4	
0900 – 1230 **With tea break from 1030-1100**	**Ethical Reasoning and Moral Foundations in Cybersecurity** (Leong Ching)	In leading their organsations, leaders and managers will frequently need to deal with moral-ethical issues. In this session, participants will: • Gain knowledge and understand how ethics, moral principles, and definitive beliefs frame how we react or respond to policies and messages. • Develop capability to apply moral reasoning as a theoretical framework to frame policy decisions and messages • Learn to develop strategies for effective stakeholder management, ensuring transparency, accountability, and ethical decision-making process • Sharing of used cases/examples from the cybersecurity context	• Ethical Reasoning • Capability Development • Stakeholder Management • Strategy, Policy and Planning
1230 – 1330	LUNCH		
1330 – 1700 **With tea break from 1500 – 1530**	**Navigating Complexity and Strategic Thinking in Digital Landscape** (Adrian Kuah)	Leaders today face thorny problems stemming from inherent uncertainty and unpredictability, rapid and disruptive change, volatility and complexity. In such environments, the best solutions cannot be easily engineered or orchestrated. Policies which worked well in previous contexts are less appropriate and 'fit-for-purpose' in a fast-changing context. In the midst of these challenges, how can leaders find ways to build and sustain effective teams and organizations that will deliver on their mandates? What dilemmas and trade-offs do leaders face? The module will focus on the frames of mental models, structure, human resource, politics, and culture to answer these questions and reframe the concept and practice of leadership, in the context of cybersecurity public agency.	• Strategic Thinking • Capability Development • Strategy, Policy and Planning

PROPOSED PROGRAMME (MODULE 2 – STRATEGIC MANAGEMENT)

TIME	Session	Session Descriptions	Key Competencies
		DAY 5	
0900 – 1230 **With tea break from 1030-1100**	**Strategic and crisis communications in the digital age** (Carol Soon)	This session will cover current developments in handling crisis and strategic communications within the context of cybersecurity and tech-related government agencies in Singapore and globally. It will emphasise the significance of effective crisis and strategic communication in the digital age and foster greater trust and support from the public. Additionally, the session will highlight the latest trends in crisis and strategic communications that government agencies, especially cybersecurity entities like CSA, and its stakeholders, should consider and possibly utilise to enhance the effectiveness of their communication strategies.	• Strategic Communications • Capability Development • Stakeholder Management • Strategy, Policy and Planning
1230 - 1330	LUNCH		

PROPOSED PROGRAMME (MODULE 2 – STRATEGIC MANAGEMENT)

TIME	Session	Session Descriptions	Key Competencies
		DAY 5	
1330 – 1500	**Stakeholder Analysis and Engagement in the Digital Domain** (Francesco Mancini)	The session aims to help participants understand the dynamics of stakeholder relations and how to effectively engage with them. Participants will be equipped with strategies and tools to identify and prioritise stakeholders in the context of cybersecurity organisation, as well as develop, maintain, and maximise stakeholder engagement to achieve better results. Learning outcomes: - Introduction to stakeholder analysis: importance of understanding stakeholders, definition and type of stakeholders. - Identifying stakeholders: stakeholder mapping tool - Prioritising stakeholders: assessing stakeholders' influence vs interest - Engagement strategies: plans to engage tailored to different stakeholders, with practical case studies and group discussions.	• Capability Development • Stakeholder Management
1500 - 1530	PM BREAK		
1530 – 1700	**The Art of Strategic Negotiation & Influence for Cyber Leaders** (Francesco Mancini)	The session will provide participants with strategies and tools that can be used to gear towards a positive and successful negotiable outcome with stakeholders of different challenges and complexities, within and beyond the cybersecurity and tech-related landscape and beyond. Learning outcomes: - Understanding negotiation principles and frameworks (win-win, win-lose, distributive, BATNA, etc) - Prepare and apply negotiation frameworks, utilising techniques and stategies - Manage difficult negotiations - Gain practical experience through examples and group discussions	• Capability Development • Stakeholder Management

