



Факультет Мировой Экономики
и Мировой Политики

Научно-учебная группа «АСЕАН+,
БРИКС+, НАТО+: перспективы азиатской
интеграции в новом мировом порядке»

Москва 2025

«ИНДЕКС КИБЕРМОЩИ КНР: ПОДХОД, ПАРАМЕТРЫ И ПОЗИЦИОНИРОВАНИЕ»

Тришкина Валерия, стажер-исследователь



Факультет Мировой
Экономики
и Мировой Политики

Научно-учебная группа «АСЕАН+, БРИКС+,
НАТО+: перспективы азиатской интеграции
в новом мировом порядке»

Москва 2025

<#>

ЗАДАЧА ПРОЕКТА

Провести пилот Индекса кибермощи для:

- Вьетнама
- Индонезии
- КНР
- Малайзии
- САР КНР Гонконга и Макао
- Таиланда
- Тайваня
- Японии.





Факультет Мировой
Экономики
и Мировой Политики

Научно-учебная группа «АСЕАН+, БРИКС+,
НАТО+: перспективы азиатской интеграции
в новом мировом порядке»

Москва 2025

<#>

НУГ

АСЕАН+
БРИКС+
НАТО+

CYBER
SECURITY



ФКН



Сайберус

Фонд развития результативной
кибербезопасности

Работа над индексом

- **НУГ «АСЕАН+, БРИКС+, НАТО+: перспективы азиатской интеграции в новом мировом порядке»** — проводила сбор данных, предварительную валидацию и расчёты по странам, входящим в нашу панель.
- **ФКН НИУ ВШЭ** — консультирование по методологии, операционализации индикаторов и статистическим процедурам.
- **Cyberus (Фонд развития результативной кибербезопасности)** — партнёрская экспертиза и интерес к применению индекса для оценки зрелости национальных киберэкосистем и разработки практических метрик.



Факультет Мировой
Экономики
и Мировой Политики

Научно-учебная группа «АСЕАН+, БРИКС+,
НАТО+: перспективы азиатской интеграции
в новом мировом порядке»