Note: Sessions may be subject to change based on availability of Faculty

PROPOSED PROGRAMME (MODULE 3 – SECURITY TRENDS & INDUSTRY INSIGHTS)

TIME	Session	Session Descriptions	Key Competencies
		DAY 6	
0900 – 1030	**(5mins) Welcome and Overview of Week 2** (Woo Jun Jie) **Overview of Security Trends & Industry Insights** (CSA Assistant Chief Executive and Chai Chin Loon, Former GCISO, Govtech)	[Reserving 1 session for CSA and/or GovTech sharing session]	• Strategic Insights & Alignment • Strategy, Policy and Planning
1030 - 1100	AM BREAK		
1100 - 1230	**Will ASEAN Survive the US-China Cyber Confrontation?** (Chan Heng Chee)	The relationship between US and China is one of the most critical and complex geopolitical dynamics in the world today. This session will examine the implications of the US-China cyber rivalry for the future of global security, technological innovation, and geopolitical stability and explore the challenges and opportunities faced by ASEAN in navigating this complex landscape.	• Strategic Insights & Alignment • Strategy, Policy and Planning
1230 - 1330	LUNCH		
1330 – 1500	**Conflicts in Gaza and Middle East: Implication on Singapore's Cybersecurity Landscape** (Tommy Koh)	This session offers a nuanced analysis of the implications of the conflicts in Gaza and the wider Middle East region on Singapore. Participants will gain a better understanding of how these conflicts can shape Singapore's politics, economy, security, and society, as well as potential implications on cybersecurity in Singapore.	• Strategic Insights & Alignment • Strategy, Policy and Planning
1500 - 1530	PM BREAK		
1530 - 1700	**The Challenges of Governance in a Complex World: from National Security to Cybersecurity** (Peter Ho)	The session will provide an in-depth exploration of the multifaceted challenges faced by governments in effectively governing and ensuring security in an increasingly complex and interconnected world. Participants will understand the complexities of governance and the evolving nature of security from traditional national security concerns to the emerging domain of cybersecurity.	• Strategic Insights & Alignment • Strategy, Policy and Planning

PROPOSED PROGRAMME (MODULE 3 – SECURITY TRENDS & INDUSTRY INSIGHTS)

TIME	Session	Session Descriptions	Key Competencies
		DAY 7	
0900 – 1030	**Panel Discussion: Digital Resilience for Security and Innovation** Proposed Panelists Silvanus Lee, AI Founder and Investor (Former Managing Director, Twitter APAC Engineering Centre); and Chai Chin Loon, Former GCISO, Govtech	In today's digital environment, cyber-attacks can cripple the entire business operations if an organisation is unprepared. Investing in cybersecurity technology alone is insufficient to address cyber threats. Creating an informed and knowledgeable organisational culture that emphasises cybersecurity is a must for the entire organization, and with business/operational leaders taking the lead is now an imperative. Participants will hear from thought leaders and explore the critical role that leadership plays in promoting and sustaining digital resilience, including driving cultural change and strategic decision-making.	• App & Product Management • Technology Management • Strategy, Policy and Planning
1030 - 1100	AM BREAK		
1100 - 1230	**AI, Cybersecurity and Public Policy for a Safer Cyberspace** (Yaacob Ibrahim)	This session will delve into the various definitions of cybersecurity and their implications for a digital world. Who are the likely actors and the possible responses? Participants will explore some of the possible responses in strengthening the digital systems from specialized operations centres (SOCs) to various techniques to safeguard data and electronic systems, with a focus on incorporating security features as part of technology, app and product management. The session will also discuss the various policy initiatives that governments and businesses can adopt to enhance their cybersecurity measures, such as developing secure digital solutions. It will highlight the critical elements of the digital ecosystem, including the integration of security in product lifecycle management, and address the trade-offs between security and innovation. Furthermore, the session will discuss the concept of digital resilience in the ecosystem and building robust and secure products. Participants will examine the long-term implications for digitalization transformation from smart cities to new business models, focusing on how product management practices can align with cybersecurity objectives to support sustainable innovation.	• App & Product Management • Technology Management
1230 - 1330	LUNCH		