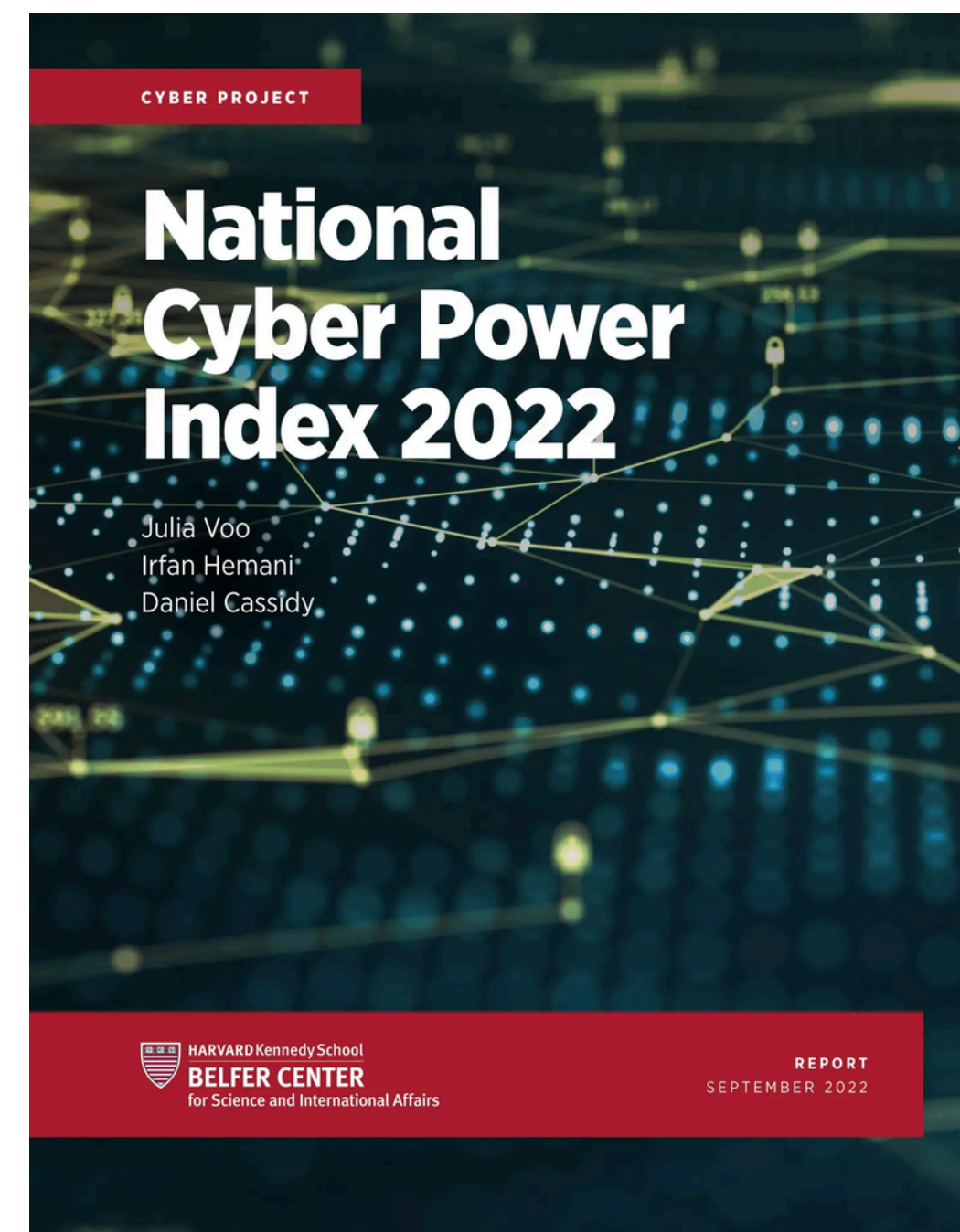
Москва 2025

<#>

ПРОТОТИП: THE NATIONAL CYBER POWER INDEX (NCPI), *BELFER CENTER*

ВЕБ-ПОРТАЛ

$$\text{National Cyber Power Index (NCPI)} = \frac{1}{8} \sum_{x=1}^8 \text{Capability}_x \times \text{Intent}$$

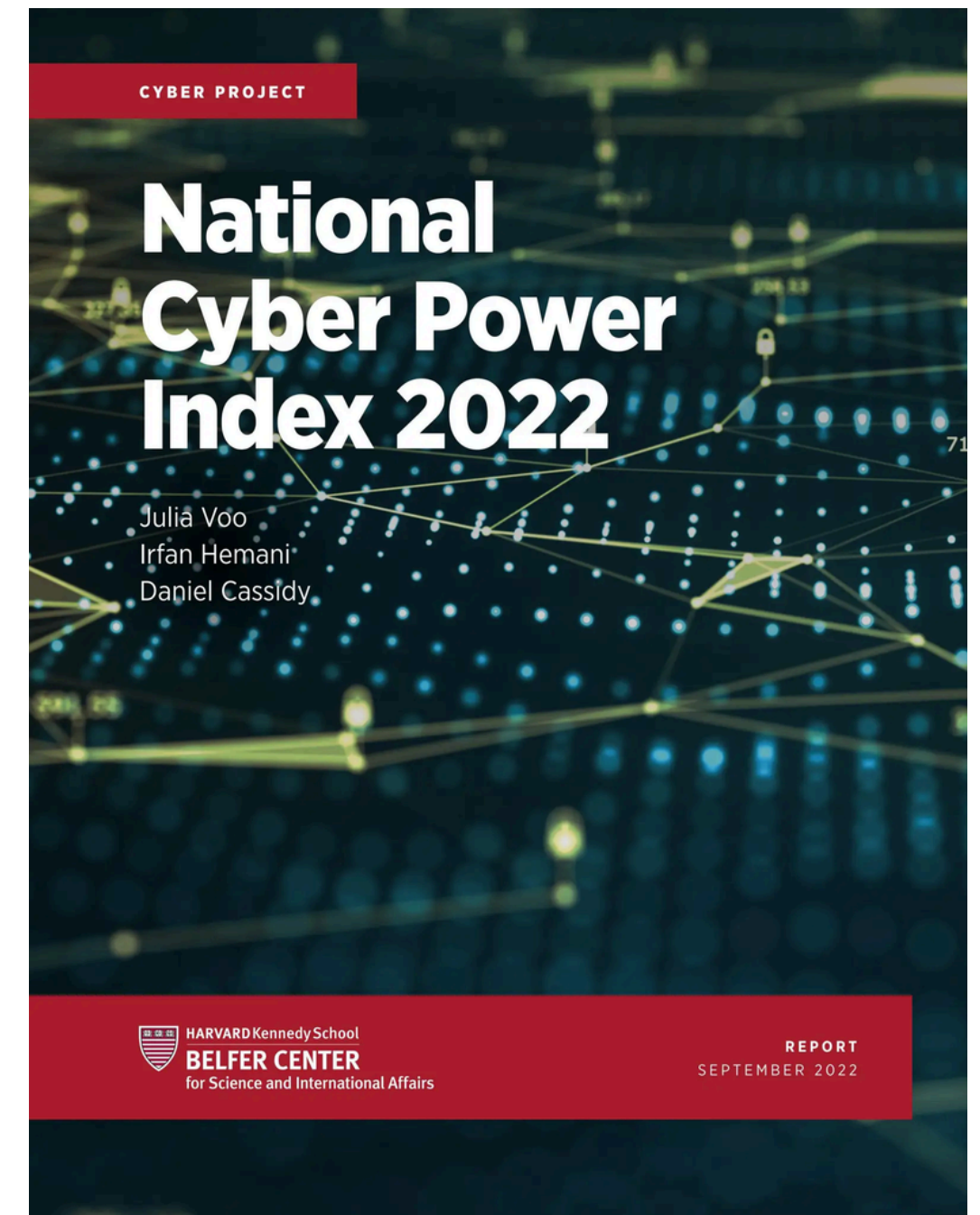




СЛЕПЫЕ ЗОНЫ И МЕТОДОЛОГИЧЕСКИЕ УЯЗВИМОСТИ

$$\text{National Cyber Power Index (NCPI)} = \frac{1}{8} \sum_{x=1}^8 \text{Capability}_x \times \text{Intent}$$

- В ряде индикаторов просматривается **западоцентричная оптика**
- **Неполное страновое покрытие:** в выборку NCPI не включён ряд государств, которые анализируются в рамках НУГ
- **Методологическая непрозрачность** отдельных параметров
- **Показатели разного уровня агрегируются в одном контуре**, что иногда усложняет интерпретацию итоговых баллов.





Факультет Мировой
Экономики
и Мировой Политики

Научно-учебная группа «АСЕАН+, БРИКС+,
НАТО+: перспективы азиатской интеграции
в новом мировом порядке»

Москва 2025



КОММЕНТАРИИ ФКН НА ПИСЬМО ГАЛИНЫ-ЮРЬЕВНЫ НИКИПОРЕЦ-ТАКИГАВА, РУКОВОДИТЕЛЯ НУГ

- Отмечено, что интерпретация соотношения намерений и возможностей может варьироваться в зависимости от того, как именно формализована модель.
- Подчёркивается, что само по себе отношение показателей не задаёт приоритета ни одному из компонентов — смысл зависит от выбранной логики агрегирования.
- Указывается на необходимость фиксировать выбранную интерпретацию, чтобы обеспечить аналитическую прозрачность и воспроизводимость в рамках будущих итераций индекса.
- Рекомендовано проводить чувствительный анализ, демонстрирующий, как изменение весов или структуры формулы влияет на итоговые значения.
- В целом комментарии подчеркивают, что концептуальная связка «намерения—возможности» допускает несколько корректных научных трактовок, и выбор среди них определяется исследовательской задачей и теоретической рамкой.



ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВАНИЯ РАЗРАБОТКИ ИНДЕКСА

- Сформулировано **авторское определение** кибербезопасности и стратегии национальной кибербезопасности (СНКБ).
- Анализ стратегии предлагается вести в рамках **неоклассического реализма**, где кибербезопасность трактуется как гибридный, тяготеющий к военному вид безопасности.
- **Центральное понятие — кибермощь**; именно через неё операционализируется СНКБ.
- СНКБ понимается как *«план действий по достижению, поддержанию и наращиванию кибермощи»*.
- *Необходимость укреплять кибермощь* рассматривается как внешний системный вызов (независимая переменная), а *реакции государств* — как результат вмешивающихся переменных.
- Измеримые компоненты кибермощи включают **активность государства в 7 сферах**
- Кибермощь рассчитывается как **соотношение возможностей и намерений государства**.
- Предложенная концепция подчёркивает, что **развитие кибербезопасности требует индивидуальных национальных усилий**.



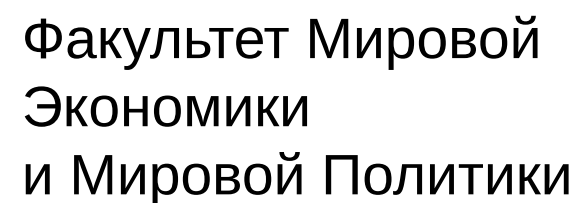
✓ **Разработать собственный индекс** стран региона Восточной и Юго-Восточной Азии по совокупности параметров: «кибермощь», «партнер-блок», «партнер-страна», «киберугрозы», «Россия среди киберугроз», «подход», «партнеры России»



✓ В ходе решения задачи проекта «Выявить эволюцию трендов кибербезопасности по параметру «подход» на временном отрезке 2000-2025 гг. подтвердить гипотезу, что *«американоцентричный» подход к партнерству в области кибербезопасности сменяется более национально ориентированным*



- ✓ Продолжена валидация и расширение массива данных, включая уточнение источников и стандартизацию показателей по странам региона.
- ✓ Проведена корректировка общей формульной конструкции, без раскрытия специфики расчётов, с учётом замечаний по интерпретации намерений и возможностей.
- ✓ Уточнены параметры и наблюдаемые характеристики, относящиеся к концепции кибермощи, а также пересмотрены критерии их пригодности к количественной оценке.
- ✓ Выполнено разделение качественных и количественных индикаторов, обеспечивающее сопоставимость внутри параметров.
- ✓ В ряде случаев выделены новые показатели, отражающие особенности региональной киберполитики и национальных стратегий государств.



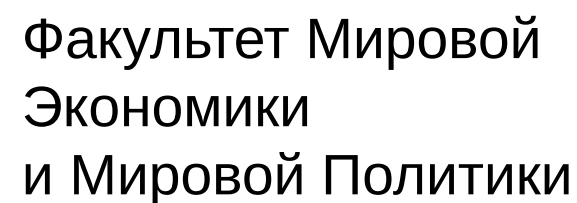
Научно-учебная группа «АСЕАН+, БРИКС+, НАТО+: перспективы азиатской интеграции в новом мировом порядке»

Москва 2025

CAPABILITY

- Совокупность ресурсов, инфраструктуры и практик, которые позволяют государству действовать в киберсфере.
- Отражает фактический потенциал, подтверждённый измеряемыми данными (финансирование, институты, ИКТ-база, операционные возможности).
- Показывает, что государство может делать реально, а не только декларировать.