PROPOSED PROGRAMME (MODULE 3 – SECURITY TRENDS & INDUSTRY INSIGHTS)

TIME	Session	Session Descriptions	Key Competencies
		DAY 7	
1330 – 1500	**National Security and Defence Acquisition** (Lui Pao Chuen)	This session will discuss the processes and strategies undertaken by nations to manage resources and acquire cutting-edge technologies to maintain a strategic advantage in their national defense. This may include investing in research and developments in advancements in areas such as cybersecurity, unmanned systems, and artificial intelligence. Participants will gain insights into the lifecycle management of defense technologies, apps and product, from research and development to deployment and continuous improvement. The session will highlight how these technologies products and applications are effectively integrated into defense strategies, aligning with national security objectives. Additionally, the session will address the challenges of incorporating emerging technologies into defense systems, focusing on the balance between innovation and risk management. It will explore how adaptable and secure defense solutions can be applied, ensuring that technological advancements translate into tangible strategic advantages.	• App & Product Management • Technology Management
1500 - 1530	PM BREAK		
1530 - 1700	**Technology & Data: Legal Perspectives** (Warren B. Chik - SMU) **OR** **Big Data: Applications and Possibilities** *(Ng See Kiong - NUS)*	Despite the growing prevalence of big data and analytics in the work of businesses and governments, the legal implications of collecting and using data remains relatively under-studied. In this session, participants will learn about the legal aspects and implications of big data. Participants will learn from a leading legal expert on information technology and big data, and the potential implication for cybersecurity and tech-related agencies. Big data presents powerful opportunities for policymakers, with data providing important and actionable insights. In this session, participants will gain exposure to cutting edge research on translational applications of big data. How has big data contributed to policy effectiveness? How can data scientists and information technology specialists contribute to policy?	• Technology Management • Strategy, Policy and Planning

PROPOSED PROGRAMME (MODULE 3 – SECURITY TRENDS & INDUSTRY INSIGHTS)

TIME	Session	Session Descriptions	Key Competencies
		DAY 8	
0900 – 1030	**Sharing on CyberSG by Prof Chen Tsuhan** And/Or **Panel Discussion by TIG Centre & CRPO**	[Reserving 1 session by CyberSG and/or TIG Centre & CRPO, as advised by CSA]	• Strategic Insights & Alignment • Strategy, Policy and Planning
1030 - 1100	AM BREAK		
1100 - 1230	**The Metaverse Beyond the Internet**	Just as the evolution of the Internet has transformed the way people live and work, so too the next significant iteration of the Internet, commonly referred to as the Metaverse, which the authors suggest will go beyond the Internet as a sort of successor state to the Internet, will also lead to significant societal change. This session will examine issues that are likely to test the law and its response including in the areas of online harms, intellectual property, digital assets, and potential cybersecurity challenges.	• Technology Management
1230 - 1330	LUNCH		

PROPOSED PROGRAMME (MODULE 3 – SECURITY TRENDS & INDUSTRY INSIGHTS)

TIME	Session	Session Descriptions	Key Competencies
		DAY 8	
1330 – 1630 With tea break from 1500 – 1530	**Ransomware Tabletop Exercise**	In this session, participants will be guided by a cybersecurity expert and go through a simulated targeted attack scenario as a means of evaluating the organisation's incident response capabilities against ransomware scenarios on our tecnological applications or products. The exercise is useful to test an organization's readiness for ransomware attack response plans and recovery of the organisation's app, product and technological management. The ransomware tabletop exercise is an accumulative and concluding activity to wrap up the modules covered in the Singapore Component. The session will be beneficial for the participants to apply the knowledge and insights they gained during throughout course, for example negotiation, stakeholder management, crisis communication, leadership and management in times of crises, legal perspective, ethical and moral reasoning, etc.	• App & Product Management • Technology Management • Capability Development
1630 – 1700	**Overview of Overseas Component**	In this session, participants will be briefed on the plan and schedule for the overseas component and what to prepare for this component.	
Note: Sessions may be subject to change based on availability of Faculty			