<div> <div>13:57</div> <div>Telegram</div> <div> <div></div> <div></div> <div></div> <div>89</div> </div> </div>									
<div> <div><</div> <div>↶</div> <div>↷</div> <div>+</div> <div>☰</div> <div>...</div> </div>									
A	B	C	D	E	F	G	H	I	J
	Индикатор	Подиндикатор	Value	Источник	Assessing & Protecting Health	Information Control	International Cyber Norms	Disabling Adversary Infrastructure	
1									
2		Уровень цифровой грамотности	67%	https://www.csis.org/analysis/global-digital-literacy					
3	Awareness of cybersecurity and risk literacy	Количество программ по киберобразованию	62%	https://www.csis.org/analysis/global-digital-literacy					
4	Biateral Cyber Agreements	For each of the agreements between states: 1 - meeting, remarks 2 - Joint Statement, cooperation, framework 3 - Agreement / MOU	15						
5	Computer Infection Rates (%)		47%	https://www.csis.org/analysis/global-digital-literacy					
6	Cyber Military Staffing (nonmilitary)		60000	https://www.csis.org/analysis/global-digital-literacy					
7	Cyber Security Laws	0+ no laws, 1+ laws that cover one of the following: content, privacy, and crime 2+ laws that cover two of the following: content, privacy, and crime 3+ laws that cover content, privacy, and crime, updated (< 5 yr 2000) 4+ laws that cover content, privacy and cybersecurity, recent update (< 5 yr 2000)	4						
8	Data Privacy Laws and Governance								
9	Ecommerce economy		USD 153 tpm	https://www.csis.org/analysis/global-digital-literacy					
10	Existence of Cybersecurity Incident Response Teams (CSIRTs)	0 = no response team 1+ plans to establish a CSIRT 2 = new national CSIRT team (less or equal 5 years) 3 = established national CSIRT team (more than 5 years) 4 = established national CSIRT team (more than 5 years) + member of the first response team	4						
11	Freedom On The Net Score		9/100 0.09	https://www.csis.org/analysis/global-digital-literacy					
12	Global Soft Power		72.8 vs 100	https://www.csis.org/analysis/global-digital-literacy					
13	Global Top 100 Technology Firms (nonmilitary)		3	https://www.csis.org/analysis/global-digital-literacy					
14	High Impact State-sponsored Attacks (nonmilitary)								
15				Fittarelli A. PAPERWALL: Chinese Websites Poising as Local News Outlets Target Global Audiences with Pro-Beijing Content [Электронный ресурс] // The Citizen Lab (University of Toronto) - 07.02.2024. - URL: https://citizenlab.ca/2024/02/paperwall/					



Научно-учебная группа «АСЕАН+, БРИКС+, НАТО+: перспективы азиатской интеграции в новом мировом порядке»

Москва 2025

- Стратегические установки и цели, зафиксированные в нормативных документах, доктринах и официальных заявлениях.
- Отражает направленность и амбиции государства в области кибербезопасности и кибермощи.
- Показывает, что государство планирует или стремится делать, даже если фактические возможности пока ограничены.

	A	B	C	D	E	F	G	H
		Индикатор	Пояснение / источник	Метод вычисления	Value	Источник	Assessing & Protecting Health	Information Control
1		Observed in attributed cyber attack	Use CFR Cyber Operations Tracker figures to assess whether a state has been attributed as conducting 1 or more attacks	Observed in 1 or more attacks Yes/ No		CFR Cyber Operations Tracker		
2		Data protection law strength	Using CIA Paper's Data Protection rating for each state: https://www.dia.iciser.net/protection.pdf	Heavy/ Robust/ Moderate/ Limited/ No information	Robust			
3		Does the state's cyber military planning or strategy documents, or wider military planning or strategy documents, acknowledge that the state has cyber capabilities to control and manipulate the information environment?	Analysis of the online presence of each state's Ministry of Defence (MOD) and/or Armed Forces to find relevant documents. Relevant documents include defence plans, defence strategies, military doctrine, defence white papers, defence cyber plans, defence cyber strategies, military cyber doctrine, defence cyber white papers, statements from senior military leaders, statements from MOD politicians on the state's cyber capabilities.	Yes/No	Yes	https://www.fishbase.org/cn/publications/20200726/comment_W5479438dcd9f84c8f22283a1.htm		
4		Does the state's military cyber unit or command acknowledge that the state has cyber capabilities to control and manipulate the information environment?	Analysis of the online presence of each state's military cyber force to assess whether it acknowledges this objective. Also looked for public comments by national politicians and senior cyber military leaders on the capabilities that specific military units possess.	Yes/No	Yes	https://www.swp-berlin.org/publication/the-transformation-of-the-chinese-peoples-liberation-army-into-a-world-class-military/ https://docs.cerami.com/p/D0CUMENTPUBLICATIO%0003701.html		
5		Does the state's signals intelligence agency or foreign intelligence service acknowledge that the state has cyber capabilities to control and manipulate the information environment?	Analysis of the online presence of each state's intelligence agency to assess whether it acknowledges this objective. Also looked for public comments by national politicians and senior cyber intelligence agency leaders on the capabilities that the intelligence community possess.	Yes/No	Yes	http://www.ncsc.gov.cn/2017/06/27/content_2024529.htm		
6		Consistency of objective: Is it pursued in n' Strategy	Compare the objectives listed in the most recent strategy with those listed in the previous strategy (if one exists).	Objective present in +1 strategy: Yes/No	Yes			
7		Observed in attributed cyber attack	Any/Yes	Yes/No	Yes			
8		How many of the past five UN Cyber Government Group of Experts (GGE) consultations has the state participated in?	Figures taken from: https://www.unidir.org/files/publications/pdf/gge-unite-d-nations-cyberpac-e-security-en-69f.pdf	1 = five times, 0.8 = 4 times, 0.6 = 3 times, 0.4 = 2 times, 0.2 = 1 time, 0 = none of		https://www.reachingcriticalwill.org/dissemination/factsheets/gge https://www.unidir.org/files/publications/unite-d-nations-cyberpac-e-security-en-69f.pdf https://www.partnershipforinnovation.org/opinion/ufg-2019-the-fall-of-the-digital-wall/ https://www.en.cfr.ca/2020-10/09/c_32772943.htm?utm_source=chatham&utm_medium=article https://www.vic.org/cr/article/18703078257848320.html https://indico.in-oregon.fr/105252registrations/participants https://www.consmc.com/en/Au/MediaCenter/2017_7342020207_0302020_Au6e6.htm		
9		Has the state participated in the Internet Governance Forum (IGF) between 2010-2021?		0.25 for government/ civil society/ technical community/ private sector				
10		Has the state						



Факультет Мировой
Экономики
и Мировой Политики

Научно-учебная группа «АСЕАН+, БРИКС+,
НАТО+: перспективы азиатской интеграции
в новом мировом порядке»

Москва 2025

КЕЙС КИТАЯ, ПЛЮСЫ

- Последовательный и повторяющийся стратегический дискурс, позволяющий надёжно отслеживать намерения.
- Развёрнутая система нормативных документов и программ, дающая богатый материал для анализа.
- Чёткая институциональная архитектура управления киберсферой.
- Долгосрочное планирование, обеспечивающее устойчивость паттернов и прогнозируемость стратегий.