PROPOSED PROGRAMME (OVERSEAS COMPONENT)

TIME*	Session	Session Descriptions	Key Competencies
		DAY 9	
0900 – 1130	**Regional Insights to Geopolitical Trends in the Cyber Sphere: South Korea's Perspectives** (SNU Graduate School of International Studies)	This session will provide participants with a broad overview of the geopolitical trends and challenges that South Korea faces today, and the potential implication on cybersecurity landscape. This includes ongoing geopolitical tensions in the region as well as the strategic and political-economic rise of South Korea in the modern era.	• Strategic Insights & Alignment • Strategy, Policy and Planning
1130 – 1400	LUNCH		
1400 – 1630	**Korea Internet & Security Agency (KISA)**	In the current global landscape, fierce competition for dominance in emerging technologies such as Artificial Intelligence, blockchain, big data, and quantum computing is evident. There lies a constant threat to citizens' daily lives and national security with cyberattacks, hacking, and personal data breaches. Through this site visit, participants will have an understanding of how KISA develops its cybersecurity strategy to handle national cyber crises and how they stay vigilant. Participants will also gain insights into the operations, initiatives, and best practices of KISA in the areas of internet infrastructure, cybersecurity, and data protection.	• Technology Management • Strategic Insights & Alignment

***including travelling time between site visits and lunch**

PROPOSED PROGRAMME (OVERSEAS COMPONENT)

TIME*	Session	Session Descriptions	Key Competencies
		DAY 10	
0900 – 1130	**KAIST Cyber Security Research Centre**	In this session, participants will visit a think tank that focuses on cybersecurity where they will learn about cutting edge research on cybersecurity technologies from leading experts and discover how industries and end-users can effectively implement these innovations to strengthen cyber and digital security across their services and products	• Technology Management • Strategic Insights & Alignment
1130 – 1330	LUNCH		
1330 – 1430	**Site Visit: Coupang**	Coupang is one of the largest e-commerce companies in South Korea. With a vast array of products and services, Coupang has developed sophisticated cybersecurity measures to protect its platform, ensure data privacy, and secure transactions, making it a leader in e-commerce cybersecurity. Participants will: • Gain insights into Coupang's robust cybersecurity framework. • Understand the latest cybersecurity technologies and solutions used by Coupang. • Learn about threat intelligence, incident response, and vulnerability management practices. • Explore future trends and R&D initiatives in cybersecurity.	• App & Product Management • Technology Management
1430 – 1530	Travel to AhnLab		
1530 – 1700	**Site Visit: AhnLab**	The site visit to AhnLab is to gain insights into the company's advanced cybersecurity solutions, understand their approach to threat intelligence, and discover how their innovative technology can strengthen your organisation's defence against evolving threats.	• App & Product Management • Technology Management

***including travelling time between site visits and lunch**

PROPOSED PROGRAMME (OVERSEAS COMPONENT)

TIME	Session	Session Descriptions	Key Competencies
		DAY 11	
0900 – 1130	**Cybersecurity Technology: Trends and Challenges in South Korea**	This session presents a deep dive into the current state of cybersecurity technology in South Korea. Participants will learn about the steps that South Korea has taken to strengthen cybersecurity advancements as well as the challenges that it faces.	• Technology Management • Strategy, Policy and Planning
1130 – 1330	LUNCH		
1330 – 1500	**Site Visit: Samsung**	Samsung, a global leader in technology and electronics, has developed robust cybersecurity measures to protect against cyberattacks. Their cybersecurity team is at the forefront of developing innovative solutions to mitigate cyber threats and ensure the security of their systems and data. The site visit will provide participants with a deeper understanding of Samsung's cybersecurity infrastructure and explore their cutting-edge security technologies. Participants will also gain practical insights and ideas for enhancing cybersecurity within their organisation.	• App & Product Management • Technology Management
1500 – 1530	PM BREAK		
1530 – 1700	**Final Reflections** **Closing & Certificate Ceremony**	In this session, participants will be given the opportunity to reflect on the lessons they have learned as well as share their thoughts and experiences.	NA