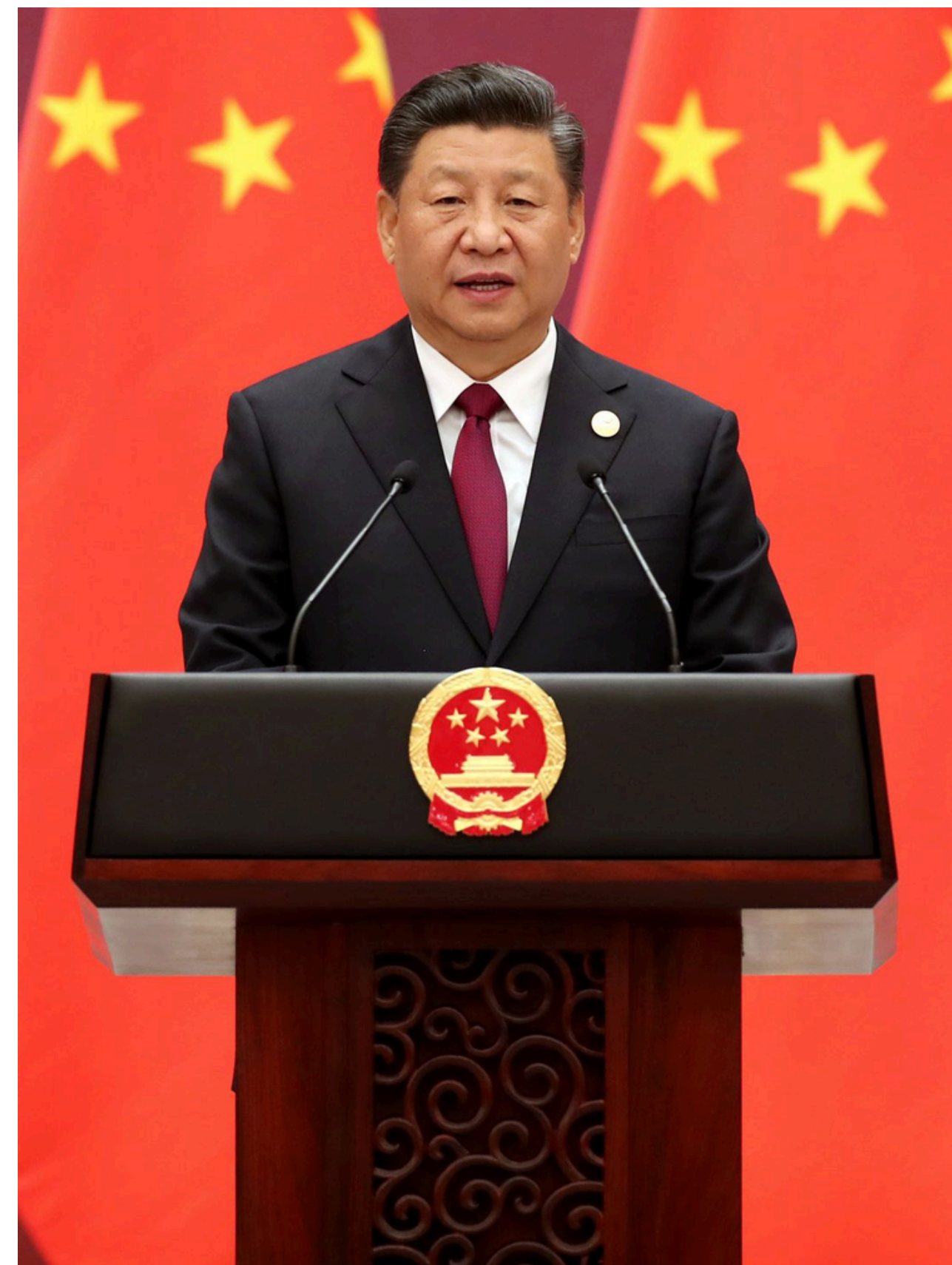
Факультет Мировой
Экономики
и Мировой Политики

Научно-учебная группа «АСЕАН+, БРИКС+,
НАТО+: перспективы азиатской интеграции
в новом мировом порядке»

Москва 2025

ПОЗИЦИОНИРОВАНИЕ КИТАЯ В ИНДЕКСЕ

- Демонстрирует высокий уровень согласованности «intent» и «capability».
- Стратегические установки в киберсфере стабильны во времени, что повышает надёжность оценки намерений.
- По ряду направлений возможностей Китай формирует сильный профиль кибермощи.
- В дискурсе закреплён приоритет «суверенного контроля» и «безопасной цифровой модернизации», что отражается в параметре «подход».





Факультет Мировой
Экономики
и Мировой Политики

Научно-учебная группа «АСЕАН+, БРИКС+,
НАТО+: перспективы азиатской интеграции
в новом мировом порядке»

Москва 2025

ОСОБЕННОСТИ КИТАЙСКОЙ МОДЕЛИ КИБЕРМОЩИ

- Централизованное управление и вертикаль цифровой безопасности
- Сильная интеграция кибербезопасности с промышленной, оборонной и технологической повесткой.
- Активная нормотворческая деятельность (в стандартах, нормах, концепциях данных).

TC260-PG-20245A

网络安全标准实践指南

——粤港澳大湾区（内地、香港）个人信息
跨境处理保护要求

(v1.0-202411)

全国网络安全标准化技术委员会秘书处

香港个人资料私隐专员公署

2024 年 11 月

本文档可从以下网址获得:

www.tc260.org.cn/



全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC



香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong



**ТЕЛЕГРАМ-
КАНАЛ**



САЙТ

